

Using Phase Space Attractors to Evaluate System Safety Constraint Enforcement: Case Study in Space Shuttle Mission Control Procedure Rework

By

Brandon D. Owens

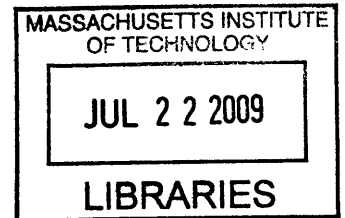
B.S. Aeronautical and Astronautical Engineering, Purdue University, 2003
M.S. Aeronautics and Astronautics, Stanford University, 2005

SUBMITTED TO THE ENGINEERING SYSTEMS DIVISION IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN ENGINEERING SYSTEMS
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2009

© 2009 Massachusetts Institute of Technology. All rights reserved.

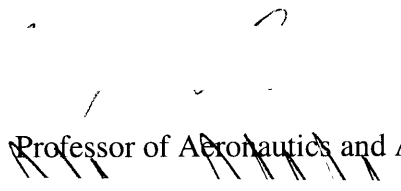


ARCHIVES

Signature of Author: _____

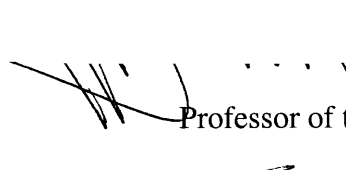
Engineering Systems Division
February 6, 2009

Certified by: _____


Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

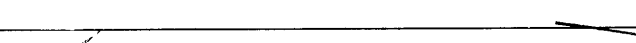
Nancy G. Leveson
Thesis Supervisor

Certified by: _____


Professor of the Practice of Aerospace Engineering
Committee Member

Jeffrey A. Hoffman
Committee Member

Certified by: _____


Professor of Behavioral and Policy Sciences and Engineering Systems
Committee Member

John S. Carroll
Committee Member

Accepted by: _____


Chair, Engineering Systems Division Education Committee

Nancy G. Leveson

[Page Intentionally Left Blank]

Using Phase Space Attractors to Evaluate System Safety Constraint Enforcement: Case Study in Space Shuttle Mission Control Procedure Rework

by

Brandon D. Owens

Submitted to the Engineering Systems Division in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Engineering Systems on February 6, 2009

ABSTRACT

As the complexity and influence of engineering systems in modern society increases, so too does their potential to create counterintuitive and catastrophic accidents. Increasingly, the accidents encountered in these systems are defying the linearized notions of accident causality that—though developed for the simpler engineered systems of the past—are prevalently used for accident prevention today. In this dissertation, an alternative approach to accident prevention based on systems theory—the Systems-Theoretic Accident Model and Processes (STAMP) and STAMP-based hazard analysis (STPA)—is augmented with the notion of using phase space attractors to evaluate how well STAMP safety control structures enforce system safety constraints.

Phase space attractors are mathematical results that emerge from the behavior of systems with dynamic structures that draw or constrain these systems to specific regions of their phase space in spite of a range of conditions. Accordingly, the goal in using this notion for the evaluation of safety constraint enforcement is to identify and analyze the attractors produced by a safety control structure to determine if it will adequately “attract” the system to safe states in spite of a range of unforeseeable conditions. Support for this approach to evaluating STAMP safety control structures is provided through the study of a safety control structure in an existing complex, socio-technical system. This case study is focused on a safety control process—referred to as *Procedure Rework*—used in Space Shuttle Mission Control to update procedures during in-flight operations as they are invalidated by changes in the state of the Space Shuttle and its environment. Simulation models of procedure rework are developed through physical and human factors principles and calibrated with data from five Space Shuttle missions; producing simulation results with deviations from the historical data that are—as characterized by Theil Inequality Statistics—small and primarily due to cycles and noise that are not relevant to the models’ purpose. The models are used to analyze the attractor produced by the Procedure Rework Process across varied conditions, including a notional crewed spacecraft mission to a distant celestial body. A detrimental effect in the process is identified—and shown to be potentially far more severe than light delay on a mission to a distant celestial body—and approaches to mitigating the effect are explored. Finally, the analysis conducted is described as a generalizeable process for using phase space attractors to evaluate system safety constraint enforcement in engineering systems.

Thesis Supervisor: Nancy G. Leveson

Title: Professor of Aeronautics and Astronautics and Engineering Systems



Acknowledgements

I have to apologize in advance for the length of this acknowledgements section. I am a firm believer that the acknowledgements in theses are windows into the personality and support network of the author that are not to be treated as hastily assembled afterthoughts to an eight-to-ten year endeavor (including undergraduate studies). It is a place for jokes, heart felt thanks, dedications, and even the occasional ode to Chuck Norris (see Tom Krenzke's master's thesis in the Aero/Astro Library). Personally, I would feel as though I had gone against my humble, Midwestern upbringing if I did not take a few pages to talk about the numerous people that have helped me along the way. This section belongs to them. So in short, I have a lot to people to thank and a lot to say.

No one is more deserving of my gratitude than my family. My parents R. Doug Owens and Deborah C. Owens provided me with everything that I needed as a child and made me believe that I am capable of anything. My fiancé Magen S. Farrar showed me the other half of my soul and remained supportive of me during the difficult time that we had to spend apart while I worked on this dissertation. My elder sister, Christina Owens Heilman always looked out for me and otherwise endured the burdens of the first-born child, thus making things easier for me. Additionally, the rest of my family (in alphabetical order: the Harters, Daniel Heilman, Julia Kennedy, Alta Lile, Charles Lile, Clifford Dewain Lile, James Lile, Jay Lile, Meranda Lile, Pearl Lile, Theresa Lile, Don Manual, Tim Manual, Rimma Manual, Sarah Manual, Mary Sullivan, the Vests, and others) helped me in more ways than I can remember and made family gatherings *interesting*. I am grateful to all of you for what you have done for me; this dissertation is dedicated to you. Finally, to Owen William Heilman—who was born less than four months ago—welcome to this world and thank you in advance for making me a proud uncle.

When distinguishing between the nature of friendship and family, it is often said that you can pick your friends, but you cannot pick your family. However, it is unclear what this saying means about your family's friends. My feelings on the matter are that some of the most important people in your life are the ones selected by your immediate family. My *selected family* includes (in alphabetical order): Jennifer Discher, Michael Discher, Kristen Edwards, Liz Edwards, Stephanie Edwards, Steven Edwards I, Steven Edwards II, Virginia Edwards, Bill Limeberry, Bill Manning, Ruthie Manning, Fairuz Munger, Faten Munger, Josh Ramirez, Ryan Ramirez, Gregg Weile, Donna Williams, and others. To all of you, thanks for being such good friends to my mom, dad, sister, and me.

With that said, the next group of individuals chose to allow me into their lives during those crucial years before I went to college. Though I never had a brother, I feel no need to complain because for as long as I can remember, my friend Matt Inabnitt has been there for me. Additionally, my friends Michael Vandegriff, Amanda Gillentine, Kory Marshall, David Pulse, Angela Pressler, and Justin Fratzke usually come to mind when I think about the good times that I had before college. To all of you, thank you for being such good friends to me.

The next group of people deserving of my gratitude are those who made direct technical contributions to this dissertation. My advisor Prof. Nancy G. Leveson developed the theoretical bases of this research (i.e., STAMP and STPA), routinely advised me on how this dissertation could be improved, and gave me the opportunity to come to MIT to do this research. Committee member Prof. Jeffrey Hoffman provided a former astronaut's perspective on my research throughout its development (even as early as when I was working on my application to MIT) and helped me gain access to the data I needed for the dissertation case study. Committee member Prof. John Carroll challenged me to think about what my research means to non-engineers. My officemates Margaret Stringfellow, Joseph Laracy, and Dr. Nicolas Dulac routinely suggested improvements to the ideas that I bounced off of them and made my work environment an enjoyable place to be. Prof. Betty Barrett, Justin Colson, Matthieu Couturier, Prof. Joel Cutcher-Gershenfeld, Karim Hardy, Michael Moore, Shuichiro Ota, Prof. Joseph Sussman, and John Thomas all offered advice and questions on this research at various stages of its development during *Columbia* Group meetings. Additionally, NASA employees and contractors such as Dr. Fred Bickley, Linda Delapp, Dr. Michel Ingham, David Lengyel, and Dr. Katie Weiss (a former member of my research group) provided answers to my questions on the inner workings of NASA and access to data throughout the various research projects I participated in during my time at MIT. To all of you, thank you for helping me bring this dissertation together.

The case study of this dissertation required me to understand the inner workings of Space Shuttle Mission Control. I developed most of this requisite understanding during my two cooperative education stints as a United Space Alliance employee at the NASA Johnson Space Center. These opportunities were made possible by my hiring managers Steve Jordan and Arthur Hsu and James Johnson, the head of the United Space Alliance cooperative education program. Additionally, I received valuable advice and guidance throughout these experiences from the following NASA Johnson Space Center, United Space Alliance, and Barrios Technology employees (in alphabetical order): Robert Banfield, David Brady, Robert Estep, Darren Fasbender, Michael Fitzpatrick, Sandy Fletcher, Lisa Harris, Robert Harvey, Pete Hasbrook, Rachel Hinterlang, Caroline Kostak, Michael Meyer, Blair Nader, Ken Peek, Stephen Tripodi, Katie Rogers, and many others. To all of you, thanks for my cooperative education opportunities in Mission Control and helping me make the most of them.

Of course, doctoral studies at MIT involve more than writing a dissertation. Doctoral exams, coursework, dealing with red tape, eating, preparing a dissertation defense presentation, and having fun are essential to the process and I received help in these areas from various people (in addition to those already mentioned). David Broniatowski, Pech Colat, Daniel Gillespie, Erica Gralla, Daniel Livengood, Jorge Oliveira, Matthew Richards, Sidharth Rupani, and Dr. Frank Field all helped me prepare for the Engineering Systems Division General Examination during study and discussion group meetings. Tatsuya Arai, Julie Arnold, Shardul Phadnis, Andrew Rader, Scott Sheehan, Leia Sterling, and Scott Van Broekhoven all partnered with me on MIT course projects. Elizabeth Milnes and Brian O'Conaill both went above and beyond the call of duty in helping me deal with administrative issues. Tom Krenkze, Joseph Thomer, Leslie

Rogers, and Xia Hua helped me start and maintain several eating clubs at the Sidney-Pacific Graduate Dormitory. Dr. Luca Bertuccelli and Dr. Carl Nehme both offered critical constructive criticism of my dissertation defense presentation. Dr. Michael Hanowsky united my fellow ESD Ph.D. students and me for many wonderful social events. Finally, my ESD Ph.D. colleague/dive instructor Yves Boussemart and my ESD dive buddies Mark Avnet, Katherine Dykes, and Laurent Guérin shared adventures with me that I will remember for a *very* long time. Thanks to all of you for making my time at MIT both productive and special.

Similarly, I am indebted to the people at Stanford University for the role that they played during the first two years of my graduate studies. Prof. John Chachere—who at the time was a fellow graduate student and my roommate—provided me with a tremendous amount of advice on being a graduate student and helped steer my research interests towards safety risk management. Prof. Robert Twiggs and Prof. Stanley Weiss—in addition to teaching me many interesting things—wrote excellent recommendation letters for my MIT application. Nooshin Kaviani, Amy Lee, Ruixue Liu, Jennifer O’Meara, Stephanie Pereira, Leonid Sapronov, and Oznur Yucelen all made life at the Crothers Memorial Graduate Residence Hall memorable and enjoyable. Fraser Cameron, San Gunawardana, Gregor Hanuschak, Michael Souder, Lara Thompson, and Alan Zorn spent many hours by my side studying the fundamentals of aeronautics and astronautics. Dr. Alberto Makino and the rest of the Breakers Eating Club introduced me to the concept of an eating club (an idea that I would later spread to MIT). Karl Stahl sent me a critical email informing me of an open research assistantship at Gravity Probe B, a satellite mission made possible by the tremendous efforts of Prof. Francis Everitt and many others. Then, Gaylord Green (another wonderful recommendation letter writer) and Greg Picard gave me the opportunity to participate in this mission as a mission planner. To all of you, thank you for helping me make the most out of my time at Stanford.

Additionally, the individuals I met at Purdue University shaped the experiences there that would serve as the foundation for my experiences at the NASA Johnson Space Center, Stanford, and MIT. Scott Reasoner, Andrew Schultz, James Newby, and Jeff Barnhart each shared cramped dorm rooms with me at various times in my stint at Purdue. Prof. Steven Collicott (yet another wonderful recommendation letter writer), Fred Mark Kuipers, Michael Scott, and Sarah Steinhardt all teamed up with me to design, build, and fly an experiment on a NASA microgravity research aircraft. David Loffing and John Hawkins spent many hours by my side studying the fundamentals of aeronautics and astronautics. Juanita Mascarenhas shared many interesting dinner conversations with me, helped me organize several residence hall events, and took the Graduate Record Examination along with me. Prof. Kathleen Howell taught me the fundamentals of orbit mechanics (a subject area that would later serve as the basis of my work on Gravity Probe B) and wrote a wonderful recommendation letter for my Stanford application. Marc Braun, Candice Gentry, and Craig Lammert all made life at Purdue memorable and enjoyable. To all of you, thank you for your help during the crucial time period when I was laying the foundations of my academic and professional career. Also, to the 2002-2003 residents of Tarkington Hall NW 1, note that your former counselor remembers you and continues to wish you well in your future endeavors.

Finally, it should go without saying that I could not have written this dissertation without my health. Robert E. Dicks, M.D. and Gary Taylor, D.D.S. have been the “go-to” guys for my overall and dental health, respectively, since I was born. Additionally, Michael H. Goldstein, M.D., Jessica Stejna, O.D., Sampson O. Nosike, O.D., and the rest of the staff at the New England Eye Center helped me achieve better-than-20/20 vision through the wonder of “lasers”. To all of you, thank you for my health.

To everyone mentioned in the acknowledgements (and others who I could not mention), I thank you all. I would like to say that it is truly an honor to be able to preserve a portion of your story in this document, which will reside, among other places, in the library under the Great Dome—perhaps one of the most recognizable and storied academic landmarks in the world.

BRANDON D. OWENS
CAMBRIDGE, MASSACHUSETTS
FEBRUARY 6, 2009

Biographical Note

Brandon D. Owens was born in Indianapolis, Indiana and completed his primary and secondary education in the nearby suburb of Greenwood, Indiana. Prior to his doctoral studies at MIT, he received a bachelor of science in Aeronautical and Astronautical Engineering from Purdue University and a master of science in Aeronautics and Astronautics from Stanford University.

As an undergraduate at Purdue University, Brandon participated in a rotating internship or “co-op” program for United Space Alliance at the Johnson Space Center in Houston, Texas. Before graduating in 2003, he completed a total of 12 months of work at JSC in the departments of Cargo Operations and Flight Control and Environmental Systems where his duties entailed support of Mission Control flight controllers during pre-flight, in-flight, and post-flight operations. During this time he became one of only a few co-ops to ever graduate from the United Space Alliance Flight Operations Training Academy and participate as a pre-certified operator of a Mission Control MPSR console (Life Support) in dozens of FCT simulations and one integrated simulation. Brandon twice participated (once on a ground crew and once on a flight crew) in NASA’s Reduced Gravity Student Flight Opportunities Program, which allowed undergraduate students to conceive, develop, and fly an experiment on a NASA aircraft used for microgravity training and research. During his senior year at Purdue, he was also a residence hall counselor at Tarkington Hall.

As a graduate student at Stanford, Brandon worked as a research assistant on the Gravity Probe B (GP-B) Project, which was a collaboration of NASA, Stanford, and Lockheed Martin to test Einstein’s Theory of General Relativity through a low-Earth orbit gyroscope experiment. Brandon’s responsibilities for the GP-B mission included mission planning, real-time commanding of the spacecraft, development of a situation awareness display for the mission operations center, and investigation of a radiation-induced anomaly that affected the experiment at various times throughout the mission. Additionally, Brandon was a system engineer for a student pico-satellite program known as MAST, which was launched in 2007 to demonstrate the survivability of a multi-strand tether in low-Earth orbit.

Brandon is a member of the American Institute of Aeronautics and Astronautics, Sigma Gamma Tau National Aerospace Honor Society, Purdue Alumni Association, and Stanford Alumni Association

Contents

CHAPTER 1: INTRODUCTION	21
1.1 Motivation.....	21
1.2 Background.....	39
1.3 Dissertation Research Question and Approach.....	44
1.4 Dissertation Synopsis	46
CHAPTER 2: LITERATURE REVIEW.....	48
2.1 Chapter Overview	48
2.2 Linear Accident Models.....	49
2.3 Organizational Risk Theories	54
2.4 An Emerging Notion of Resilience, Flexibility, Adaptability, and Robustness to Manage Uncertainty	56
2.5 “Macro-Human Factors”	58
2.6 Safety Risk Management Literature Summary.....	61
CHAPTER 3: CONTROL THEORY CONCEPTS	62
3.1 Chapter Overview	62
3.2 Variables of System State	63
3.3 Components of a Control System.....	64
3.4 Control Authority.....	65
3.5 Linear Control Theory Concepts.....	68
3.6 Paradigms for Nonlinear Control Engineering Research and Practice	75
3.7 Chapter Review	79
CHAPTER 4: PHASE SPACE ATTRACTORS AND THEIR RELEVANCE IN SYSTEM SAFETY CONSTRAINT ENFORCEMENT	81
4.1 Chapter Overview	81
4.2 Phase Space Attractors	82

4.3	Engineering Phase Space Attractors to Enforce Safety Constraints	94
4.4	Practical Applications of Phase Space Attractor Engineering	101
4.5	Phase Space Attractors and Safety-Driven Design.....	105
CHAPTER 5: CASE STUDY BACKGROUND – SPACE SHUTTLE MISSION CONTROL		110
5.1	Chapter Overview	110
5.2	Overview of Mission Control throughout NASA’s Human Spaceflight Programs	110
5.3	Current Mission Control Responsibilities, Workstations, and Staffing	117
5.3	The Scholars of Flight Control.....	125
5.4	Procedure Rework in Space Shuttle Mission Control.....	133
5.5	Mission Control Literature Review	136
CHAPTER 6: CASE STUDY PURPOSE, SCOPE, AND METHODOLOGY ...		139
6.1	Chapter Overview	139
6.2	Case Study Purpose and Scope	140
6.3	Development of the Dynamic Models for Procedure Rework in Space Shuttle Mission Control	141
6.4	Data Collection	145
6.5	Data Processing	153
6.6	Model Description	162
CHAPTER 7: CASE STUDY ANALYSIS RESULTS AND A PROCESS TO USE PHASE SPACE ATTRACTORS TO EVALUATE SAFETY CONSTRAINT ENFORCEMENT		187
7.1	Chapter Overview	187
7.2	Analysis	188
7.3	A Proposed Process for Using Phase Space Attractors to Evaluate System Safety Constraint Enforcement	221
CHAPTER 8: SUMMARY OF CONTRIBUTIONS, FUTURE WORK, AND CONCLUDING REMARKS		232
8.1	Chapter Overview	232

8.2	The Dissertation Hypothesis Revisited	232
8.3	Contributions to the Management of Uncertainty in Engineering Systems.....	233
8.4	Contributions to Procedure Rework Processes for Human Spaceflight and Other Applications	235
8.5	Future Work.....	237
8.6	Concluding Remarks	240
APPENDIX 1: LIST OF ACRONYMS AND ABBREVIATIONS		241
APPENDIX 2: DETAILED SPACE SHUTTLE FLIGHT DATA TABLES.....		244
STS-97 Data Tables		245
STS-115 Data Tables		265
STS-116 Data Tables		283
STS-117 Data Tables		304
STS-120 Data Tables		322
Tables of Data from All Flights Studied		355
APPENDIX 3: SYSTEM DYNAMICS MODEL DOCUMENTATION		356
Basic Procedure Rework Model.....		356
Light Delay Model		361
Flight Specific Procedure Rework Models.....		366
The Flow Controlled Procedure Rework Model.....		374
Light Delayed Procedure Rework Model		376
The Light Delayed, Flow Controlled Procedure Rework Model.....		387
BIBLIOGRAPHY		390

List of Figures

Figure 1. Preliminary results of Gravity Probe B data analysis (Everitt 2007).	34
Figure 2. The location of the GP-B spacecraft during SBEs.	35
Figure 3. The location of the GP-B spacecraft during MBEs (Owens et al. 2006).	36
Figure 4. The “Vee” Model of Systems Engineering (adapted from Forsberg and Mooz 1992).	40
Figure 5. The elements of basic control systems.	65
Figure 6. An example Bode Diagram of three variants of a linear, time-invariant system.	71
Figure 7. Example of task execution in a linear, time-invariant feedback control system.	72
Figure 8. Example of disturbance rejection in a linear, time-invariant feedback control system.	73
Figure 9. Example of system adaptation in a linear, time-invariant feedback control system.	74
Figure 10. Stock and flow structure of the system modeled by [Eq. 9] and [Eq. 10]......	84
Figure 11. Phase Portrait for three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.	84
Figure 12. Time history of the state variable X after three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.....	85
Figure 13. Time history of the state variable Y after three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.....	85
Figure 14. Stock and flow structure of the Van der Pol Equations.....	86
Figure 15. Phase Portrait for three simulation runs of the Van der Pol Equations, each with different initial conditions.....	87
Figure 16. Time history for the state variable X after three simulation runs of the Van der Pol Equations, each with different initial conditions.	87
Figure 17. Time history for the state variable Y after three simulation runs of the Van der Pol Equations, each with different initial conditions.	88
Figure 18. Stock and flow structure of the Lorenz Equations.	89
Figure 19. The time history of state variable Y after 2000 simulation runs of the Lorenz Equations in which the initial value of Y ranges between 0.01 and 1.	90
Figure 20. Histogram of values for state variable Y after 2000 simulation runs of the Lorenz Equations in which the initial value of Y ranges between 0.01 and 1.....	91
Figure 21. The phase portraits in X-Y phase space produced by the Lorenz Equations following four simulations with different initial values of state variable Y.	92
Figure 22. X-Y Phase portrait for three simulation runs of the system modeled by [Eq. 9] and [Eq. 10] with $a = 0.5$ and three different initial conditions (i.e., $X = 3, Y = 3$; $X = 0, Y = 3$; and $X = -1.5, Y = 0$).	93
Figure 23. A “tipping point” in ITA effectiveness and credibility (Dulac 2007, Dulac et al. 2007c, Dulac et al. 2005, Leveson et al. 2005).	97
Figure 24. The X-Y phase portraits of the spiral-in equilibrium point attractors produced by bifurcating the Lorenz Attractor through varying two of its parameters.	98

Figure 25. The state variable Y time histories of the spiral-in equilibrium point attractors produced by bifurcating the Lorenz Attractor through varying two of its parameters.	98
Figure 26. Stock and flow structure of the Lorenz Equations with the bifurcation control scheme described by [Eq. 19].	99
Figure 27. The phase portrait of the Tsembaga human and pig populations (derived from Kampmann 1991).	102
Figure 28. The phase portrait of Tsembaga human and pig populations when a slightly larger pig population is allowed (derived from Kampmann 1991).	103
Figure 29. The phase portrait of Tsembaga human and pig populations under an alternative ritual cycle (derived from Kampmann 1991).	104
Figure 30. Phase portraits of the Genesis spacecraft trajectory (Lo et al. 1998).	105
Figure 31. Leveson's taxonomy for inadequate control actions (Leveson 2009, Stringfellow 2008, Stringfellow et al. 2008, Owens et al. 2008).	106
Figure 32. Generic STPA low-level process control loop (Owens et al. 2008).	106
Figure 33. Leveson's taxonomy of control flaws and inadequate control executions (Leveson 2009, Stringfellow 2008, Owens et al. 2008).	107
Figure 34. The organizational boundaries of Mission Control and the organizational groups at NASA with which it primarily interfaces during a mission.	112
Figure 35. The primary flight control room used for Project Mercury and the initial flights of Project Gemini (source: http://spaceflight.nasa.gov/).	113
Figure 36. One of the MOCRs used during Gemini, Apollo, and early Space Shuttle missions (source: http://spaceflight.nasa.gov/).	113
Figure 37. The current FCR for Space Shuttle Mission Control (source: http://spaceflight.nasa.gov/).	114
Figure 38. The current FCR for ISS Mission Control (source: http://www.nasa.gov/mission_pages/station/multimedia/ISS_FCR.html).	115
Figure 39. An example twelve-hour, re-planned portion of a flight plan for a Space Shuttle mission.	119
Figure 40. Labeled schematic of Space Shuttle FCR workstations (image from http://spaceflight.nasa.gov/).	120
Figure 41. A typical flight controller console in the Space Shuttle FCR (image from http://spaceflight.nasa.gov/).	124
Figure 42. The distribution of authority for SBBs, RBBs, and KBBs in U.S. human spaceflight operations.	126
Figure 43. Example certification flow for a flight controller in the Space Shuttle environmental systems group.	130
Figure 44. A portion of the Space Shuttle real-time operations safety control structure.	136
Figure 45. The Rework Cycle dynamic structure (adapted from Lyneis et al. 2001). ...	142
Figure 46. A computer-generated rendering of the anticipated final configuration of the ISS (source: http://spaceflight.nasa.gov/).	146
Figure 47. The configuration of the ISS as STS-97 first approached it (source: http://spaceflight.nasa.gov/).	147
Figure 48. The configuration of the ISS when STS-97 undocked from it (source: http://spaceflight.nasa.gov/).	147

Figure 49. The configuration of the ISS as STS-115 first approached it (source: http://spaceflight.nasa.gov).	148
Figure 50. The configuration of the ISS as STS-115 undocked from it (source: http://spaceflight.nasa.gov).	148
Figure 51. A kink in the port side of the P6 array during retraction (source: http://spaceflight.nasa.gov).	149
Figure 52. STS-116 astronauts retracting the port side of the P6 SAW during an unscheduled spacewalk (source: http://spaceflight.nasa.gov).	150
Figure 53. The configuration of the ISS at the conclusion of STS-116 (source: http://spaceflight.nasa.gov).	150
Figure 54. The configuration of the ISS at the conclusion of STS-117 (source: http://spaceflight.nasa.gov).	151
Figure 55. The tear that developed in photovoltaic blanket of the P6 SAW (source: http://spaceflight.nasa.gov).	152
Figure 56. An astronaut "rides" on the end of the OBSS to repair a tear in the P6 SAW (source: http://spaceflight.nasa.gov).	152
Figure 57. The P6 SAW after the repair of the tear (source: http://spaceflight.nasa.gov).	153
Figure 58. The external configuration of the ISS at the conclusion of STS-120 (source: http://spaceflight.nasa.gov).	153
Figure 59. Histogram of time gaps between when updates were identifiable and issued and when updates were issued and expected to be executed.	156
Figure 60. The core stock and flow structure of the procedure rework models.	162
Figure 61. The stock and flow structure of the Basic Procedure Rework Model.	166
Figure 62. The stock and flow structure of the Flow Controlled Procedure Rework Model.	170
Figure 63. The stock and flow structure of the Light Delay Model.	172
Figure 64. The stock and flow structure of the Light Delayed Procedure Rework Model without the elements from the Light Delay Model.	174
Figure 65. Results of model calibration against STS-97 data.	180
Figure 66. Results of model calibration against STS-115 data.	180
Figure 67. Results of model calibration against STS-116 data.	181
Figure 68. Results of model calibration against STS-117 data.	181
Figure 69. Results of model calibration against STS-120 data.	182
Figure 70. Update times for all missions studied normalized to their time of landing preparation.	188
Figure 71. The rate of procedure rework over the course of missions with rework propagation and without rework propagation.	189
Figure 72. The actual average rate of procedure rework over the missions studied with normalized update times.	191
Figure 73. The actual and simulated average rates of procedure rework (excluding discrete event updates) over the missions studied with normalized update times.	191
Figure 74. The actual and simulated average rates of procedure rework (excluding latent updates at launch and discrete event updates) over the missions studied with normalized update times.	192

Figure 75. The time history of the <i>Inactive Procedures Needing Rework</i> stock for scenarios with and without rework propagation.	193
Figure 76. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with and without rework propagation.	195
Figure 77. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with negative and positive rework propagation.	196
Figure 78. The <i>Daily Procedure Rework Completion Rate</i> Time History for simulations with negative and positive rework propagation.	197
Figure 79. Time history of the <i>Daily Procedure Rework Completion Rate</i> for four simulation runs with flow control and one without flow control.....	202
Figure 80. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with and without a sudden increase in the procedure rework time horizon.	203
Figure 81. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with and without a shift dedicated to rework beyond the time horizon.	204
Figure 82. The time history of the light delay affecting a spacecraft on a Hohmann Transfer to Mars perihelion.	206
Figure 83. Time history of the <i>Daily Procedure Rework Completion Rate</i> for simulation runs of Mars transit duration missions with and without light delay.....	206
Figure 84. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with and without light delay on a Mars transit duration mission.	207
Figure 85. Time history of the <i>Daily Procedure Rework Completion Rate</i> for simulation runs of Mars transit duration missions with and without a dedicated shift for flow control.	209
Figure 86. Phase portraits in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for simulations runs with and without a dedicated shift for flow control on a Mars transit duration mission.....	210
Figure 87. Time history of the value of the <i>Active Procedures Needing Rework</i> stock at the Disaster Dynamics bifurcation point of the system.	211
Figure 88. Phase portrait in the <i>Valid Procedures-Procedures Needing Rework</i> Phase Space for a simulation at the Disaster Dynamics bifurcation point of the system.	212
Figure 89. Phase portrait in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for a simulation at the Disaster Dynamics bifurcation point of the system.	213
Figure 90. The Disaster Dynamics Bifurcation value of the <i>Rework Recognition Delay Attention Shifting Factor</i> parameter as a function of the <i>Baseline Procedure Invalidation Rate</i> parameter.....	214
Figure 91. Time histories for a simulation in which the system dynamics were unintentionally constrained.	215
Figure 92. Phase portrait in the <i>Valid Procedures-Procedures Being Reworked</i> Phase Space for a simulation in which the system dynamics were unintentionally constrained.	216
Figure 93. The eroding safety goals archetype (recreated from Marais et al. 2006).	227

List of Tables

Table 1. A description of the severe MBE Events for GP-B (adapted from Owens et al. 2006).	35
Table 2. Definitions of adaptability, flexibility, resilience, and robustness in the literature.	52
Table 3. Description of control system elements.	64
Table 4. Brief descriptions of Space Shuttle FCR console positions (Part 1 of 2, adapted from NASA JSC 2005a).	121
Table 5. Brief descriptions of Space Shuttle FCR console positions (Part 2 of 2, adapted from NASA JSC 2005a).	122
Table 6. Description of Space Shuttle FCR console features.	125
Table 7. Procedure update statistics for the Space Shuttle missions analyzed.	154
Table 8. Number of updates associated with each update rationale categorization relating to the downside of uncertainty.	159
Table 9. Number of updates associated with each update rationale categorization relating to the upside of uncertainty.	160
Table 10. Summary of the number of procedure updates due to discrete events.	161
Table 11. A description of the procedural flows in the core stock and flow structure of the procedure rework models.	163
Table 12. Description of the parameters in the Basic Procedure Rework Model (Part 1 of 2).	167
Table 13. Description of the parameters in the Basic Procedure Rework Model (Part 2 of 2).	168
Table 14. Description of the parameters needed to implement flow control in the Flow Controlled Procedure Rework Model.	171
Table 15. Summary of update classifications for all five Space Shuttle missions studied.	177
Table 16. Parameter constraints used for calibration runs using the modified Powell Search Algorithm in Vensim [®]	178
Table 17. Summary of the results from the final calibration run using the modified Powell Search Algorithm in Vensim [®]	179
Table 18. Summary statistics for the fit of flight specific model simulation results to the flight data.	184
Table 19. Summary statistics for the fit of model simulation results and flight data in Figure 73 and Figure 74.	192
Table 20. Number of propagated updates associated with each update rationale categorization relating to the upside of uncertainty.	199
Table 21. Number of propagated updates associated with each update rationale categorization relating to the downside of uncertainty.	200
Table 22. Results of the combined flow control scheme "optimization" run.	204
Table 23. The author's responses to Sterman's (1991) checklist of questions to ask to evaluate the validity of a model and its appropriateness as a tool for a specific problem (Part 1 of 2).	220

Table 24. The author's responses to Sterman's (1991) checklist of questions to ask to evaluate the validity of a model and its appropriateness as a tool for a specific problem (Part 2 of 2).....	221
Table 25. Listing of the electronic messages sent to the STS-97 crew (Part 1 of 4).	245
Table 26. Listing of the electronic messages sent to the STS-97 crew (Part 2 of 4).	246
Table 27. Listing of the electronic messages sent to the STS-97 crew (Part 3 of 4).	247
Table 28. Listing of the electronic messages sent to the STS-97 crew (Part 4 of 4).	248
Table 29. Procedure update designations for STS-97 (Part 1 of 6).	249
Table 30. Procedure update designations for STS-97 (Part 2 of 6).	250
Table 31. Procedure update designations for STS-97 (Part 3 of 6).	251
Table 32. Procedure update designations for STS-97 (Part 4 of 6).	252
Table 33. Procedure update designations for STS-97 (Part 5 of 6).	253
Table 34. Procedure update designations for STS-97 (Part 6 of 6).	254
Table 35. Key flight days for each STS-97 procedure update (Part 1 of 3).	254
Table 36. Key flight days for each STS-97 procedure update (Part 2 of 3).	255
Table 37. Key flight days for each STS-97 procedure update (Part 3 of 3).	256
Table 38. STS-97 update rationales (Part 1 of 7).....	257
Table 39. STS-97 update rationales (Part 2 of 7).....	258
Table 40. STS-97 update rationales (Part 3 of 7).....	259
Table 41. STS-97 update rationales (Part 4 of 7).....	260
Table 42. STS-97 update rationales (Part 5 of 7).....	261
Table 43. STS-97 update rationales (Part 6 of 7).....	262
Table 44. STS-97 update rationales (Part 7 of 7).....	263
Table 45. The STS-97 data time history for the variable <i>Number of Procedures Needing and Being Reworked</i>	263
Table 46. List of specially designated STS-97 procedure updates.	263
Table 47. STS-97 update times normalized to landing preparation time.	264
Table 48. Listing of the electronic messages sent to the STS-115 crew (Part 1 of 6)...	265
Table 49. Listing of the electronic messages sent to the STS-115 crew (Part 2 of 6)...	266
Table 50. Listing of the electronic messages sent to the STS-115 crew (Part 3 of 6)...	267
Table 51. Listing of the electronic messages sent to the STS-115 crew (Part 4 of 6)...	268
Table 52. Listing of the electronic messages sent to the STS-115 crew (Part 5 of 6)...	269
Table 53. Listing of the electronic messages sent to the STS-115 crew (Part 6 of 6)...	270
Table 54. Procedure update designations for STS-115 (Part 1 of 5).	271
Table 55. Procedure update designations for STS-115 (Part 2 of 5).	272
Table 56. Procedure update designations for STS-115 (Part 3 of 5).	273
Table 57. Procedure update designations for STS-115 (Part 4 of 5).	274
Table 58. Procedure update designations for STS-115 (Part 5 of 5).	275
Table 59. Key flight days for each STS-115 procedure update (Part 1 of 2).	275
Table 60. Key flight days for each STS-115 procedure update (Part 2 of 2).	276
Table 61. STS-115 update rationales (Part 1 of 5).....	277
Table 62. STS-115 update rationales (Part 2 of 5).....	278
Table 63. STS-115 update rationales (Part 3 of 5).....	279
Table 64. STS-115 update rationales (Part 4 of 5).....	280
Table 65. STS-115 update rationales (Part 5 of 5).....	281

Table 66. The STS-115 data time history for the variable <i>Number of Procedures Needing and Being Reworked</i> .	281
Table 67. List of specially designated STS-115 procedure updates.	282
Table 68. STS-115 update times normalized to landing preparation time.	282
Table 69. Listing of the electronic messages sent to the STS-116 crew (Part 1 of 6).	283
Table 70. Listing of the electronic messages sent to the STS-116 crew (Part 2 of 6).	284
Table 71. Listing of the electronic messages sent to the STS-116 crew (Part 3 of 6).	285
Table 72. Listing of the electronic messages sent to the STS-116 crew (Part 3 of 6).	286
Table 73. Listing of the electronic messages sent to the STS-116 crew (Part 4 of 6).	287
Table 74. Listing of the electronic messages sent to the STS-116 crew (Part 5 of 6).	288
Table 75. Listing of the electronic messages sent to the STS-116 crew (Part 6 of 6).	289
Table 76. Procedure update designations for STS-116 (Part 1 of 6).	289
Table 77. Procedure update designations for STS-116 (Part 2 of 6).	290
Table 78. Procedure update designations for STS-116 (Part 3 of 6).	291
Table 79. Procedure update designations for STS-116 (Part 4 of 6).	292
Table 80. Procedure update designations for STS-116 (Part 5 of 6).	293
Table 81. Procedure update designations for STS-116 (Part 6 of 6).	294
Table 82. Key flight days for each STS-116 procedure update (Part 1 of 3).	294
Table 83. Key flight days for each STS-116 procedure update (Part 2 of 3).	295
Table 84. Key flight days for each STS-116 procedure update (Part 3 of 3).	296
Table 85. STS-116 update rationales (Part 1 of 6).	296
Table 86. STS-116 update rationales (Part 2 of 6).	297
Table 87. STS-116 update rationales (Part 3 of 6).	298
Table 88. STS-116 update rationales (Part 4 of 6).	299
Table 89. STS-116 update rationales (Part 5 of 6).	300
Table 90. STS-116 update rationales (Part 6 of 6).	301
Table 91. The STS-116 data time history for the variable <i>Number of Procedures Needing and Being Reworked</i> .	302
Table 92. List of specially designated STS-116 procedure updates.	302
Table 93. STS-116 update times normalized to the landing preparation time.	303
Table 94. Listing of the electronic messages sent to the STS-117 crew (Part 1 of 6).	304
Table 95. Listing of the electronic messages sent to the STS-117 crew (Part 2 of 6).	305
Table 96. Listing of the electronic messages sent to the STS-117 crew (Part 3 of 6).	306
Table 97. Listing of the electronic messages sent to the STS-117 crew (Part 4 of 6).	307
Table 98. Listing of the electronic messages sent to the STS-117 crew (Part 5 of 6).	308
Table 99. Listing of the electronic messages sent to the STS-117 crew (Part 6 of 6).	309
Table 100. Procedure update designations for STS-117 (Part 1 of 5).	309
Table 101. Procedure update designations for STS-117 (Part 2 of 5).	310
Table 102. Procedure update designations for STS-117 (Part 3 of 5).	311
Table 103. Procedure update designations for STS-117 (Part 4 of 5).	312
Table 104. Procedure update designations for STS-117 (Part 5 of 5).	313
Table 105. Key flight days for each STS-117 procedure update (Part 1 of 2).	314
Table 106. Key flight days for each STS-117 procedure update (Part 2 of 2).	315
Table 107. STS-117 update rationales (Part 1 of 4).	316
Table 108. STS-117 update rationales (Part 2 of 4).	317
Table 109. STS-117 update rationales (Part 3 of 4).	318

Table 110. STS-117 update rationales (Part 4 of 4).....	319
Table 111. The STS-117 data time history for the variable <i>Number of Procedures Needing and Being Reworked</i>	320
Table 112. List of specially designated STS-117 procedure updates.	320
Table 113. STS-117 update times normalized to the landing preparation time.....	321
Table 114. Listing of the electronic messages sent to the STS-120 crew (Part 1 of 9).	322
Table 115. Listing of the electronic messages sent to the STS-120 crew (Part 2 of 9).	323
Table 116. Listing of the electronic messages sent to the STS-120 crew (Part 3 of 9).	324
Table 117. Listing of the electronic messages sent to the STS-120 crew (Part 4 of 9).	325
Table 118. Listing of the electronic messages sent to the STS-120 crew (Part 5 of 9).	326
Table 119. Listing of the electronic messages sent to the STS-120 crew (Part 6 of 9).	327
Table 120. Listing of the electronic messages sent to the STS-120 crew (Part 7 of 9).	328
Table 121. Listing of the electronic messages sent to the STS-120 crew (Part 8 of 9).	329
Table 122. Listing of the electronic messages sent to the STS-120 crew (Part 9 of 9).	330
Table 123. Procedure update designations for STS-120 (Part 1 of 11).	330
Table 124. Procedure update designations for STS-120 (Part 2 of 11).	331
Table 125. Procedure update designations for STS-120 (Part 3 of 11).	332
Table 126. Procedure update designations for STS-120 (Part 4 of 11).	333
Table 127. Procedure update designations for STS-120 (Part 5 of 11).	334
Table 128. Procedure update designations for STS-120 (Part 6 of 11).	335
Table 129. Procedure update designations for STS-120 (Part 7 of 11).	336
Table 130. Procedure update designations for STS-120 (Part 8 of 11).	337
Table 131. Procedure update designations for STS-120 (Part 9 of 11).	338
Table 132. Procedure update designations for STS-120 (Part 10 of 11).	339
Table 133. Procedure update designations for STS-120 (Part 11 of 11).	340
Table 134. Key flight days for each STS-120 procedure update (Part 1 of 4).	341
Table 135. Key flight days for each STS-120 procedure update (Part 2 of 4).	342
Table 136. Key flight days for each STS-120 procedure update (Part 3 of 4).	343
Table 137. Key flight days for each STS-120 procedure update (Part 4 of 4).	344
Table 138. STS-120 update rationales (Part 1 of 10).....	344
Table 139. STS-120 update rationales (Part 2 of 10).....	345
Table 140. STS-120 update rationales (Part 3 of 10).....	346
Table 141. STS-120 update rationales (Part 4 of 10).....	347
Table 142. STS-120 update rationales (Part 5 of 10).....	348
Table 143. STS-120 update rationales (Part 6 of 10).....	349
Table 144. STS-120 update rationales (Part 7 of 10).....	350
Table 145. STS-120 update rationales (Part 8 of 10).....	351
Table 146. STS-120 update rationales (Part 9 of 10).....	352
Table 147. STS-120 update rationales (Part 10 of 10).....	353
Table 148. The STS-120 data time history for the variable <i>Number of Procedures Needing and Being Reworked</i>	353
Table 149. List of specially designated STS-120 procedure updates.	354
Table 150. STS-120 update times normalized to the landing preparation time.....	354
Table 151. Update times and rates for all flights normalized to a set of reference update times.....	355

Chapter 1: Introduction

"Scientists study the world as it is; engineers create the world that has never been." –Theodore von Kármán, Former NASA JPL Director and Caltech Professor.

"Sadly, many students have been led to believe that engineering science is engineering! In a curriculum of 120 or more credits leading to a bachelor's degree in a branch of engineering, the typical student is required to take one, or maybe two, courses in design. Everything else, aside from general-education requirements, focuses on the analysis, rather than the creation, of engineered objects. Graduate education often has no design orientation at all. So, engineering as taught really deals with only a part of engineering as it is practiced." –Michael D. Griffin (2007), NASA Administrator from 2005 to 2009.

"A focus on design for uncertainty implies a major cultural change in thinking about the engineering paradigm. This is because the traditional pattern in engineering is to design to specifications set outside the engineering process; as by client wishes, design codes or governmental regulations. The traditional engineering task is to optimize the technology so that it meets a set of criteria." – MIT Engineering Systems Division Uncertainty Management Committee (2004).

"In systems theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. Systems are not treated as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. For safety, the original design must not only enforce appropriate constraints on behavior to ensure safe operation (the enforcement of the safety constraints), but it must continue to operate safely as changes and adaptations occur over time." –Nancy G. Leveson et al. (2004).

1.1 Motivation

Uncertainty can lead to negative consequences for the cost, schedule, safety, and scope/performance of engineering endeavors. Thus, engineering researchers and practitioners have found it prudent to define distinct categories of risk (e.g., cost, schedule, safety, scope/performance risks, etc.). Additionally, uncertainty can create opportunities for increased profit, safety, and scope as well as early completion, leading to similar categorizations of opportunity. The focus of this dissertation is on how safety is affected by system uncertainty (i.e., safety risk). However, those interested in cost, schedule, and scope risks and opportunities should not ignore this dissertation, as there are significant overlaps among these concepts and safety risk.

The author's intention in writing this dissertation is to describe a new way of thinking about the cause of complex system accidents and the uncertainty that engineers and

operators face in their attempts to prevent them. Accordingly, the following vignettes are provided to motivate the reader to consider the author's argument. The vignettes deal with tragic and near-tragic subject matter (a total of fourteen deaths resulted directly from the first two vignettes and the third vignette involves incidents that could have derailed an effort to which a number of dedicated people had devoted a large portion of their life). However, the overall message to take away from these vignettes is meant to be a positive one: forces were working against the tragic outcomes and though they did not always succeed, future tragedies may be prevented if we learn how to better foster the forces in opposition to tragic outcomes.

Each vignette is meant to be a vivid example of how a narrow emphasis on the elimination of "component failure" is an inferior approach for safety risk management to a focus on robustness, adaptability, flexibility, and resilience in the enforcement of system safety constraints¹. Each vignette identifies a hazard state that the system was not able to avoid (later, when concepts of STAMP/STPA are introduced, the safety constraints are explicitly defined). Additionally, each vignette highlights the fallacies in attributing the accidents to "component failure". Finally, the vignettes also describe the elements of robustness, adaptability, flexibility, and resilience displayed in these systems; why these elements fell short in preventing the accidents; and identifies available, yet excluded, technologies that would have enhanced the robustness, adaptability, flexibility, and resilience of these systems.

Vignette 1: The *Challenger* Accident

Much has been written about the Space Shuttle *Challenger* Accident (see Appendix B of Leveson 1995 for a brief summary and discussion of the events surrounding the accident). The accident investigation commission (Rogers 1986) established that hot gas leakage through a pseudo-redundant² set of O-rings in the right Solid Rocket Booster (SRB) was the most probable technical "cause" of the accident. The commission cited the "relentless pressure" on NASA management due to the Space Shuttle's role as the nation's principle space launch capability, poor communication among NASA field centers, and NASA's weak and "silent" safety organization as other contributing causes to the accident. The report also provides a vivid reconstruction of a teleconference the night before the launch in which Thiokol³ engineers concerned about the ability of the O-rings to seal the hot gases in the cold weather (and equipped with data from previous launches) were overruled by a handful of NASA and Thiokol managers. One engineering manager at Thiokol who was initially supportive of his engineers' objections to launching was apparently asked to "take off his engineering hat and put on his management hat" in the debate (Rogers 1986). In countless publications and engineering/management ethics class discussions since the issuing of the report, the decision to launch *Challenger* on that cold morning in January of 1986 has rightfully been scrutinized. Even the *Columbia*

¹ These terms and emphases will be defined more precisely throughout the remainder of this dissertation.

² Though there were two O-rings, both were rendered ineffective by the ambient temperature in the hours before the launch and the SRB segment joint rotation caused by the firing of the Space Shuttle Main Engines (SSMEs) six seconds before the ignition of the SRBs.

³ Thiokol produces the Space Shuttle SRBs.

Accident Investigation Board (CAIB) (Gehman 2003) aptly identified “echoes” of the *Challenger* Accident in their investigation of the subsequent *Columbia* Accident.

However, a more fundamental question deserves some attention: why is it that the leakage in the O-rings actually mattered (why were the lives of the astronauts dependent on it not occurring)? Though the question may seem too obvious or trivial to explore, the following facts indicate that there are additional degrees of complexity to the issue:

- 1) the Space Shuttle Orbiter did not disintegrate until seventy-three seconds after SRB ignition (roughly 60% of the total time that the SRBs nominally remain attached to the system after ignition) (Rogers 1986),
- 2) the right SRB continued firing for almost forty seconds after vehicle disintegration (until the range safety officer issued a destruct command for it) (Rogers 1986), and
- 3) the crew probably survived the Orbiter disintegration and possibly remained conscious until the crew compartment impacted the ocean two minutes and forty-five seconds after the Orbiter disintegrated (Kerwin 1986).

The purpose of a rocket launch is to accelerate a payload to a certain velocity while maintaining acceptable acceleration loads on the payload. In order to safely create these accelerations, the Space Shuttle system must maintain a desired attitude and the structural integrity of the Orbiter-External Tank (ET)-SRB assembly (the “stack”) throughout the first stage of flight⁴. Initially, the O-ring leakage of the right SRB did not prevent the maintenance of proper attitude or compromise the structural integrity of the stack. For roughly the first sixty seconds of SRB operation, the leak was not large enough to create a significant difference in thrust between the left and right SRBs and even in the thirteen seconds in which it did before disintegration of the stack, the desired attitude was maintained (Rogers 1986). Even though the leak reduced the axial thrust of the right SRB and created radial thrust on it, the attitude of the stack was held in check by the ability of the Orbiter to detect slight deviations in attitude and correct them by pivoting both the Orbiter’s and SRBs’ engines. However, even though the thrust mismatch in the SRBs was being compensated for by engine pivoting, there was another problem: the hot gases leaking from the SRB were flying directly into the ET and its lower attachment point to the right SRB. For roughly thirteen seconds, the surface materials of the ET and its aft SRB attachment strut endured the high temperatures of the leaking gases, and then the tank ruptured and the strut was severed (or pulled off of the ET) (Rogers 1986). Ironically, the right SRB separated from the stack and continued flying, albeit in an uncontrolled manner, until the range safety officer successfully commanded it to destroy itself (shortly before the time that it would nominally have separated from the stack). After separation of the right SRB, the stack could neither maintain its attitude nor protect the cryogenic fuels in the ET from igniting in the atmosphere and thus, the vehicle began to disintegrate. As a result of the disintegration, the compartment of the Orbiter that carried the crew was severed from the rest of the Orbiter—possibly remaining intact enough to continue holding cabin pressure—and several of the crew members activated

⁴ The liquid fuel in the ET must be stored in a pressured environment (i.e., inside a tank) and kept at subzero temperatures. A breach in the tank would allow the fuel to rapidly expand and vaporize.

their personal emergency air supplies, which they carried in the event that they had to evacuate the Orbiter on the launch pad (Kerwin 1986).

Of the nine recommendations the commission provided to NASA (Rogers 1986), six deserve further attention:

- 1) changes in NASA management structure, including the hiring of astronauts into management positions,
- 2) review of criticality and hazard analysis techniques at NASA and its primary Space Shuttle contractors,
- 3) the establishment of a safety organization on the associate administrator level of the agency,
- 4) improvements in communication among NASA field centers, with the Marshall Space Flight Center (i.e., the center employing the NASA employees that participated in the pre-launch teleconference with Thiokol) being singled out as needing the most work,
- 5) the abolition of the nation's reliance on the Space Shuttle as its principle launch capability, and
- 6) the introduction of the capability for the crew to escape the system during certain emergency situations in flight.

The first five of the recommendations listed above seem targeted toward strengthening the resistance to decisions like those made by the dominant participants in the NASA-Thiokol teleconference: people with firsthand knowledge of the personal risk the astronauts take were to be given more power, analysis and interpretation of hazards were (hopefully) to be improved, advocates for safety were to be more visible and active in the decision making process, and launch schedule pressure on management was to be reduced.

The final recommendation, on the other hand, seemingly acknowledges the uncertainty in the decision making process (and the possible weakening of resistance to unsafe decisions) and thus seeks to resist the consequences of an unsafe launch decision if it is made (either in defiance of resistance to the decision or as the result of a legitimate level of ignorance over the consequences). A crew escape subsystem is typically used to allow the crew to separate themselves from elements of the system (e.g. an exploding or out of control booster, a spacecraft unable to safely land, etc.) that will not keep them safe in their current, hazardous environment. During the Soyuz T-10-1 mission, for example, the crew escape system was successfully used to separate the crew capsule from the booster as it exploded on the launch pad (Hall and Shayler 2003). Up until the Space Shuttle was declared "operational" after its fourth test flight, no human spaceflight system had been flown without a crew escape system for launch⁵. The decision not to include a crew escape system in the Space Shuttle was not without controversy. In his memoirs, former

⁵ The first four Space Shuttle missions were considered test flights to be flown by no more than two people at a time. They also included ejection seats. These ejection seats were removed after these flights and the standard crew size for subsequent missions was increased.

Space Shuttle Astronaut Richard “Mike” Mullane (2006) attributed this decision to complacency at NASA following the immensely successful Apollo program:

“The lack of an escape system aboard operational space shuttles—indeed, the very idea that NASA could even apply the term operational to a spacecraft as complex as the shuttle—was a manifestation of NASA’s post-Apollo hubris. The NASA team responsible for the design of the space shuttle was the same team that had put twelve Americans on the moon and returned them safely to Earth across a quarter million miles of space. The Apollo program represented the greatest engineering achievement in the history of humanity...The men and women who were responsible for the glory of Apollo had to have been affected by their success. While no member of the shuttle design team would have ever made the blasphemous claim, ‘We’re gods. We can do anything,’ the reality was this: The space shuttle itself was such a statement.”

While it is, in principle, conceivable that a crew escape subsystem could have separated a crew compartment from the disintegrating stack and negated the fatal implications of the decision to launch *Challenger*⁶, the overall architecture of the Space Shuttle was not conducive to such a subsystem. Thus, NASA’s attempt to implement the crew escape capability recommendation was hindered by this fact. Ultimately, the Orbiter was retrofitted with the capability to allow the crew to parachute to safety if the Orbiter, after using almost all of the fuel in the ET and separating from the stack, could not safely land (NASA 1987). However, this capability is not intended to be useful for a *Challenger*-like scenario (i.e., stack disintegration while rocket engines are firing). Current plans for the launch system to replace the Space Shuttle include a crew escape capability for *Challenger*-like scenarios (Stanley et al. 2006, Stanley et al. 2005).

Challenger faltered not simply because it possessed “failed” components, but because it could not, as an integrated, socio-technical system, maintain the appropriate velocity and acceleration in the appropriate direction while preventing its liquid propellants from being exposed to the atmosphere (or at least maintaining acceptable accelerations and air pressure in an escape compartment for the crew). On the social side, an unprecedented architectural decision not to include crew escape capability was made despite opposition to it and a launch decision was made despite objections from engineers wielding evidence from previous launches of the system. On the technical side, the right SRB, the subsystem that housed the “failed” technical component, did not disintegrate and trigger a chain-reaction disintegration throughout the “stack” nor did it significantly alter the orientation of the overall stack. The stack’s disintegration was triggered by the severing of an interface between two of its subsystems, the ET and the right SRB, and the nearly simultaneous puncturing of the tank in the ET that contained cryogenic fuel. Had the hot gas leaked out the other end of the right SRB (i.e., away from the ET) the stack may have maintained its attitude and structural integrity until and beyond the nominal separation of the SRBs from the stack. However, even the point of the leak on the SRB O-ring

⁶ As mentioned above, the difference in chamber pressure and thrust of the two SRBs was detectable for several seconds before stack disintegration, the crew compartment remained relatively intact despite stack disintegration, and the crew was responsive for some unknown time period after stack disintegration.

circumference may be a matter of the interfacing between the SRB and ET. Indeed, before ruling the point of the leak on the SRB as an unfortunate coincidence, one would first have to rule out the effect of joint rotation (caused by the SSMEs firing six seconds before the SRBs) and proximity of the O-ring to the cryogenic fuel⁷ as factors in determining where the O-ring would leak. All and all, it was the interactions between system components that influenced how this tragedy unfolded.

Vignette 2: The *Columbia* Accident

Like the *Challenger* Accident before it, the *Columbia* Accident has also been the subject of many publications and engineering/management ethics discussions. Additionally, it too was a matter of the integrated, socio-technical system's inability to maintain the vehicle's velocity and deceleration in the appropriate direction while maintaining its structural integrity. In its report (Gehman 2003), the CAIB identified the technical cause of the accident as a hole in the leading edge of the left wing of the Orbiter created by a piece of insulating foam that fell from the forward Orbiter/ET attachment and hit it during launch. This area of the wing experiences high temperatures during the Orbiter's reentry into the Earth's atmosphere (when the kinetic and potential energy of the vehicle generated during launch is largely converted to thermal energy) and therefore is thermally protected by Reinforced Carbon-Carbon (RCC) panels. However, the hole created in one or more of these panels, in addition to affecting lift and drag on the left wing, allowed hot gases to damage the wing further, thus affecting the mass of and lift and drag on the wing further. Eventually, the increasing effects of wing damage on lift, drag, and wing mass led to a loss of attitude control, thus exposing the Orbiter to extreme and unanticipated aerodynamic loads that would ultimately disintegrate it⁸.

The CAIB also identified flaws in decision making at NASA by vividly reconstructing and critiquing NASA's handling of the ET foam debris incidents before and during the final flight of *Columbia*. Moreover, while recognizing that some important changes had occurred at NASA following the *Challenger* Accident, the CAIB drew parallels in the state of decision making in NASA during both the *Challenger* and *Columbia* accidents (Gehman 2003):

“By the eve of the Columbia accident, institutional practices that were in effect at the time of the Challenger accident—such as inadequate concern over deviations from expected performance, a silent safety program, and schedule pressure—had returned to NASA.”

Ultimately, changes made to improve decision making after the *Challenger* Accident had eroded to a state of ineffectiveness in the interval between the two accidents; the CAIB pointed, in particular, to complacency resulting from the success of eighty-seven

⁷ In Appendix B of Appendix L of Volume II of the accident investigation commission's report (Rogers 1986), it is noted that the ET likely cooled the SRBs through convection and that the right SRB was likely cooled more than the left SRB. Figure B.80 of that appendix shows the results of an analysis of the temperature of the aft segment of the right SRB at different locations around its circumference in the hours preceding the launch. The portions of the circumference closest to the ET were the coldest.

⁸ See NASA JSC (2008) for an analysis of crew survivability following loss of Orbiter attitude control.

missions between the accidents and cost and schedule pressures from the U.S. Congress and President associated with the completion of the International Space Station (ISS) as potential contributing factors to this erosion.

In short, the CAIB, like the Rogers Commission, aptly brought both technical and organizational flaws in the Space Shuttle system to light. However, as was the case in Vignette 1, it is also worthwhile to examine what may have been working in opposition to these flaws. The CAIB was helpful in this regard, having explicitly identified eight “missed opportunities” for discovery of the debris damage to the wing (Gehman 2003, Volume 1, pp. 140-167):

- 1) an unaddressed inquiry on Flight Day 4 by Rodney Rocha, NASA’s designated chief engineer for the damaged Thermal Protection System, to determine if the crew had been asked to inspect the left wing for damage,
- 2) an unused opportunity by the MCC to ask a crew member on Flight Day 6 to downlink video he had taken of ET separation (the video may have revealed missing foam on the ET),
- 3) a Flight Day 6 discussion between NASA and the National Imagery and Mapping Agency that produced no request for imagery,
- 4) a Flight Day 7 discussion between Wayne Hale, the Space Shuttle Program Manager for Launch Integration, and DoD representatives about imaging assets, that was not acted on due to the orders of Linda Ham, chair of the STS-107⁹ Mission Management Team (MMT),
- 5) a Flight Day 7 discussion between Mike Card, a NASA Headquarters Office of Safety and Mission Assurance (OSMA) manager and a Johnson Space Center (JSC) Safety and Mission Assurance Directorate representative that did not result in a request for imagery,
- 6) a Flight Day 7 discussion between Mike Card and the Associate Administrator (AA) of OSMA about imagery requests that did not result in a request for imagery,
- 7) a Flight Day 8 discussion between JSC Mission Operations Directorate (MOD) representative Barbara Conte (acting on behalf of Rodney Rocha) and STS-107 ascent/entry flight director Leroy Cain that did not result in an imaging request, and
- 8) a Flight Day 14 discussion between Michael Card and the AA for the NASA Space Flight Directorate that did not result in an imagery request.

Missed Opportunity 7 (i.e., the Flight Day 8 discussion between Barbara Conte and Leroy Cain) is of particular interest due to the fact that NASA flight directors—as will be discussed in the Space Shuttle Mission Control Center (MCC) case study in this dissertation—have the documented authority to conduct any action that they feel is necessary to ensure the safety of the crew. According to the CAIB, Barbara Conte encouraged Rodney Rocha to present his concerns directly to the flight directors after Space Shuttle Program Management had decided against requesting on-orbit imagery, but he elected not to because he (perhaps mistakenly) believed that Space Shuttle Program

⁹ STS-107 was the designation for the mission in which the *Columbia* Accident occurred.

Management would have to support an imaging request by the flight directors. It was thus up to Barbara Conte to informally relay Rocha's concerns to Leroy Cain who—not having a chance to hear the concerns formally from Rocha himself—decided not to act on the information.

Additional information from the CAIB report and a broader view of the accident yields even more missed opportunities for discovery of the wing damage and crew escape/survival:

- 9) Numerous foam loss/Orbiter damage events occurred throughout the history of the Space Shuttle Program and during STS-112 in particular, less than four months before the *Columbia* Accident, a substantial piece of foam fell off of the ET and struck an SRB at its ET interface (Gehman 2003). As was typically the case for such events, the working group responsible for tracking launch debris (i.e., the Intercenter Photo Working Group) identified the event and recommended that it be classified as an In-Flight Anomaly, a classification that would have prompted an investigation of the incident that would have to be closed before the next launch (i.e., STS-113) could be allowed. However, in an unprecedented decision on how to handle foam strikes, Space Shuttle Program Management rejected this classification and ultimately decided that the investigation could remain open until shortly after the STS-107 mission (Gehman 2003).
- 10) As Space Shuttle Program Management was apparently drifting to a new level of foam debris impact acceptance during and after STS-112, the Intercenter Photo Working Group was testing equipment that would allow a new level of completeness in their documentation of launch debris. The mission included an experimental camera mounted on the forward end of the ET looking back toward the right side of the Orbiter (NASA KSC 2002). The footage provided by the camera used on STS-112 prominently featured the leading edge of the right wing of the Orbiter before the camera view was obscured by exhaust from the pyrotechnics that separated the SRBs from the stack¹⁰. Similar cameras used on subsequent missions, after being repositioned to avoid the pyrotechnics exhaust and also to show part of the left wing, have been used to identify a number of ET foam shedding events (NASA 2005, NASA JSC 2005b). Unfortunately, ET cameras of this type were not used on STS-113 or STS-107 and thus, the Intercenter Photo Working Group did not have the type of footage offered by these cameras at their disposal when they expressed their concerns about the debris strike to Space Shuttle Program Management. With the footage that they obtained from other types of cameras, the Intercenter Photo Working Group still provided Space Shuttle Program Management with what the CAIB referred to as “remarkably accurate” initial estimates of foam debris size, speed, origin, and the point of impact (Gehman 2003). However, they were forced to seek visual confirmation of damage through requests to imaging resources outside of NASA, an alternative that ultimately was not allowed by Space Shuttle Program Management.

¹⁰ As of the writing of this dissertation, the video footage provided from this camera was available for download at <http://spaceflight.nasa.gov/gallery/video/shuttle/sts-112/html/fd1.html>

- 11) More than half of the Space Shuttle missions prior to STS-107 included a Canadian-built robotic arm formally known as the Shuttle Remote Manipulator System (SRMS) and nicknamed the “Canadarm” (CSA 2006). Because the SRMS has cameras on its “elbow” joint and “wrist” joint, it has been used for on-orbit observation of portions of the Orbiter that were not visible to the crew. During STS-41D, the SRMS was used to observe and remove an icicle from the wastewater dump port (CSA 2006, Mullane 2006). Ironically, this action was performed because of Mission Control’s concern over the possibility of the icicle breaking off during reentry and causing damage to the left side of the Orbiter. Yet, even though this device had potentially saved a crew and Orbiter in the pre-*Challenger* era of Space Shuttle operations, it was not considered a mandatory piece of equipment; mission planners could exclude it from missions in order to maximize payload mass and minimize crew training. STS-107 was the first flight since STS-99 not to include the SRMS (CSA 2006), an interval of fifteen flights and nearly three years. The CAIB’s location estimate for damage to the left wing’s RCC panels was well within the SRMS’s range of view. Without the SRMS, the only means available to the Intercenter Photo Working Group and the ad hoc STS-107 Debris Assessment Team to obtain on-orbit imaging of the wing damage were to have the crew conduct a contingency spacewalk or request imaging from government agencies other than NASA. Both options proved to be unacceptable to Space Shuttle Program Management at the time. Since STS-107, an instrumented extension to the SRMS referred to as the Orbiter Boom Sensor System (OBSS) has been designed (NASA 2005) and used along with the SRMS on every mission to inspect the Orbiter for foam damage. The results of these inspections have led to contingency spacewalks for Orbiter repair on STS-114 and other missions¹¹.
- 12) After the Debris Assessment Team had reluctantly rescinded its request for imaging¹² the JSC engineer responsible for landing gear/tires/brakes contacted engineers at the NASA Langley Research Center and NASA Ames Research Center to evaluate scenarios in which the debris impact led to landing gear damage (Gehman 2003). According to the CAIB, these engineers conducted “after-hours” simulations, uncovered potential scenarios for landing attempts without deploying the landing gear, and distributed information on these scenarios to JSC engineers, including members of the Debris Assessment Team. Additionally, they uncovered less favorable scenarios, but chose not to distribute information on them to as wide of an audience.
- 13) As was the case during the *Challenger* Accident, several technical elements of *Columbia* worked to compensate for the hazardous changes in vehicle attitude in the final seconds of the mission. The CAIB noted that as the wing damage caused unanticipated changes in lift and drag on the wing and wing mass, *Columbia*’s

¹¹ Additionally, as discussed in the case study of this dissertation, the OBSS was used in the repair of a damaged solar array on the ISS.

¹² The CAIB reported that though the Debris Assessment Team concluded that the debris damage was not a “safety-of-flight” issue, they felt that the uncertainty in their analysis (the damage model they used had to be extrapolated 400 times beyond its validated limits) warranted on-orbit imaging. They maintained this view throughout the flight, but ultimately stopped trying to convince program management to honor their requests.

ailerons and thrusters responded in an attempt to maintain vehicle attitude (Gehman 2003). While the ailerons and thrusters were initially able to maintain vehicle attitude, they were eventually overwhelmed by the increasing effects on lift, drag, and wing mass due to additional damage to the wing from hot gases. As mentioned in Vignette 1, *Columbia* did include features for crew escape added after the *Challenger* Accident, but in order for them to be useful, the ailerons and thrusters would have had to maintain vehicle attitude long enough for the vehicle to slow below Mach 1¹³.

- 14) Additional compensatory actions were evident in the actions of STS-107 flight controllers. During *Columbia's* final seconds of controlled flight, flight controllers in the MCC detected and discussed problems with the left side of the vehicle (four hydraulic sensors in the left wing stopped transmitting data and shortly thereafter, tire pressure sensors in the left main landing gear went silent) (Gehman 2003). In fact, the last transmission from the *Columbia* crew was in response to an MCC message related to the faulty tire pressure indications (Gehman 2003). These indications and the discussion that they generated indicated that, in principle, the MCC had and was processing the information that it would have needed in order to advise a crew escape action if the vehicle had somehow managed to maintain attitude until it slowed below Mach 1.

Columbia, like *Challenger*, did not disintegrate simply because it contained “failed” components. Each missed opportunity represents an instance in which 1) a system component exerted additional effort—albeit unsuccessfully—to compensate for the hazardous behavior of other components or 2) a proven system component that could have been used for additional hazardous behavior compensation was excluded from the mission. Moreover, the issue of foam debris is a matter of component interaction rather than component failure: the foam fell uncontrolled from an interface between two system components (i.e., the Orbiter/ET forward attachment) and struck other components (i.e., RCC panels) that are, by design, subjected to extreme conditions. Thus, a key aspect in the prevention of accidents like the *Columbia* Accident is the fostering of compensatory actions between components to reduce hazardous situations rather than a narrow focus on the elimination of component failure. Accordingly, even though foam debris still falls from the ET after extensive effort by NASA to reduce it (NASA 2005, NASA JSC 2005b), select elements of NASA are engaged in increased compensatory behavior (e.g., improved imaging of the ET during and immediately after launch, mandatory inspection of Orbiter RCC panels and thermal tiles with the SRMS and OBSS, the development of thermal tile and RCC repair methods, etc.) during each post-*Columbia* mission to ensure that foam debris damage will never again lead to the loss of a crew.

Vignette 3: Gravity Probe B Radiation Anomalies

Unlike the *Challenger* and *Columbia* accidents, little has been written to date about a series of radiation anomalies encountered during the Gravity Probe B (GP-B) mission. GP-B was a low-Earth orbit satellite launched on April 20, 2004 to test Albert Einstein’s Theory of General Relativity. The basic idea for the project was first envisioned at Stanford University over 40 years before the launch date: the spacecraft, once launched,

¹³ The vehicle was traveling a little under Mach 20 when it lost attitude control (Gehman 2003).

would hold a fixed inertial orientation by pointing at a distant star while instrumented gyroscopes inside of it (isolated from Newtonian torques) would change orientation as the spacecraft moved through curves in space-time caused by the Earth (Turneure et al. 2003).

Throughout the project's developmental phase, tremendous effort was expended towards overcoming its technological and political uncertainty. The eventual Principle Investigator (PI) for GP-B and the first person to commit to it full-time, C. W. Francis Everitt, joined the project in 1962 with little expectation that it would occupy him for the next forty-five to fifty years (Overbye 2004). However, because the Earth's effect on space-time is theorized to be very small, it was necessary for the experiment to be carried out with extreme precision and thus, several new technologies had to be developed. The developmental cost exceeded \$700 million (Hecht 2004) and over ninety doctoral dissertations related to the project were written and defended at six universities before the spacecraft had even collected its first bit of data¹⁴. Additionally, while the project dealt with numerous technical delays, other General Relativity experiments were conducted and their results were published, undermining the value of the GP-B project in the eyes of some critics (Clark and Jamieson 2007, Mullins 2004, Overbye 2004). Due to this waning support for the project in the scientific community and both cost and schedule overruns, the mission was cancelled at least seven times, and each time the PI and other scientists had to successfully lobby Congress to get it restored (Hecht 2004, Overbye 2004).

By the time GP-B was inserted into its operational orbit, it appeared as though many of the project's challenges were behind it¹⁵. However, the GP-B operations team would encounter a number of challenges that threatened the success of the project. The basic difficulties were that GP-B had to collect a large amount of data before its liquid helium fuel/coolant was exhausted and that interruptions in data collection had negative consequences—the precision of the result improved as a function of the data collection interval time.

One source of interruption that arose multiple times during the project's data collection phase was the rebooting of the spacecraft computers due to radiation anomalies known as Multiple Bit Upsets (MBUs). When radiation particles strike certain types of digital memory cells in electronics, they sometimes “upset” or change the value of the bit of information contained in the cell (i.e., change a “1” into a “0” or vice versa)¹⁶. The implication of upset events is that the upset bit(s), which contain false information as a result of the upset, may be used by a computing device in the electronics to inform a

¹⁴ This dissertation can unofficially be classified as one of the first to result from the data that GP-B collected. The author worked for the GP-B project at Stanford University as a master's-level graduate research assistant from October 2003 to August 2005. This experience greatly shaped his manner of thinking about safety risk management and this dissertation is in part an attempt to describe that manner of thinking.

¹⁵ In fact, the Delta II launch vehicle that carried GP-B spaceward greatly exceeded expectations of the precision in which it would insert the spacecraft into the desired orbit (NASA MSFC 2004).

¹⁶ If only one bit is upset by a particular radiation particle the event is referred to as a Single Bit Upset (SBU) and if more than one bit is upset the event is referred to as an MBU.

process being controlled by the electronics. In other words, an upset can cause digital electronics to perform functions in erroneous ways. To counteract the problems associated with upsets, computing devices often examine bits of information in clusters, known as logical words, that are arranged to provide both the information for the function to be performed by the device and information that would indicate if one or more bits in the logical word have been upset. Next, if it is apparent that one or more bits in an examined logical word have been upset—conditions referred to as Single Bit Errors (SBEs) and Multiple Bit Errors (MBEs), respectively—the computing device enacts a number of corrective responses. For the GP-B spacecraft, the programmed responses to MBEs sometimes led to computer reboots that interrupted data collection for hours and days at a time.

The reason that GP-B was programmed to sometimes respond to MBEs through computer reboots relates to the manner in which MBE uncertainty was represented. Radiation particle collisions with digital memory cells are understood as stochastic phenomena: it is not possible to know when an upset will occur or in which logical word it will occur. It is, however, possible to determine an approximate number of MBEs in a device over a span of time the memory device is exposed to radiation provided that: 1) a large set of historical data that is representative the devices' intended usage is available, 2) the time span of exposure is sufficiently large to allow convergence to the statistical median of the historical data, and 3) the number of logical words in the device is sufficiently large to allow convergence to the statistical median of the historical data. Unfortunately, the historical data set used by GP-B engineers to estimate the expected number of MBEs during the mission was *not* representative of the behavior of the memory device selected for use on GP-B. The selected memory device had memory cells containing bits from the same logical word arranged physically adjacent to each other while memory cells related to the same word in memory devices from the historical database were usually scattered (Owens et al. 2006)¹⁷. This oversight in the analysis led to what would prove to be an extremely optimistic estimate of expected MBEs (i.e., less than five). Ultimately, this estimate suggested that MBEs were not going to be major problem during the mission and that the following actions would be acceptable for MBE response (Owens et al. 2006):

- 1) The spacecraft computers would periodically scan their memory for SBEs and MBEs. All SBEs—which were expected to occur several orders of magnitude more frequently than MBEs—would be automatically corrected by the computers while MBEs would only be recorded by the computers. If necessary, human operators of the spacecraft would manually correct the MBEs through software patches or intentional reboots of the computer.
- 2) Shortly before executing a logical word, the relevant computer would scan it for SBEs and MBEs, correct any SBEs, and record the MBEs.

¹⁷ The physical arrangement of memory cells in a digital memory device is important because radiation particles colliding with the memory device with sufficient incidence to the plane of the memory device can pass through a number of adjacent cells and upset the bits of data that they contain (Koga et al. 1993). If the adjacent, upset bits are related to different logical words, the event will cause multiple SBEs instead of MBEs.

- 3) If three MBEs were detected on three consecutive tenth-of-a-second intervals during the main flight computer's memory scans, that computer would reboot.
- 4) If an executed MBE prevented the computers from properly resetting their watchdog timers¹⁸, the watchdog timers would reboot the computers.
- 5) If an executed MBE prevented the function being performed from executing properly, safety responses associated with that function would presumably reboot the computer.

Of course, there were other MBE response options available, most notably one that would correct MBEs automatically once they were detected, but such options would use up limited computational and data storage resources on the spacecraft and may have had negative effects on the spacecraft development cost and schedule. If the MBE estimates were to be trusted, it indeed may have been wasteful for the project to pursue these other options. Unfortunately, the prediction of zero to five MBEs over the entire mission (i.e., roughly fifteen months) was off by an order of magnitude; ironically, the first MBE occurred within the first few hours of the mission.

During GP-B's data collection phase, the six computers on the spacecraft incurred a total of at least thirty-eight MBEs, thirty-two of which were corrected manually by spacecraft operators before a reboot occurred (Owens et al. 2006). Five MBEs led to computer reboots and another halted data collection for twelve hours without causing a reboot; in all, three percent of GP-B's data collection opportunities and thousands of GP-B employee hours were lost to complications caused by MBEs (Owens et al. 2006). Additionally as illustrated by the prominent data gap in the preliminary results released by the GP-B science team (see Figure 1), the interruptions led to shorter data collection intervals.

¹⁸ Watchdog timers are devices used to independently check the health of a computing device. They reboot the computing device after a prescribed time if it is not able to successfully reset the timer periodically (the action of resetting the watchdog timer is effectively a periodic "statement" by the computer that it is okay).

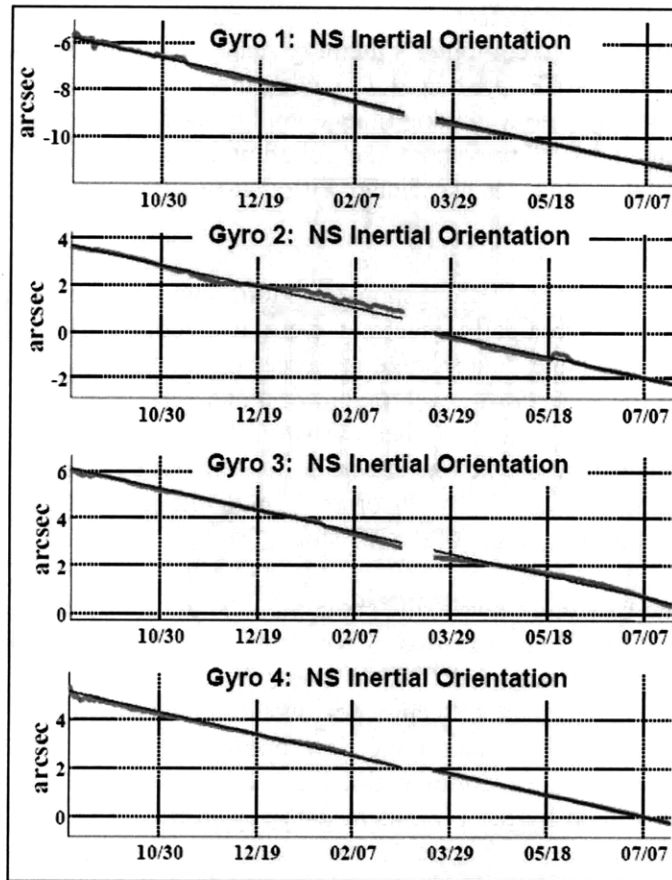


Figure 1. Preliminary results of Gravity Probe B data analysis (Everitt 2007).

However, as bad as these outcomes may seem, the situation would have been worse without the compensatory efforts of the spacecraft operators. In addition to manually correcting almost every MBE, the operators, as shown in Table 1, reduced the time it took to recover from an MBE-induced reboot of the main flight computer by nearly half each time the main flight computer rebooted (Owens et al. 2006). Furthermore, they confirmed that the MBEs almost exclusively occurred while the spacecraft was in three well-documented high-radiation regions over the Earth¹⁹, see Figure 2 and Figure 3 below, and avoided scheduling critical events whenever the spacecraft was in those regions. These measures reduced the risk that an MBE occurring in these regions would lead to a complication that triggered a reboot. Finally, they questioned the utility of the third MBE response listed above, came to the conclusion that it was more harmful than helpful, increased its activation threshold from three consecutive MBE indications to nine consecutive indications, and changed the response from a full reboot of the main flight computer to a stoppage in its command sequence timeline (Owens et al. 2006).

¹⁹ These regions are the South Atlantic Anomaly, North Polar Region, and South Polar Region. The heightened radioactive activity in these regions is linked to the structure of the Earth's magnetic field.

EVENT ID	COMPUTER	TIME (GMT)	IMPACT
MBE A	Main Flight Computer	[O]–May 3, 2004 05:03:53 [R]–May 8, 2004	~5 day (120 hour) slippage of data collection initiation
MBE B	Main Science Computer	[O]–Nov. 11, 2004 00:59:19 [R]–Nov. 11, 2004 22:10:27	21.2 hour data loss
MBE C	Main Flight Computer	[O]–Mar. 4, 2005 15:18:12 [R]–Mar. 7, 2005 17:48:30	74.5 hour data loss
MBE D	Main Flight Computer	[O]–Mar. 15, 2005 07:38:58 [R]–Mar. 16, 2005 13:32:54	29.9 hour data loss
MBE E	Main Flight Computer	[O]–Mar. 18, 2005 15:18:10 [R]–Mar. 19, 2005 06:43:15	15.4 hour data loss
MBE F	Gyro 4 Suspension Computer	[O]–Mar. 27, 2005 10:14:00 [R]–Mar. 27, 2005 21:59:00	~12 hour stoppage of the command sequence timeline

Note: [O] = Onset of event, [R] = Recovery of capabilities lost

Table 1. A description of the severe MBE Events for GP-B (adapted from Owens et al. 2006).

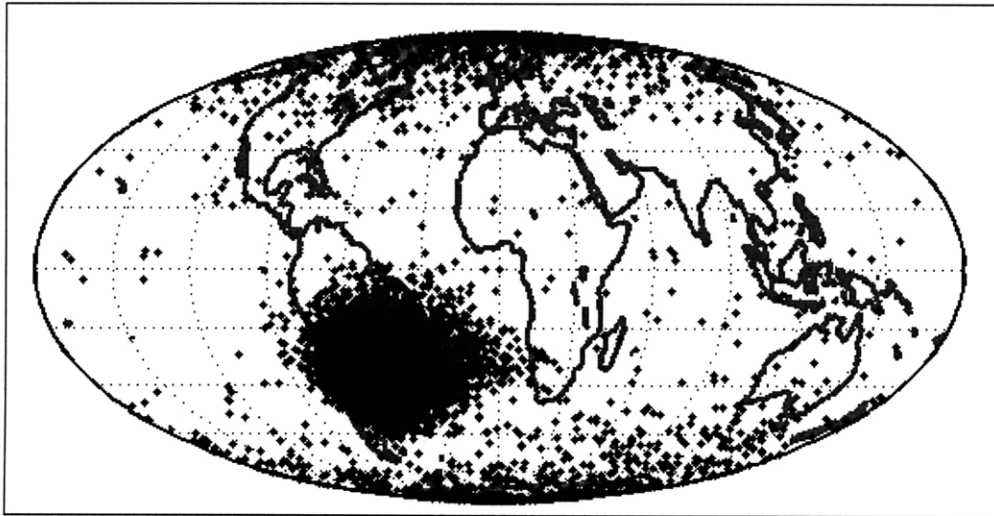


Figure 2. The location of the GP-B spacecraft during SBEs.²⁰

²⁰ SBE data from the Main Flight Computer is not shown in this plot due to corruption of the Main Flight Computer SBE data caused by the stuck bit(s) described in Owens et al. (2006).

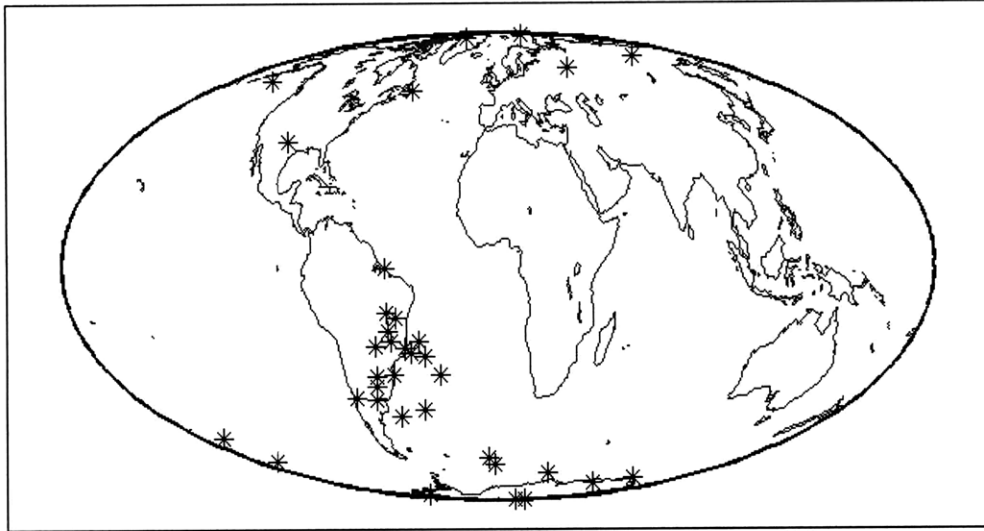


Figure 3. The location of the GP-B spacecraft during MBEs (Owens et al. 2006).

Unfortunately, as was the case in Vignettes 1 and 2, additional capabilities for compensatory action by the spacecraft operators were excluded from the system design. MBEs in the main science computer could not be corrected through software patches, resulting in one reboot (i.e., MBE B in Table 1) that could have been avoided (Owens et al. 2006). Furthermore, once it was recognized that the project's initial MBE estimates were overly optimistic, the upset scanning routines could not be altered to correct MBEs as they were detected and bits in logical words could not be reassigned in a manner that would reduce the physical adjacency of their memory cells. These exclusions in the design limited the operations team's efforts to reduce the impact of MBEs and to a certain extent relegated them to a reactive role when they had the appropriate knowledge for a more proactive role.

The overall impact of the radiation anomalies on GP-B's data collection and analysis effort will not be fully known until the final results are published and responded to by the scientific community. Immediately after the preliminary results were released, skepticism arose as to whether or not the GP-B team would be able to improve upon the accuracy of previous General Relativity experiments because of the radiation anomalies and an unexpected Newtonian torque on the gyroscopes during data collection (Wesson and Anderson 2008, Jamieson 2007, Clark and Jamieson 2007). In 2008, a review committee, citing this skepticism over the expected final accuracy of GP-B's results, recommended that NASA terminate funding for the data analysis by the start of the 2009 fiscal year (Hecht 2008). However, the GP-B team soon issued rebuttals to the review committee's report citing a more favorable November 2007 assessment of their data analysis progress by an independent peer review committee and potential inconsistencies in the NASA review process due to the agency's organizational structure (Everitt 2008, Stanford University 2008a). As of the writing of this dissertation, NASA has terminated funding of the project, and the GP-B team has secured funding from alternative sources to continue reducing the error in their measurements through December 2009 (Wesson and Anderson 2008, Stanford University 2008b).

What can be said at this point about the complications from the radiation anomalies is that they, like the destruction and fatalities in the first two vignettes, resulted from the overall socio-technical system's inability to maintain a goal, which in this case was continuous data collection. The system did not falter due to "failed" components; in fact, in this situation it is unclear what one would label as the "failed" component. While the memory device allowed its data to be corrupted, it reliably provided that data—along with the data needed to identify the MBEs—to the computing device and overwrote the data whenever requested. Had the overall spacecraft automation been equipped with the capability to correct MBEs when they were detected, the memory device would have reliably provided the computing device with the corrupted data *and* all of the information needed to correct it. More to the point, the corrupted data only caused problems when the computing devices were allowed to use them to control other components in the system. In order for that to happen, the data corruption would have to persist despite the compensatory actions of the spacecraft operators and automation. Also, one cannot neglect the role of external pressures on the system in shaping the situation; had other General Relativity experiments not allegedly undermined the value of GP-B before it was launched, the significance of the MBEs would have been reduced and the financial/schedule pressures on the project when the memory device was selected may have been different. Once again, component interactions with each other and the system's environment reigned supreme in determining how the situation would unfold; an attempt to attribute the matter to a simple "component failure" would grossly misrepresent it.

Discussion of the vignettes

A common feature in all of the vignettes was that the overall performance of each system was not equal to the sum performances that all of its individual components would produce if they were not a part of the system (i.e., the performances of the systems were a nonlinear aggregation of the performances of their parts). While certain components in the systems faltered, other components reacted in an attempt to compensate (e.g., *Challenger's* rocket nozzles pivoted to counteract thrust inadequacies due to the O-ring leak, *Columbia's* reaction control thrusters fired to oppose the torques caused by the hole-induced forces on its left wing, space shuttle engineers objected to their management's willingness to launch *Challenger* and to proceed with the *Columbia* mission without imaging the damaged wing, the GP-B's operations team learned from each MBE-induced reboot of the main flight computer and reduced the recovery time by nearly half each time, etc.). Another feature is that there were previously-utilized components that were excluded from each system (e.g., a crew escape subsystem, the SRMS, error scanning routines that automatically corrected MBEs, etc.) that potentially could have increased the systems' compensation for the faltering of some of their components enough to avoid the two tragedies and one near-tragedy.

In all three vignettes, a decision was made under uncertainty (i.e., to launch *Challenger* without a clear understanding of the effect of cold weather on the O-rings, to continue the mission of *Columbia* as planned without visual confirmation of the wing damage caused by the foam strike, and to accept a specific probabilistic representation of uncertainty as grounds for using a memory device without many commonly used radiation hardening

features) and both political and financial pressure on the decision makers. Though in hindsight, almost all of these decisions appear to be misguided²¹, they were, at the time that they were made and from the perspective of those making them, reasonable and perhaps even rational. However, as has been indicated above, these decisions were at roughly the same time unacceptable from different perspectives and resisted throughout the vignettes (though unfortunately, the resistance was often not powerful enough). These instances of portions of the system resisting the intendedly rational (though unsafe) actions of other parts of the system are examples of system nonlinearities that enhance the system's robustness, adaptability, flexibility, and resilience in opposition to unsafe decisions and component behaviors.

Before framing the problem of maintaining the safety of complex, engineered systems despite uncertainty as a matter of establishing robustness, adaptability, flexibility, and resilience in opposition to unsafe decisions and component behaviors, it is important to note that such efforts are not a struggle between "good" and "evil" (or even the blameworthy versus the non-blameworthy). Cause and effect in complex systems are not closely related in time and space (Senge 2006, Forrester 1971) and thus, those making the unsafe decisions may do so not because they are "evil," but because they cannot understand the consequences of their actions. In fact, as time passes and more information on the effects of the decision become apparent, the very individual that made the decision might even come to actively resist its consequences (e.g., a number of the engineers and managers on GP-B that selected the memory device used would later play instrumental roles in reducing the impact of MBEs on GP-B data collection).

Furthermore, expectations for the performance of complex systems often change along with the environments that they operate in, further clouding the decision maker's ability to make safe decisions. Increasing pressure on the GP-B project to justify its continuance despite the results of other experiments, for example, was a factor in its struggle to avoid cancellation, but such expectation changes are not limited to systems as "exotic" as fifty-year-long General Relativity experiments. Even systems that we encounter on a daily basis can be thrust into roles unforeseen when they were designed: retired subway cars, for example, are increasingly being used to make artificial reefs along the U.S. Atlantic Coast (Urbina 2008). The reality of complex system design and operation is that these systems must face evolving environments and expectations and must be equipped to safely endure these changes.

Overall, the sources of robustness, adaptability, flexibility, and resilience in opposition to the unsafe decisions and component behavior in the vignettes were underutilized or overwhelmed. Additionally other potential sources of such robustness, adaptability, flexibility, and resilience were excluded from the systems so that other priorities could be

²¹ The decision to use the memory device used on GP-B may be the only exception. It is unclear whether the GP-B mission could have avoided cancellation with the additional development costs and delays associated with the use of other memory devices or additional memory device testing. However, it is now clear that the probabilistic representation of MBE likelihood that was used was misleading and thus, a different approach to the treatment of MBE uncertainty, such as tracking it as a larger risk before launch and during the early stages of the mission, would have been more appropriate.

addressed. While these facts create reason to be pessimistic about the safety of complex, engineered systems (see Perrow 1999), they also suggest areas in which contributions to our understanding of robustness, adaptability, flexibility, and resilience in opposition to unsafe decisions can improve the safety of these systems. If we can learn to better design and utilize the sources of robustness, adaptability, flexibility, and resilience for opposing unsafe decisions and component behavior and to value them enough to include them in the system design despite competing priorities, we will be better equipped to safely deal with the complex, dynamic nature of our engineered systems and the environments in which they operate.

1.2 Background

The Engineering Systems Paradigm for engineering research

What can engineering research teach us about the uncertainties that engineers and operators faced in the above vignettes and how they could have been better handled? First, it is necessary to draw distinctions between the science, engineering science, and engineering systems paradigms for research. Such distinctions will better allow us to identify the knowledge that the older (i.e., science and engineering science) paradigms have provided in this regard and the type of knowledge that works in the new (i.e., engineering systems) paradigm (such as this dissertation) could provide.

As hinted at in the Theodore von Kármán and Michael Griffin quotes provided at the beginning of this chapter, each paradigm of research is meant to further different types of knowledge. Vincenti (1990) and Pitt (2001) describe science as an effort to explain the natural universe and engineering as an effort to create artifacts; for science, knowledge is an end in itself and for engineering, knowledge is a means to any number of ends.

To more clearly illustrate this distinction between science and engineering, the author shall draw upon an adapted form of the “Vee” model of systems engineering introduced by Forsberg and Mooz (1992), provided in Figure 4. Slightly above the left leg of the “Vee” we have a set of stakeholders with a set of needs. The “Vee” begins with the specification of system-level goals and requirements and proceeds downward to the specification of system components. Following fabrication of the system components (at the bottom of the “Vee”), the components are tested (the right leg of the “Vee”) individually at first and then as part of the integrated system to ensure that the goals and requirements of the system can be met. Finally, above the right leg of the “Vee”, the system as a whole is used to satisfy the stakeholder needs.

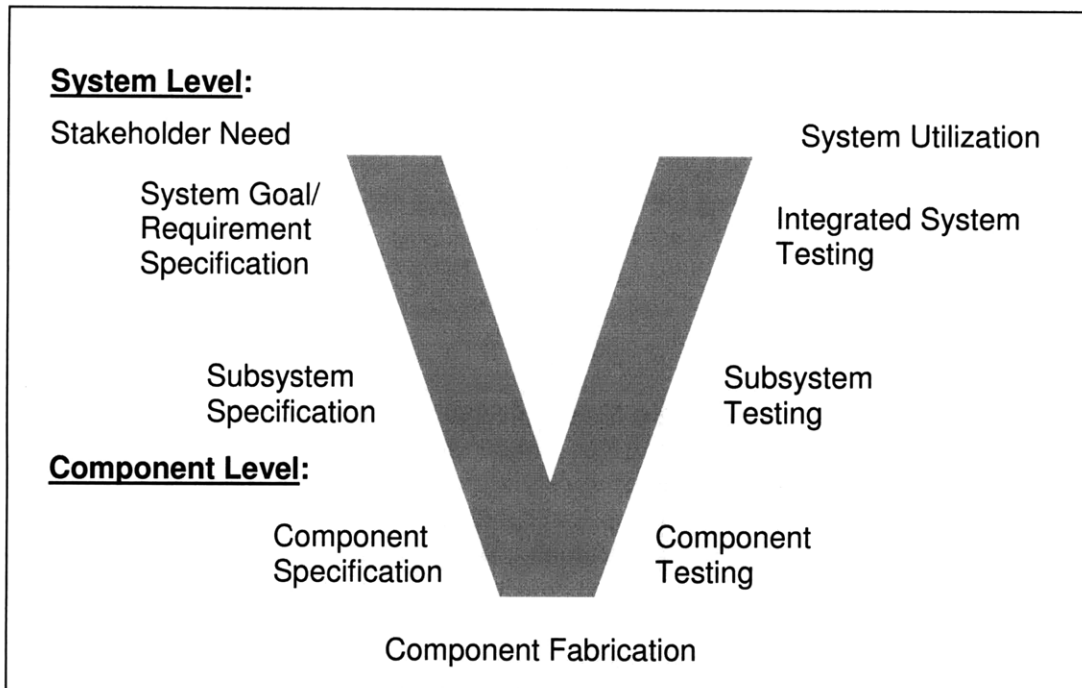


Figure 4. The “Vee” Model of Systems Engineering (adapted from Forsberg and Mooz 1992).

The “Vee” in the model provided in Figure 4 is a simple²², descriptive representation of the process of engineering a complex system. The process of scientific inquiry, on the other hand, perhaps only draws parallels to the right leg of the “Vee”, particularly the lower portion of it. The scientist examines the already-fabricated components (i.e., the natural universe) with the hope of explaining their role in the integrated system. However, while stakeholder utilization of the system may be improved by the scientist’s investigation, the scientist does not necessarily interest him or herself throughout the process with stakeholder utilization of the system. The scientist proceeds upward from the bottom of the “Vee” with a primary interest in knowledge and is therefore hesitant to compromise the robustness of that knowledge in order to reach the upper-right end of the “Vee”. The scientist isolates the components from each other and their environment; changes one variable of study at time; and whenever possible, approximates the relationships between variables as linear altogether or linear in the vicinity of critical points and events in the system. The products of the scientist’s labor are theories that must be subjected to possible refutation (Popper 1934). The process makes for a slow climb up the “Vee”, but if the theories are eventually refuted, the fruit of the scientist’s

²² The adapted “Vee” model is not to be used as a prescriptive model of the engineering process. Rarely, if ever, does the process of translating stakeholder needs into an integrated system to serve those needs proceed along a monolithic “Vee”-shaped trajectory. Iterations are likely to occur at multiple stages in the process and the use of legacy hardware, software, or processes may alter the starting point of the process. Thus, problems could result from “forcing” the process into a “Vee” trajectory. Instead, the key concept to derive from the model as presented is that when a system is too complex to design and fabricate as an “irreducible” artifact, there is a series of intermediate steps in the design process in which components must be conceptualized, created, and integrated into the system in order to prepare it to satisfy stakeholder needs.

labor will be lost or at the very least diminished²³. In other words, the scientist hopes to create theories impervious to refutation and is not necessarily interested in providing a means to stakeholders to meet their needs (i.e., in reaching the upper-right end of the “Vee”).

Heretofore, the author has established distinctions between scientists and engineers that point to differences not only in the types of systems that they examine (i.e., natural vs. designed), but also in the motivation behind their manner of inquiry. Because the engineer is concerned with delivering a system that can be utilized for stakeholder needs, he or she may not be concerned with creating indestructible theories. As stated by Hills and Tedford (2003):

“Because engineers are problem solvers, they cannot, as do scientists, follow the line of least resistance and simplify the context to suit their convenience.”

However, the generalizations that the author has used up to this point to describe engineering do not capture key differences within subcultures of engineering, particularly the academic and non-academic cultures. While engineers are indeed problems solvers, the types of problems that they face in academia are different than those faced outside of academia and thus differences have emerged in the ways that engineers approach problems in academia and elsewhere. For reasons that will not be explored in this dissertation, a culture of engineering referred to as engineering science has come to dominate engineering education and research in academia. Researchers that subscribe to the engineering science paradigm do not stray too far from the scientific method.

Like scientists, engineering scientists tend to isolate the system components from each other and their environment; change one variable of study at a time; and whenever possible, approximate the relationships between variables as linear altogether or linear in the vicinity of critical points and events in the system²⁴. Newberry (2005) refers to “methodological localization” processes in engineering science (e.g., simplifying assumptions, idealizing constraints, system decomposition, isolating control volumes, etc.) meant to reduce the scope and complexity (i.e., to remove contextual/global considerations) of research and design problems. Even Vincenti (1990) in his attempt to distinguish engineering from science points to a tendency in engineering science to ignore the contextual factors of system design by stating that in the lowest levels of the system design, knowledge is predominantly derived from the internal needs of the design rather than the contextual factors in which the system as a whole will exist.

Thus, the engineering process described in the simple model provided in Figure 4 is not fully analogous to the engineering science paradigm of engineering research. In fact, the

²³ The fruit of the engineer’s labor, on the other hand, will only be lost if the artifact that they wish to create does not get built or does not work to address the needs of the stakeholder. In this sense engineering knowledge does not have to apply “universally”, it just has to adequately apply for the specific application that it was created for and therefore, it is not destroyed by refutation as is scientific knowledge (Pitt 2001).

²⁴ These practices will be demonstrated through the discussion of Probabilistic Risk Assessment (PRA) and linearization methods in control theory in the chapters to follow.

engineering science paradigm appears to be best represented by the lower-left and lower-right sections of the “Vee” and as was the case with the scientific paradigm for research, questions arise on the motivation of the researcher to reach the upper-right end of the “Vee”. If an actual artifact is to be created from the research, the engineer (or more precisely the engineering organization creating the artifact) has a clear incentive to reach the top of the “Vee”. However, if the research is to be conducted without a clear deadline for artifact creation, as is the case in many studies in academia, the motivation to reach the top of the “Vee” may be subjugated to the desire to create robust theories of engineering utility. While such theories are needed for the success and improvement of the engineering process as a whole, there is also a need for improved knowledge of the upper section of the “Vee”. Though movement into the upper-right section of the “Vee” often exposes engineering knowledge to refutation, academia should not abdicate its role in informing this process by restricting itself to the more refutation resistant portions of the “Vee”. In other words, a new paradigm of engineering research is needed in academia to complement the engineering science paradigm.

It is the author’s belief that the new engineering systems paradigm of engineering research should complement the engineering science paradigm of engineering research to inform the engineering process as a whole. This form of symbiotic cohesion of paradigms in engineering research is analogous to already articulated views of the relationships between systems engineering/architecting and component/design engineering in engineering practice. In the original “Vee” model created by Forsberg and Mooz (1992), a line dividing the upper portion of the “Vee” from the lower portion was drawn to represent the distinction between system engineering responsibility and design engineering responsibility. System engineering was said to be responsible for work above the line with design engineering providing technical assistance, while below the line, design engineering was responsible with system engineering performing technical audit. Additionally, Maier and Rechtin (2000) proclaim:

“The art of [systems] architecting, therefore, complements its science where science is weakest: in dealing with immeasurables, in reducing past experience and wisdom to practice, in conceptualization, in inspirationally putting disparate things together, in providing ‘sanity checks’, and in warning of likely but unprovable trouble ahead. Terms like reasonable assumptions, guidelines, indicators, elegant design, and beautiful performance are not out of place in this art, nor are lemon, disaster, snafu, or loser—hardly quantifiable, but as real in impact as any science.”

In this dissertation, the engineering systems paradigm for engineering research is viewed as being primarily concerned with the sections of the “Vee” in Figure 4 above the “Component Level” label. Furthermore, the left and right legs of the “Vee” are seen as mutually dependent: efficacious specification of the system and subsystems depends on an understanding of the techniques that will be used to integrate the system and integration of the components into a system depends on a complete and coherent set of specifications. Thus, this dissertation is focused on improving our understanding of the translation of stakeholder needs (characterized by system properties) into system and

subsystem specifications and our understanding of how the products of those specifications can be used as a whole to produce the desired system properties. In other words, the author seeks to improve the process of specifying system components for the engineering scientists to analyze and of making sense of the varied context-neutral theories that arise from the engineering science analyses in order to create a system with properties that will meet the stakeholder needs.

A Systems View of Safety Risk Management

The engineering science paradigm has given us several linear models of accident causality based largely on component failure events, but because safety²⁵ is an emergent property of systems (Leveson 2009, 2004, 1995) and not a linear extrapolation of component-level properties, researchers have sought alternative models (refer to the next chapter for a review of some of the linear models and the models proposed to replace them). The accident causality model and associated risk management framework that is meant to be advanced through this dissertation is the Systems Theoretic Accident Model and Processes (STAMP) framework and associated STAMP-based Analysis (STPA) techniques first proposed by Leveson (2002, 2003, 2004). In STAMP and STPA, system safety engineering is grounded in the control theory paradigm of system state management: hazards are defined in terms of unsafe system states, constraints are identified to restrict the hazards, and a safety control structure is engineered and operated to enforce the constraints despite adaptations within the system and in its environment.

These concepts will be described more fully in later chapters, but for now, the reader is encouraged to think back to the vignettes described earlier in this chapter. For the two Space Shuttle accidents, the relevant hazard is “exposure of the crew to unacceptable accelerations” and in the case of Gravity Probe B, the relevant hazard was “inability to collect data.” In the earliest stages of system specification, the safety constraints that would follow from the hazards would likely read:

- 1) “The astronaut crew must never be subjected to accelerations greater than or equal to X_1 forward g’s, X_2 backward g’s, X_3 lateral g’s, or X_4 radians per second squared and must not be subjected to greater than X_5 forward g’s, X_6 backward g’s, X_7 lateral g’s, or X_8 radians per second squared for greater than X_9 seconds.” Where X_1 through X_9 represent theorized survivability limits.
- 2) “The GP-B spacecraft must be able to continuously collect General Relativity data for X days.” Where X is the theorized duration necessary to achieve the desired measurement accuracy.

Ideally, upon further specification and analysis of the system, safety constraints similar to the following could emerge on the subsystem and component levels:

²⁵ An accident, as defined by Leveson (2009) is, “An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, etc.).” Accordingly, she defines safety as “Freedom from accidents (loss events),”

- 1) “Thrust mismatches in the left and right SRBs must not lead to crew compartment attitude errors of Y_1 degrees or Y_2 degrees per second.” Where Y_1 and Y_2 are the theorized limits for rotational stability of the crew compartment during launch.
- 2) “Depressurization of the ET propellant tanks, at either nominal or off-nominal rates, must not lead to crew compartment attitude errors of Y_1 degrees or Y_2 degrees per second.”
- 3) “The RCC panels on the Orbiter must be inspected before the vehicle is committed to a nominal re-entry.”
- 4) “All software and all data written by the software must be read for execution as written by the software logic or human programmers” (Owens and Leveson 2006).

These constraints put an emphasis on preventing hazardous states rather than the elimination of component “failure” where the term “failure” is used with respect to the nominally expected performance of component. They leave room open for component “failure” (including the occasional poor decision by decision makers) provided that other components can detect and compensate for these failings. Furthermore, though these constraints may suggest certain levels of component functionality (e.g., the first two safety constraints in particular strongly suggest a need for crew escape capability and the third strongly suggests the usage of an SRMS, etc.), there is no set manner in which to satisfy them; ultimately, the component behavior is of secondary concern to the system’s ability to obtain its desired results.

1.3 Dissertation Research Question and Approach

The research described in this dissertation is driven by the question:

“How can we evaluate and improve the robustness, adaptability, flexibility, and resilience of complex socio-technical systems in order to oppose the unsafe decisions and component behaviors occurring in them under uncertainty?”

The research builds on recent developments in STAMP and STPA (see the next chapter) through the creation of techniques for advanced dynamic analysis of control flaws in a safety control structure (i.e., conditions that can potentially lead to hazard states). The notion that a safety control structure is an “engine” for robustness, adaptability, flexibility, and resilience to oppose unsafe decisions and component behaviors should be self-evident, but the issue of modeling the behavior of the safety control structure under both certain and uncertain conditions to inform safety control structure design and operation is still (and perhaps always will be) a matter of scholarly debate. In this dissertation, the author takes the approach of modeling the output of system safety control structures as phase space attractors (to be described in later chapters) with nonlinear, continuous dynamics subject to uncertain initial (or disturbance) conditions. In a way, taking this approach is an assertion of the following hypothesis:

“Modeling the output of system safety control structures as phase space attractors with nonlinear, continuous dynamics subject to uncertain initial (or

disturbance) conditions will provide useful insights in the design and operation of system safety control structures.”

However, it is acknowledged that this hypothesis is notoriously difficult to refute using the notions of refutation held in the science and engineering science paradigms. In some systems such a representation may capture the dynamics adequately while in others, it may not (e.g., a model using discrete dynamics may be better). Furthermore, while such a representation may only represent the actual dynamics of some systems crudely, it may also facilitate a “great leap forward” in the system-level designers’ and decision makers’ understanding of these systems (and on the other hand, it may represent a backward leap in some systems). In other words, the “theory” purported by this hypothesis cannot be context-neutral because it is context that makes each engineering system unique and worthwhile to build and operate.

With that said, support for the hypothesis is presented through the case study of the real-time procedure update process in Space Shuttle Mission Control. Procedures are a means of knowledge transfer in spaceflight operations between the in-depth operational and engineering expertise on the ground (i.e., Earth) and the executive capability on the spacecraft. In human spaceflight, procedures serve as a basis for astronaut training and in robotic and human spaceflight alike, procedures and directives dictate the specific actions of spacecraft automation. However, all procedures are based on assumptions about the operational state of the spacecraft and its environment and it is thus possible for these assumptions to be invalidated over the course of a mission. Accordingly, a process that the author calls *Procedure Rework* has emerged as a primary function of real-time ground operations teams in order to update invalid procedures before astronauts or the spacecraft automation execute them. This process is a system safety control substructure to reduce the impact of a control flaw—similar to the control flaw presented by MBEs on GP-B—in which invalid information is used to conduct a function relevant to the system-level behavior.

In the case study, a set of models for numerical simulation of procedure rework is developed through physical and human factors principles and calibrated with data from five Space Shuttle missions. These models produce simulation results with deviations from the historical data that are—as characterized by Theil Inequality Statistics—small and primarily due to cycles and noise in the data that are irrelevant with regard to the purpose of the models. These models are used to analyze the attractor produced by the Procedure Rework Process across varied conditions, some of which NASA is expected to encounter in future human spaceflight missions. Accordingly, a detrimental effect in the Procedure Rework Process is identified and approaches to mitigating the effect are explored.

This analysis and the insights that resulted from it are discussed in the case study along with the overall implications of using phase space attractors with nonlinear, continuous dynamics as a model of system safety control structure output. A process—derived as a result of this analysis—is proposed to assist STPA analysts in evaluating and potentially re-engineering the continuous dynamics of safety control structures in engineering

systems. This process is meant to occur within the overall context of a safety-driven design effort and is derived from a type of reasoning that rejects the notion of random component failures, random initiating events, and the linear superposition of the component contributions to risk as the central concepts in safety risk management. Instead, nonlinear component interactions are accounted for by conducting analyses throughout the process on the system-level of abstraction. Though there is uncertainty in the system's inputs and some aspects of its internal dynamics—and the system's behavior might therefore “appear” random—the system is tuned throughout the process to be attracted to safe system states. Overall, the analysis presented in the case study: 1) demonstrates how to use phase space attractors to evaluate system safety constraint enforcement, 2) identifies potential improvements for current and future Mission Control procedure rework processes, and 3) provides an example that other systems can learn from in order to develop safe procedure rework processes.

1.4 Dissertation Synopsis

In this chapter, three vignettes relating to accidents and incidents in complex socio-technical systems were presented to highlight the nonlinearity of these systems and their potential for robustness, adaptability, flexibility, and resilience in opposing unsafe decisions and component behavior under uncertainty. The question was then raised as to how engineering research could be used to improve such resistance to these types of decisions and behaviors. Distinctions were then drawn between the science, engineering science, and engineering systems paradigms of research in order to frame the manner in which this question would be approached. Safety risk management was defined as a subset of uncertainty management and the author's preferred framework for safety risk management (i.e., STAMP/STPA) was identified. Finally, the specific research question and approach for this dissertation were discussed.

Chapter 2 consists of a review of the literature for which this dissertation's contributions are targeted. Linear risk management models are critiqued along with several organizational models proposed to replace them. Literature promoting an emerging notion of resilience, adaptability, flexibility, and robustness to manage uncertainty (both its upside, opportunity, and its downside, risk) is then discussed (the STAMP and STPA literature is included in this discussion). Finally, the “macro-human factors” literature (i.e., an intersection of human factors and organizational research) is mentioned to highlight human-induced nonlinearities and robustness, adaptability, flexibility, and resilience in the design and operation of complex socio-technical systems.

In Chapter 3, the fundamental concepts of control theory are discussed to provide the reader with sufficient background to understand the remainder of the dissertation. The parts of a control system and notion of variables of system state are defined along with the concept of *control authority* over system states for the purpose of task execution, disturbance rejection, and adaptation. Furthermore, a simple demonstration of these concepts is provided through the analysis of a linear control system, followed by a discussion of how these concepts differ in linear and nonlinear systems. Finally, a brief summary of paradigms for nonlinear control system analysis is provided.

Chapter 4 contains an explanation of the theoretical concepts involved in modeling and engineering the phase space attractors produced by safety control structures. Phase space attractors are explained and previous mathematical representations of STAMP/STPA safety control structure behavior are reviewed. Real-world examples are then provided of phase space attractors in social and technical systems, and the relationship between the concept of phase space attractors and safety-driven design is explained. Finally, a preview of a case study application of the concept of using phase space attractors for system safety constraint enforcement—which is presented in Chapters 5, 6, and 7—is provided.

Background information for the Space Shuttle Mission Control Procedure Rework Case Study is presented in Chapter 5. A historical overview of Mission Control throughout the various U.S. human spaceflight programs is provided. Flight Controller responsibilities, facilities, staffing, and training are then detailed with an emphasis on how they enhance flight controller capability for original thought and problem solving in real-time operations. Then the Procedure Rework Process is described in order to prepare the reader for the formal analysis presented in Chapters 6 and 7. Finally the research literature pertaining to Mission Control is reviewed in order to highlight the gaps in knowledge that could potentially be filled by using the notion of phase space attractors to model safety control structure behavior.

The purpose, scope, and methodology of the Space Shuttle Mission Control Procedure Rework Case Study are discussed in Chapter 6. First, the case study purpose and scope are described. Next, the initial actions taken to develop dynamic models of the Procedure Rework Process are discussed along with the actions taken for data collection and processing. Then, a description is provided of the dynamic models and how they were calibrated.

The analyses performed in the Space Shuttle Mission Control Procedure Rework Case Study, along with their results and limitations, are detailed in Chapter 7. These analyses explore a range of flight conditions that NASA is expected to encounter as it executes its vision for space exploration and highlight potential ways in which the Procedure Rework Process can be improved. Additionally, a general process for using phase space attractors to evaluate and improve safety control structures is presented with the case study serving as an example application.

In Chapter 8, the author closes his argument. First, the author's hypothesis is revisited and his contributions to the management of uncertainty in engineering systems are summarized. Next, the author's contributions to procedure rework processes in human spaceflight and in general are reviewed. Then, the author describes possible directions for further research. Finally, the author summarizes the entire dissertation and provides a closing statement.

Chapter 2: Literature Review

“The odd term normal accident is meant to signal that, given the system characteristics, multiple and unexpected interactions of failures are inevitable. This is an expression of an integral characteristic of the system, not a statement of frequency. It is normal for us to die, but we only do it once.” –Charles B. Perrow (1999).

“The meaning of probability has been in debate ever since the concept was first developed at the end of the seventeenth century and, perhaps contrary to popular imagination, is still far from agreed.” –Stephen R. Watson (1994)

“Probability is a model, with a unique characteristic: It exists as a description of the likelihood of outcomes prior to an event but collapses at the instant of the event and thereafter. These events are ‘gambles’ with positive and negative values assigned to the outcomes. Risk is the downside of such a gamble. Underlying all probability models is the belief that the future will behave as in the past.” –William D. Rowe (1994).

“As a psychology of pragmatics, human factors adopted the Cartesian-Newtonian view of science and scientific method...These views are with us today. They dominate thinking in human factors and system safety. The problem is that linear extensions of these same notions cannot carry us into the future. The once pragmatic ideas of human factors and system safety are falling behind the practical problems that have started to emerge from today’s world.” –Sidney W. A. Dekker (2005)

“Operators and craftspeople who have their hands on the equipment are concerned with resilience, coping with the expected and unexpected deviations from the designers’ image of perfection.” –John S. Carroll (1998).

2.1 Chapter Overview

The issue of uncertainty management in complex systems—especially as it relates to system safety—spans several areas of research. In this chapter, the literature that was targeted for the key contributions of this dissertation is discussed (i.e., the safety risk management literature). Work from other literatures (e.g., the control theory literatures, etc.) that were targeted for secondary contributions of the dissertation or that are simply being invoked to enhance the literature described in this chapter, are mostly discussed throughout the other chapters of this dissertation.

2.2 Linear Accident Models

Currently, the most widely used accident models in safety risk management are what Hollnagel (2006) refers to as the simple and complex linear accident models²⁶. In these models, accidents are viewed as the result of a linear sequence or chain of events and thus, it is believed that preventing any one of the events will prevent the accident (Leveson 1995). The simplest linear accident models can be represented graphically in event trees and fault trees (Paté-Cornell 1984) or combinations thereof referred to as “bow-ties” (see Chevreau et al. 2006 for an example), while the more complex linear accident models can only be represented graphically in a rudimentary manner. Perhaps the most famous complex linear accident model is the Swiss Cheese Model (Reason 1995, Reason 1990), which depicts technical and organization barriers to event propagation as slices of Swiss cheese with “holes” that could align and provide a trajectory for events to cascade into an accident.

One of the most compelling indictments of the completeness and accuracy of linear accident models is the difficulty in using them to describe an increasingly recognized “drift into states of high risk” phenomenon associated with major accidents in socio-technical systems. In the “drift into states of high risk” phenomenon, systems slowly migrate over time to a hazardous state in which they became practically defenseless against a number of accident scenarios (Leveson et al. 2006, Woods 2006, Dekker 2005, Leveson 2004, Rasmussen 1997). Dekker (2005) provides the following account of “drift into states of high risk” in explaining the maintenance procedures on an aircraft component that failed in flight, causing an accident:

“Starting from a lubrication interval of 300 [flight] hours, the interval at the time of the Alaska 261 accident had moved up to 2,550 hours, almost an order of magnitude more. As is typical in the drift toward failure, this distance was not bridged in one leap. The slide was incremental: step by step, decision by decision. In 1985, jackscrew lubrication was to be accomplished every 700 hours, at every other so-called maintenance B check (which occurs every 350 flight hours). In 1987, the B-check interval itself was increased to 500 flight hours, pushing lubrication intervals to 1,000 hours. In 1988, B checks were eliminated altogether, and tasks to be accomplished were redistributed over A and C checks. The jackscrew assembly lubrication was to be done each eighth 125-hour A check: still every 1,000 flight hours. But in 1991, A-check intervals were extended to 150 flight hours, leaving a lubrication every 1200 hours. Three years later, the A-check interval was extended again, this time to 200 hours. Lubrication would now happen every 1,600 flight hours. In 1996, the jackscrew-assembly lubrication task was removed from the A check and moved instead to a so-called task card that specified lubrication every 8 months. There was no longer an accompanying flight-hour limit. For Alaska Airlines, 8 months

²⁶ According to Hollnagel, the difference between simple and complex linear accident models is whether or not the model is static or dynamic, respectively. In a complex linear model, the likelihood of the events in the chain are acknowledged—qualitatively or quantitatively—to change over time. In the Swiss Cheese model—which Hollnagel provides as an example complex linear model—the barriers can erode or otherwise change over time, thus changing the likelihood of an accident over time.

translated to about 2,550 flight hours. The jackscrew recovered from the ocean floor, however, revealed no evidence that there had been adequate lubrication at the previous interval at all. It might have been more than 5,000 hours since it had last received a coat of fresh grease.”

Fitting “drift into states of high risk” scenarios like the one mentioned above into a simple linear chain of events model *before* the fact is a difficult, if not intractable task. An alternative approach that has been used in the probabilistic risk assessment (PRA) community is to model “drift into states of high risk” through complex linear chain of events models in which the probability of each event is treated as a Markov process (see Paté-Cornell et al. 1996 for an example related to anesthesiology). Markov processes are a special type of system evolution process based on memory-less system state transitions, and while their use in complex linear chain of events models enhances model completeness, it also adds assumptions and complexity that further cast doubt on model accuracy, especially if the models are to be used for system optimization.

Probabilistic Risk Assessment (PRA)

In safety risk management based on linear accident models, uncertainty is often accounted for quantitatively through probabilistic estimates of event likelihood. Paté-Cornell (1996) describes six levels of the treatment of uncertainty in risk analysis ranging from least quantitative to most quantitative: 1) hazard and failure mode identification, 2) description of the “worst case” scenario, 3) description of “quasi-worst cases” or worst case scenarios that can be reasonably expected, 4) best and/or central value (i.e., mean, median, or mode) estimates, 5) Probabilistic Risk Assessment (PRA) yielding a single risk curve, and 6) PRA yielding multiple risk curves. This classification largely implies that the use of probabilistic methods is necessary to achieve increasing levels of sophistication in the treatment of uncertainty and indeed, if an event-based accident model is accepted, the effective use of deterministic methods may be precluded. However, as will be shown in Chapter 4, alternative accident models (i.e., accident models based on system state) allow for a blend of deterministic and probabilistic methods.

Although PRA is widely used, it has received a great deal of criticism in the mainstream media (Rickards 2008, Davidson 2003) and scholarly literature (Perrow 1999, Leveson 1995) and, as acknowledged by PRA advocates, is often viewed with great skepticism when it is introduced into a new industry (Apostolakis 2004, Seife 2003, Paté-Cornell and Dillon 2001). A key issue fueling the criticism and skepticism of PRA is its use as part of an optimization process. A common goal of PRA analyses is to identify risk reduction investments that will lead to the most risk reduction per dollar (or other metrics of value) so that those investments can be prioritized over others (see Dillon et al. 2003 for an example related to NASA unmanned spacecraft missions). However, optimization is always a relative, rather than absolute concept. Whenever an analyst provides a characterization of optimality, be it a probabilistic or deterministic characterization, that characterization depends on the analyst’s model of the system’s behavior and the criteria that the analyst used to distinguish good behavior from undesirable behavior. In other words, the characterization of an optimal solution depends on the characterizer’s

perception of all of the system's possible futures and what makes one future "better" than another. That perception could be inappropriate or outright wrong²⁷.

The first and most basic complication associated with using PRA for optimization relates to the meaning of probability. As suggested in the quote by Watson (1994) at the beginning of this chapter, the very definition of probability is a source of controversy. Essentially, there are "objective" and "subjective" schools of thought on what probability should mean. The objective school—often referred to as the frequentist school—views probability as the limit of the relative frequency of certain events among an overarching set of events as the number of events in that set goes to infinity. The subjective school—sometimes referred to as the Bayesian school—views probability as a degree of belief in event likelihood. Most PRA advocates subscribe to the subjective school of thought on the meaning of probability (Paté-Cornell 1996). According to Watson (1994):

"...[probabilistic safety assessment] PSA should be interpreted as reasonable argument, rather than an objective representation of truth."

Furthermore, Apostolakis (1990) states:

"Probability is always a measure of degree of belief...it is important at this time and in light of the confusion that persists in practice to clearly state that there is only one logical and workable interpretation of probability and it is that of degrees of belief."

While a subjective view of probability is not necessarily problematic in and of itself—and in fact may be more aligned with the engineering systems paradigm for engineering research than the frequentist view²⁸—using this view as a basis for optimization is perhaps paradoxical. Optimization is fundamentally a process of utilizing an objective basis to customize a system for an assumed future (or set of futures) and often results in the removal of potential sources of resilience, robustness, flexibility, and adaptability—see Table 2 for definitions of these terms—that the system could use to respond to alternative futures. Thus, in using the subjective view of probability for optimization, one could simultaneously acknowledge the potential inadequacy of their assumed future—probability estimates would after all be impossible to objectify "degrees of belief"—while seeking to objectively remove the capabilities that the system could need for alternative futures. Furthermore, as noted by Apostolakis (1990), most engineers and scientists associate with the objective view of probability by virtue of their education and

²⁷ Refer to Freudenburg (1988) for a discussion on typical errors made by probabilistic risk assessors, including the omission of knowledge from the social sciences and the disregard of public opinion in matters of high consequence, low consensus, scarce experience with the relevant technology or system, and unequal distribution of burdens and benefits.

²⁸ As discussed in Chapter 1, the contextual factors of complex, socio-technical systems are crucial in the engineering systems paradigm for engineering research. These factors make the systems and their behavior highly unique, thus limiting the usefulness of knowledge relating to the limiting relative frequency of certain system events.

training, thus leading to a great deal of confusion in the conduct and interpretation of PRA in engineering trade studies²⁹.

TERM	DEFINITIONS IN THE LITERATURE
Adaptability	<ol style="list-style-type: none"> 1. <i>“The property of a system that can change its structure, processes, and behaviour to meet changing requirements in its environment; in biology when adaptation is successful the organism will increase the likelihood of its reproduction; the changes under adaptability may be more complex than is available from flexibility” –MIT ESD Symposium Committee (2002)</i> 2. <i>“A type of system changeability in which the agent of change is internal to the system” –Ross et al. 2008</i> 3. <i>“A characteristic of a system amenable to change to fit altered circumstances, where ‘circumstances’ include both the context of a system’s use and its stakeholders’ desires.” –Engel and Browning (2008)</i>
Flexibility	<ol style="list-style-type: none"> 1. <i>“The ability of a system to undergo changes with relative ease in operation, during design, or during redesign. The basic metric is the degree of change per unit of effort (or cost including engineering, investment, etc.)” –MIT ESD Symposium Committee (2002)</i> 2. <i>“A type of system changeability in which the agent of change is external to the system” –Ross et al. 2008</i>
Resilience	<ol style="list-style-type: none"> 1. <i>“The property of a system that can quickly return to its original function and performance following a disturbance or shock; a resilient system may use its flexibility to achieve robustness” –MIT ESD Symposium Committee (2002)</i> 2. <i>“In our conception, resilience is the ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property.” –Leveson et al. (2006)</i>
Robustness	<ol style="list-style-type: none"> 1. <i>“Related to resilience, demonstrated or promised ability to perform under a variety of circumstances; ability to deliver desired functions in spite of changes in the environment, uses, or internal variations that are either built-in or emergent” –MIT ESD Symposium Committee (2002)</i> 2. <i>“The ability to remain “constant” in parameters [i.e., physical, functional, and other performance aspects of a system] in spite of system internal and external changes”—Ross et al. (2008)</i>

Table 2. Definitions of adaptability, flexibility, resilience, and robustness in the literature.

Second, in addition to the issues with the interpretation of probability, the completeness and accuracy of PRA analyses in complex, socio-technical systems has consistently been an area of concern. Even PRA advocates have acknowledged that the following items are either not handled well or at all by current quantitative risk assessments (Apostolakis 2004): human “errors” in system operations, manufacturing, and design; “software

²⁹ Reconciling this confusion among informed system stakeholders—which is a vastly important issue in an optimization process—may be more than a simple matter of training engineers and scientists to accept a subjective view of probability. Indeed such confusion may be inherent to the subjective nature of the analysis as each system stakeholder is bound to have his or her own degrees of belief in event likelihood.

failures”; and safety culture. One controversial aspect of analysis completeness in particular is the selection of the first or “initiating” event in the chain (the last event is the accident or alternative outcomes). The selection of an initiating event is subjective and varies widely among analysts (Leveson 1995). Though a small group of researchers have attempted to quantitatively trace the initiating event back to organizational factors³⁰ (Paté-Cornell 1990, Paté-Cornell and Murphy 1996, Murphy and Paté-Cornell 1996, Paté-Cornell et al. 1996), many analyses do not trace the initiating event beyond the more easily quantifiable technical factors related to the accident or final outcome. Accuracy of PRA analyses is contentious as well, particularly when probabilistic characterizations have to be made for events related to system components for which little to no data is available on their performance as part of the integrated system in its ultimate operating environment. It is common for the probability estimates to be derived from tests of the component’s performance outside of the integrated system or the system’s ultimate operating environment. Another approach is to rely on expert opinion to derive estimates of the integrated system’s performance (Paté-Cornell 1996), but that approach is subject to potential inaccuracies stemming from the many heuristics and biases affecting human decision making under uncertainty (Tversky and Kahneman 1974).

Finally, there is the issue of achieving a consensus among system stakeholders as to what metrics the analysts should use to derive the optimal solution. The most contested of the metrics often necessary in the use of PRA for optimal risk reduction is the value of a human life. Graham and Vaupel (1981) argued as early as the first issue of the journal *Risk Analysis* that the actual value assigned does not always impact the conclusions of the analysis or that the assignment of a number can be avoided altogether through relative metrics such as cost per life saved. Since then, many others have made similar arguments. However, as illustrated by the following comment by Perrow (1999), the issue of valuing a human life and other valuables at risk is deeply complex and perhaps not conducive to objective quantification:

“Death by diabetes should have the equivalent impact on people as death by murder, is the implication of a study that deplors the public’s unawareness that the former is a cause of many more deaths than the latter...But consider how a murder death affronts human values such as dignity, and the desire for security and predictability; the researchers themselves note it is not to be equated with a diabetes death, and public estimations of death rates reflect that, but the public is still held to be ‘biased’. To take another case, for some economists and risk assessors (often the same people) there is no difference between the death of fifty unrelated people from many communities and the death of fifty from a community of one hundred. Social ties, family continuity, a distinctive culture, and valued human traditions are unquantified and unacknowledged.”

Weinberg (1972) referred to such questions of valuation as “trans-scientific” questions because they attempt to take a scientific approach to assessing issues based on judgment

³⁰ Note that such efforts still assume a linear relationship between these organizational events and the technical factors that follow.

rather than fact. Accordingly, Leveson (1995) argues that the role of the system safety scientist is to identify the boundaries between scientific and trans-scientific issues and work on the scientist's side of the boundary while leaving the trans-scientific issues to be solved through political processes.

Ultimately, an attempt to optimize a system with respect to safety risk, assuming stakeholder alignment on system priorities, is an attempt to remove its resilience, flexibility, robustness, and adaptability in response to uncertainty (i.e., to "fine-tune" the system for a specific prediction of the system's future)³¹. Such an act can be desirable when system uncertainty is well characterized, as system elements enhancing resilience, flexibility, robustness, and adaptability can be wasteful in such situations. However, when the technical and organizational uncertainty of a system cannot be sufficiently characterized, resilience, flexibility, robustness, and adaptability are helpful in ensuring the avoidance of disasters and even the realization of unforeseen opportunities for system improvement.

The Swiss Cheese Model

As mentioned above, the Swiss Cheese Model depicts technical and organization barriers to event propagation as slices of Swiss cheese with holes that could align and provide a trajectory for events to cascade into an accident. It qualitatively traces accident sequences beyond the proximate technical factors to organizational decisions, referred to as latent failures (Reason 1995, Reason 1990). It is considered to be a complex linear accident model because it partially acknowledges "drift into states of high risk" in the sense that the latent failures or "holes" accumulate and potentially lie dormant for long periods of time (and presumably can be corrected during this time). However, the linear representation of the events leading to the accident directs attention towards the "holes" in the barriers (i.e., failures) rather than the processes creating the "holes" and oversimplifies the interactions between the barriers by assuming independence in the formation of "holes" in the different barriers. Nevertheless, the Swiss Cheese Model has been widely accepted as a non-quantitative alternative to PRA in research fields in which qualitative methods are typically favored, such as human factors. The aviation human factors community in particular has widely adopted the Swiss Cheese Model in their processes for investigating and classifying aviation accidents (Wiegmann and Shappell 2003).

2.3 Organizational Risk Theories

In the 1980s and 1990s, two sociological schools of thought emerged to develop an understanding of the organizational aspects of system safety: Normal Accident Theory (NAT) and the theory of High Reliability Organizations (HRO).

Normal Accident Theory (NAT)

Charles Perrow developed NAT in the aftermath of the near disaster at the Three Mile Island nuclear power plant and popularized it through his book *Normal Accidents: Living*

³¹ Indeed, "drift into states of high risk" as exemplified by the Alaska Airlines crash, often coincides with the removal of system resilience, flexibility, robustness, and adaptability through optimization processes during system operations that emphasize system priorities other than safety (e.g., profitability).

with *High-Risk Technologies*, which was first released in 1984 and updated in 1999 (Perrow 1999). In the time since the release of *Normal Accidents*, Perrow and other scholars—most notably Sagan (2004a, 2004b, 1993)—have promoted and advanced NAT in a number of disciplines and application areas. Perrow criticized PRA and traditional engineering risk management techniques (e.g., redundancy) for many of the reasons mentioned above. He also identified two system properties that he believed would make major accidents inevitable in a number of complex, socio-technical systems: interactive complexity³² and tight coupling³³. His proposed solution to the problems of interactive complexity and tight coupling is to reduce these properties in our systems when possible or abandon these systems if such a reduction is not possible.

Leveson et al. (2009) re-iterated the importance of Perrow's contribution in identifying interactive complexity and tight coupling as contributing factors to system accidents, but also proclaimed NAT as incomplete and pessimistic. Their criticism centered on Perrow's vague and sometimes shifting definitions of accidents and complexity; tendency to confuse reliability with safety; classification of whole industries as interactively complex and tightly coupled rather than specific engineering designs; and his implication that traditional safety risk management techniques, especially redundancy, are the only tools that we have or ever will have to ensure safety in complex, socio-technical systems. They then conclude their argument by proposing the abandonment of traditional (primarily event-based) safety risk management techniques for systems approaches to safety risk management, one of which (i.e., STAMP and STPA) will be discussed in detail throughout the remainder of this dissertation.

High Reliability Organizations (HRO)

The theory of HROs arose as a response to NAT, initially promoted by Karlene Roberts, Gene Rochlin, Karl Weick, Todd La Porte, and Paula Consolini (Weick et al. 1999, La Porte 1996, La Porte and Consolini 1991, Roberts 1990a, Roberts 1990b, Rochlin et al. 1987, Weick and Roberts 1993, Weick 1987). Instead of focusing on accidents and hazardous behavior, HRO researchers attempted to place emphasis on what behaviors and structures made organizations successful in spite of interactive complexity and tight coupling. They defined HROs as organizations that averted catastrophic consequences on a regular basis (e.g., tens of thousands of times) and they qualitatively described what they believed were key aspects of high reliability operations. Some of the more commonly cited aspects include: a drive for technical predictability (La Porte and Consolini 1991); prioritization of both safety and performance (La Porte and Consolini 1991); simultaneously decentralized and centralized operations (Weick 1987); imagination, vicarious experiences, stories, simulations, and other symbolic representations of technology and its effects as substitutes to learning through trial-and-error (Weick 1987); and extensive use of redundancy (La Porte 1996, La Porte and Consolini 1991, Roberts 1990b). As noted by Roberts (1990b), while it is unclear that

³² Interactive complexity is a property in which components of the system interact through unfamiliar, unplanned, or unexpected sequences that are either not visible or not immediately comprehensible (Perrow 1999).

³³ Tight coupling is a property in which changes to one part of the system rapidly affect other parts of the system (Perrow 1999).

the HRO properties identified from any observational study of one type of HRO universally apply in other types of HROs, it is suspected in the HRO community that those organizations that have few, if any, of the properties will probably be accident prone.

In the updated edition of his seminal book, Perrow (1999) characterizes HRO research as too optimistic. First, he cites a fundamental lack of incentives (and presence of disincentives) for system “elites” to prioritize safety over or alongside performance as an obstacle to avoiding normal accidents in interactively complex and tightly coupled systems. Next, he claims that effective organizational learning is easier said than done in interactively complex, tightly coupled systems. Finally, he suggests that the recommendations of HRO researchers may be helpful for some systems, but not the ones that he had argued to abandon.

Leveson et al. (2009) offer a number of criticisms on the consistency and applicability of the HRO literature. First, they point out that the “high reliability” label and accompanying definitions of an HRO appear to highlight confusion in the literature on the key differences between reliability and safety. For example, they note that HRO researchers tend to correctly point out the need for operators to occasionally break established rules in order to prevent accidents (a safety enhancing behavior), but incorrectly label the behavior as reliable. Next, they assert that a number of the systems studied by HRO researchers do not have significant conflict between safety and other goals (as most complex, socio-technical systems do) and are not sufficiently interactively complex and tightly coupled to draw conclusions from on how to effectively cope with these properties. In fact, they point out that even HRO researchers cast doubt on the interactive complexity of these systems by claiming that HROs can establish technical predictability—noting that technical uncertainty is inherent in the definition of interactive complexity. Furthermore, they note that while the use of redundancy and simultaneously centralized and decentralized operations may be effective in the systems observed by HRO researchers, it may actually lead to accidents in systems that must deal with higher degrees of interactive complexity and tight coupling.

2.4 An Emerging Notion of Resilience, Flexibility, Adaptability, and Robustness to Manage Uncertainty

As mentioned above, Leveson et al. (2009) highlight inadequacies of the organizational risk theories while promoting the use of systems approaches to risk management. They also note that other researchers (Dekker 2005, Woods and Cook 2002, Rasmussen 1997) have made similar calls for systems approaches. Systems approaches center on emergent properties of the systems under study. These properties are not revealed through examination of the system components outside of their operational context, but through analysis of the integrated system as it exists in its environment. Key emergent system properties in the management of safety risk in particular and uncertainty in general include: resilience, flexibility, adaptability, and robustness. In the paragraphs below, recent research into the relation of these properties to uncertainty management is highlighted.

The Systems Theoretic Accident Model and Processes (STAMP) Framework

Introduced by Leveson (2002, 2003, 2004), the Systems Theoretic Accident Model and Processes (STAMP) framework emphasizes control of system state rather than the reduction of event probability. In STAMP, hazards are viewed not as events, but as system states that would permit accident events when combined with certain conditions in the system's environment. It thus follows that safety—which is viewed as an emergent system property—can only be actively maintained through constraint of the states of the system (refer to the water contamination accident analysis by Leveson et al. 2004 for an example of inadequate constraint enforcement on a system state). Enforcement of constraints on system state is tasked to hierarchical control structures that must encompass the entire socio-technical system and adapt as necessary throughout the life of the system.

Early work into the development of the STAMP framework and STAMP-based Analysis (STPA) is ongoing and has centered on basic principles for developing safety control structures (Leveson 2004, Dulac and Leveson 2004, Leveson 2003), the definition of the property of resilience within the STAMP framework (Leveson 2006), using system dynamics modeling to evaluate safety control structure adaptation (Dulac 2007, Dulac et al. 2007a, Dulac et al. 2007b, Dulac et al. 2007c), and the development of STPA-related, safety-driven systems engineering processes (Stringfellow 2008, Stringfellow et al. 2008, Owens et al. 2008, Weiss et al. 2006). As mentioned in Chapter 1, further advancements to STAMP and STPA are explored in this dissertation.

Engineering Resilience

Engineering resilience was recently the topic of a symposium that produced an accompanying book (Hollnagel et al. 2006). The book includes contributions from several researchers (Woods and Hollnagel 2006, Hollnagel 2006, Woods and Cook 2006, Dekker 2006, Leveson et al. 2006, McDonald 2006, Dijkstra 2006, Sundstrom and Hollnagel 2006, Wreathall 2006, Woods 2006, Cook and Woods 2006, Hollnagel and Sundstrom 2006, Hollnagel and Woods 2006) that stress the need to move beyond linear accident models and to make use of the adaptive capabilities of humans in the system in order to cope with “drift into states of high risk”. The researchers provide definitions of resilience, descriptions of resilient system properties, guidelines for designing resilience into systems, and brief accounts of resilient operations in industry. The overall result of the symposium is not an authoritative characterization of resilience, but rather the beginnings of the “confused consensus” (Dekker 2006) from which to move forward. The following definition of resilience, provided by Leveson et al. (2006), serves as a key building block for the research described in this dissertation:

“In our conception, resilience is the ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property.”

Real Options and Design for the “-ilities”

Much attention is paid throughout this dissertation to the management of safety risk. However, it is worth noting that uncertainty has advantages as well as disadvantages. For example, demand for a product can vastly exceed expectations, potentially leaving the

product producer with an opportunity to increase profit by deviating from its initial business plan. Thus, some work has recently been devoted to managing both the advantages and disadvantages of uncertainty (MIT ESD Uncertainty Management Committee 2004). For example, the concept of “Real Options” (which was derived from financial options theory as described in De Neufville 2003), has been suggested for the mitigation of financial risk related to market uncertainties for spacecraft constellations (Hassan et al. 2005, De Weck et al. 2004) and other systems. Additionally, leading systems engineering researchers have called for systems to be designed for a host of “-ilities” related to the management of uncertainty: changeability (Ross et al. 2008, McManus and Hastings 2006, Fricke and Schulz 2005), adaptability (Engel and Browning 2008), survivability (Richards et al. 2008), reconfigurability (Siddiqi 2006), etc.

2.5 “Macro-Human Factors”

If increased emphasis on resilience, flexibility, adaptability, and robustness to counter or even benefit from uncertainty in complex systems is to be adopted—as suggested in the previous section—it may be necessary to allocate more responsibility to the operators of these systems. The engineering discipline normally used to evaluate how the systems should be designed to accommodate the humans within them is referred to as human factors. While much of the work in human factors prior to the 1990s focused on the immediate human-system interface (Carroll 1993, Reason 1990), developments in the field, such as Reason’s Swiss Cheese Model described above, have broadened the scope of the field to include the role of organizational factors on human performance. Additionally, there are calls for cross-fertilization and debate between management scholars and engineers on issues such as organizational design (Bourrier 2005). Thus, one might instead characterize the new direction of the field as “Macro-Human Factors.” In the paragraphs below, some of the “Macro-Human Factors” issues most relevant to system safety will be discussed.

Human Error and Blame

The question of whether or not humans—particularly front-line operators—cause accidents is central to the debate on the role that humans should play in complex, socio-technical systems. Many accidents have been attributed to human error (Leveson 1995), but when evaluating what decisions should follow from blame, it is important to understand what one is trying to accomplish when they assign blame. Blame can be issued absent of a sound causal justification and thus one should be cautious in using it to guide safety risk management decisions. For example, Zemba et al. (2006) noted differing logics for blame in collective- versus individual-agency cultures, citing a tendency for collective-agency cultures to blame casually innocent individuals as a symbolic proxy for the culpable collectivity. Furthermore, as pointed out by Rasmussen (1990), if one is constructing an event chain model of an accident, a human error provides a convenient stopping point in the subjective task of defining the first event in the accident sequence.

In recent years, researchers have begun to look past blame in the interest of understanding how to reduce safety risk. According to Woods and Hollnagel (2006):

“When researchers in the early 1980s began to re-examine human error and collect data on how complex systems had failed, it soon became apparent that people actually provided a positive contribution to safety through their ability to adapt to changes, gaps in system design, and unplanned for situations.”

Leveson (1995) pointed out that 1) humans do make errors, but they also correct them and 2) while almost every accident is traceable to a human error of some kind, an operator who fails to prevent an accident caused by design deficiencies is more likely to be blamed than the designer. Rasmussen (1990, 1987) argues that human workers are in a continuous state of learning and adaptation characterized by movement through three levels of cognitive control (skill-based behavior³⁴, rule-based behavior³⁵, and knowledge-based behavior³⁶) from which “errors” cannot be studied separately³⁷.

These points help to highlight a view of system operators not as potential sources of error, but as individuals with the potential to correct design deficiencies. Consider Rasmussen’s levels of cognitive control in the context of the lifecycle of a system. In system design and operations, all levels of behavior are relevant in each lifecycle phase, but for the most part, the designer’s work is more often associated with the knowledge- and rule-based behaviors than the work of the operator. “Errors” in the skill- and rule-based levels are perhaps most amenable to identification by an independent observer (they also are probably the most easily correctable by the individual who committed them or his colleagues)³⁸. However, when we look to knowledge-based behavior, particularly in system design, making the distinction between “errors” and “compromises” is difficult. Design tasks are highly iterative—refer to Eppinger et al. (1994) for a general method for representing design task coupling and a specific example of such coupling in semiconductor design at Intel. In order to make progress on an interrelated set of design tasks, the tasks must occur concurrently or assumptions about the outcome of one or more of the tasks must be made so that the other tasks can begin. Once the tasks are complete, the assumptions can be revisited through analysis and testing and if they are deemed unreasonable, the entire set of tasks can be reiterated. However, system development budgets and schedules may only allow for a limited number of iterations when they are anticipated and none if they are discovered late in the design process³⁹. As a compromise, system designers may decide to leave these unresolved issues for the

³⁴ Skill-based behavior involves work (e.g., walking, driving, etc.) that can be performed with little cognitive effort after an initial period of learning (i.e., migration from the knowledge- and rule- based behavior levels).

³⁵ Rule-based behavior involves work requiring the recognition of cues to invoke a set of stored procedures.

³⁶ Knowledge-based behavior involves reasoning and cognitive effort beyond what is required for skill- and rule-based behaviors.

³⁷ Norman et al. (2003) provide a similar three-level model of affect and cognition in humans that includes: the reaction level, the routine level, and the reflection level.

³⁸ Indeed, Norman (1983) created a classification system for operator errors in order to develop design rules to reduce these errors. The error class in this system that has perhaps received the most attention—and relates most to the skill- and rule-based levels—is a slip. Norman defines a slip as an error in which the operator fails to properly carry out an intent that could either be appropriate or inappropriate.

³⁹ Interestingly, a self-reinforcing blame dynamic is said to occur when design assumptions are found to be inappropriate late in the design process and design tasks must be re-iterated (Repenning 2001). However, in such situations, the designers are blamed for compromising schedule and budget rather than safety.

system operators to work around. In other words, the designers may leave it up to the system operators to use their knowledge-based behaviors in order to develop the rules and skills necessary to operate the system despite the compromises made by the system designers. Indeed, Dulac (2007) and Dulac et al. (2007a, 2007b, 2007c), in their investigation of the development of human spaceflight systems at NASA, collected interview data acknowledging the existence and effects of the practice of accepting design work with unresolved integration and safety problems and accordingly, modeled it as a negative factor in the ultimate safety of the operational systems.

Of course, there is also the matter of design inconsistencies that go unrecognized throughout the entire system design process, designs purposefully placing extraordinary demands on system operators, or design assumptions failing to capture the evolution of the system's operating environment throughout its lifecycle. Arguments can be made that these are knowledge-based behavior "errors" on the part of the designers as well and that they are left to the operators to cope with through knowledge-based behavior.

Organizational Design, Learning, and Change

The design of an organization and its ability to learn and change determines the context in which work is performed and evaluated. The literatures on organizational design, learning, and change—literatures far too large to review semi-exhaustively in this dissertation⁴⁰—have stressed emergent and nonlinear behavior as inherent aspects of organizational life and therefore point us away from our traditional, linear approaches to safety risk management.

Dunbar and Starbuck (2006) emphasize the need to evolve organization designs to be contextually relevant (i.e., to focus on emergent fits). Bourrier (2005) seconds this need for emergent fit and argues that organizational design is at the center of the debate on organizational factors of safety as it can influence deviation from expected behavior. Carroll et al. (2002) present a stage model, based on empirical work, of organizational learning in high-hazard organizations acknowledging that different parts of the organization can be "in" different stages at a given time and that being "in" a stage does not restrict behavior to the behaviors of that stage alone. Furthermore, Carroll (1998) identifies logics of incident review in high-hazard industries indicating a lack of appreciation for resilience and learning.

Further descriptions of nonlinearities in organizational life abound. Senge (2006) describes linear thinking as an obstacle to organizational learning and provides several nonlinear behavioral archetypes to explain undesirable system adaptations resulting from people clinging to linear perceptions of their systems. Morgan (1997) uses the nonlinear dynamics and chaos theory concept of attractors and their bifurcations as a metaphor for organizational change. Additionally, research into the temporal structuring of organizations (Ancona and Waller 2007, Ancona et al. 2001a, Ancona et al. 2001b), suggests that the timing of work (in terms of synchronization of its internal elements and

⁴⁰ For example, Huber (1991) summarizes the organizational learning literature into four constructs (knowledge acquisition, information distribution, information interpretation, and organization memory), each with their own sub-constructs and sub-sub-constructs.

synchronization with environmental disturbances to the system) leads to performance effects that would not exist if the behaviors of the system components truly were additive.

2.6 Safety Risk Management Literature Summary

Overall, one could speculate that the safety risk management literature is in the midst of a “paradigm shift” in the sense described by Kuhn (1970). Linear accident models—particularly when they are used for safety risk optimization—are failing to suffice in the management of safety risk in the increasingly relevant complex, socio-technical systems that modern societies engineer. Some proclaim that “business as normal” will inevitably lead to unacceptable accidents and that the only appropriate course of action would therefore be to abandon these systems. Others are instead questioning the utility of linear accident models and looking elsewhere for solutions to contemporary safety risk management. It is becoming increasingly recognized that system nonlinearities can no longer be ignored and that emergent system properties such as resilience, flexibility, adaptability, and robustness must be fostered in response to both the upside and downside of uncertainty. Additionally, some are recognizing the need for an increased role of system operators and organizational designers to properly ensure that these emergent properties come to fruition in beneficial ways.

In the preceding chapter of this dissertation, the role of system nonlinearities in three accidents/incidents was briefly described along with a new paradigm for engineering research (i.e., the engineering systems paradigm) that is perhaps better positioned to investigate these nonlinearities than the traditional engineering research paradigm. In the remaining chapters of this dissertation, this new paradigm in general—and the STAMP/STPA framework in particular—is put into action to begin addressing the gaps in the literature described in this chapter.

Chapter 3: Control Theory Concepts

“The central problem in control is to find a technically feasible way to act on a given process so that the process adheres, as closely as possible to some desired behavior. Furthermore, this approximate behavior should be achieved in the face of uncertainty of the process and in the presence of uncontrollable external disturbances acting on the process.” –Graham C. Goodwin, Stefan F. Graebe, and Mario E. Salgado (2001)

“An advantage of the closed-loop control system is the fact that the use of feedback makes the system response relatively insensitive to external disturbances and internal variations in system parameters. It is thus possible to use relatively inaccurate and inexpensive components to obtain the accurate control of a given plant, whereas doing so is impossible in the open-loop case. From the point of view of stability, the open-loop control system is easier to build because system stability is not a major problem. On the other hand, stability is a major problem in the closed-loop control system, which may tend to overcorrect errors that can cause oscillations of constant or changing amplitude. It should be emphasized that for systems in which the inputs are known ahead of time and in which there are no disturbances it is advisable to use open-loop control. Closed-loop control systems have advantages only when unpredictable disturbances and/or unpredictable variations in the system components are present.” –Katsuhiko Ogata (1997)

“Control is essential to the operation of systems from cell phones to jumbo jets and from washing machines to oil refineries as large as a small city. The list goes on and on. In fact, many engineers refer to control as a hidden technology because of its essential importance to so many devices and systems while being mainly out of sight.” –Gene F. Franklin, J. David Powell, and Abbas Emami-Naeini (2002)

3.1 Chapter Overview

In this chapter, the fundamental concepts of control theory are discussed. The parts of a control system and notion of variables of system state are defined along with the concept of *control authority* over system states for the purpose of task execution, disturbance rejection, and adaptation. Furthermore, a simple demonstration of these concepts is provided through the analysis of a linear control system, followed by a discussion of how these concepts differ in linear and nonlinear systems. Finally, a brief summary of paradigms for nonlinear control system analysis (i.e., linearization of nonlinear systems, nonlinearity exploration and exploitation, optimal control, and “-ilities” control) is provided.

3.2 Variables of System State

The use of the word “control” in control theory differs from its use in everyday language. In the context of individuals, groups, and organizations, for example, one may view the word control as synonymous with coercion or dominance and associate it with militaristic “Command and Control” hierarchical organizational structures. However, in control theory, the word control means to deliberately affect the state of a dynamic system^{41, 42}. When a control theorist or engineer talks about the system state that he or she wishes to affect, he or she can be referring to a number of things: the pitch of an airplane, the velocity of a car, the amount of carbon dioxide in the cabin of a space station, the temperature of a room, etc. Often, control theorists and engineers focus on system state as it applies to physical (i.e., electromechanical) systems, but the concept of system state can also apply to biological systems, economic systems, social systems, and so forth (Ogata, 1997). Therefore, the concept of system state can also encompass system properties—such as the production capacity of a manufacturing company, the number of employees of a firm in a service industry, the number of soldiers willing to obey the orders of their commanding officer, etc.—that managers, politicians, and other leaders attempt to affect in their daily work.

In other words, in the context of socio-technical systems, the word control need not be associated with the control of people or the militaristic “Command and Control” hierarchy. In cases where one of the system states that we wish to affect is the obedience of some workforce, the goal *is* to control some aspect of a person’s or group’s behavior and the militaristic “Command and Control” hierarchy may be appropriate. However, in cases in which it is desired to control the safety of the system and the ability of the organization running it to learn from its own mistakes, for example, the “Command and Control” hierarchy may inhibit learning as suggested by Carroll et al. (2002) after their observation of incident investigation and response at nuclear power plants.

Thus, the central concept of control theory is the identification of *which* system state variables to control and the appropriate *means* to control these variables. Leveson (1995), for example, defines a hazard as “a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).” With this view of hazards as system states, safety risk management can be approached as a control problem; the desired system states and constraints on system behavior to keep the system in those states can be identified and a socio-technical control structure can be engineered to enforce the system

⁴¹ Ogata (1997) defines the state of a dynamic system as, “the smallest set of variables (called state variables) such that the knowledge of these variables at [an initial reference time], together with the knowledge of the input [to the system after the reference time], completely determines the behavior of the system for any time [after the reference time].”

⁴² Forrester (1968) classifies system state variables, which he refers to as “levels”, as one of the two fundamental variable types that form the feedback loops that create a system (the other variable type that he refers to are “rates”, which are the instantaneous changes in or time derivatives of the state variables). He also states that state variables are the accumulation of the effect of past action in and on the system that continue to exist even if there is no activity in or on the system and determine (along with constants, which can be thought of as fixed state variables) the behavior of the rate variables. Thus he asserts, “Levels completely describe the system condition.”

safety constraints (Leveson 2004, Dulac and Leveson 2004, Leveson 2003). As implied in the analysis throughout this dissertation, it is often the case that the control structure or means to control the relevant system states depends upon the physical *and* organizational structure of the system.

3.3 Components of a Control System

In the application of control theory, once the desired system state or goal of the system is established, it is then input into a system of logical and physical elements referred to as the control system or control structure. The control system converts the goal into actions upon the system to be controlled that are intended to achieve or maintain the goal. There are two basic forms of control systems: *open-loop* control structures and *closed-loop* or *feedback* control structures. The fundamental elements of control systems are described in Table 3 and illustrated in Figure 5.

CONTROL SYSTEM ELEMENT:	DESCRIPTION:
Controller	The controller is the logic of the control system (stored in electronics, human minds, regulations, procedures, etc.) that determines the control actions to be pursued. The controller contains a model of the rest of the system, including the other control elements.
Actuator	The actuator is the physical object or agent that imposes the intent of the controller on the system by executing the control action.
Observer	The observer is the element of the control system (e.g., electromechanical sensor and estimation logic, person, etc.) that ascertains the system state.

Table 3. Description of control system elements.

In open-loop control, the observer, if one exists, does not feed system state information back to the controller. In other words, the controller does not take real-time system state information into account when determining the appropriate control actions to command the actuator to perform. Thus, in open-loop control, the implicit assumption is that the controller's model will accurately predict the state of the system throughout the control action.

In closed-loop control or feedback control, the observer (or observers) feeds system state information back to the controller (or controllers). The controller compares this information with the goal and then determines (through use of its system model) a control action to move the system into that state. In some control systems, the controller uses the information from the observer to update its model and change the manner in which it controls the actuator or even to control a different actuator. For example, in the Apollo 13 crisis, the lunar module, an actuator for achieving lunar landing goals, was used as an actuator for survival goals once it became apparent that the landing was not going to happen. Thus, the implicit assumption made for closed-loop control is that the controller's model will not be able to accurately predict the state of the system prior to and throughout the control action, but it will be able to drive the system to the desired state as information of its present state becomes available.

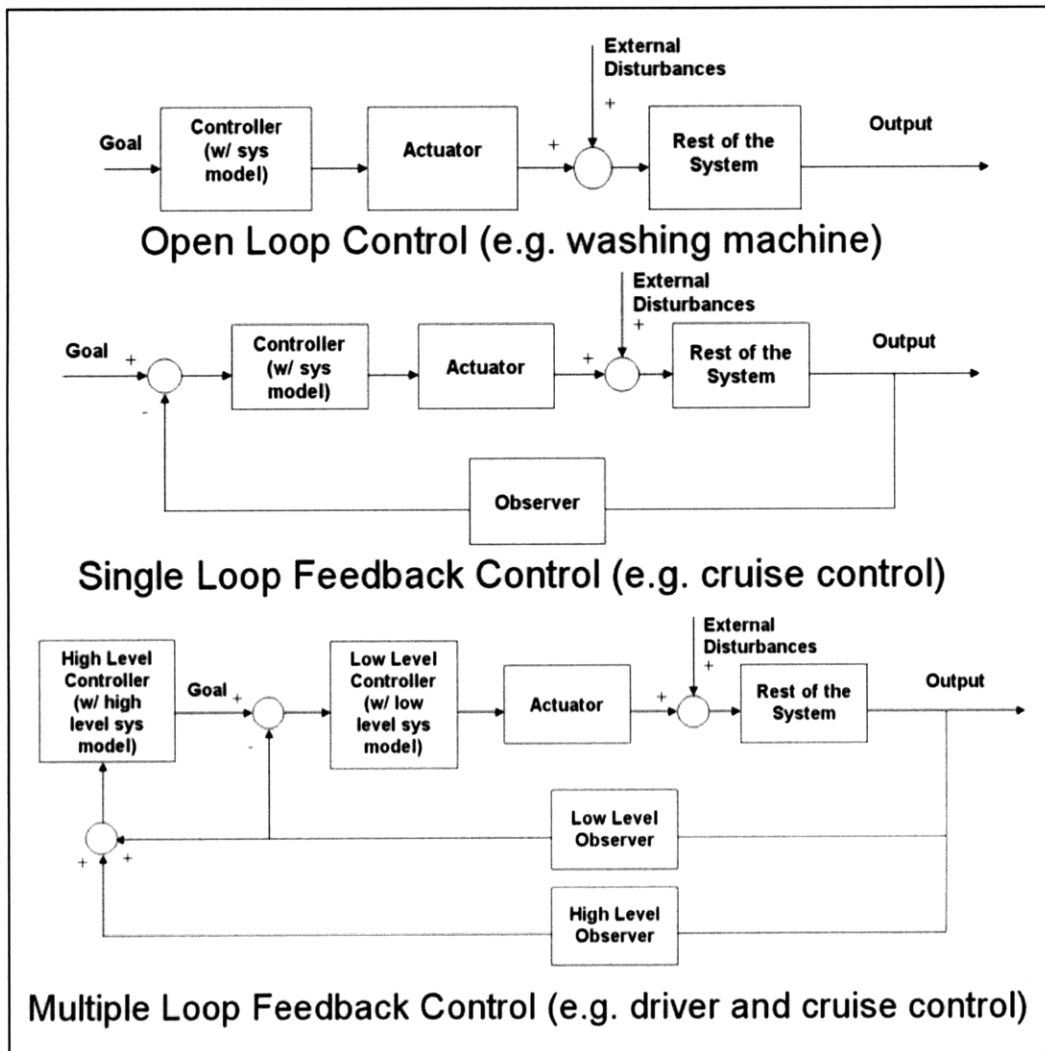


Figure 5. The elements of basic control systems.

3.4 Control Authority

There are three main uses for control systems: task execution, disturbance rejection, and adaptation. These uses are closely related to each other (reclassification of a use in a given system can usually be achieved simply by redefining the system boundaries or goals) and it is often the case that a control system will serve more than one of these uses throughout its lifecycle. In the paragraphs below, these uses are described in order to develop the concept of *control authority*, a system property that permits the ability to affect the system state.

Task Execution

Task execution is the planned alteration of system state under an assumed system environment and goal. When the uncertainty in the control system's ability to make the desired alteration of system state is perceived to be non-existent or negligible, the designer(s) of the control system may choose an open-loop control approach. As an

example, a manager may assume that writing a procedure, assigning it to an employee to execute, and trusting him or her to follow it verbatim will lead to the achievement of the desired state change. However, when the control systems or system under control are complex, there is a possibility for unanticipated and undesired interactions between system components during task execution (e.g., the system state at the beginning of the task may be uncertain, higher order effects of the task processes may be unpredictable, etc.). In other words, the possibility of internal inconsistencies⁴³ in the planned system state changes is a major source of uncertainty in task execution. In cases in which this uncertainty is present and recognized, the designer(s) of the control system may choose a closed-loop control approach.

For system safety constraint enforcement during task execution, it is important to eliminate as many internal inconsistencies as possible and include the capability to delay or alter task execution when internal inconsistencies are identified. Adherence to completeness criteria defined by Leveson (1995, Ch. 15), for example, is a means of ensuring that requirements for the system's behavior, especially as related to software, contain as few inconsistencies as possible.

Disturbance Rejection

Disturbance rejection is the alteration of system state to nullify undesired changes in system state due to external (i.e., environmental) influences on the system. It is perhaps the control system use most strongly associated with robustness⁴⁴ in that its purpose is to minimize deviance from expected system behavior. Open-loop control systems can resist disturbances through adding sources of energy dissipation (e.g., physical barriers, damping, etc.). However, closed-loop control systems can often be far more effective than open-loop control systems in rejecting disturbances (Franklin et al. 2002).

Many of the risk management techniques used in reliability engineering are intended for disturbance rejection. Redundancy, for example, is often intended to allow a system to nullify a disturbance to system state that induces the failure of a system component by shifting the failed component's function to another component (i.e., serial redundancy) or duplicating its functionality with another component (i.e., parallel redundancy). Similarly, modularity allows the failed component to be removed from the system and replaced.

Adaptation

Adaptation is the change of system structure or settings in response to changes in system context or goals. It is perhaps the control system use most strongly associated with changeability in that its purpose is to make more use of the system's operating envelope than task execution. A system can adapt in order to continue effective enforcement of safety constraints or—as exemplified by the Alaska Airlines jackscrew maintenance

⁴³ Internal inconsistencies can appear in many forms: the resource usage by two or more actuators/sensors may exceed the resources available at a given time; actuators might end up using obsolete data; task outputs can be nondeterministic; steps can occur out of sequence; steps can be started, but not completed or unexpectedly paused; etc.

⁴⁴ See Chapter 2, Table 2.

problems described in Chapter 2—to serve properties of the system that compete with the enforcement of safety constraints.

Though system adaptation is by definition not planned in the initial architecting of the system, system architects have many tools at their disposal to allow system operators, maintenance personnel, manufacturers, and re-designers to adapt the system when needed. Real Options, which are defined as rights but not obligations to change systems, have received a good deal of attention recently as tools for uncertainty management through adaptation (MIT ESD Uncertainty Management Committee 2004, De Weck et al. 2004, De Neufville 2003). Additionally, modularity allows the removal and replacement of system modules with newly designed modules.

The interplay of task execution, disturbance rejection, and adaptation

As mentioned above, it may be necessary in the design of a control system to consider all three of the uses for control systems listed above. In system operations, disturbances occurring during task execution may need to be rejected. Additionally, it may be discovered that an internal inconsistency in the system's design or manufacturing will prevent task execution as planned and thus adaptation would be necessary to work around the inconsistency. It is also possible that the system's operating environment may evolve in a manner that makes rejection of the disturbances from the environment increasingly less desirable in comparison to adaptation to the environment (in other words, at some point it may be wise to stop resisting the environmental disturbances and evolve in a manner to take advantage of or simply tolerate them). Hardware and software providing capability for disturbance rejection or system adaptation may increase system complexity leading to the introduction of internal inconsistencies in task execution⁴⁵. Finally, it may be the case that the system components adapt asynchronously (Leplat 1987), creating internal inconsistencies in the system that would hinder task execution or disturbance rejection as planned unless the system can adapt in another part of the system to counteract the negative effects of the initial adaptation.

The relation of control authority to robustness, adaptability, flexibility, and resilience

Given the preceding discussion, control authority can be defined as the ability to change system state on a certain timescale for the purpose of system task execution, disturbance rejection, or adaptation. Referring back to the standard control loop elements in Figure 5, control authority is affected by elements of system structure and the logic involved in the actuation of control and observation of the system.

When designing control authority into a system or evaluating the control authority in an existing system, a number of factors must be considered, each dependent on circumstances that the system will encounter. For some applications, large changes in state may be required and thus, the upper bound of the control authority may be paramount. In other applications, the ability to make precise changes to system state (i.e., changes that are tiny or have minimal direct impact on state variables other than the one

⁴⁵ Indeed, Sagan (2004a, 2004b, 1993), Perrow (1999), and Leveson (1995) point out that redundancy can increase interactive complexity in complex, socio-technical systems.

targeted for change) may be paramount⁴⁶. In still other applications, the frequency at which the system state can be changed may be of most importance. Additionally, in some applications great importance may lie in whether control authority is allocated to front-line system operators (i.e., an operations-centric approach to control authority) instead of system designers/re-designers (i.e., a design-centric approach) or vice versa. Finally, the sustainability of these properties of control authority throughout systems' lifecycles could be the difference between systems that age gracefully and systems that drift into states of high risk, low profitability, etc.

Building on the definitions for robustness, adaptability, flexibility, and resilience in Table 2 in Chapter 2 and the above descriptions of the three control system uses (i.e., task execution, disturbance rejection, and adaptation), the following statements are provided to summarize the relationship of these overlapping properties to control authority:

- A resilient system must maintain and make appropriate use of the desired properties of its control authority for task execution, disturbance rejection, and adaptation throughout the system's lifecycle,
- Flexible and adaptable systems must have an appropriate level of control authority for responding to changes in their context or goals (i.e., adaptation), and
- A robust system must have an appropriate level of control authority for disturbance rejection and must use its control authority for task execution in an internally consistent manner.

It follows from these statements and Leveson's (2004) description of safety as a system property maintained by a safety control structure, that safety relies on a delicate balance of the system's robustness, adaptability, flexibility, and resilience in the enforcement of safety constraints and these properties are made possible by control authority.

3.5 Linear Control Theory Concepts

In order to firmly develop the concept of control authority, in a mathematical sense, as it relates to resilience, flexibility, robustness, and adaptability in complex socio-technical systems, a discussion of both linear and nonlinear dynamics is warranted. The dynamics of socio-technical systems are governed by multiple state variables and because chaotic and otherwise nonlinear behavior is believed to be more common than linear behavior as the number of system states increases (Dechert et al. 1999, Strogatz 1994, Lorenz 1993), it follows that nonlinear behavior is likely to be the rule rather than the exception in socio-technical systems. In the paragraphs below, the concept of control authority as it relates to task execution, disturbance rejection, and adaptation is demonstrated through the dynamics of a linear, time invariant system. Nonlinear dynamics are discussed in the next chapter.

Linear, time-invariant systems are systems in which the effects of system components on system state are additive and depend on the system state rather than time (i.e., the

⁴⁶ Imprecise control authority is a potential source of interactive complexity and tight coupling in complex, socio-technical systems.

response of the system will be identical at two distinct times if the state is the same at each time). The following equation describes the general form of an autonomous⁴⁷ system of linear differential equations:

$$[\text{Eq. 1}] \quad \dot{\mathbf{X}} = \frac{d\mathbf{X}}{dt} = \mathbf{A}\mathbf{X}$$

where \mathbf{X} is a vector of state variables, $\mathbf{X} = \{X_1, X_2, \dots, X_N\}$, and \mathbf{A} is an $N \times N$ matrix of state variable coefficients that remain constant if the system is time invariant or else change as a function of time.

If the linear system has inputs, its general form is represented by the following equation:

$$[\text{Eq. 2}] \quad \dot{\mathbf{X}} = \frac{d\mathbf{X}}{dt} = \mathbf{A}\mathbf{X} + \mathbf{B}\mathbf{u}$$

where \mathbf{X} is a vector of state variables, $\mathbf{X} = \{X_1, X_2, \dots, X_N\}$, \mathbf{A} is an $N \times N$ matrix of state variable coefficients, \mathbf{u} is a vector of input variables, $\mathbf{u} = \{u_1, u_2, \dots, u_r\}$, and \mathbf{B} is an $r \times r$ matrix of input coefficients.

The outputs of a linear system, if they are affected by the system's inputs both directly and indirectly (i.e., through the system's reaction to the inputs) is as follows:

$$[\text{Eq. 3}] \quad \mathbf{Y} = \mathbf{C}\mathbf{X} + \mathbf{D}\mathbf{u}$$

where \mathbf{Y} is a vector of outputs $\mathbf{Y} = \{Y_1, Y_2, \dots, Y_m\}$, \mathbf{X} is a vector of state variables, $\mathbf{X} = \{X_1, X_2, \dots, X_N\}$, \mathbf{C} is an $N \times N$ matrix of state variable coefficients, \mathbf{u} is a vector of input variables, $\mathbf{u} = \{u_1, u_2, \dots, u_r\}$, and \mathbf{D} is an $r \times r$ matrix of input coefficients.

The control authority of linear, time invariant feedback control systems with single inputs and single outputs is commonly described through a Bode Diagram. Figure 6 is a Bode Diagram for three variants of the following open-loop example system (Franklin et al. 2002, pg. 317):

$$[\text{Eq. 4}] \quad \dot{X}_1 = \frac{dX_1}{dt} = -2X_1 - 2501X_2 - 2500X_3 + u$$

$$[\text{Eq. 5}] \quad \dot{X}_2 = \frac{dX_2}{dt} = X_1$$

$$[\text{Eq. 6}] \quad \dot{X}_3 = \frac{dX_3}{dt} = X_2$$

⁴⁷ An autonomous system has no inputs or "forcing."

$$[\text{Eq. 7}] \quad \dot{X}_4 = \frac{dX_4}{dt} = X_3$$

$$[\text{Eq. 8}] \quad Y = 2500X_4$$

The closed-loop response of the simplest variant, labeled as the “Uncompensated” variant, is dictated only by the observed difference between the desired system state and the actual system state. The responses of the other two variants are based on the amplification and altering of the observation of the difference between the desired system state and the actual system state⁴⁸. The amplification and altering is a means of compensating for the relatively inadequate response of the “Uncompensated” variant. A Bode Diagram depicts the response of the system (including any compensation that may apply) to sinusoidal inputs to the system. In linear, time-invariant systems the response to a sine wave input is always a delayed and amplified or attenuated sine wave of the same frequency as the input sine wave. The upper plot of the Bode Diagram shows the magnitude of the amplification of the sine wave as a function of its frequency while the lower plot of the Bode Diagram shows the delay (or phase lag) of the output sine wave as a function of frequency.

The Bode Diagram is useful for illustrating the control authority of linear, time-invariant systems not because we are interested in sinusoidal differences between desired and actual state per se, but because it provides an indication of the different speeds at which the system will alter system state and the magnitude of the changes at the different speeds. If we were to envision each frequency as a different component or individual in the system, the Bode Diagram would tell us how each component or individual would respond to directions to change system state. Because the contributions of each component or individual are additive, we would therefore have an indication of the overall system response. For example, if we see that one component or individual amplifies the input with a delay on the order of the amount of time it takes the input to reverse in direction (i.e., -180 degrees of phase lag), we would be able to tell that that component or individual would continuously change the system state in the opposite direction of where it needs to be changed. In other words, this component or individual would continuously drive the system further and further from its desired state, and because this component or individual’s contribution is additive with the contributions from other components or individuals, the system would never get to the desired state (in fact, it would diverge away from it towards infinity).

⁴⁸ The label “Lead-Lag” indicates that the state observation is conditioned with lead and lag filters while the label “Lead-Lag-Notch” indicates that the state observation is conditioned with lead, lag, and notch filters (see Franklin et al. 2002).

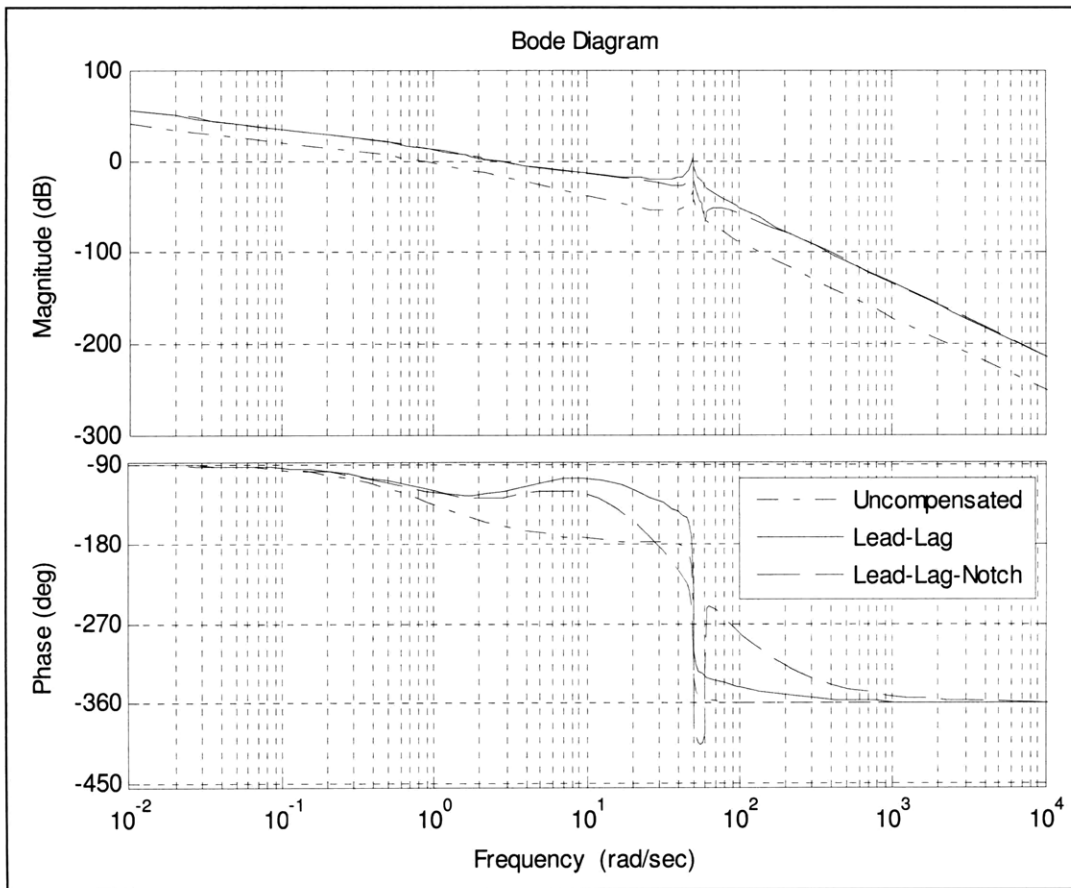


Figure 6. An example Bode Diagram of three variants of a linear, time-invariant system.

The description of the example system in the Bode Diagram of Figure 6 tells us that the input is generally amplified at frequencies in which there is an acceptable delay (i.e., frequencies with no more than -180 degrees of delay) and always attenuates the input at frequencies with unacceptable delays. Thus, we can infer that the system will converge to the desired state if the input stabilizes. Additionally, we can infer that the uncompensated system will respond slower than the compensated systems because the compensated systems amplify the input signal at higher frequencies (i.e., they have more control authority at these frequencies). Figure 7, Figure 8, and Figure 9 demonstrate how the three variants of the system perform in an example of task execution, disturbance rejection, and adaptation, respectively.

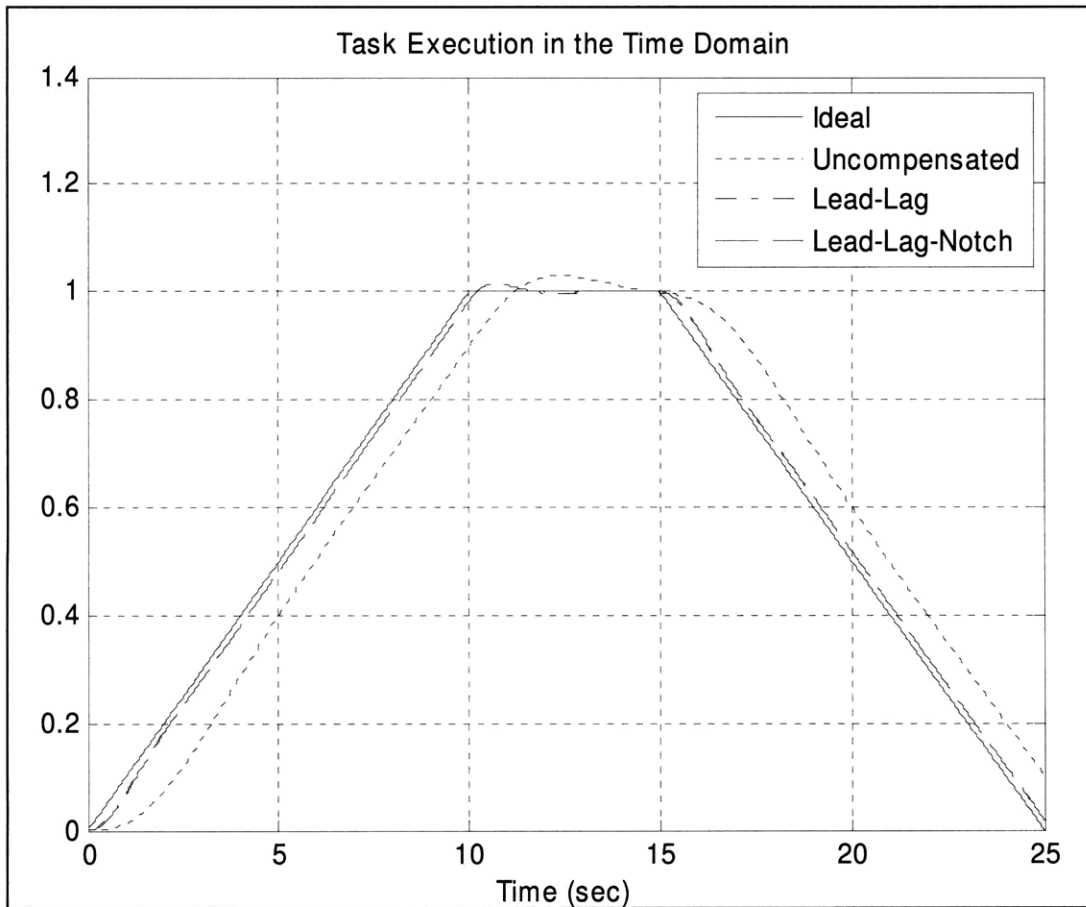


Figure 7. Example of task execution in a linear, time-invariant feedback control system.

In the task execution example, the system is directed to steadily increase the system output (e.g., temperature, pressure, etc.)—which, as indicated in [Eq. 8] is directly related to the state variable, X_4 —from an initial condition that may or may not be known beforehand to a desired state that it shall maintain for five seconds before steadily decreasing the system state back to its initial condition. As shown in Figure 7, the uncompensated variant, which has less control authority at higher frequencies, is slower to respond to the directive than the compensated variants and does a poorer job of maintaining the desired system output for five seconds.

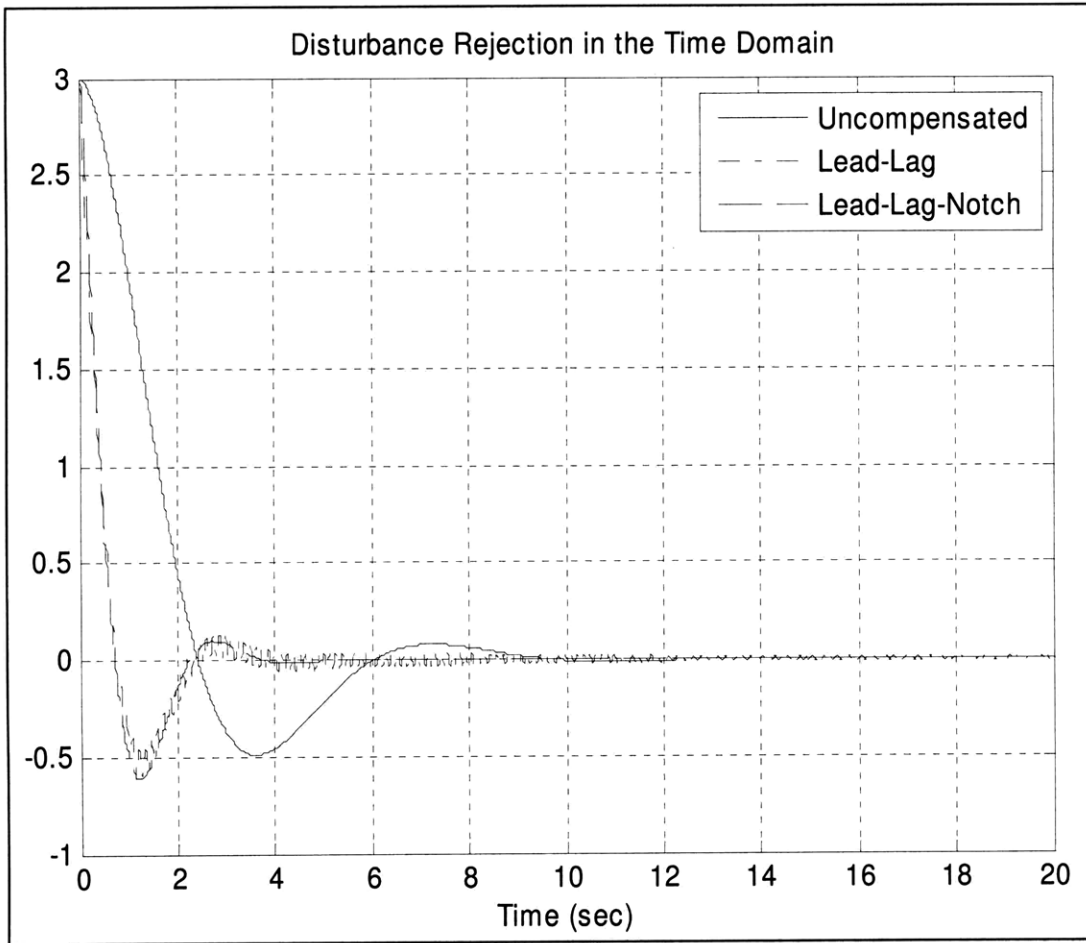


Figure 8. Example of disturbance rejection in a linear, time-invariant feedback control system.

In the disturbance rejection example, the system is directed to maintain the controlled system output at a value of zero. However, an unexpected, temporary disturbance at the start of the simulation shown in Figure 8 places the system output at a value of three. As can be seen in the figure, the uncompensated variant nullifies the disturbance more slowly than the compensated variants. Also, it is apparent that the “Lead-Lag” variant has more high frequency oscillation in its response than the “Lead-Lag-Notch” variant. This oscillation is due to additional control authority at a specific frequency (refer to Figure 6 and compare the upper plots of the two compensated variants). It could be the case that in certain applications, this high frequency oscillation in the response, resulting from the extra control authority at the key frequency, is unacceptable and would therefore need to be removed—a function performed by the notch filter in the “Lead-Lag-Notch” variant.

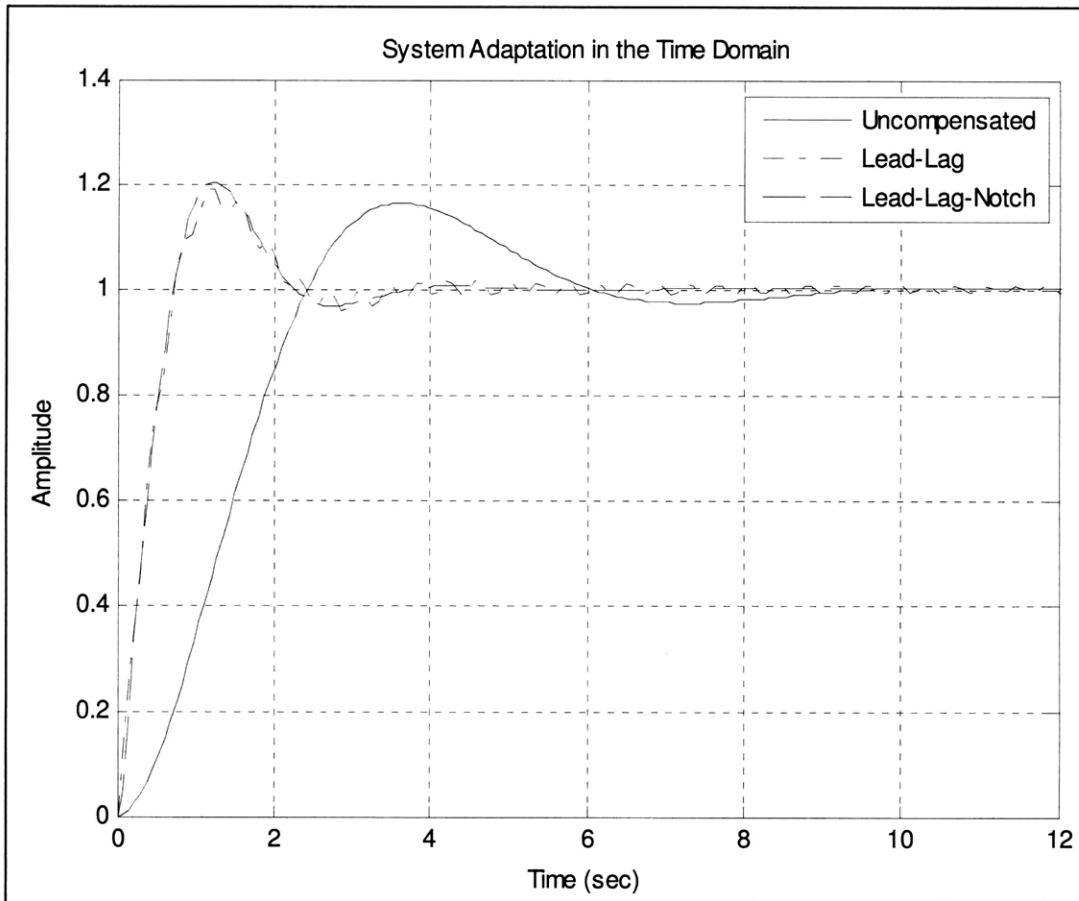


Figure 9. Example of system adaptation in a linear, time-invariant feedback control system.

Finally, in the system adaptation example, the system is given a new goal: to increase the output to a value of one and maintain it at that value instead of the zero value. The simulation shown in Figure 9 begins with the initiation of the new goal. As can be seen in the figure, the uncompensated variant is slower than the compensated variants in adapting the system to the new goal. However, it should also be pointed out that the compensated variants both temporarily overshoot the desired system state to a greater extent than the uncompensated variant. In certain applications, the overshoot induced by the extra control authority in the compensated variants may be unacceptable and therefore, for the purpose of the adaptation occurring in the example it may be desirable to temporarily or permanently disable the compensation.

The breakdown of linearity and time invariance in socio-technical systems

The example above details some of the design considerations in the allocation of control authority in linear, time-invariant systems. However, socio-technical systems are often neither linear nor time-invariant, due to the following non-exhaustive and non-mutually exclusive list of issues:

- Saturation nonlinearity: the output of an actuator may saturate at high input signals (Ogata 1997) or the absorptive capability of a “sink” inside the system or in its environment may saturate at high system or component output levels;
- Dead-zone nonlinearity: an actuator or observer may not respond to their inputs over a given range of input variation (Ogata 1997);
- Square-law nonlinearity: the output of an actuator or observer may only have an approximately linear relationship to their input for a small range of input variation, (e.g., the relationship between signal input and output may follow a “square-law”) (Ogata 1997);
- Aging and wear: actuators and observers may deteriorate over time, leading to eroding control authority;
- Resource depletion or conflict: the resources that actuators, observers, and controllers use to function may become depleted over time or unavailable at times due to resource conflicts;
- Experience curves: actuators, observers, and controllers can become more efficient as they gain experience with a certain control function;
- Drifting time delays: the amount of time that it takes for material, information, and energy to travel between controllers, actuators, observers, and combinations thereof can change over time (e.g., light delays⁴⁹ on interplanetary spacecraft missions).
- Drifting control logic: expectations of system performance and environmental conditions can change, leading to more/less conservative control strategies,
- Net material/information/energy gain or loss: a sustained, net inflow or outflow of material, information, or energy can lead to changes in fundamental system properties relevant to its system dynamics (e.g., the depletion of the mass of a spacecraft over the course of its mission).

Therefore, nonlinear analytical tools are needed to further develop the concept of control authority as it relates to resilience, flexibility, robustness, and adaptability of safety control structures in complex, socio-technical systems. A set of these tools is discussed in the next chapter.

3.6 Paradigms for Nonlinear Control Engineering Research and Practice

Though most developments in the mathematical rigor of the control of nonlinear dynamical systems have occurred within the last century, research and practice in this field can be traced back to antiquity (Bennett 1996, Lewis 1992, Ch. 1). Additionally, as suggested in the quote by Franklin et al. (2002) at the beginning of this chapter, engineering artifacts created with the help of knowledge accrued in control theory have infiltrated a wide swath of modern society. Thus, reviewing the key accomplishments of and approaches to nonlinear control research and practice in this dissertation is not possible. What is possible, however, is a brief overview of the key paradigms that shape the way in which researchers and practitioners view the process and usefulness of

⁴⁹ Light delay is the amount of time it takes for information transmitted at the speed of light to travel from a sender to a receiver.

nonlinear control research and practice. The paradigms listed below are not necessarily collectively exhaustive and may not necessarily be invoked by researchers and practitioners in a mutually exclusive manner.

Linearization of Nonlinear Systems

For a large number (perhaps even a majority) of control theory researchers and practitioners, one of the first thoughts that come to their mind when presented with a nonlinear system is how to “linearize” that system. Linearization of nonlinear systems involves the development of linear models (i.e., a set of linear differential equations) that approximate the nonlinear dynamics of the system near equilibria and critical operating points or the cancellation of system nonlinearities through alteration of the system (Franklin et al. 2002, pg. 68; Ogata 1997, pg. 100-105). Interestingly, this paradigm is not motivated by the ubiquity of linear systems—in fact, it could be said that the only “true” linear systems are the ones imagined by scholars—but by the established base of knowledge, which is more developed in regards to linear system analysis techniques than nonlinear system analysis techniques⁵⁰. Thus, even though this paradigm has been used with much success in a number of applications, there are legitimate concerns relating to its appropriateness as a default worldview.

Nonlinearity Exploration and Exploitation

Linearization, while prevalent, is not always the preferred approach to addressing a control problem. Many scholars and practitioners will only pursue linearization to a reasonable limit. Additionally, some scholars and practitioners even prefer to investigate and exploit the nonlinearities in the systems they study. The major accomplishments and views of one such research community—the System Dynamics community—are described below as an example of research driven by this paradigm. While the works of this community comprise only a subset of the established knowledge in nonlinearity exploration and exploitation, they are the most influential to the work in the case study of this dissertation.

System Dynamics

The field of System Dynamics was developed in the 1950s at the MIT Sloan School of Management by computing pioneer Jay Forrester⁵¹. Distinguishing System Dynamics from other nonlinear control theory research fields—especially those that subscribe to the nonlinearity exploration paradigm—is difficult. The following traits are common, but not necessarily required in System Dynamics research:

- a primary focus on social, socio-ecological, and socio-technical systems, rather than purely technical systems (probably due of the origin of the field in a school of management);

⁵⁰ Not surprisingly, this knowledge base was built through the science and engineering science paradigms of research, which as mentioned in Chapter 1, favor linear and reductionist approaches to the creation and refutation of knowledge.

⁵¹ Jay Forrester is also known for inventing random access magnetic core memory in the development of a flight simulator for the U.S. Navy (see <http://web.mit.edu/invent/iow/everett=forrester.html>).

- a belief that all decisions are made with models (either formal or mental), all models have inconsistencies and limitations (i.e., “all models are wrong”), and that numerical simulation is often needed to identify inconsistencies in mental models (even if numerical relationships between variables are poorly understood) (Sterman 2002, Sterman 2000, Forrester 1968);
- a focus on capturing the dynamics of a system by closing feedback loops rather than relying on time-dependent forcing functions (i.e., making the dynamics endogenous to the system rather than exogenous), identifying the reinforcing and balancing dynamics in the loops (i.e., positive and negative feedback, respectively), and the relative strength of feedback loops (i.e., loop dominance);
- visualization methods such as: causal loop diagramming (Senge 2006, Sterman 2000) and stock and flow structures⁵² (Sterman 2000) to explicitly show feedback relationships rather than condensing them with matrix notation;
- human decision modeling through assumptions of bounded rationality of the decision maker rather than the contemporary economics and game theory assumptions of rational expectations (Sterman 2000, Morecroft 1983);
- model development primarily through principles of the system’s physical and informational structure (including policies that guide decision-making) instead of statistical analysis of time-series data (Forrester 1971);
- a focus on political and technical solutions exploiting long-term, high-leverage dynamics (which are usually nonlinear) rather than short-term, low-leverage dynamics (which are usually linear); and
- inspiration from a broad literature that is loosely centered on the seminal works of Forrester (1961, 1968), Sterman (2000), Senge (2006), and articles in the journal *System Dynamics Review*.

According to Meadows et al. (1982):

“Thomas Kuhn [1970] has observed that a major part of the training of scientific disciplines is, in effect, a process of socialization to a particular world view. Included in this view is a host of subconscious and unrecognized values and assumptions about the nature of the world. For example, the systems dynamics modeler sees the world as a collection of feedback loops and non-linear relations. He or she values the kind of understanding that comes from clarifying relations between causal structure and dynamic behaviour.”

Furthermore, Sterman (2002) states:

“While it’s hard to define what system dynamics is, I don’t have any trouble answering why it is valuable. As the world changes ever faster, thoughtful leaders increasingly recognize that we are not only failing to solve the persistent

⁵² In a stock and flow structure, the state variables of the system are represented in boxes called “stocks” while the time derivatives of the state variables are represented by pipes called “flows.” A flow may connect two state variables or it may connect a state variable to a source or sink represented by a cloud.

problems we face, but are in fact causing them. All too often, well-intentioned efforts to solve pressing problems create unanticipated 'side effects.' Our decisions provoke reactions we did not foresee. Today's solutions become tomorrow's problems. The result is policy resistance, the tendency for interventions to be defeated by the response of the system to the intervention itself. From California's failed electricity reforms, to road building programs that create suburban sprawl and actually increase traffic congestion, to pathogens that evolve resistance to antibiotics, our best efforts to solve problems often make them worse. At the root of this phenomenon lies the narrow, event-oriented, reductionist worldview most people live by. We have been trained to see the world as a series of events, to view our situation as the result of forces outside ourselves, forces largely unpredictable and uncontrollable...System dynamics helps us expand the boundaries of our mental models so that we become aware of and take responsibility for the feedbacks created by our decisions."

Overall, the emphasis of System Dynamics research is not to identify ways in which the system of study can be linearized, but to identify ways in which the system of study might wrongly be linearized. As suggested by the above quote by Sterman (2002), linearized perceptions of a control problem at hand can lead to solutions that may be desirable in the short-term, but disastrous in the long-term. Additionally, as suggested by Forrester (1971), by appreciating the nonlinear dynamics of a system, one can identify ways to use nonlinear effects to his or her advantage over time⁵³. Key accomplishments in this field include:

- an urban growth model (Forrester 1969) that inspired both intense political debate and an immensely popular video game series (Seabrook 2006) by suggesting that all major urban policies in the U.S. at the time were “between neutral and highly detrimental” in terms of effectiveness towards their stated goals (Forrester 2007a);
- the *Limits to Growth* series of human population growth models (Meadows et al. 2004, Meadows et al. 1992, Meadows et al. 1982, Meadows et al. 1974, Forrester 1973, Meadows and Meadows 1973, Meadows et al. 1972) that led to Congressional hearings and reportedly inspired a man to successfully run for Congress (Forrester 2007b);
- a number of world-famous interactive games or “management flight simulators” used for K-12, university, and executive education (Meadows 2007); and
- numerous consultations of government and industry projects, including the resolution of legal disputes involving project management (Lyneis et al. 2007, Lyneis et al. 2001, Sterman 2000).

⁵³ Indeed, there is another subfield of nonlinear control theory referred to as chaos control that seeks to take advantage of the fact that certain nonlinear systems (i.e., chaotic systems) are highly sensitive to small changes in initial conditions (Boccaletti et al. 2000). Essentially, the sensitivity of these systems to initial/disturbance conditions allow for control solutions in which a small amount of control effort can be used to dramatically impact the dynamics of the system in a desirable way.

Optimal Control

The optimal control paradigm relates to the use of feedback control to minimize task operating time or some other performance index associated with system task execution (Bryson 1996, Lewis 1992, Ch. 1). In other words, the design problem associated with this paradigm is not simply to create a stable controller, but to create the “best” controller (which includes the challenge of determining the meaning of “best”) (Bennett 1996). Accordingly, great emphasis is placed on model exactness in this paradigm, which can discourage researchers from analyzing systems with uncertainties or encourage them to neglect key uncertainties. According to Bennett (1996) one leading researcher publicly lamented in 1984 (after the emergence of the optimal control as a dominant paradigm in academia) that:

“It is amazing how many [control theory Ph.D.’s] are unaware that the primary reason for feedback in control is uncertainty.”

Additionally, a number of early controllers developed through the principles of optimal control had “serious robustness problems” (Bryson 1996). Thus, in recent years the need to balance control system “optimality” and capability for coping with uncertainty has become more widely recognized (Lewis 1992, Ch. 1).

“-ilities” Control

The final paradigm in this list emphasizes the attainment/maintenance of desired system properties in the face of uncertainty, rather than the minimization of a performance index. Thus, this paradigm can be described as “-ilities” control for its focus on system “-ilities” (e.g., two modern control theory subfields of this paradigm, adaptive control and robust control, emphasize the system properties of adaptability and robustness, respectively). Though the focus on system properties despite uncertainty embodied by this paradigm is said to have been largely absent in control theory research during the early years of the “Modern” period of control theory, it is said to have been prevalent in both research and practice in the “Classical” period and in the midst of a revival in the last decades of the 20th Century (Bennett 1996, Lewis 1992, Ch.1).

3.7 Chapter Review

In Chapters 1 and 2, the importance of nonlinearities in the management of safety risk for complex socio-technical systems was established. Additionally, the STAMP/STPA framework and its inherent philosophy of treating safety as a control problem was introduced and vetted against linear safety risk management approaches. In this chapter, the fundamental concepts of control theory (i.e., variables of system state, the components of control systems, and control authority) were introduced. Next, a mathematical description of these concepts was presented in the context of an example linear system. This linear example was used not because linear control theory will play a major role in the remainder of this dissertation, but to help the reader develop an intuition for the fundamental control concepts (which, at present, can perhaps be most easily described in terms of linear systems) and the deficiencies involved in viewing a nonlinear system as though it were linear. Indeed, the paradigms that primarily motivated the research described in the remainder of this dissertation are the nonlinearity exploration

and exploitation and “-ilities” control⁵⁴ paradigms, which were discussed along with several other paradigms for nonlinear control engineering towards the end of this chapter. In the next chapter, an approach for the analysis and design of nonlinear safety control structures is introduced.

⁵⁴ Recall that in STAMP and STPA, safety is defined as an emergent system property or “-ility.”

Chapter 4: Phase Space Attractors and their Relevance in System Safety Constraint Enforcement

“The space shuttle flies with five redundant computers. Any fully digital airliner has a minimum of three. Apollo had only one. It never failed in flight...[the designers of the Apollo computer] took the position that there is no such thing as a random failure; rather, failures always occur ‘based on cause and effect principles’ (an approach credited with success in other parts of Apollo as well). All failures had a source, and for electronic devices, most of those were ‘the result of poor process control or the vendor’s lack of complete technical knowledge of his process.’ Reliability was not simply a matter of statistics, but also ‘always an integral and basic part of design, or procurement, and of operation,’ best left to the ‘judgment and wisdom of the engineers’ [Draper et al. 1963]. Key to this approach was standardization—build systems out of the smallest possible numbers of different parts and focus a great deal of effort on improving every aspect of the process of producing them.” –David A. Mindell (2008).

“The focus on attractor patterns thus creates a powerful perspective for the management of stability and the management of change, suggesting that transformational change ultimately involves the creation of ‘new contexts’ that can break the hold of dominant attractor patterns in favor of new ones.” –Gareth Morgan (1997)

“Planners are not, after all, scientists. Planners seek understanding not as an end in itself but as a means to an end—namely, as a basis for making informed judgments about the effects of intervention. Rather than looking for ever more detailed information on and ever more accurate models of their systems, planners should look instead for patterns of system behavior, or points to which systems seem to return (which mathematicians call “attractors”), even if not in any predictable way.” –T. J. Cartwright (1991)

4.1 Chapter Overview

This chapter contains an explanation of the theoretical concepts involved in modeling and engineering the phase space attractors produced by safety control structures. Phase space attractors are explained and previous approaches for quantitative modeling of STAMP/STPA safety control structure behavior are reviewed. Real-world examples are then provided of phase space attractors in social and technical systems. Finally, the relationship between the concept of phase space attractors and safety-driven design is presented along with a preview of the dissertation case study.

4.2 Phase Space Attractors

The *phase space* of a system is the space encompassing all possible states of the system (i.e., all possible values of all of the system's state variables). For example, in a bounded, two-dimensional system (i.e., a system with two state variables), the phase space can be depicted on a plot with the possible values of the two state variables represented on the horizontal and vertical axes, respectively. A *phase space attractor* is a mathematical result achieved when the system converges to or remains in a certain region of the phase space despite being subjected to a range of initial and disturbance conditions for the state variables. As is mentioned below, these concepts relate to safety control structures because they describe how the system responds to unpredictable, but not uncontrollable system inputs or internally-induced (i.e., endogenous) changes in system state.

Referring back to the quote provided at the beginning of this chapter by Mindell (2008), it is stated that MIT IL engineers rejected the notion of a “random” failure in designing the Apollo Guidance Computer and relied on a more deterministic mindset for the overlap of reliability and safety risk management. This mindset, when contrasted with the more stochastic mindset adopted in probabilistic risk assessment, raises a number of questions about the relative importance of the mindsets and their relative usage as a basis for safety risk management. PRA is an optimization-centric approach; accepting the notion of random failures leads to a black-box, “take it or leave it” view of safety risk management in which the objective is to buy and arrange the black-boxes (i.e., the components) in a manner that minimizes perceived risk. Of course, optimization is desirable for obvious reasons, however, the difficulty of defining and proving optimality is immense in systems characterized by uncertainty. Consider the following statement from Sterman (1991):

“Whenever the problem to be solved is one of choosing the best from among a well-defined set of alternatives, optimization should be considered. If the meaning of best is also well defined, and if the system to be optimized is relatively static and free of feedback, optimization may well be the best technique to use. Unfortunately, these latter conditions are rarely true for the social, economic, and ecological systems that are frequently of concern to decision makers.”

While the objective of finding an optimal way to reduce risk looms large over the field of risk analysis, an overly utilitarian focus for risk analysis may distract us from looking for sound risk reduction opportunities in the interactions of system components, especially when uncertainties abound.

In contrast to the stochastic mindset in which component/system failures (and their successes) are perceived to be random, the deterministic mindset attributes safety—where it overlaps with reliability—to the system's built-in reactions to system state. Through cycles of feedback, the states of the components are affected by the states of the system, which are affected by the states of the components and the system's environment. Components therefore tend to interact with each other through their reaction to system state, essentially compensating for the faltering of each other or interfering with each other (refer to the vignettes in Chapter 1 for examples). Thus, it is necessary in the

deterministic mindset to eliminate the “black-box” boundaries around components (i.e., to conduct analysis at a system level of abstraction) and account for system interactions and their effects on the desired system states.

With that said, it is necessary to address what could be perceived as a paradox. In considering a system characterized by uncertainty, one might ask how one would know enough about the system to characterize the system’s interactions as suggested by the deterministic mindset. This question is exactly where the concept of attractors (and system testing⁵⁵) is useful. As suggested in the quotes by Morgan (1997) and Cartwright (1991) at the beginning of the chapter and demonstrated throughout the rest of this chapter, phase space attractors result from dynamic structures that respond strongly to unpredictable disturbances to the system and unexpected endogenous dynamics. Thus, due to the random inputs to the system and unforeseen changes in system state caused by endogenous dynamics, the actions of a system capable of producing an attractor may “appear” random and unpredictable, but in fact, its behavior is deliberately tuned to system state.

Equilibrium Point Attractors

Equilibrium Point Attractors are values in the phase space to which the system converges. In other words, if the system has an equilibrium point attractor, but does not “start out” at that attractor or is displaced from it by a disturbance, the system will return to that attractor over time. Depending on the damping properties of the system, the system will either return to the attractor with or without overshooting it. Whenever a system overshoots its equilibrium point attractor in the process of converging to it, a spiral-like trajectory is produced in its phase space and thus the attractor is referred to as a *spiral-in equilibrium*. The following system produces a spiral-in equilibrium point attractor (Boyce and DiPrima 1997, pg. 382):

$$[\text{Eq. 9}] \quad \dot{X} = \frac{dX}{dt} = aX + bY \quad \text{where } a = -0.5 \text{ and } b = 1$$

$$[\text{Eq. 10}] \quad \dot{Y} = \frac{dY}{dt} = cX + dY \quad \text{where } c = -1 \text{ and } d = -0.5$$

When using the “stock and flow structure” notation of System Dynamics, [Eq. 9] and [Eq. 10] are represented as shown in Figure 10.

⁵⁵ System testing is one approach to reducing system uncertainty.

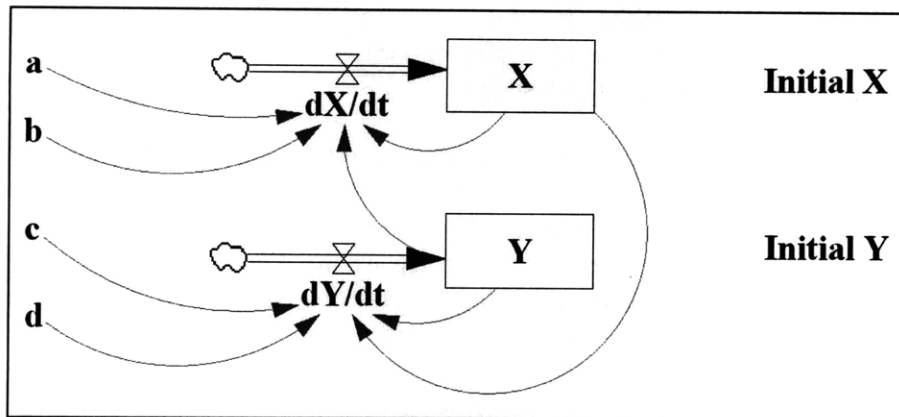


Figure 10. Stock and flow structure of the system modeled by [Eq. 9] and [Eq. 10].

Because this system is attracted to an equilibrium point, it will converge to this point despite a range of initial conditions. As shown in Figure 11, the “spiral-in” trajectories to the equilibrium point ($X = 0, Y = 0$) are produced in the X-Y Phase Space for each of three simulated initial conditions for the system (i.e., $X = -1.35, Y = -2.1$; $X = 2, Y = 2$; and $X = -2.4, Y = 2.25$).

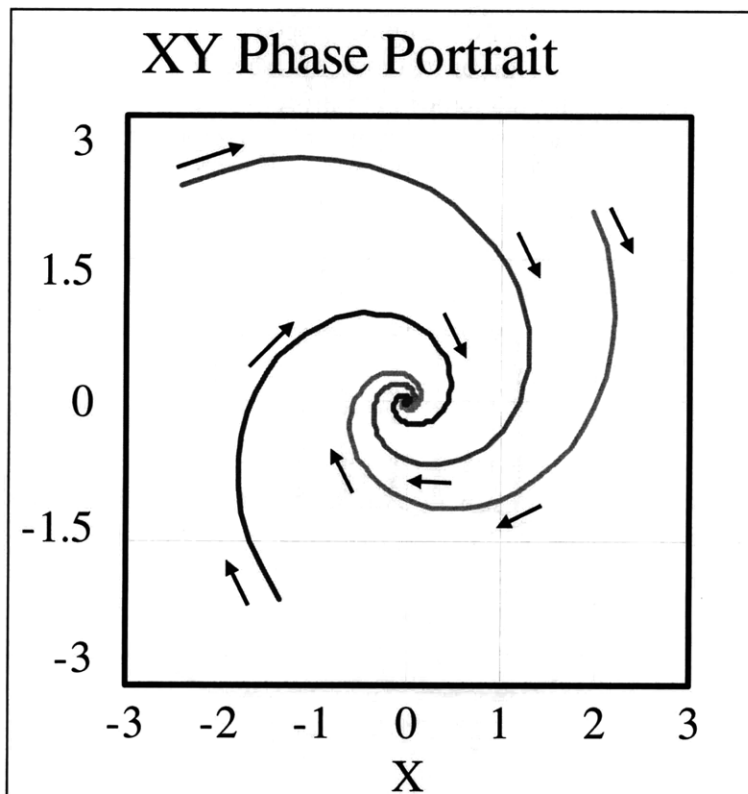


Figure 11. Phase Portrait for three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.

The system's attraction to point $(X = 0, Y = 0)$ can also be determined by looking at the time histories of state variables X and Y , Figure 12 and Figure 13, respectively. However, as will be shown later when more complex attractor structures are discussed, attraction tendencies of the system will not be as easily decipherable when examining state variable time histories alone.

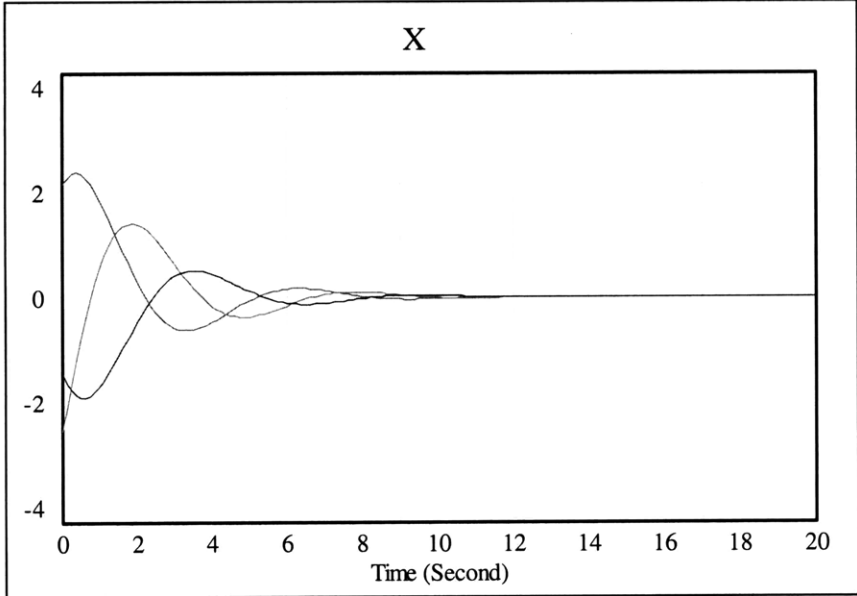


Figure 12. Time history of the state variable X after three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.

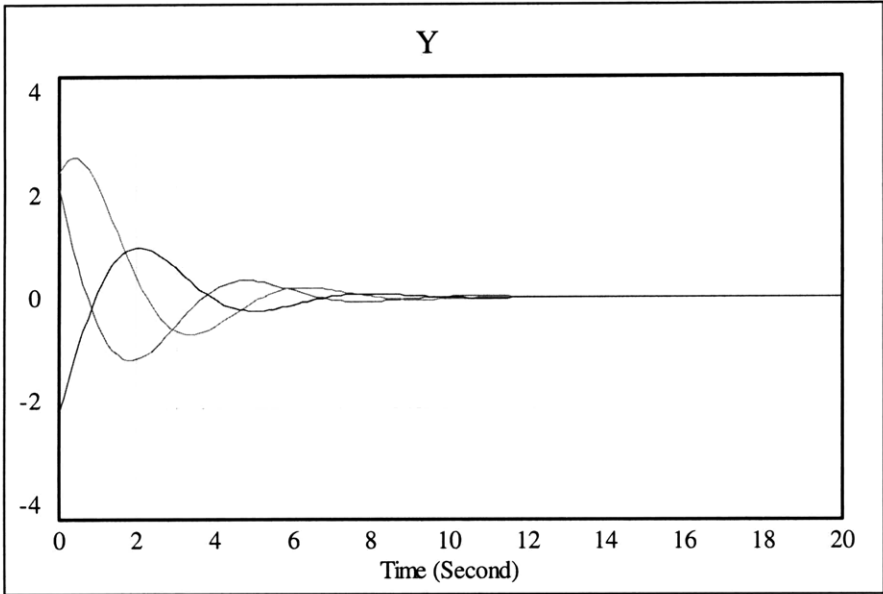


Figure 13. Time history of the state variable Y after three simulation runs of the system modeled by [Eq. 9] and [Eq. 10], each with different initial conditions.

In the context of safety control structures, it may be desirable in a number of applications for the structure to produce an equilibrium point attractor in order to hold one or more state variables at or near a safe state (characterized by the equilibrium point) despite unforeseeable (and perhaps unavoidable) initial conditions and disturbances. An example of such a situation is provided in the case study analysis in Chapter 7.

Attracting Limit Cycle

An *attracting limit cycle* is a stable, periodic oscillation to which certain dynamical systems can be drawn following a range of initial/disturbance conditions. The following system, described by the Van der Pol Equations, produces an attracting limit cycle (Boyce and DiPrima 1997, pg. 527):

$$[\text{Eq. 11}] \quad \dot{X} = \frac{dX}{dt} = Y$$

$$[\text{Eq. 12}] \quad \dot{Y} = \frac{dY}{dt} = -X + \mu(1 - X^2)Y \quad \text{where } \mu = 1$$

An alternative (i.e., stock and flow structure) representation of these equations is shown in Figure 14.

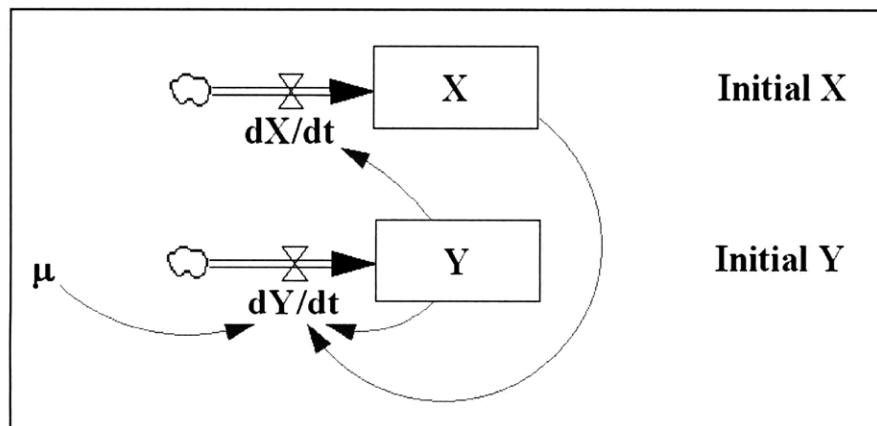


Figure 14. Stock and flow structure of the Van der Pol Equations.

As can be seen in Figure 15, the system converges into a closed trajectory or “orbit” in the X-Y Phase Space for each of three simulated initial conditions for the system (i.e., $X = 1, Y = 0$; $X = 3, Y = 2.4$; and $X = 1.65, Y = -2.4$). The closed orbit in the figure is the attracting limit cycle.

The system’s attraction to a stable, periodic oscillation can also be seen in the time histories for state variables X and Y, shown in Figure 16 and Figure 17, respectively. However, due to the difference in initial conditions, the oscillations are not synchronized in the time history, making it slightly more difficult for the analyst to interpret attraction tendencies.

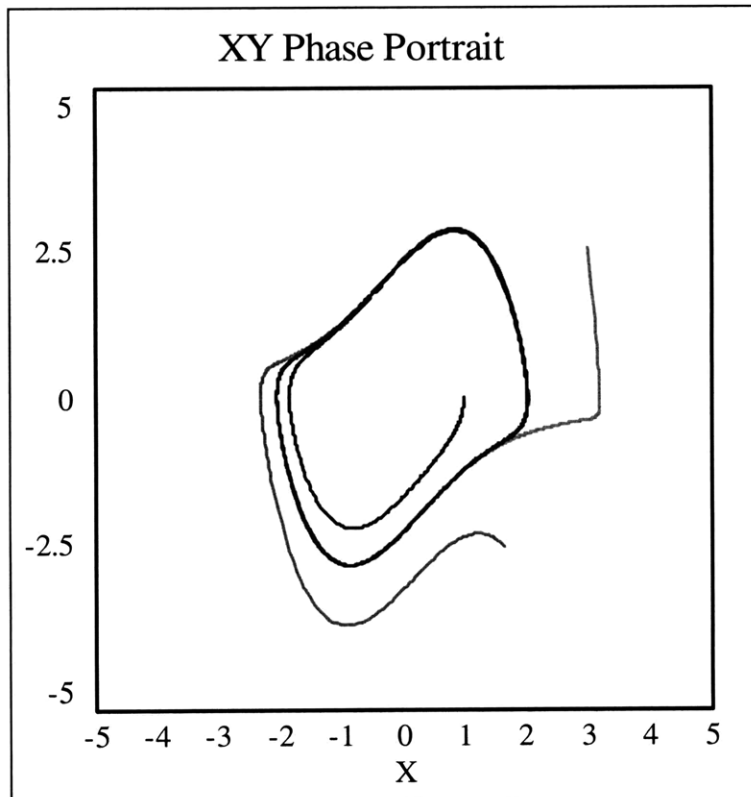


Figure 15. Phase Portrait for three simulation runs of the Van der Pol Equations, each with different initial conditions.

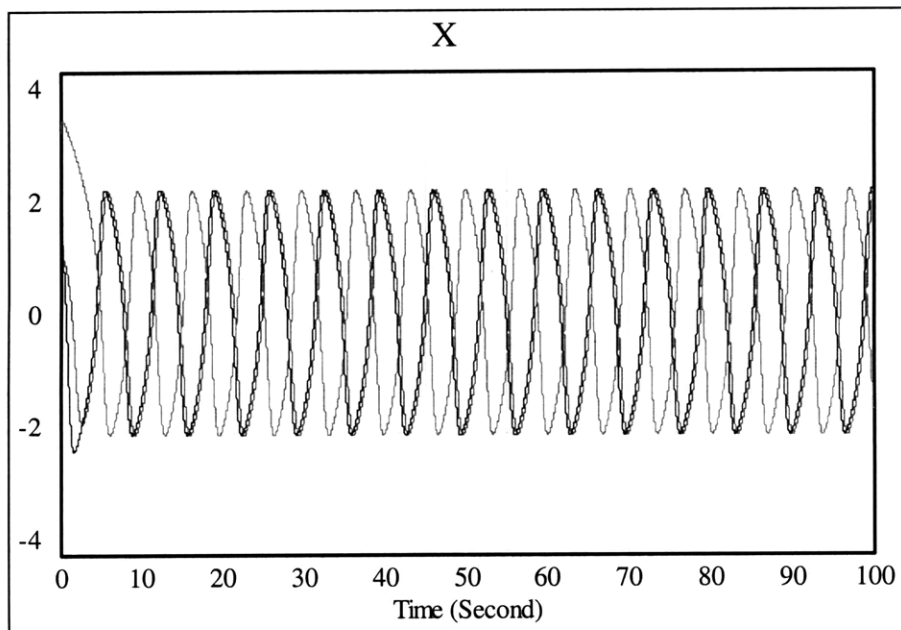


Figure 16. Time history for the state variable X after three simulation runs of the Van der Pol Equations, each with different initial conditions.

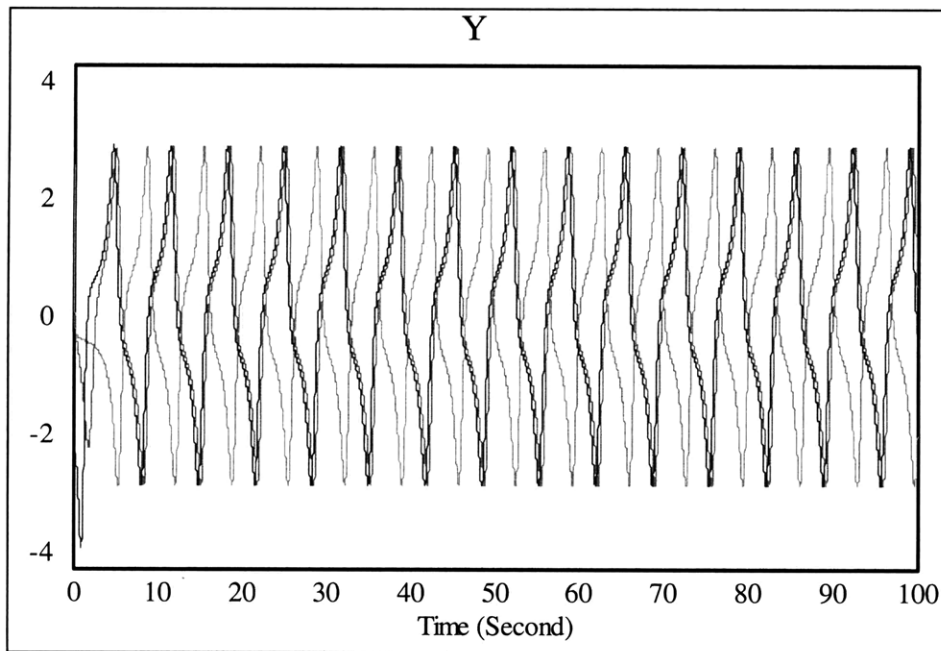


Figure 17. Time history for the state variable Y after three simulation runs of the Van der Pol Equations, each with different initial conditions.

In the context of safety control structures, limit cycle attractors may be desirable results of the structure's performance in a number of applications. With the many delays inherent to "actual" safety control structures, a stable oscillation of the system through a desirable (i.e., non-hazardous) portion of the phase space may be a more obtainable goal in certain situations than the degree of system constraint implied by an equilibrium point attractor (refer to the Tsembaga example later on in this chapter). However, one important caveat must be considered in designing safety control structures to produce attracting limit cycles: true limit cycles can only occur in systems with only two state variables and thus, in systems with more than two state variables one can only hope for behavior approximating an attracting limit cycle. As will be shown later, behavior approximating that of an attracting limit cycle is possible in systems with more than two state variables and can be used to enforce safety constraints in these systems.

Strange or "Chaotic" Attractors

Strange or "chaotic" attractors, like equilibrium point attractors and attracting limit cycles, result from the confinement of a dynamical system to a given region of its phase space despite a range of initial/disturbance conditions. However, systems that produce strange/chaotic attractors do not settle into equilibrium or stable oscillations and are highly sensitive to initial/disturbance conditions. Accordingly, the time histories of state variables in systems producing strange/chaotic attractors can vary so much when given even a minor variation in initial/disturbance conditions that observers of these systems may be unable to comprehend their dynamics and may conclude that their behavior is "random."

The most famous strange/chaotic attractor, known as the Lorenz Attractor, was developed to demonstrate the futility of long-term, deterministic weather forecasting (Lorenz 1993). Lorenz (1963) first used this attractor—which was the simplest example of a strange/chaotic attractor that he could think of—to imply that even tiny measurement errors in determining the initial conditions used for weather simulation would render the simulation results unreliable. The following equations produce the Lorenz Attractor:

[Eq. 13] $\dot{X} = \frac{dX}{dt} = \sigma(Y - X)$ where $\sigma = 10$

[Eq. 14] $\dot{Y} = \frac{dY}{dt} = rX - Y - XZ$ where $r = 28$

[Eq. 15] $\dot{Z} = \frac{dZ}{dt} = XY - bZ$ where $b = \frac{8}{3}$

An alternative (i.e., stock and flow structure) representation of these equations is provided below in Figure 18.

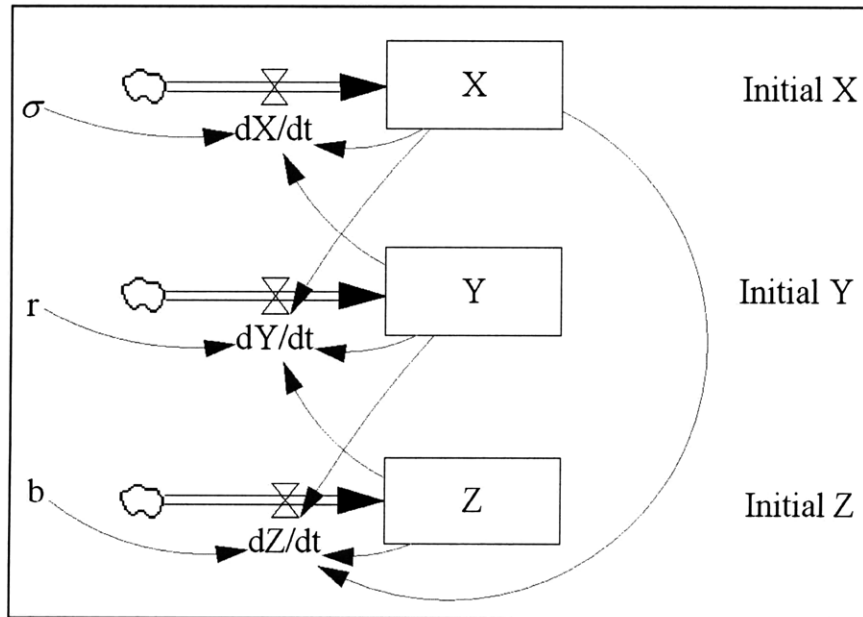


Figure 18. Stock and flow structure of the Lorenz Equations.

As can be seen in Figure 19, the time history of state variable Y is drastically affected by a relatively small variation in its initial condition⁵⁶. Over the 2,000 simulation runs shown in the figure, the range of values for Y after ten seconds is roughly fifty times the range of variation in the initial condition of Y.

⁵⁶ The time histories of state variables X and Z are affected to a similar degree by the same variation in the initial condition of state variable Y.

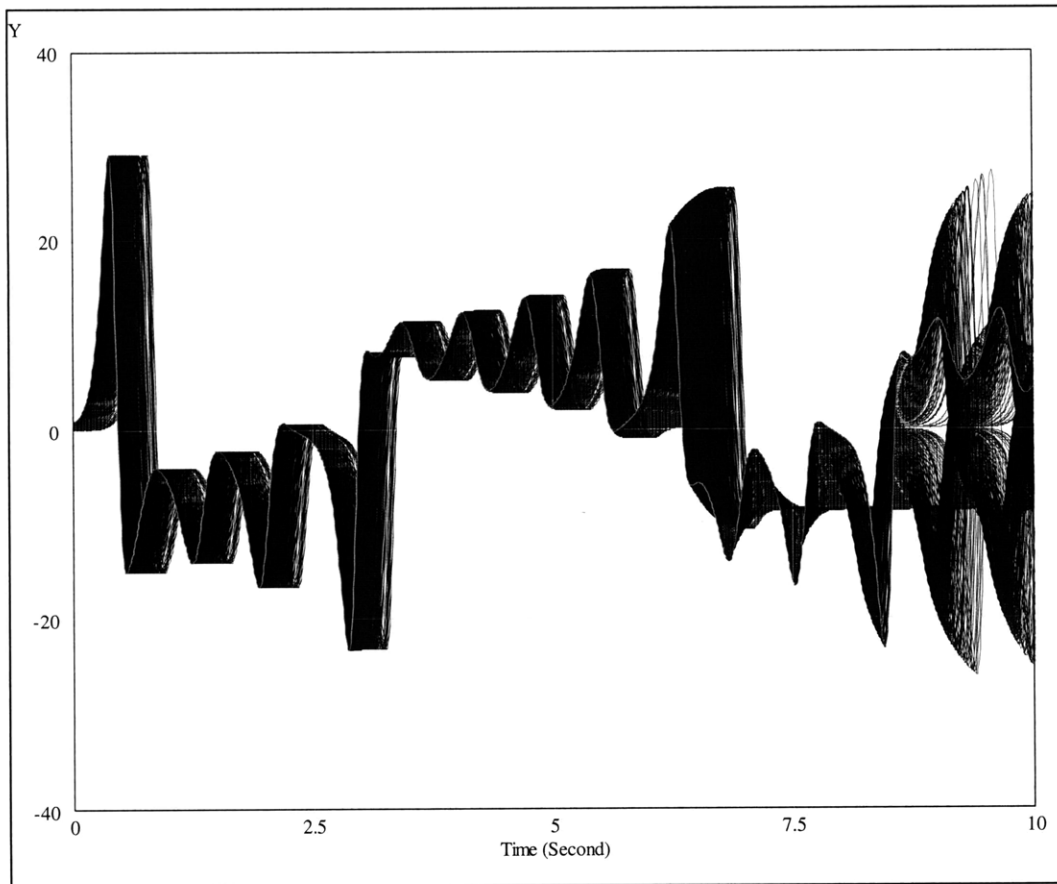


Figure 19. The time history of state variable Y after 2000 simulation runs of the Lorenz Equations in which the initial value of Y ranges between 0.01 and 1.

If one were to empirically observe this system at given points in its time history following multiple disturbances, he or she could easily (and mistakenly) infer that this system is random and that stochastic reasoning would be necessary to understand it⁵⁷. Indeed, as illustrated by the histogram in Figure 20 of Y values after 10 seconds in the simulation runs, he or she could make a claim at knowing the system's "probability density function."

⁵⁷ The author's use of the term "random" comes with a caveat: pure or complete determinism is effectively a mathematical abstraction and thus, some degree of randomness would exist in empirical observations of any system. In fact, the initial values for state variable Y in the simulation runs shown in Figure 19 were produced using a random number generator set to create a random uniform distribution of initial Y values from 0.01 to 1. However, it is clear from the time history that the deterministic dynamics of this system ultimately account for much more variation in the results than the initial random variation, and therefore labeling the system as "random" would undermine the importance of the deterministic dynamics. For a deeper discussion on what it means for a system to be random as opposed to just looking random, see the first chapter of Lorenz (1993).

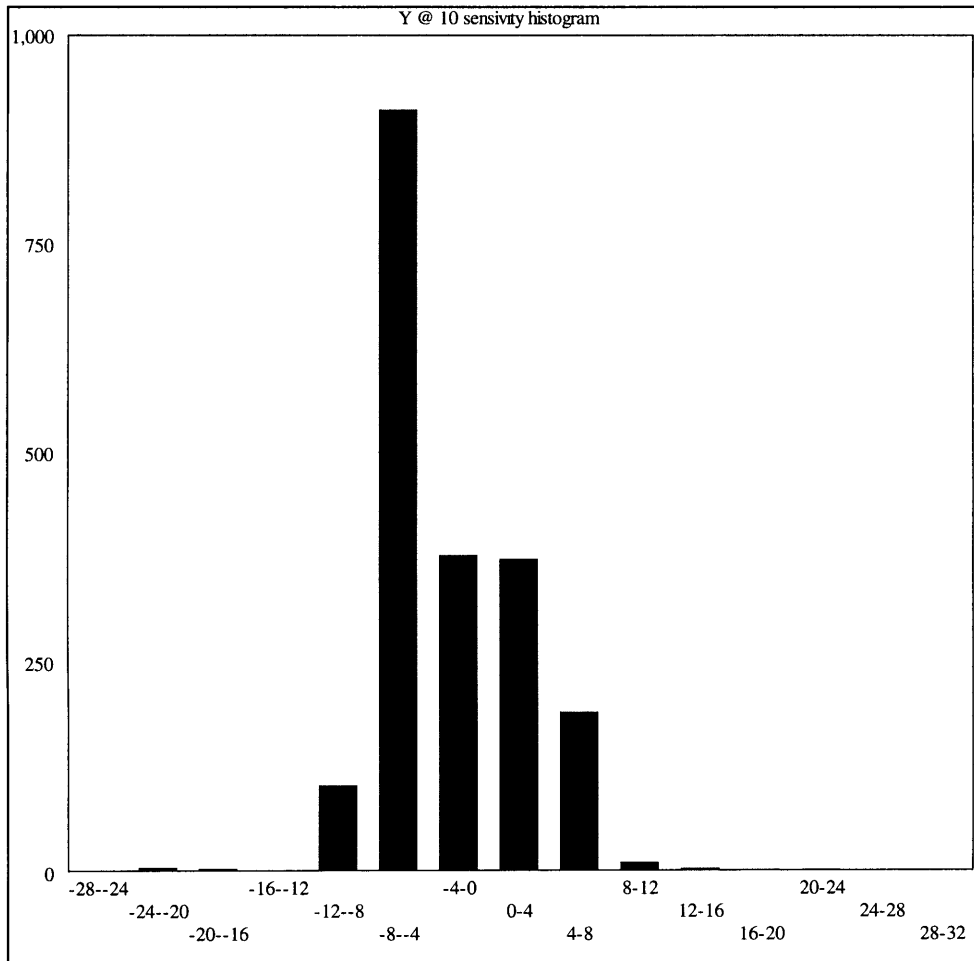


Figure 20. Histogram of values for state variable Y after 2000 simulation runs of the Lorenz Equations in which the initial value of Y ranges between 0.01 and 1.

However, a look into the phase space of the system reveals information about the system’s feedback relationships that is conveyed with more subtlety in its time history. Figure 21 contains four portraits of the X-Y phase space of the system after four runs with substantially different initial values of state variable Y. Though these four initial values produce vastly different time histories of the system, as illustrated above, their effect on the phase portraits is relatively small. Each phase portrait in Figure 21 shows the region in phase space to which the system is attracted and illustrates the “back and forth” feedback relationship between state variables X and Y. At first, state variables X and Y increasingly counteract each other; in other words, they produce a trajectory that spirals out from a given point. Then, rather than spiraling out to infinite values of X and Y, the system moves towards a point in the opposite quadrant of the XY phase space only to spiral out from that point back towards the original point. Similarly, the X-Z and Y-Z phase portraits of the system—which are not shown below in the interest of brevity—indicate that “back and forth” feedback relationships also exist between state variables X and Z and Y and Z, respectively.

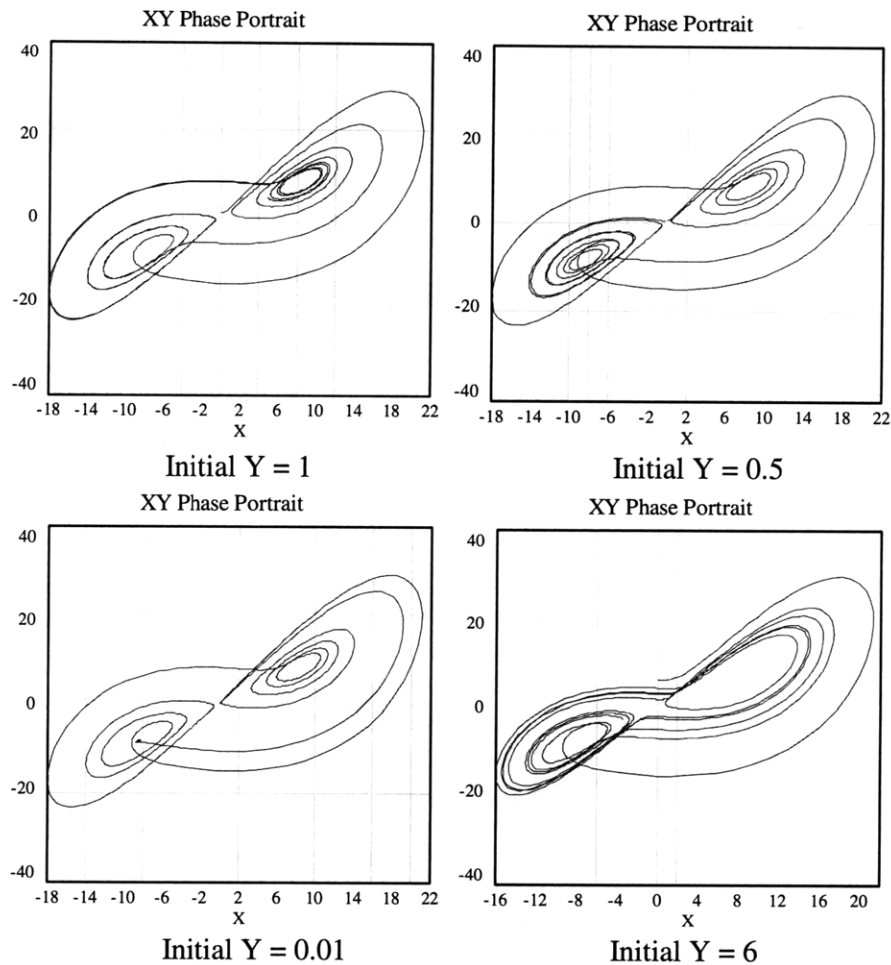


Figure 21. The phase portraits in X-Y phase space produced by the Lorenz Equations following four simulations with different initial values of state variable Y.

Overall, the phase portraits illustrate that the feedback relationships between state variables X, Y, and Z are balanced in the sense that no feedback relationship dominates the system’s dynamics. While this information may also be discernible from the system’s equations and state variable time histories, the relative ease of inferring the nature of these feedback relationships from these sources is debatable. What can be said is that the phase portraits, time histories, and the system’s equations comprise a set of analytical tools that together provide a range of perspectives on the system’s dynamic “story”.

In the context of safety control structures, strange/chaotic attractors may be desirable results of the structure’s performance in a number of applications. In fact, given the complexity and resource conflict inherent in “actual” safety control structures, the chaotic confinement of systems to desirable (i.e., non-hazardous) portions of the phase space may often be more obtainable than the degree of constraint implied by attracting limit cycles and equilibrium point attractors (though not directly related to system safety, the Genesis spacecraft trajectory example later on in this chapter illustrates this point). Moreover,

numerical studies suggest that chaotic behavior becomes more common as the number of system state variables increases (Albers et al. 2006, Dechert et al. 1999, Sprott 1993).

Attractor Bifurcations

In some systems, it is possible to bifurcate an attractor or fundamentally change its qualitative structure by varying a parameter of the system (Strogatz 1994). For example, referring back to [Eq. 9], as the parameter a is varied from -0.5 to 0.5 , it takes the system longer to converge to the equilibrium point at $X = 0, Y = 0$. However, as shown in Figure 22, once a reaches a value of 0.5 , the system no longer spirals in towards the equilibrium point. Instead, it spirals out toward infinity. In other words, the spiral-in attractor has been destroyed by the variation in the parameter a , representing one type of bifurcation to which attractors are susceptible⁵⁸.

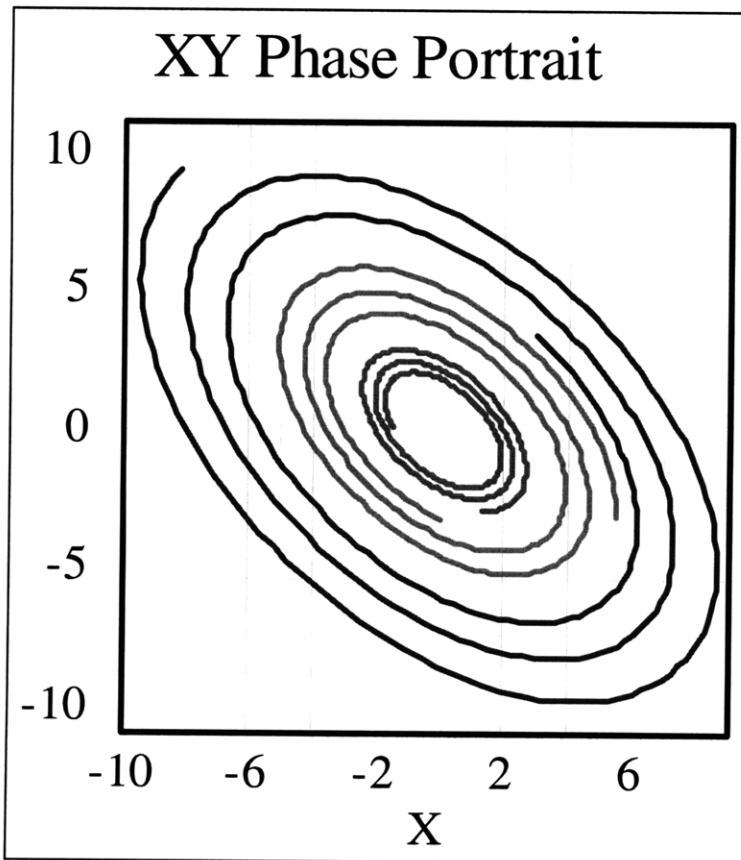


Figure 22. X-Y Phase portrait for three simulation runs of the system modeled by [Eq. 9] and [Eq. 10] with $a = 0.5$ and three different initial conditions (i.e., $X = 3, Y = 3$; $X = 0, Y = 3$; and $X = -1.5, Y = 0$).

In the context of safety control structures, attractor bifurcations are important because they represent ways in which the control structures can be weakened or strengthened. A

⁵⁸ Note that if the parameter a were varied in the opposite direction (e.g., from $a = 1$ to $a = 0.5$), a spiral-in attractor would be created.

safety control structure's responsibility is to constrain the system state in a certain manner or, in mathematical terms, to produce a phase space attractor. Because bifurcations can create, destroy, or otherwise alter phase space attractors qualitatively, they can lead to violations of safety constraints. Therefore it may be necessary to alter the system or constrain its parameter values to prevent such bifurcations. On the other hand, certain types of bifurcations can improve the manner in which safety control structures enforce a constraint, and therefore, it may be beneficial to design the system to facilitate the parameter values associated with the bifurcation.

4.3 Engineering Phase Space Attractors to Enforce Safety Constraints

Before proceeding with the analysis of the phase space attractors produced by safety control structures, the following question must be addressed:

“Why is it necessary to introduce the abstract mathematical concepts of phase spaces, attractors, and their bifurcations in order to improve our understanding of safety control structure performance?”

The purpose of a safety control structure is to prevent the system from entering hazardous states to the extent that it is possible and to ensure that if a system ends up in a hazardous state—due to some unanticipated disturbance or internal flaw in the structure—that it will return to a safe state in a manner that causes the least damage possible. This purpose is the classical control paradigm and its mathematical result, if successful, is an attractor in the phase space of the system. Additionally, a phase portrait of a system's performance provides information about the feedback relationships in the system that may not be as easy to grasp when shown in a time history of the relevant state variables. If one looks, for example, at the time history of the state variable Y in the Lorenz Attractor (see Figure 19), the conclusion that may be drawn is that the system's behavior is “random” or without a high degree of order. Alternatively, when one looks at the phase portraits of state variables X and Y under a range of initial conditions (see Figure 21), it is clear that the feedback relationships of these state variables are sufficiently balanced to constrain the system to a certain region of the phase space without allowing it to settle into an equilibrium.

Therefore, it is necessary to introduce the “abstract” mathematical concepts of phase spaces, attractors, and their bifurcations because they provide mathematical tools and descriptions for advanced analysis of safety control structures. While it may not be necessary to use such terminology in presenting the results of an analysis to system stakeholders and decision makers or even STPA novices, advanced STPA practitioners and researchers should benefit from knowledge of these concepts. In the following subsections, state-of-the-art processes and methods for prior and potential safety control structure evaluation are reviewed and comments are made regarding how the mathematical concepts of phase spaces, attractors, and their bifurcations are relevant to these processes/methods.

Safety Control Structure Modeling based on Discrete and Hybrid Dynamics

In a number of situations, the behavior of safety control structures can be described through discrete⁵⁹ or hybrid⁶⁰ dynamics. An example mathematical formulation to describe discrete system behavior (or the discrete dynamics of a hybrid system) is a state machine model, which characterizes a system's behavior through a finite number of system states and transition paths between those states. The goal when using a state machine model for hazard analysis is to determine how a system can reach a hazardous state. With this knowledge, one could then re-engineer the system to prevent such transitions.

Traditional State Machine Hazard Analysis involves forward searches from an initial state in a state machine to determine if the system can reach the unsafe states. However, the number of system states and state transition paths “explodes” as the requisite complexity is added to make state machines realistically represent the behavior of real-world systems. This explosion of state machine complexity sometimes makes effective hazard analysis computationally impossible and thus, an alternative approach was developed by Leveson before STAMP and STPA were introduced (Leveson and Stolzy 1987). This method—and variants of it, such as Neogi's (2002)—employs backward searches from hazardous states and only requires portions of the state machine to be specified (the hazardous states and the states that transition into them). This approach allows for the identification (and elimination) of transitions to hazardous system states while limiting the complexity of the state machine. However, its drawback is that some of the hazardous states may not have been reachable anyway and thus, system designers may be led to take action to prevent unrealistic state transitions.

Ultimately, when using a state machine or other discrete representations of system behavior to identify and prevent transitions to hazardous states, the objective is to strengthen the system's attraction to safe system states (i.e., the safe regions of the system's state space). In other words, while the mathematical details of system attraction to safe states differ for discrete systems and continuous systems (which are the focus of this dissertation), the fundamental objective is the same. In fact, hybrid systems may require the simultaneous use of mathematical concepts from both types of systems for proper safety constraint enforcement.

Modeling Safety Risk Management at NASA

Recently, attempts were made to quantitatively evaluate aspects of NASA's safety control structures for crewed spaceflight operations and spacecraft/launch vehicle development—the systems studied were the NASA Independent Technical Authority (ITA) (Dulac 2007, Leveson et al. 2005, Dulac et al. 2005) and the NASA Exploration Systems Mission Directorate (ESMD) (Dulac 2007, Dulac et al. 2007a, Dulac et al. 2007b, Dulac et al. 2007c). The inspiration for the quantitative approaches in these studies was from the System Dynamics field of nonlinear control theory research—

⁵⁹ Discrete dynamics—as opposed to continuous dynamics—involve system changes over time (i.e., “jumps”) between a finite set of system states rather than an infinite continuum of states.

⁶⁰ Hybrid dynamics involve both continuous and discrete dynamics. The system can transition or “jump” between a finite set of states while continuously evolving within each of those states.

discussed in the previous chapter—and the ultimate result was a STAMP-related methodology (Dulac 2007) intended to engage STAMP novices⁶¹ in dynamic safety risk management modeling.

Because the methodology is targeted towards STAMP novices, it is somewhat beside the point to comment on how the methodology itself would benefit from the addition of the concepts presented in this chapter. It is appropriate, however, to comment on the advantages that advanced STAMP practitioners and researchers would realize in applying these concepts, along with the methodology. First, there was a great deal of interest throughout both studies in the identification of “tipping points” in the safety control structure’s dynamics—see Figure 23⁶². These “tipping points” are merely bifurcations of the relevant attractors in the system and perhaps could be easier to identify with more theoretical grounding in the concept of bifurcation. Next, most (if not all) analysis of the models was scenario-based and results were drawn only from time histories of the state variables, their time derivatives, and their auxiliary variables. For simple models, such an approach can be adequate for a relatively complete and efficient analysis. However, the completed ITA and ESMD models contained more than thirty and seventy explicitly modeled state variables, respectively, and several more state variables implicitly modeled in Table Functions⁶³. With this level of model complexity, this approach to analyzing the model was cumbersome and required a good deal of modeler “intuition” in order to efficiently glean key insights into the dynamic behavior of the system. As demonstrated above and later in the case study analysis in Chapter 7, phase portrait analysis provides another perspective on the dynamic “story” of the system and is helpful in analyses involving models this complex (or more complex).

⁶¹ Dulac’s (2007, pg. 126) target audience for his methodology are described as system stakeholders, including engineers, managers, and safety analysts with acceptable training, as opposed to STAMP-specialized consultants acting as facilitators, model-builders, and analysts.

⁶² This “tipping point” involves two behavior modes—indicated by a 1 and 2 in the figure—associated with variation in the amount of work NASA contracted out. According to Dulac (2007, pp. 180-182) this result was achieved by varying the fraction of work contracted out from 4% to 96% in the ITA model.

⁶³ Table Functions are mathematical functions commonly used in System Dynamics models to describe the relationship between two variables. In a Table Function, the relationship between the two variables is described by a table of data points rather than an analytic function (Sterman 2000, Chapter 14). In using a Table Function to describe a nonlinear relationship between two variables, the modeler does not need to explicitly identify the state variables inducing the nonlinearity (he or she only needs to specify data points).

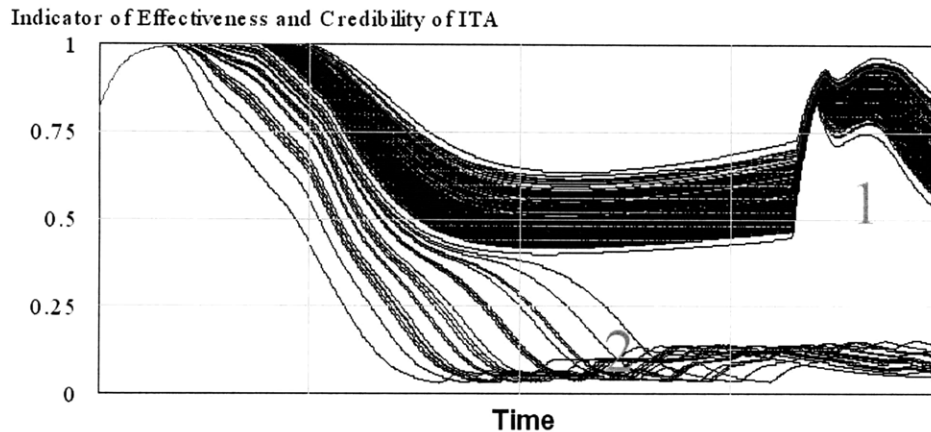


Figure 23. A “tipping point” in ITA effectiveness and credibility (Dulac 2007, Dulac et al. 2007c, Dulac et al. 2005, Leveson et al. 2005).

Bifurcation Control

One set of approaches to making safety control structures produce allowable attractors involves altering or exploiting the bifurcation properties of the attractor. *Bifurcation Control* is a relatively new subfield of nonlinear control systems research involving the design of a control system to produce desirable bifurcation characteristics for a nonlinear system (Efimov and Fradkov 2006). Until the writing of this dissertation, no one had explicitly attempted bifurcation control of the phase space attractors produced by safety control structures.

Typical objectives of bifurcation control include delaying the onset of an inherent bifurcation, stabilizing a bifurcated solution, changing the parameter value of an existing bifurcation point, modifying the shape or type of a bifurcation chain, introducing a new bifurcation at a preferable parameter value, optimizing system performance near a bifurcation point, or a combination of some of these objectives (Chen et al. 2000).

For example, one could simply bifurcate the attractor into another type of attractor. As shown in Figure 24 and Figure 25, the Lorenz Attractor bifurcates into a spiral-in equilibrium point attractor that stabilizes at a positive Y value whenever parameter σ in [Eq. 13] is decreased from 10 to 2.82 or parameter r in [Eq. 14] is decreased from 28 to 12.05, respectively. Such bifurcations would eliminate the internal chaotic behavior of the original system that occasionally attracts the system to specific regions of the phase space that could be undesirable in certain applications.

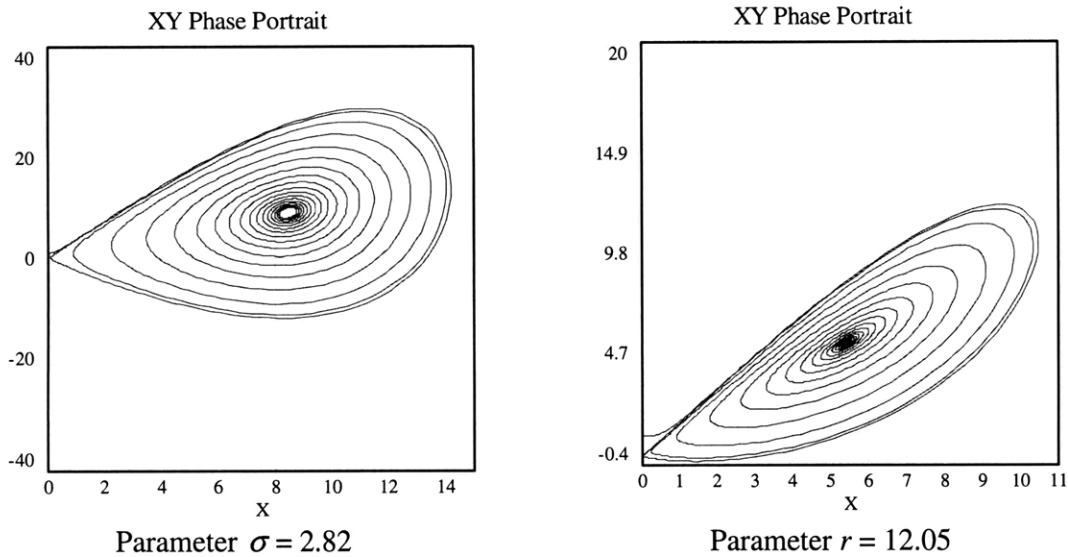


Figure 24. The X-Y phase portraits of the spiral-in equilibrium point attractors produced by bifurcating the Lorenz Attractor through varying two of its parameters.

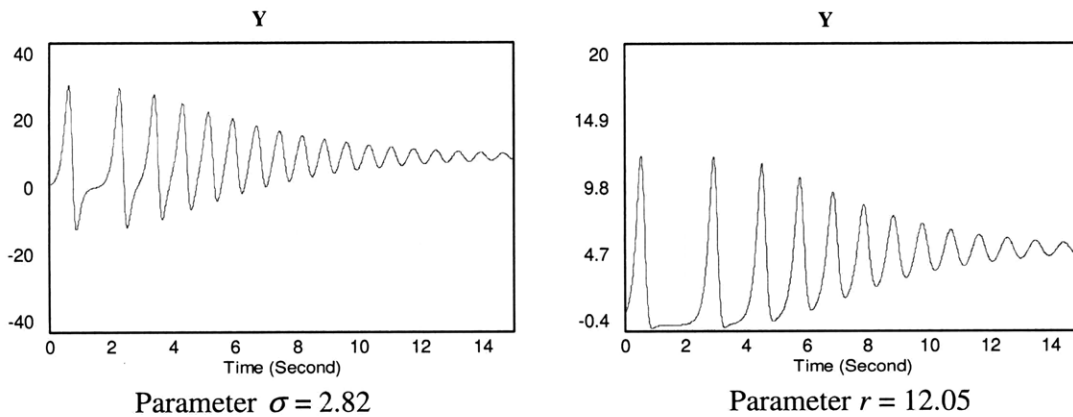


Figure 25. The state variable Y time histories of the spiral-in equilibrium point attractors produced by bifurcating the Lorenz Attractor through varying two of its parameters.

These bifurcations could be realized by constraining the parameter values of the system, if possible, or by changing the system's response to these parameters. For example, consider the alternative systems shown in [Eq. 16] through [Eq. 19] and [Eq. 20] through [Eq. 22], respectively.

$$[\text{Eq. 16}] \quad \dot{X} = \frac{dX}{dt} = \sigma(Y - X)$$

where $\sigma = 10$

$$[\text{Eq. 17}] \quad \dot{Y} = \frac{dY}{dt} = rX - Y - XZ$$

$$[\text{Eq. 18}] \quad \dot{Z} = \frac{dZ}{dt} = XY - bZ$$

$$\text{where } b = \frac{8}{3}$$

$$[\text{Eq. 19}] \quad \dot{r} = \frac{dr}{dt} = f(t) - \frac{r - (\text{Desired } r)}{\text{Time to Change } r}$$

where *Desired r* = 11.5 and *Time to Change r* = 0.05 seconds

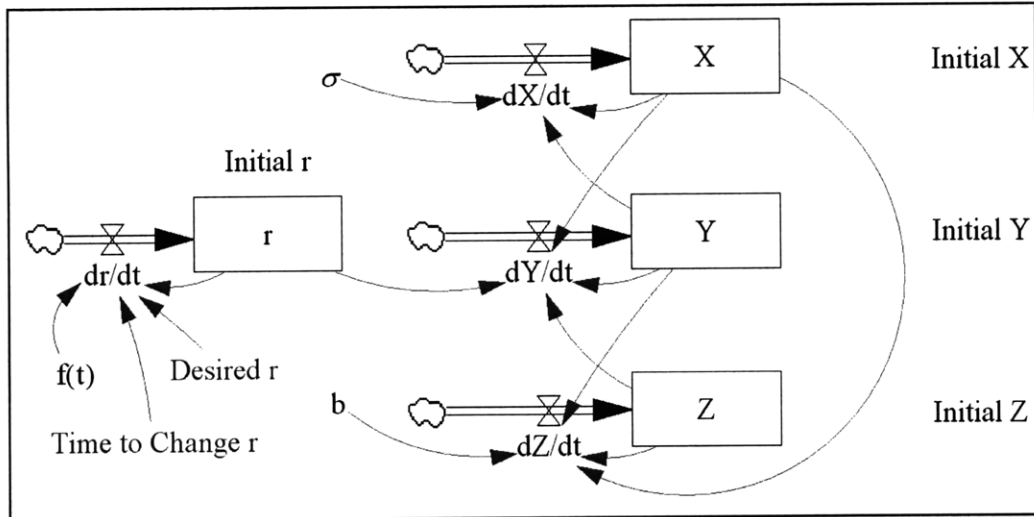


Figure 26. Stock and flow structure of the Lorenz Equations with the bifurcation control scheme described by [Eq. 19].

The bifurcation control scheme used in the system described by [Eq. 16] through [Eq. 19] and Figure 26 employs simple proportional control of the former parameter r . In this system, r is considered to be a state variable rather than a parameter, and as indicated in [Eq. 19], its time derivative is subject to a disturbance input modeled as an exogenous function of time, $f(t)$. The controller in the system (i.e., the second term in [Eq. 19]) compares the most recent value of r with a desired value of r (i.e., *Desired r*) and divides this value by a time constant (i.e., *Time to Change r*) in order to produce a change in the time derivative of r that is proportional to the difference between the desired and actual value of r . This particular scheme is capable of bifurcating the attractor to its spiral-in form despite a wide range of initial conditions for r . Additionally, it is capable of preventing the bifurcated attractor from reverting to its chaotic form in spite of a number of potential magnitudes and behavior modes of $f(t)$ (e.g., step input, sinusoidal input, pulse input, etc.).

Alternatively, one could employ a variety of other bifurcation control schemes, such as the one used in the following system:

$$[\text{Eq. 20}] \quad \dot{X} = \frac{dX}{dt} = \sigma(Y - X)$$

$$\text{where } \sigma = 10$$

$$[\text{Eq. 21}] \quad \dot{Y} = \frac{dY}{dt} = 0.43rX - Y - XZ \quad \text{where } r = 28$$

$$[\text{Eq. 22}] \quad \dot{Z} = \frac{dZ}{dt} = XY - bZ \quad \text{where } b = \frac{8}{3}$$

Note that the only difference between this system and the original Lorenz Equations is the multiplication of parameter r by a factor of 0.43 in [Eq. 21]. The factor of 0.43 effectively changes the bifurcation point of the system from $r = 12.05^+$ to $r = 28^-$, thus allowing the desired bifurcation to occur without changing the value of the parameter. Such an approach may be preferable when changing the parameter value is more difficult than changing the system's response to the parameter value⁶⁴.

Flow Control

Another set of approaches to producing an allowable attractor involves altering the rates or “flows” (i.e., the time derivatives) of the state variables of the system. This set of approaches—hereafter referred to as *flow control* in this dissertation—has a different objective than bifurcation control (i.e., to induce temporary and/or moderate alterations of the attractor rather than bifurcating it). Examples of flow control are provided in the case study of this dissertation.

Discussion of the Relative Advantages of Bifurcation Control and Flow Control

As demonstrated later in the dissertation case study, flow control can require significantly more real-time effort from the control elements to enforce the safety constraint than bifurcation control. In general, the choice between bifurcation control and flow control approaches can invoke many of the trade considerations commonly explored when determining whether or not to include system operators (whether human or automated) as part of the solution to an engineering problem. While bifurcation control schemes can provide elegant, operator-less solutions to safety constraint enforcement—if they are physically possible for the given application—they could require an upfront investment in equipment, research, and testing in order to physically implement the scheme or sufficiently reduce uncertainty over the values of the system parameters. Furthermore, bifurcation control schemes may over-constrain the system. For example, consider the vast difference between the chaotic Lorenz Attractor and the spiral-in attractor produced after bifurcation of it; if optimal system output were to result from behavior more closely approximating the chaotic form of the attractor, for example, bifurcating the system to a spiral-in attractor could be very inefficient. Flow control schemes, on the other hand, address some of these issues while introducing other potential problems⁶⁵. Ultimately,

⁶⁴ As noted earlier, Forrester (1968) claims that there are only two fundamental variable types: state variables and their time derivatives. Parameters are essentially state variables that maintain a constant value throughout the simulation timeframe of the model. In some situations, it may be practical to intentionally alter and regulate the value of a parameter within the simulation timeframe of the model. In other situations, it may not be practical to alter or regulate the value of the parameter within the simulation timeframe or even the lifespan of the universe.

⁶⁵ One set of problems introduced by flow control relates to the system's ability to consistently respond to system state changes according to the control law throughout the system's operational lifetime, especially

any given application may require either type of scheme or some combination thereof and it is therefore necessary for a system designer to understand what both types of schemes offer in his or her application.

4.4 Practical Applications of Phase Space Attractor Engineering

While the concept of engineering phase space attractors into socio-technical systems may seem abstract, it should be noted that such behavior has been common in the design of technical systems and has even been observed in “primitive” social systems. In the following two subsections, examples are provided of practical applications of phase space attractors in social and technical systems, respectively. These examples, when combined with the case study of a socio-technical system in the next two chapters, will hopefully build up the reader’s intuition in applying the abstract concepts presented in this chapter to real problems.

Example Phase Space Attractor in a “Primitive” Social System

One example of the reliance of a social system on a phase space attractor is the population control mechanism of a tribal society observed during Roy Rappaport’s (1968) classic anthropological study of the Tsembaga tribe of the New Guinea highlands. Due to the terrain that the Tsembaga tribe lived in, expansion of their agricultural land was limited and thus, they required some form of population control to prevent overcrowding and collapse of their society. What Rappaport (1968) observed was a Tsembaga ritual in which the pig-herding tribe would ceremonially slaughter a portion of their pig herd when it grew too cumbersome to maintain and simultaneously declare a short war on neighboring tribes. Shantzis and Behrens (1973) developed a simulation model of this ritual based on Rappaport’s observations and showed that the ritual created a pseudo-limit cycle⁶⁶ in the phase plane of the human and pig populations, thus preventing overcrowding over a wide range of possible initial conditions for these two state variables. Moreover, they demonstrated that suppression of the ritual in simulation runs led to overcrowding and a subsequent collapse in both the yield of Tsembaga agricultural lands and the tribe population. Additionally, years later, when Kampmann (1991) identified and fixed several technical errors in the model (e.g., strong sensitivity to the simulation time step, problems in how food was divided among the tribesmen and pigs, the possibility for the pig slaughtering value to be negative, etc.) the pseudo-limit cycle persisted, indicating the robustness of it not only to initial/disturbance conditions, but also to subtleties in model structure.

The phase portrait of the human and pig populations provided in Figure 27 is derived from a simulation run of 500 years using Kampmann’s (1991) version of the Tsembaga model. Initially, the human and pig populations are 196 people and 40 pigs, respectively. Throughout the simulation, the system moves towards the left of the phase portrait until it

when human operators are involved in the response. Another set of problems relates to the compressed time frame associated with altering system state during real-time operations.

⁶⁶ Recall that a limit cycle can only exist in a two-dimensional system and thus, systems with more than two dimensions, like the Tsembaga system as modeled by Shantzis and Behrens (1973), can only approximate the behavior of limit cycles.

reaches a nearly closed orbit that it cycles along throughout the remaining duration of the simulation. If the initial human population is held constant while the pig population is varied from values of 7 pigs to 90 pigs in separate simulations, this behavior of leftward drift to the pseudo-limit cycle persists (a rightward drift to the pseudo-limit cycle ensues when the initial pig population is varied from 90 pigs to 2320 pigs). Similarly, a leftward drift to the pseudo-limit cycle persists if the pig population is held constant and human population is varied from 182 people to 462 people (a rightward drift to the pseudo-limit cycle occurs when human population is varied from 7 people to 182 people).

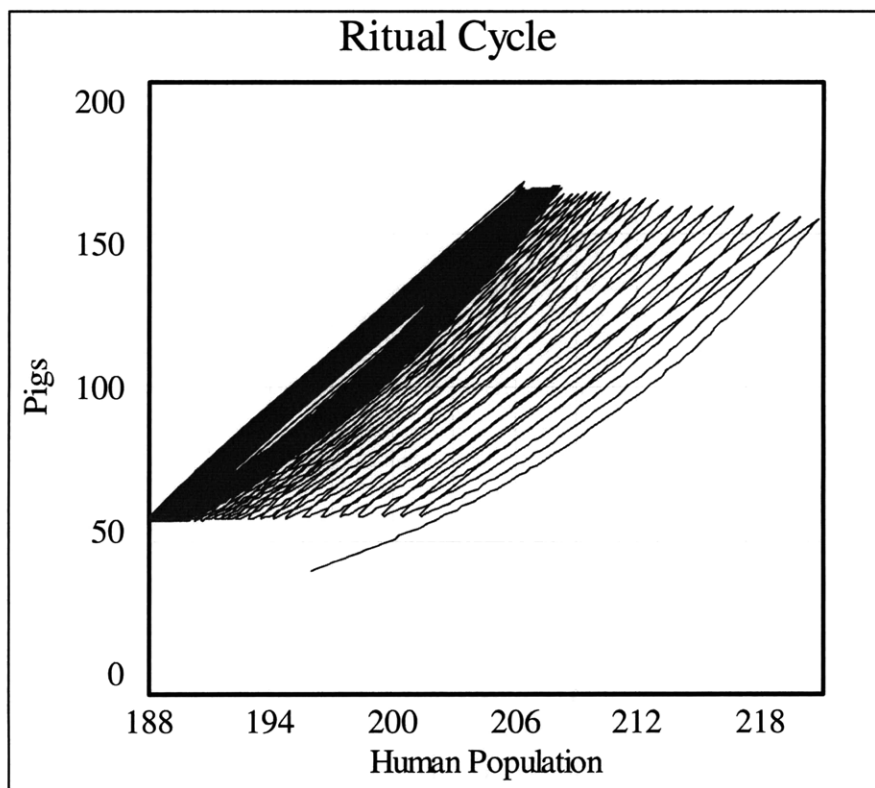


Figure 27. The phase portrait of the Tsembaga human and pig populations (derived from Kampmann 1991).

The ability of the Tsembaga to serendipitously construct a set of customs that produces a pseudo-limit cycle and the persistence of this attractor in spite of wide variation in initial/disturbance conditions and some aspects of the model structure speaks to the practicality and power of creating phase space attractors to mitigate the effects of uncertainty. Furthermore, analysis of this attractor using the conceptual tools presented in this chapter speaks to the potential applicability of these tools in real-life situations. Identifying bifurcations of the attractor, for example, provides clues on the control flaws that can develop in this safety control structure for the tribe population. The Tsembaga essentially used the pig population as a leading indicator of impending problems for their population: when the pig population was deemed to be too large, the humans took steps to reduce their own population and the pig population. This feedback relationship leads to some sort of attractor in the Human Population-Pig Population phase space. If the

human and pig food needs are balanced with the agricultural capacity of the land, the resulting attractor is a pseudo-limit cycle, otherwise, the pseudo-limit cycle is bifurcated or “broken.” As shown in Figure 28 below, allowing the pig population to grow larger before initiating the ritual⁶⁷ causes the attractor to bifurcate within a 500 year time span from a pseudo-limit cycle to an equilibrium corresponding to a significantly reduced human population. Such a situation would represent a control flaw in the safety control structure and thus, an additional safety constraint could be placed on the pig population threshold before initiating the ritual or on other food consumption parameters⁶⁸.

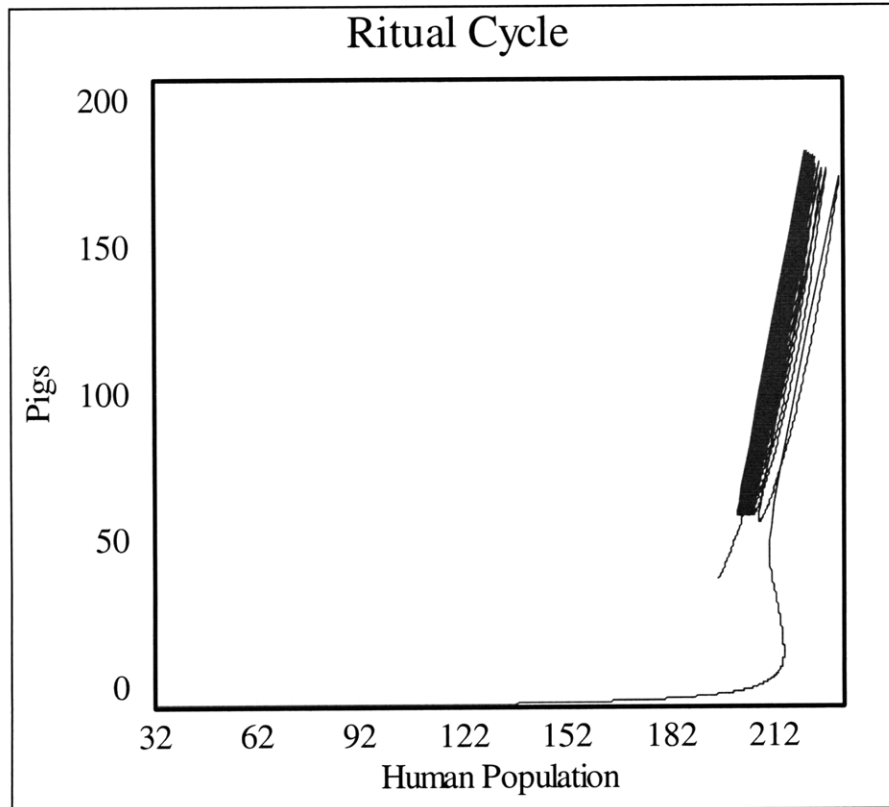


Figure 28. The phase portrait of Tsembaga human and pig populations when a slightly larger pig population is allowed (derived from Kampmann 1991).

Alternatively, one could look to flow control techniques to develop a safety control structure that avoids the concept of a ritualized war, which is a practice considered to be unacceptable in most modern societies. As discovered by Shantzis and Behrens (1973), improving the human mortality rate of the Tsembaga or simply eliminating war from the ritual produces a disastrous bifurcation of the attractor in the Human Population-Pig Population phase space. However, as shown in Figure 29, an attracting limit cycle can be

⁶⁷ In other words, increasing the *Critical Rate of Pig Incidents* parameter in Kampmann’s (1991) model from 6 incidents per year to 6.8 incidents per year.

⁶⁸ Reducing the *Desired Food Per Capita* parameter in Kampmann’s (1991) model from 742,000 calories per person per year to 692,875 calories per person per year, for example, preserves the pseudo-limit cycle even when the *Critical Rate of Pig Incidents* parameter is 6.8 incidents per year.

created by improving human mortality rate in the manner suggested by Shantzis and Behrens (1973) and restructuring the ritual so that the wars are eliminated and births are prohibited every other time period between festivals⁶⁹.

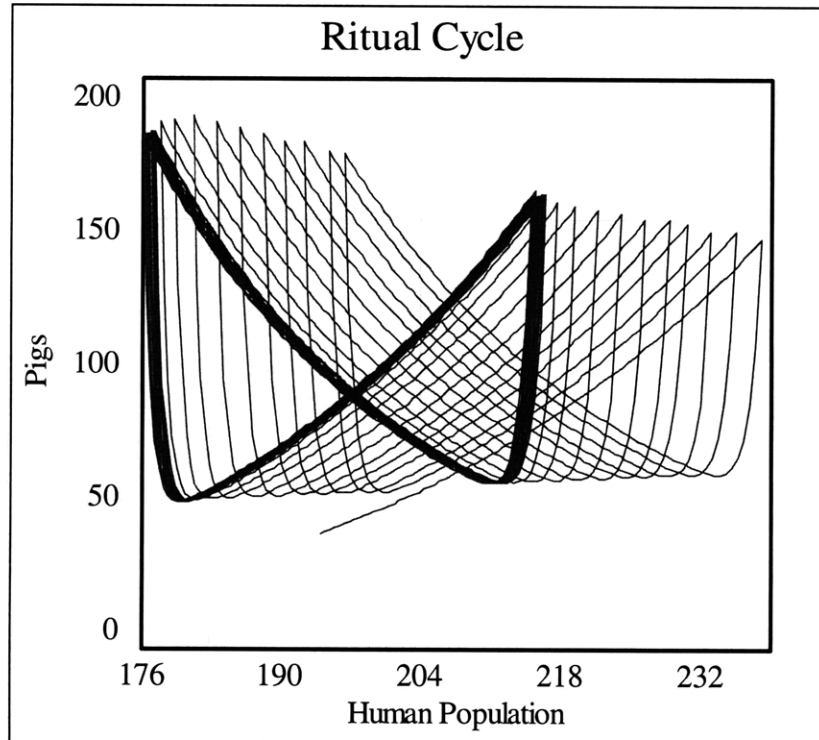


Figure 29. The phase portrait of Tsembaga human and pig populations under an alternative ritual cycle (derived from Kampmann 1991).

Example Phase Space Attractors in Technical Systems

Phase space attractors are developed in a number of technical applications, but perhaps no application of this concept is more transparent than the use of phase space attractors in spacecraft trajectory design. Instead of exploiting attractors in abstract conceptions of phase space⁷⁰, spacecraft trajectory design makes use of the attracting force of gravity to effectively maneuver an engineered object through an intuitive conception of phase space (i.e., physical space). A simple orbit around a single gravitational body is a trajectory that uses the gravitational force of the body in the form of an extremely slow spiral-in attractor. The slow spiral-in time allows the spacecraft, once inserted into the orbit, to

⁶⁹ To implement this flow control scheme, the mortality rate (i.e., the *Net Human Births* rate in the model) is improved as suggested in Kampmann's (1991) better health scenario and wars are eliminated using the *Fraction of Humans Transferred to War* parameter. Additionally, births were suppressed every other time period between festivals (roughly 10 years at a time) by setting *Net Human Births* to 0 humans per year during the birth prohibition years and introducing a death rate during those years consistent with an average life expectancy of 50 years (that number is based on the WHO 2000 life expectancy estimate of 53 years for the entire population of Papua New Guinea). It is important to note that this particular flow control scheme is a simplified demonstration of concept that has not been optimized against all parameters of the festival structure, agricultural practice, and other social considerations.

⁷⁰ For example, the human population-pig population phase space of the previous subsection.

remain at some altitude above the gravitational body while continually circumnavigating it for some time with minimal or no additional expense of fuel. Similarly, the more complicated trajectories that include gravity assists, free returns, halo orbits around libration points, and so forth make use of chaotic attractors created by the gravitational force of multiple bodies. For example, the trajectory for the Genesis solar wind sample return mission, shown in Figure 30, was designed to exploit a chaotic attractor formed by the gravitational forces of the Sun, Earth, and Moon in order to reduce fuel consumption enough to make the mission feasible (Koon et al. 2008, Stark and Hardy 2003, Lo et al. 1998, Howell et al. 1997).

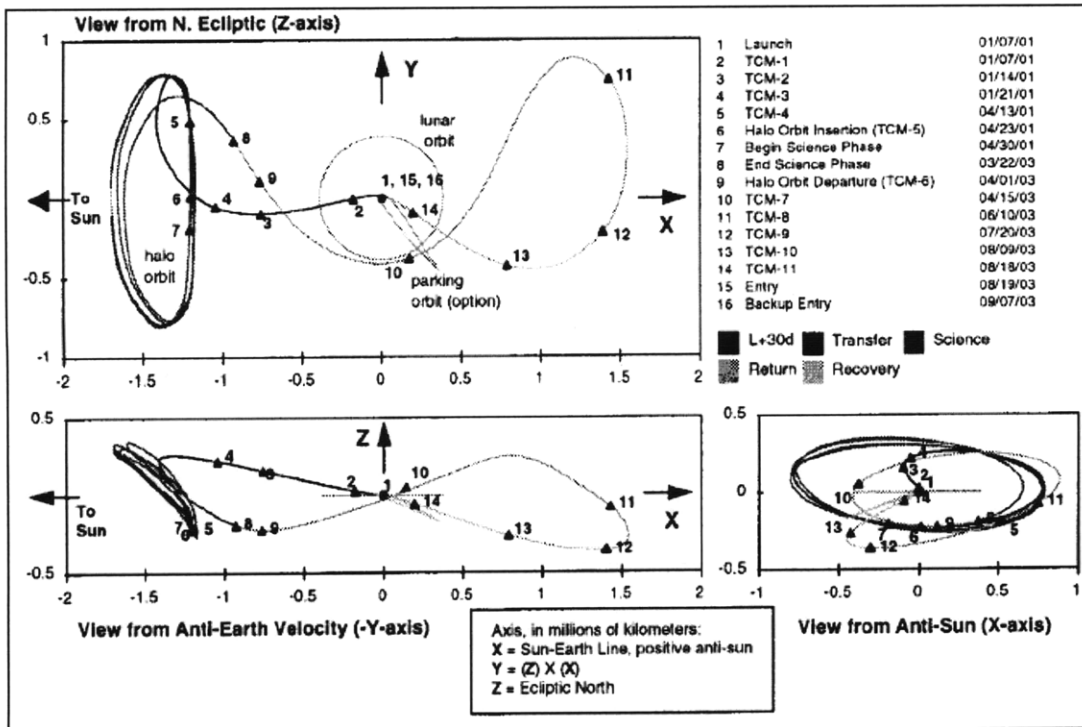


Figure 30. Phase portraits of the Genesis spacecraft trajectory (Lo et al. 1998).

4.5 Phase Space Attractors and Safety-Driven Design

In this section, attention is shifted toward the question of how the concepts in this chapter can be used as part of an overall safety-driven design effort. The author discusses how these concepts complement the many STPA-related processes and methodologies that have been published to date and previews the case study of the Procedure Rework Process in Space Shuttle Mission Control.

Qualitative system safety constraint enforcement evaluation in previously published STPA methodologies/processes and the need for quantitative evaluation

Since the introduction of STAMP and STPA, a number of processes and methodologies for utilizing STAMP and STPA as part of a safety-driven systems engineering effort have been published (Stringfellow 2008, Stringfellow et al. 2008, Owens et al. 2008, Weiss et al. 2006, Dulac and Leveson 2004, Leveson 2003). While each of these published

processes/methodologies reflect the evolution of STPA and the synthesis of it with other systems engineering techniques in safety-driven design, many fundamental elements of STPA have appeared in all of these processes/methodologies. One element of STPA that has been essential from the introduction of STPA (Leveson 2003) to the most recently proposed process/methodology (Stringfellow 2008) is the evaluation of the safety control structure’s ability to enforce the safety constraints that are defined. Figure 31 through Figure 33 contain the key qualitative elements necessary for an evaluation of the safety control structure’s ability to enforce safety constraints. The potential types of inadequate control actions that can be taken by the safety control structure—originally defined by Leveson (2003) and since updated—are listed in Figure 31. These inadequate control actions can result from problems with one or more of the elements or environment of the feedback control loops in the structure, a generic example of which is shown in Figure 32. These potential problems—defined in Figure 33 as control flaws and inadequate control executions—are identified throughout the safety control structure evaluation portion of each process/methodology and accordingly, new safety constraints are defined that, if necessary, lead to redesign or expansion of the safety control structure.

1. A required control action is not provided or is inadequately executed.
2. An incorrect or unsafe action is provided.
3. A potentially correct or adequate control action is provided too late or at the wrong time.
4. A correct control action is stopped too soon or continued too long.

Figure 31. Leveson’s taxonomy for inadequate control actions (Leveson 2009, Stringfellow 2008, Stringfellow et al. 2008, Owens et al. 2008).

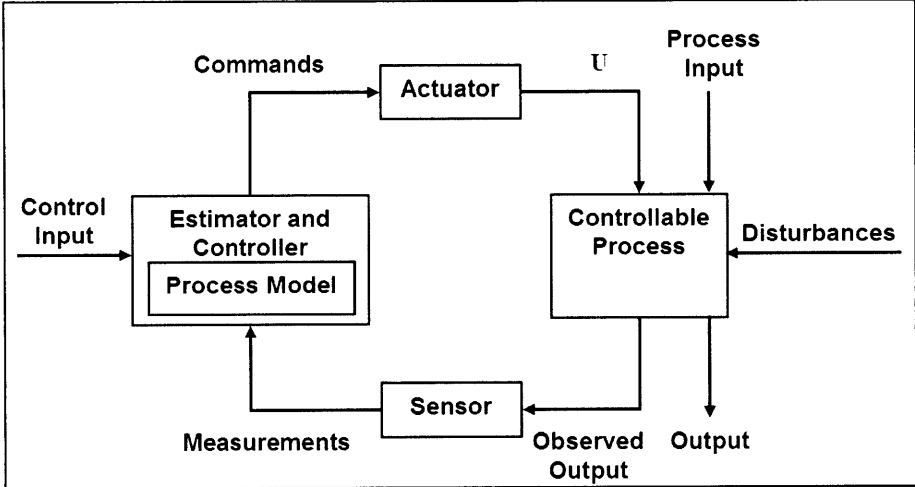


Figure 32. Generic STPA low-level process control loop (Owens et al. 2008).

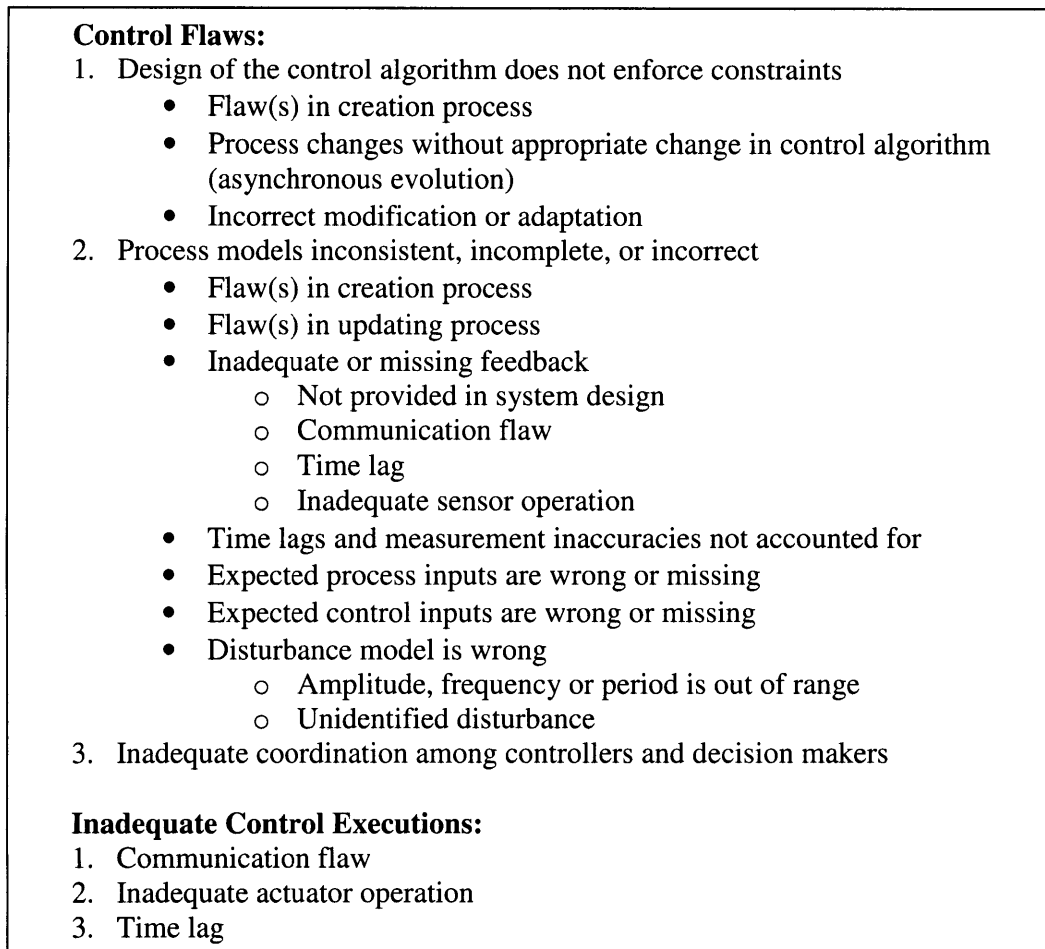


Figure 33. Leveson’s taxonomy of control flaws and inadequate control executions (Leveson 2009, Stringfellow 2008, Owens et al. 2008).

While many potential control flaws and inadequate control executions can be identified through qualitative analysis, there eventually comes a point in which quantitative analysis (e.g., numerical simulation) and experimentation/testing is needed to further identify the potential control flaws, especially those control flaws relating to problems with the control algorithms and process models. Consider the following statement by Forrester (1971):

“Inability of the human mind to use its own mental models becomes clear when a computer model is constructed to reproduce the assumptions contained in a person’s mental model. The computer model is refined until it fully agrees with the perceptions of a particular person or group. Then, usually, the system that has been described does not act the way the people anticipated. There are internal contradictions in mental models between assumed structure and assumed future consequences.”

This statement provides an argument for numerical simulation of safety control structure behavior to partially verify the consistency of assumptions about the control structure behavior. Any inconsistencies found in the simulation process are potential control flaws that could potentially necessitate additional safety constraints and redesign/expansion of the safety control structure.

Preview of the dissertation case study

In the case study of this dissertation, a process was created for using the concepts in this chapter to evaluate safety control structures. This process is proposed in Chapter 7 for more general use. It is meant to assist the STPA analyst in evaluating and potentially re-engineering the continuous dynamics of safety control structures. This process is intended to be self-contained enough to increase the depth of the STPA involved in safety-driven design efforts. In this regard, the process can thus be considered as a “sub-process” of any of the currently existing (or yet to be specified) STPA-related safety-driven systems engineering processes/methodologies. Furthermore, the process is intended to be useful, with little modification, in efforts to treat the attainment and preservation of other system-level properties (e.g., security) as a control problem.

While the process is meant to be complementary to Dulac’s (2007) methodology for the development of risk management models of a safety control structure, it differs from it in several important ways. Dulac’s methodology—developed during cases studies involving the NASA ITA (Leveson et al. 2005, Dulac et al. 2005) and NASA exploration system development (Dulac et al. 2007a, Dulac et al. 2007b, Dulac et al. 2007c)—is meant to engage STAMP novices in dynamic safety risk management modeling by centering the modeling effort on a repository of generic, customizable dynamic models of safety control structure components. The process proposed in this dissertation, on the other hand, is meant to guide the work of advanced STPA practitioners on less generalizable problems or those problems in which a necessary generic model has yet to be created for the repository available to practitioners of Dulac’s methodology⁷¹. Furthermore, the process proposed in this dissertation introduces model analysis tools from dynamical systems theory to complement the primarily scenario-based analysis tools proposed by Dulac (2007, Ch. 5).

The process laid out in this dissertation for analyzing phase space attractors produced by safety control structures is a modeling and design process meant to occur within the overall context of a safety-driven design effort. The process is derived from a type of reasoning that rejects the notion of random component failures, random initiating events, and the linear superposition of the component contributions to risk as the central concepts in safety risk management. Instead, nonlinear component interactions are accounted for by conducting analyses throughout the process on the system-level of abstraction. Though there is uncertainty in the system’s inputs and some aspects of its internal (i.e., endogenous) dynamics—and the system’s behavior might therefore “appear” random—the system is tuned throughout the process to be attracted to safe system states.

⁷¹ Needless to say, the output of the process proposed in this dissertation can further populate the repository of generic models available to practitioners of Dulac’s methodology.

The process is meant to be used in situations in which useful insights into the safety control structure's behavior can be gained through modeling this behavior with primarily continuous dynamics. With that said, it is important to note that such situations exist in the design of complex, socio-technical systems more often than one might presume. In the next two chapters, the process is used to evaluate an existing attractor (i.e., the Space Shuttle Mission Control "Procedure Rework Attractor") in a system that involves individuals altering discrete artifacts relating to highly unique missions. Intuition might suggest that such a system is not compatible with the assumptions of continuous dynamics; however, the process is nonetheless used to derive useful insights into the behavior of the system. Overall, the analysis: 1) demonstrates the use of the process in an actual complex, socio-technical system, 2) identifies potential improvements for current and future Mission Control procedure rework processes, and 3) provides an example that other systems can learn from in order to develop safe procedure rework processes.

Chapter 5: Case Study Background – Space Shuttle Mission Control

“I don’t care what anything was designed to do; I care about what it can do!” – Former NASA Flight Director Eugene Kranz as portrayed by Ed Harris in the 1995 film, *Apollo 13*.

“Based on past experience, it is probably safe to assume that the next five years will not necessarily turn out exactly as we foresee it today, and flexibility will be required to overcome future challenges.” –John J. Uri (2005) discussing the first five years of NASA research on ISS.

“As evidenced by all previous spacecraft programs, design and operations personnel will learn a great deal about the spacecraft during flight.” –Alan R. Crocker (2005).

“[MIT IL engineer Hugh Blair Smith] allows that the Apollo 11 program alarms could be called a software problem, but only if one realizes that ‘the crew procedures are part of the software, as are the ground procedures.’...These [procedures] governing people’s behavior were as important as the programs controlling the computer, and similarly embodied assumptions and links between organizations (recall that Apollo overall was called a program). In the human-machine system of Apollo, it often was not possible to distinguish between instructions for machines and instructions for people.” –David A. Mindell (2008).

5.1 Chapter Overview

Background information for the Space Shuttle Mission Control Procedure Rework Case Study is presented in this chapter. First, a historical overview of Mission Control throughout the various U.S. human spaceflight programs is provided. Flight Controller responsibilities, facilities, staffing, and training are then detailed with an emphasis on how they enhance flight controller capability for original thought and problem solving in real-time operations. Next, the Procedure Rework Process is described to prepare the reader for the formal analysis of it presented in the next chapter. Finally, the research literature pertaining to Mission Control is reviewed in order to highlight the gaps in knowledge that could potentially be filled through application of a process for safety control structure evaluation using the notion of phase space attractors.

5.2 Overview of Mission Control throughout NASA’s Human Spaceflight Programs

Since 1961, every organization that has sent humans into space has relied on the same basic formula for mission success during spaceflight operations. This formula has been to put individuals whose training emphasizes breadth rather than depth in human

spaceflight topics—except in the area of vehicle piloting—into the spacecraft and link them through radio frequency communications to a team of engineers on the ground, each highly trained in a specific area of spaceflight. In NASA, the most visible portion of this engineering team is called *Mission Control*. The people that work in Mission Control are referred to as *flight controllers* and their responsibilities include monitoring of crew, payload, and spacecraft health and status; spacecraft commanding; management of spacecraft consumables and supplies; crew activity planning; development and upkeep of spaceflight procedures, operational requirements, and flight controller reference material; and participation in crew training. The work environment of flight controllers during missions and highly realistic practice for missions—referred to as immersive or integrated simulation—are control rooms and support rooms equipped with workstations capable of customizable data display, processing, and transmission, connected to each other through a digital voice communications network referred to as the “voice loops.” Generic training for flight controllers involves several years of study and immersive simulation in control rooms, support rooms, and other facilities for the areas of specialization they practice, culminating in a series of trials that must be passed before they accept the responsibilities of their specialization.

In this section, the *Mission Control function* is organizationally scoped and a brief description of its evolution throughout NASA’s human spaceflight programs is given.

The Organizational Boundaries of Mission Control

Throughout the remainder of this dissertation, the term *Mission Control* will be used to refer to a specific organizational division of NASA. This organization is currently based at the Johnson Space Center (JSC) in Houston, Texas and is involved directly in the control of NASA human spaceflight missions. Teams involved in the control of unmanned spacecraft at the Goddard Space Flight Center, JPL, and other U.S. mission operations centers (e.g., the GP-B control center at Stanford University), are not included in this group. Furthermore, flight control teams of NASA’s international partners in human spaceflight and remote payload operations centers for human spaceflight, such as the Payload Operations Center (POC) at the Marshall Space Flight Center, are excluded in the usage of this term.

Even though many flight controllers have engineering backgrounds, are paid on engineering pay-scales, and generally consider themselves to be engineers, they are hierarchically organized separately from what is officially referred to as the “engineering” community or Engineering Directorate at JSC. Officially, the flight controllers belong to the “operations” community or Mission Operations Directorate (MOD) at JSC and the engineers who manage the development, maintenance, and evolution of flight hardware and software belong to the engineering community (Watts et al. 1996). The Mission Evaluation Room (MER) is located in the same building that houses the Flight Control Rooms (FCRs, pronounced “fickers”) and Multi-Purpose Support Rooms (MPSRs, pronounced “mip-sirs”) in which the flight controllers work. The MER is a facility for employees in the engineering community at JSC to access telemetry at workstations similar to those used by the flight controllers and keep apprised of the events that occur during a mission. Due to their detailed knowledge of the flight

hardware and software, MER engineers often contribute to flight control processes by performing analyses and hardware/software tests at the request of flight controllers and by providing an independent assessment of the analyses done by the flight controllers. In order to keep interactions between MER engineers and flight controllers from congesting the voice loops, most of the communication is done through formal MER memos or the Spacecraft Analysis Room (SPAN), which is a room staffed by individuals that mainly perform coordination functions between the various entities involved in spaceflight operations (Rusnak 2002).

Additionally, Mission Control flight controllers do not lead the launch preparations and final launch countdown at the launch site. Those functions are led by the Launch Control Center (LCC) at the Kennedy Space Center (KSC). Mission Control is said to assume the lead in spacecraft operations from the time that the launch vehicle clears the launch tower to the time that the spacecraft “splashes down” (in the case of capsule spacecraft) or rolls to a stop (in the case of the space shuttle).

Finally, while the MER, SPAN, POC, and LCC are on the horizontally adjacent boundaries of Mission Control in the overall organizational hierarchy, the Mission Management Team (MMT) resides above its vertical boundary as shown in Figure 34. The MMT is a decision-making body consisting of senior NASA management presiding over flight certification, launch preparation, and in-flight activities for any given mission.

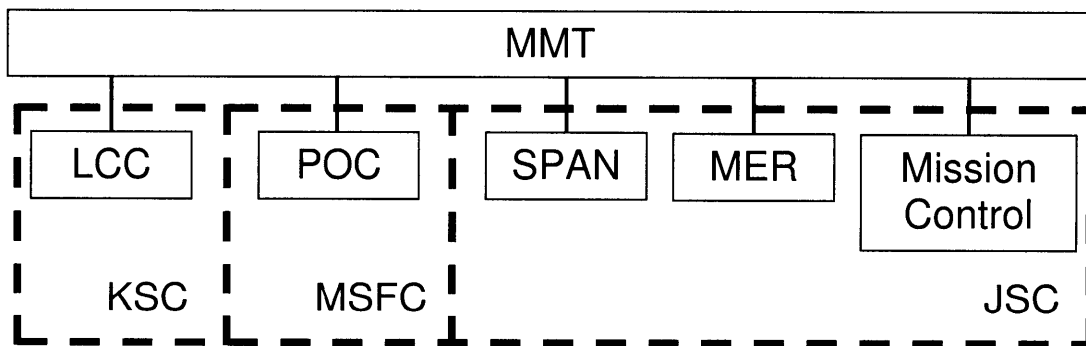


Figure 34. The organizational boundaries of Mission Control and the organizational groups at NASA with which it primarily interfaces during a mission.

Mission Control during Project Mercury

NASA’s first human spaceflight program, Project Mercury, included six crewed missions between May 1961 and May 1963, each with a single astronaut (for a historical account of the program from the perspectives of two leading flight controllers, see Kraft 2001 and Kranz 2000). These spaceflights were primarily controlled out of a facility, shown in Figure 35, at the NASA center now referred to as KSC in Florida. However, because NASA relied on ground stations during this era rather than communications satellites for communications with the controlled spacecraft, flight controllers were stationed at remote ground stations around the world.



Figure 35. The primary flight control room used for Project Mercury and the initial flights of Project Gemini (source: <http://spaceflight.nasa.gov/>).

Mission Control during Project Gemini

The follow-up program to Project Mercury, referred to as Project Gemini, consisted of ten human spaceflights between March 1965 and November 1966, each with a pair of astronauts (see Kraft 2001 and Kranz 2000 for historical accounts of this program from the perspective of leading flight controllers). For this program, starting with the second crewed flight (Gemini IV), the majority of the Mission Control function—the work done at remote ground stations excluded—was moved to Building 30 of the NASA center now referred to as JSC in Houston, Texas. The leading flight controllers for any given mission controlled the flights from one of two Mission Operations Control Rooms (MOCRs, pronounced “moe-kers”), such as the one shown in Figure 36, while a staff of supporting flight controllers assisted them from what are now called MPSRs.



Figure 36. One of the MOCRs used during Gemini, Apollo, and early Space Shuttle missions (source: <http://spaceflight.nasa.gov/>).

Mission Control during Project Apollo

The purpose of Project Gemini was to develop key engineering and operational skills and knowledge for Project Apollo, the first—and so far only—program to land humans on the

moon. Project Apollo consisted of sixteen crewed missions between January 1967 and July 1975, each with a three-astronaut crew. Overall, six of these missions successfully landed on the moon, one safely aborted a moon landing, eight⁷² successfully completed mission objectives in earth and/or lunar orbit, and one ended with a fatal launch pad fire (see Liebergot and Harland 2006⁷³, Kraft 2001, and Kranz 2000 for historical accounts of the program from the perspectives of flight controllers). As was the case for Project Gemini, the majority of the Mission Control function—the work done at remote ground stations excluded—was conducted in the MPSRs and two MOCRs at JSC.

Mission Control during the early Space Shuttle/Pre-ISS Era

NASA's next human spaceflight program, the Space Shuttle Program, began with crewed, atmospheric approach and landing tests of a Space Shuttle orbiter in 1977 and four crewed orbital test flights in 1981 and 1982. The Mission Control function for these missions and the next 66 Shuttle missions⁷⁴ was conducted in the two Gemini/Apollo Era MOCRs. However, unlike Apollo and Gemini, the importance of remote ground stations was gradually reduced by the launching of communications satellites during several of these missions. Additionally, the workstations in the MOCRs and MPSRs were upgraded several times (Kearney 1987) before the Mission Control function was moved into a modern FCR built in Building 30 at JSC—see Figure 37.



Figure 37. The current FCR for Space Shuttle Mission Control (source: <http://spaceflight.nasa.gov>).

⁷² These missions included the Apollo 7 and Apollo 9 “shakedown” of Apollo spacecraft hardware and software in earth orbit, the Apollo 8 and Apollo 10 lunar orbit flights, three missions to the Skylab space station, and one mission to rendezvous with a crewed, Soviet spacecraft.

⁷³ Liebergot and Harland (2006) even include a CD-ROM with voice loop audio files from Apollo missions.

⁷⁴ STS-70 in July, 1995 was the first mission in which the modern Space Shuttle FCR was used for the Mission Control function. The transition from the MOCR to the FCR occurred during the mission.

Mission Control during the Space Shuttle/ISS Era

The current Space Shuttle/ISS Era effectively began during the ten Space Shuttle missions to the Russian space station Mir from 1995 to 1998. It was during these missions that the coordination of the Space Shuttle Mission Control function with international operational entities became routine⁷⁵. Once ISS on-orbit construction began in 1998, a separate Mission Control team developed for the ISS Mission Control function. This team and its function grew in size and complexity as the space station progressed through its assembly. Accordingly, the ISS Mission Control function ultimately moved through several small, temporary FCRs and MPSRs in Building 30 before eventually settling into a refurbished Gemini/Apollo/Early Shuttle Era MOCR⁷⁶—see Figure 38. Additionally, the POC opened at the Marshall Space Flight Center in Huntsville, Alabama to coordinate science operations with ISS Mission Control.



Figure 38. The current FCR for ISS Mission Control (source: http://www.nasa.gov/mission_pages/station/multimedia/ISS_FCR.html).

Notable Accomplishments of Mission Control

Along with the engineers in the MER, flight controllers have assisted astronaut crews in executing tasks, rejecting system disturbances, and adapting to unforeseen situations on numerous occasions. The following list is a small sample of these accomplishments provided to help the reader appreciate the level of original thought and problem solving required to perform the Mission Control function:

⁷⁵ For ISS operations, Mission Control currently coordinates with the Columbus Control Center in Oberpfaffenhofen, Germany; the Automated Transfer Vehicle Control Center in Toulouse, France; the Japanese Experiment Module and H-II Transfer Vehicle Control Center in Tsukuba, Japan; and the Russian Federal Space Agency Mission Control Center in Korolyov, Russia.

⁷⁶ The other Gemini/Apollo/Early Shuttle Era MOCR has been restored to its Apollo configuration and designated as a Registered Historic Place by the U.S. Government.

- During Apollo 13, an oxygen tank that was damaged during ground testing exploded and crippled the Command and Service Module (CSM) that the crew needed to perform almost all critical tasks. As a result, Mission Control and the MER had to make the critically depleted consumables on the spacecraft last for more than three days as the spacecraft returned to earth and use the Lunar Module for a number of tasks for which it was not designed. The crew safely returned to earth and the mission is widely referred to as a “Successful Failure.” The event is detailed in a number of astronaut and flight controller memoirs (Liebergot and Harland 2006, Kraft 2001, Kranz 2000, Lovell and Kluger 1994) and television documentaries and it is dramatised most famously in the 1995 film, *Apollo 13*.
- During the launch of Apollo 12, the launch vehicle was stuck twice by lightning and the electrical surge disabled many CSM subsystems. However, a flight controller for that flight, John Aaron, immediately identified a corrective action after recalling a launch pad test power anomaly that he had witnessed and investigated a year earlier. The Apollo 12 crew ultimately landed on the Moon and safely returned to earth. The event is detailed in several memoirs and oral histories (Liebergot and Harland 2006, Kraft 2001, Rusnak 2000, Kranz 2000) and is dramatised most famously in the 1998 cable miniseries, *From the Earth to the Moon*.
- During the unmanned launch of the Skylab space station, a portion of its thermal insulation/micrometeoroid shield and one of its two solar panel wings fell off (the other was consequently obstructed in a manner that prevented it from properly deploying)⁷⁷. This situation left the station severely low on power and thermal protection. As a result, the first crewed mission to Skylab was delayed until a makeshift shield could be developed for the station and it was thus left up to both Mission Control and the MER to keep the damaged space station “alive” in the interim through remote commanding (Liebergot and Harland 2006).
- The assembly sequence of the ISS called for the station’s power system to be assembled one pair of Solar Array Wings (SAWs) at a time. Moreover, the first pair of SAWs (referred to as the “P6” array) was to be deployed at a temporary location on the ISS, retracted several missions later, moved to a permanent location, and redeployed. However, the SAWs neither deployed nor retracted as easily as its designers had anticipated and one partially ripped when it was ultimately redeployed. Nonetheless, Mission Control and the MER quickly developed procedures to overcome the deployment/retraction problems and fix the tear in the SAW. Furthermore, they updated SAW deployment procedures so that the second and third SAW pairs deployed without significant difficulties. These events are detailed and investigated in the next two chapters of this dissertation.
- As Neil Armstrong and Buzz Aldrin descended towards the lunar surface during the first crewed landing on the Moon (Apollo 11), several computer alarms rang, adding anxiety and confusion to an already tense and intellectually demanding situation. Though the alarms were relatively inconsequential⁷⁸, it is not

⁷⁷ Liebergot and Harland (2006) state that design engineers opted to qualify the shield “by analysis” rather than subjecting it to aerodynamic stress tests.

⁷⁸ The alarms merely indicated that the computer was overloaded and dropping low priority tasks.

unreasonable to speculate that an operator in such a situation might wrongly call for an abort of the landing—in fact, that is exactly what happened in a sim that occurred several weeks before the mission. However, due to the experiment-based approach (i.e., simulation) to the refutation of procedural knowledge taken by Mission Control, the flight control team responsible for the computer alarms recognized the irrelevance of the alarms. Overall, the events are discussed in several publications (Mindell 2008, Liebergot and Harland 2006, Kraft 2001, Kranz 2000) and are dramatised most famously in the 1998 cable miniseries, *From the Earth to the Moon*. Mindell's (2008) account of the events is of particular interest when assessing the role of designers and operators in such situations. He casts doubt on the potential for an abort—suggesting that aborts in sims are much more likely than aborts in real life—in that situation, lauds the computer's ability drop low priority tasks as a robust design feature, and points out that a procedure change by Buzz Aldrin put the system into a configuration that overloaded the computer. These arguments taken alone might suggest that the operators added little—or even negative—value to the situation. However, he also indicates that the designers made the situation unnecessarily difficult for the operators by stating the following two facts and opinion: the program alarms only existed for use in ground testing, the IL engineers approved Aldrin's procedure change because their testing facilities and processes misrepresented the affect of the change, and the decision to make the computer issue a program alarm when it dropped low priority tasks was “too dramatic and intrusive in proportion to the nature of the problem.”

5.3 Current Mission Control Responsibilities, Workstations, and Staffing

Overall, the Mission Control function consists of a number of responsibilities and requires special human interfaces and staffing plans. These responsibilities, interfaces, and staffing plans are described throughout this section.

Monitoring of Crew, Payload, and Spacecraft Health and Status

A primary responsibility of flight controllers is to monitor the health and status of the crew, payload, and spacecraft throughout the mission and recommend corrective actions when they observe unplanned events and phenomena. There are several types of data available to flight controllers to perform this function, including: telemetry, voice/text messages from the crew, and video downlink from the spacecraft. While voice, text, and video data from the spacecraft and crew are processed entirely by humans, automation (both on the spacecraft and on the ground) is used to process the telemetry data. While this automation enables flight controllers to handle the large volume of data and focus on other responsibilities, flight controllers are also expected to monitor the automation itself and stay ahead of it whenever possible.

Spacecraft Commanding

There are essentially two types of interfaces through which humans can command a spacecraft: hardware interfaces (e.g. switches, circuit breakers, dials, keyboards, etc.) and software interfaces (e.g. digitized commands). While flight controllers can provide

specific instructions (e.g. switch throws) in helping the crew command the spacecraft through hardware interfaces, they cannot interface directly with the spacecraft through these interfaces. One of the two crewed U.S. spacecraft in operation today, the Space Shuttle, is commanded almost exclusively through hardware interfaces and thus, flight controllers play mostly an indirect role in its commanding. The other spacecraft, the ISS, is commanded mostly through software commands originating from either the on board computers operated by the crew or RF signals from Mission Control. As an example of the frequency of flight controller commanding of the ISS, it's estimated that over 125,000 commands were uplinked to the ISS from Mission Control in the first year of ISS crewed operations (Crocker 2005). Each command from Mission Control is broken up into digital packets and modulated onto the RF signals sent to the ISS from Mission Control. Because bits in the packets can get lost or flipped in the transmission process, flight controllers must verify that every command is sent, received, checked for errors, and properly executed.

Management of Spacecraft Consumables and Supplies

Each human spacecraft and its crew consume physical resources such as air, food, water, propellant, and so forth in the course of operations. Additionally, certain reusable items or supplies such as tools, computers, clothing and so on are utilized frequently by the crew. Ultimately, it is up to the flight controllers to closely monitor and control the usage of the consumables in order to ensure that there will always be enough consumables available to successfully and safely complete the mission. Also, they are in charge of tracking the location and usage of the reusable items in order to:

- 1) tell the crew exactly where they are if they are needed for a task,
- 2) make arrangements for the mitigation or prevention of the failure or overuse of them, and
- 3) determine the distribution of mass throughout the spacecraft. This information is vital for accurate orbital maneuvering and vehicle pointing as well as determining whether certain items and locations on the spacecraft are inaccessible due to clutter.

Crew Activity Planning

Mission Control is responsible for both planning and re-planning the crew's daily activities. The plan produced by Mission Control, exemplified in the 12-hour Gantt Chart in Figure 39, details the actions of each crewmember—as well as the day/night cycle, RF communications opportunities, and spacecraft attitude schedule—down to five minute intervals. For missions with durations on the order of weeks (e.g., typical Space Shuttle missions), the entire flight plan is produced before the mission and revised every day during the mission. For long duration missions (e.g., ISS crew expeditions), a long-term plan is produced periodically throughout the mission and updated daily.

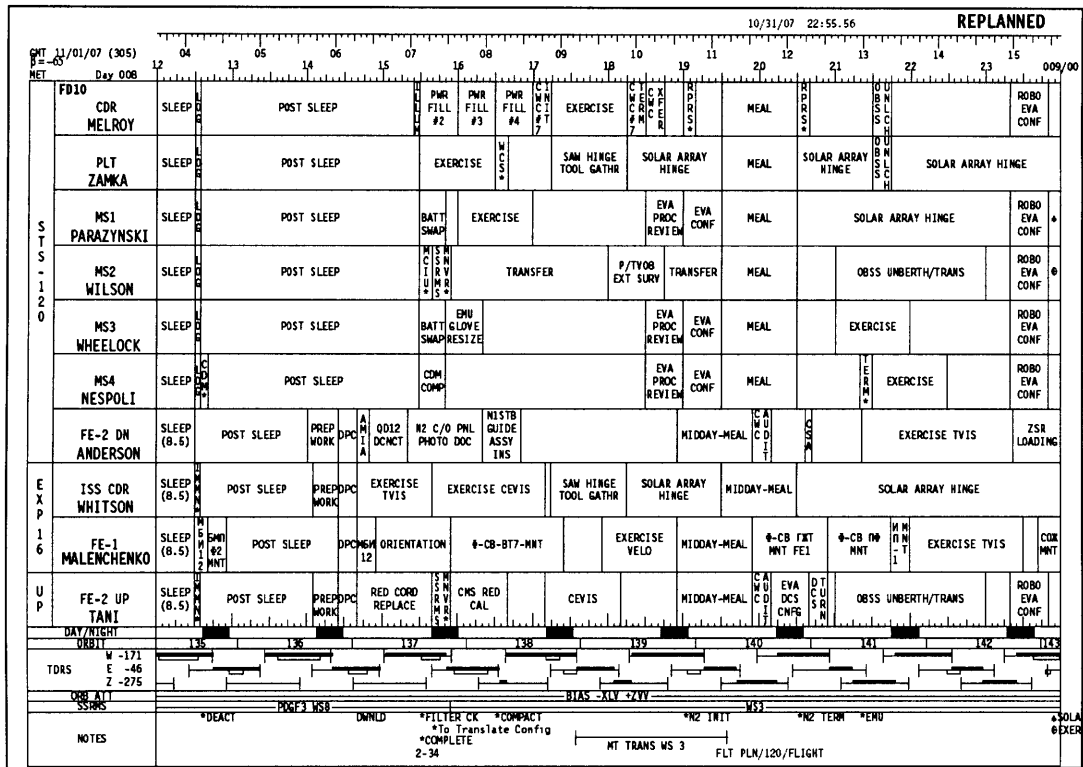


Figure 39. An example twelve-hour, re-planned portion of a flight plan for a Space Shuttle mission.

Development and Upkeep of Spaceflight Procedures

Flight controllers are responsible for developing both the generic and mission specific procedures for U.S. human spaceflight operations. Because these procedures are very detailed, both minor changes in the spacecraft hardware configuration and anomalies that arise in operations often make it necessary for the flight controllers to update the procedures both between and during the missions.

Development and Upkeep of Spaceflight Operational Requirements

Flight controllers are responsible for developing generic and mission specific operational requirements, referred to as "Flight Rules", in order to make sure that their roles and expectations are sufficiently regulated and defined to accomplish the goals of the individual missions and the program as a whole. Because goals vary from mission to mission and throughout the lifecycle of the program, it is necessary to develop new operational requirements and revise the old ones frequently.

Development and Upkeep of Flight Controller Reference Material

To ensure the quick accessibility of information vital to the Mission Control function, flight controllers spend a significant portion of their time between missions compiling generic and mission specific reference material into documents that are to be used at their workstation. Because the material in these documents (e.g. vehicle schematics, payload

list, etc.) often changes from mission to mission, it is necessary to develop new documents and update the old ones frequently.

Participation in Crew Training

Because flight controllers are heavily involved in procedure development, it is sometimes necessary for them to be directly involved in the training of astronauts even though there is a dedicated staff for training both the astronauts and flight controllers. This training usually consists of informal sessions organized by the flight controller.

Mission Control Organizational Structure and Decision Making

The Mission Control function requires a clear division of authority and required expertise among the flight control team. Furthermore, it requires a coherent staffing plan that ensures that there are flight controllers on duty whenever they are needed and that these flight controllers are well rested and well informed on the issues that arose while they rested. In this subsection, the organizational structure and decision making process used by NASA for the Mission Control function is discussed.

Staffing

During U.S. human spaceflight operations, Mission Control is staffed 24 hours a day by a large number of highly trained experts in spacecraft subsystems. Currently, there are two major types of spaceflight operations being conducted by the U.S.: Space Shuttle operations and ISS operations. Each involves its own flight control team and FCR. Figure 40 below contains a labeled illustration of the flight controller workstations in the Space Shuttle FCR. The current positions associated with the workstations are described in Table 5 and Table 5. Almost every flight controller in each of the two FCRs is supported by a team of less experienced, but more specialized flight controllers located in one of the many MPSRs in Building 30. Because the total number of MPSR positions greatly exceeds the number of FCR positions they are not listed individually in this dissertation.

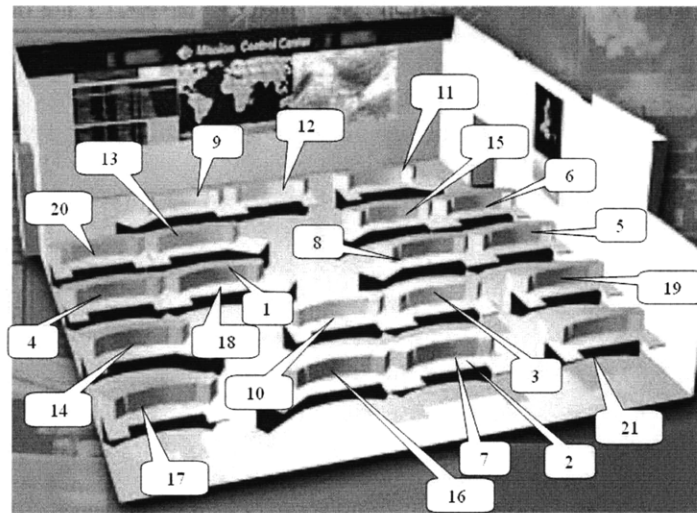


Figure 40. Labeled schematic of Space Shuttle FCR workstations (image from <http://spaceflight.nasa.gov/>).

FLAGGED POSITION NUMBER	POSITION NAME	RESPONSIBILITY
1	ACO (Assembly and Checkout Officer)	ACO is responsible for development of ISS assembly, activation, and checkout operations.
2	BOOSTER (Booster Systems Engineer)	BOOSTER monitors and evaluates the Shuttle main engines, solid rocket boosters, and external tank performance during pre-launch and ascent phases of missions
3	CAPCOM (Spacecraft Communicator)	CAPCOM serves as the prime communication link between Mission Control and the crew aboard the Shuttle and Space Station. In the days of Mercury, Gemini, and Apollo, the initials stood for "Capsule Communicator."
4	DPS (Data Processing Systems Engineer)	DPS determines the status of data processing systems including the five Shuttle onboard general purpose computers, flight-critical and launch data lines, the multifunction display system, mass memories, and system-level software.
5	EECOM (Emergency, Environmental, Consumables Manager)	EECOM is responsible for passive and active thermal control functions and life support systems including: cabin atmosphere control, avionics cooling, supply/waste water system management, and fire detection/suppression.
6	EGIL (Electrical Generation and Illumination Engineer)	EGIL, pronounced "Eagle," monitors Shuttle electrical systems, fuel cells, and associated cryogenics; AC and DC power circuits; vehicle pyrotechnics and lighting; and hardware caution and warning systems.
7	EVA (Extravehicular Activities Officer)	EVA monitors all aspects of the spacewalks based out of the Shuttle and Space Station. This includes monitoring the technical operation of the spacesuits and the spacewalk activities carried out during the mission.
8	FAO (Flight Activities Officer)	FAO plans and supports crew activities, checklists, procedures, and schedules and plans and manages the orientation of the Shuttle in space.
9	FDO (Flight Dynamics Officer)	FDO, pronounced "Fido," plans Shuttle maneuvers and monitors trajectory in conjunction with the guidance officer.
10	FLIGHT (Flight Director)	"FLIGHT" serves as leader of the flight control team and is responsible for the conduct of the overall team. Flight acts as the focal point for all decisions made relative to the on-orbit mission.
11	GC (Ground Controller)	GC directs maintenance and operation activities affecting Mission Control hardware, software, and support facilities. GC coordinates the Ground Space Flight Tracking and Data Network and the Tracking and Data Relay Satellite System used for data and voice transmissions between the Mission Control and the Shuttle or Space Station.
12	GDO-Rendezvous (Rendezvous Guidance and Procedures Officer)	Rendezvous supports Shuttle missions during deploy, rendezvous, proximity operations phases, docking, and undocking; and whenever complex crew procedures are affecting orbit dynamics.
13	GNC (Guidance, Navigation, and Control Systems Engineer)	GNC monitors all space shuttle guidance, navigation, and control systems; notifies Flight Director and crew of impending abort situations; and advises the crew regarding guidance hardware malfunctions.

Table 4. Brief descriptions of Space Shuttle FCR console positions (Part 1 of 2, adapted from NASA JSC 2005a).

FLAGGED POSITION NUMBER	POSITION NAME	RESPONSIBILITY
14	INCO (Integrated and Communications Officer)	INCO plans and monitors in-flight communications and instrumentation systems configuration, and controls Shuttle television from the ground.
15	MMACS (Maintenance, Mechanical, Arm, and Crew Systems Officer)	MMACS, pronounced “Max,” monitors the Orbiter’s hydraulic, structural, and mechanical systems. MMACS is also responsible for onboard crew equipment and In-Flight maintenance procedures.
16	MOD (Mission Operations Directorate Manager)	MOD provides a link from the Flight Control Room to top NASA and mission managers.
17	PAO (Public Affairs Officer)	PAO provides mission commentary to supplement and explain air-to-ground transmissions and flight control operations to the news media and public.
18	PAYLOADS (Payloads Officer)	PAYLOADS coordinates onboard and ground system interfaces between the flight control team and Shuttle payload user, and monitors in-cabin and cargo bay systems, experiments, and satellites.
19	PDRS (Payload Deployment and Retrieval Systems)	PDRS monitors operation of the SRMS, used to deploy, retrieve, and position satellites, the OBSS, and other cargo in the payload bay.
20	PROP (Propulsion)	PROP monitors and evaluates Shuttle reaction control and orbital maneuvering system jets and propellants and other consumables available for maneuvers.
21	SURGEON	Surgeon monitors crew health, provides crew consultations, coordinates crew medical operations and advises the Flight Director of any related issues that may affect mission success.

Table 5. Brief descriptions of Space Shuttle FCR console positions (Part 2 of 2, adapted from NASA JSC 2005a).

Every flight control team consists of at least three shifts—occasionally a fourth shift is called in during highly anomalous situations. In order to ensure that information is adequately transferred between flight controllers working on different shifts, each shift is scheduled to overlap the shift that preceded it and the shift that follows it by one hour⁷⁹. For Space Shuttle missions, one of the shifts is scheduled to coincide with the crew sleep period whenever possible⁸⁰. This shift is given the responsibility for re-planning the crew’s activities for the next day.

Chain of Command

In the hierarchical structure of Mission Control, the Flight Director acts as the flight control team integrator and assumes full responsibility for the actions of the flight control team. Ultimately, the Flight Director must approve all actions recommended or directly implemented by the flight control team. Even though Flight Directors are relatively low-level managers within NASA as a whole, they have the authority, along with the crew

⁷⁹ Consequently, each flight control shift works for nine hours per day during spacecraft operations.

⁸⁰ On some Shuttle flights the entire crew sleeps at the same time while on others, the crew is divided into two groups with different sleep cycles in order to support continuous crew operations.

commander, to overrule high-level NASA management during operations in order to take any action that they feel is necessary to ensure the safety of the crew and spacecraft (Kraft 2001). MPSR controllers report to the FCR controller that they support and the FCR controllers in turn report directly to the Flight Director.

In Mission Control, information can flow vertically, horizontally, or instantaneously to all positions. Sometimes the MPSR controllers, because of their low-level attention to subsystem issues identify an issue first and discuss it with other MPSR controllers and their associated FCR controller who in turn suggests possible actions to other FCR controllers and the Flight Director who then approves a course of action. CAPCOM, traditionally the only position allowed to speak to the crew, then relays that decision to the crew. Other times, the Flight Director may recognize a system issue and ask FCR controllers for advice, which they will derive from a discussion with other FCR controllers or their MPSR personnel. Finally, at other times, the details of an issue will be broadcast to everyone in the FCR and MPSR from the crew, spacecraft automation, or other elements of NASA.

Flight Rules

Flight Rules can be thought of as the operational requirements for Mission Control and serve as the basis for all decisions made by the flight control team in one way or another. They are developed and approved by the Flight Director Office and higher-level NASA management before the mission and their purpose is to decrease the amount of time it takes to make decisions whenever off-nominal events occur. They include, among other things, a prioritized list of mission objectives, definitions of the minimum acceptable performance level of many components, operational policies, and anomaly response strategies. Additionally the rationale for each flight rule is explicitly stated in the documentation of the rule. Because it is understood that creating a set of Flight Rules that is internally consistent in addressing all of these issues for all situations is nearly impossible given the complexity of spaceflight operations, there is also a Flight Rule that addresses conflicting requirements. Essentially, this Flight Rule allows the flight control team to use its engineering judgment to resolve any conflicts that arise among two or more Flight Rules.

Digital Voice Loops

Because flight controller teams and the astronauts that they support are physically distributed, communication in Mission Control is primarily facilitated by digital voice loops. A digital voice loop can be thought of as the aural equivalent of an online chat room. Users in Mission Control can anonymously monitor or participate in conversations occurring on a voice loop through an earpiece-microphone headset that they plug into the voice loop network. Additionally, like online chat rooms, each voice loop is reserved as a forum for discussion of a specific topic or among a specific group of users. As a result, each flight control position has specific loops that it monitors at all times and others that it monitors at its discretion. To facilitate discretionary monitoring of conversations of interest to the flight control position, there are few restrictions on the position's access to the various loops in Mission Control. While some loops can only be monitored from certain workstations and others grant talking privileges only to certain flight control

positions (e.g., only CAPCOM can talk on the loops used to converse with the astronauts), flight controllers are generally afforded the appropriate level of access to the loops that would be useful to them.

Ultimately, there are hundreds of voice loops available for flight controller communication in Mission Control. Each flight controller's interface to the voice loop network allows talking on only one loop at a time. It also makes it possible to monitor up to 24 loops simultaneously, though no flight controllers can actually monitor this many loops at the same time unless many of them are silent. Typically flight controllers only monitor between four and ten loops concurrently. They succeed at this task by learning to focus their attention only on parts of the conversations that are relevant to their position. Additionally, all flight controllers are expected to use a formal protocol of concise dialogue when conversing on the loops in order to avoid unnecessarily cluttering them. For example, even though all flight controllers have access to the Flight Director Loop and are strongly encouraged to monitor it at all times, only controllers in the FCR are allowed to talk on it under normal circumstances.

Flight Controller Consoles

While the astronauts orbit the Earth or walk on the Moon, the flight controllers monitor and advise them from a windowless building in Houston, Texas. Telemetry, voice messages from the crew, and occasional video downlinks from the spacecraft provide the only windows that flight controllers have into what is actually happening on the vehicle. Therefore, the workstation for a flight controller—referred to as a *console*—that provides this information, is vital to the flight control process. Figure 41 contains a picture of a typical Space Shuttle FCR console with numbered flags to identify its key features. These features are described further in Table 6.



Figure 41. A typical flight controller console in the Space Shuttle FCR (image from <http://spaceflight.nasa.gov/>).

FLAGGED ITEM NUMBER	DESCRIPTION OF FLAGGED ITEM
1	This display at the front of the FCR contains event logging information.
2	This display at the front of the FCR contains information that allows the flight controller to locate the spacecraft's position over the Earth.
3	These wall clock light displays provide count-downs and count-ups to and from mission critical events.
4	This display at the front of the FCR is used for high-level situation awareness. It is reconfigured multiple times in any given day of a mission. Normally it contains video footage downlinked from the spacecraft, weather maps, spacecraft attitude, maneuver displays, landing displays, etc.
5	This flat panel monitor is connected to a PC that flight controllers use for email, word processing, timeline software, Flight Note ⁸¹ editing, and internet access.
6	This digital interface is used by the flight controller to select the voice loops that they will monitor and talk on.
7	These three computer monitors are connected to two Unix machines and are used for the display of data. Data can be viewed digitally or in time history plots through custom displays designed for the various FCR positions. Furthermore, the flight controller can set limits on the data, called "Console Limits," in order to receive an aural alert when the data exceeds a limit.
8	This extra chair is used by FCR flight controllers on the incoming shift during a shift handover and flight controller trainees for observation of certified FCR flight controllers.
9	This headset plugs into the console and allows the flight controller to both listen to and talk on the voice loops.
10	This label points towards a bookshelf (not in the image) for reference manuals containing: nominal procedures, malfunction procedures, Flight Rules, vehicle schematics, etc.

Table 6. Description of Space Shuttle FCR console features.

MPSR consoles differ only slightly from FCR consoles. Most MPSR consoles have additional closed circuit television screens that allow them to view what is happening in the FCR. Additionally, because MPSR flight controllers cannot directly view the FCR wall displays—features 1 through 4 in Table 6—they usually access the information on these displays either through the Unix-driven screens of their console, feature 7 in Table 6, or their closed circuit television screens.

5.3 The Scholars of Flight Control

When given a description of the responsibilities of flight controllers—such as the one provided in the previous section—the question arises as to what kind of knowledge is required to satisfy those responsibilities. Rasmussen's (1990, 1987) framework of Skill-Based Behaviors (SBBs), Rule-Based Behaviors (RBBs), and Knowledge-Based Behaviors (KBBs) and their relation to human "error"—as discussed in Chapter 2—provides an intriguing construct for addressing this question. Information in the form of vehicle health and status data is transmitted from the spacecraft automation directly to two layers of human supervisory control: the astronaut crew and Mission Control. Mission Control and the astronaut crew coordinate their efforts through radio frequency transmission of digital voice, video, and text files. While the crew has almost full

⁸¹ Flight notes are memos that the flight control team uses to write or rewrite procedures and Flight Rules or draw attention to other issues during operations.

capability to command the automation directly, Mission Control has a more limited capability and must often initiate their desired control actions through instructions to the crew. Astronauts go through years of generic and mission specific training to understand the wide spectrum of RBBs that will be required in their flights into space, to practice the SBBs that will not be automated, and form a high-level mental model for mastery of some of the necessary KBBs. Flight controllers, on the other hand, primarily focus on the KBBs and RBBs needed for development and revision of procedures, operational requirements, flight plans, and other reference material (i.e., flight controller “publications”) and the management of vehicle consumables. Figure 42 depicts the distribution of authority and focus of Mission Control, the astronaut crew, and the spacecraft automation in regards to SBBs, RBBs, and KBBs.

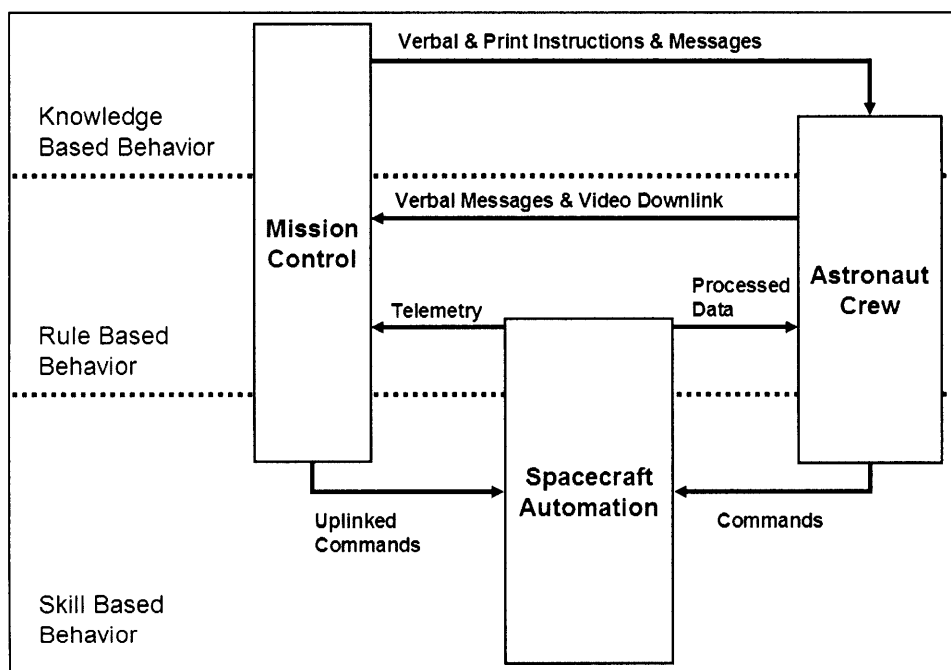


Figure 42. The distribution of authority for SBBs, RBBs, and KBBs in U.S. human spaceflight operations.

Flight controllers must not only master the knowledge in their field, but they must advance it through original thought and they must do so in a very public setting. In other words, flight controllers must become “Scholars of Flight Control” over the course of their training. Accordingly, flight controllers receive years of highly focused training in almost every known aspect of their subsystem and have to pass a series of written and oral exams before being certified to take responsibility for the execution of the KBBs and supervision of the RBBs relating to their subsystem.

While the training of a flight controller develops the trainee’s capacity for original thought and problem solving, it can be said that the focus on fostering original thought rather than preventing human “error” is understated. The concept of human reliability as the central problem to safety in the field of human factors is unfortunately so prevalent

that even operators may be led to believe it. The current chair of the AIAA Space Operations and Support Technical Committee recently wrote, “The ultimate goal of a training program is to reduce operator error” (Fuller 2003). To the contrary, the author believes that the ultimate goal of operator training is to build the operators’ mental models to the point where they understand how to apply the control authority for task execution, disturbance rejection, and adaptation allocated to them (explicitly and implicitly) in order to successfully or at least safely perform the mission. In the remaining paragraphs of this section, the elements of a typical flight controller’s training are discussed.

United Space Alliance Flight Operations Training Academy

Most flight controllers are entry-level engineers, and while all are required to have an engineering, science, or mathematics degree from a university, few have graduate school or significant prior work experience. Typically the first major training milestone that flight controller trainees achieve in their flight control career is graduation from a four-to-six week training program provided by NASA’s prime contractor for spaceflight operations, the United Space Alliance. This program, commonly referred to as “Training Academy,” is offered several times a year and flight controller trainees are usually expected to attend it during its first offering after their hire date. While the structure and content of the program evolves from year-to-year, the format consists mostly of lectures, facility tours, and reading assignments relating to the high-level details of the U.S. human spaceflight program in general and each of its operational vehicles. The program is broken up into several sections, each of which is followed by comprehensive exams consisting of multiple sections that are graded individually. If a flight controller trainee fails one or more sections of an exam—which happens to almost every flight controller trainee as they go through the program—the trainee is required to retake the failed section(s) in order to achieve a passing score.

Computer Based Trainers (CBTs)

Flight controller trainees are required to individually complete dozens of short (i.e. one to three hours in duration), online training courses referred to as Computer Based Trainers (CBTs) throughout their flight certification process. Normally these courses involve the review of a series of narrated slides and the completion of multiple choice tests. The topics of these CBTs range from universal engineering workplace issues such as intellectual property rights of workers to highly specific topics relating to the subsystems for which the flight controller trainee will be responsible.

Hardware Familiarization in Spacecraft Mockup Facilities

The majority of U.S. spaceflight hardware assembly and maintenance occurs at KSC in Florida. Consequently, there are few opportunities for flight controllers to examine flight hardware in person—especially early on in their careers when they are training for their flight control responsibilities. This situation presents an enormous challenge to flight controller trainees in the development of their mental model of the systems for which they will be responsible, and it is partially remedied by the existence of semi-functional, full scale mockups of the major crew compartments of each type of human spacecraft operated by NASA. A number of short courses are offered in these mockups for

hardware familiarization and each flight controller trainee is required or encouraged to complete a subset of them. Flight controller trainees are also given the option to reserve time in these mockups for individual and group study of the hardware. In all, these mockup facilities are frequently used to reduce trainees' reliance on hardware/software documentation, images, and video footage for the development of a viable mental model of the hardware/software relevant to their flight control responsibilities.

Single System Trainers (SSTs)

Because flight controllers are often required to write and update crew procedures and supervise the crew while they complete them, a portion of their training is devoted to understanding procedure execution from the perspective of an astronaut. This type of training is mostly conducted in Single System Trainers (SSTs), which are mockups of the crew's interfaces to spacecraft software and subsystem electro-mechanical interfaces (e.g. valve switches, power switches, etc.). Flight controller trainees are required to complete a number of short courses in SSTs where they act out the role of astronaut crewmembers in the execution of both nominal and contingency procedures.

Flight Controller Trainers (FCTs)

Actual simulation of the flight control process is a crucial part of the training of each flight controller. Early on in the flight control career of trainees, it is usually not practical for the trainees to participate in simulations with a full flight control team because they will usually not be able to keep pace with more experienced flight controllers. Furthermore, there will be a number of training scenarios that are of immense value to the trainee, but not the flight control team as whole. Therefore, flight controllers have access to facilities known as Flight Controller Trainers (FCTs) where they can run through simulations alone with an instructor or with just a handful of flight controllers—typically those who work on their FCR/MPSR team.

Each FCT contains a small number of flight controller consoles—minus a few features—that can be loaded with simulation data to respond much like a real console would in flight. Because everyone involved in the simulation is typically in the same room, voice loops normally are not used—though there is limited capability to conduct a simulation in more than one FCT and link trainees in each FCT through voice loops. Because certain flight control and astronaut positions are not represented directly in the simulation, the instructor in charge of the simulation normally acts out the roles of these positions.

FCT simulation sessions are typically three hours in length and are orchestrated by senior members in the flight control groups involved or personnel from the flight controller training division. Each flight control group that uses the FCTs for training has a required curriculum of scenarios that trainees must successfully pass. The trainees are exposed to these scenarios in a non-predictable order and if they successfully complete one scenario early in the session, they may be exposed to another. Conversely, if trainees struggle in a scenario, they may have to spend the whole session on it and be exposed to it again in later sessions until they perform satisfactorily in it. Once trainees successfully work through a number of scenarios and demonstrate an acceptable level of competence in flight control relating to their position, they begin participation in simulations with full

flight control teams. However, this transition usually does not signal the end of the trainees' participation in FCT simulations as it is often necessary for trainees to continue to use the FCTs to sharpen their skills in between simulations with full flight control teams.

Integrated Simulations

Integrated simulations or “sims” are conducted in a FCR and its associated MPSRs and involve a full flight control team and usually a crew of astronauts. They range in duration from a few hours to a few days and are organized by a team of certified flight controller training personnel. While the shorter sims can be completed by a single shift of flight controllers, the longer ones cannot and thus require shift changes⁸². Ultimately sims are among the most crucial elements of a flight controller's training because they most closely resemble the actual flight control process during contingency situations. In fact, they are considered to be so useful that even certified flight controllers participate in them regularly to maintain generic proficiency or prepare for specific events to be conducted during actual flight operations.

Normally, the flight control team is exposed to a handful of system and subsystem level malfunctions and difficulties throughout the course of a sim and the performance of each flight controller is evaluated closely⁸³. The trainees in particular are evaluated for their overall progress in developing a viable mental model for flight control in their assigned position. Once trainees become comfortable in participating in integrated sims at their position, they are put through an evaluation process known as an “interim certification sim” in which their position is a point of intense focus for malfunctions and difficulties in the course of a sim. If trainees perform well in their interim certification sim, they will shortly thereafter get to participate in a similar, yet more intense evaluation sim referred to as a “final certification sim,” which is usually the final task that they must successfully complete before certification. Conversely, if trainees perform poorly in their interim certification sim they will have to participate in sims and FCT sessions until they can demonstrate a level of progress that would address the concerns that their flight control group might have in putting them through a final certification sim.

In-Flight Training

Flight controller trainees are also strongly encouraged to observe and participate in the actual flight control process at various stages throughout their training. As illustrated above in Figure 41 there is one extra seat and voice loop interface at every console in Mission Control. In the seven hours of each shift between the shift handovers this seat and interface is usually available for flight controller trainees to sit next to the certified flight controllers in order to observe and assist them. This type of experience is meant to give the trainee—who in this role is referred to as an On-the-Job-Trainee (OJT)—exposure to the aspects of the flight control process that cannot be simulated. As a result, each flight control group has a set number of hours that it would like its trainees to serve

⁸² Because shift changes are considered an important part of the flight control process, it is sometimes the case that shift changes are scheduled even during the shorter duration sims.

⁸³ At the conclusion of every sim both the Flight Director and the simulation supervisor debrief the simulation with the entire flight control team.

as OJTs before they become certified. However, this number of hours is usually considered a guideline rather than a requirement because the flight schedule does not always provide enough opportunities for OJT experience.

Generic Certification Process

As mentioned above, the final certification sim typically serves as the final barrier to certification for a flight controller trainee. It is essentially a way to subjectively evaluate the trainees' readiness to serve at the flight control position that they will occupy. As is the case in the interim sim, the trainee is forced to deal with a spate of malfunctions and other difficulties. The scenarios are designed to expose the trainee's level of knowledge and capacity for original thought and problem solving to the fullest extent possible. Flight controllers in some groups also take a written exam shortly before their final certification sim. Each flight control group has different requirements for their final certification sims and thus, the sim pass/failure rate and the maximum number of opportunities that a trainee is given to retake the sim varies from position to position.

Once flight controller trainees receive certification, they are qualified to work at the flight control position that they have been training at in FCTs and sims. Usually this position will be only one of several positions that they will eventually work at in their career. Figure 43 provides an example of the progression of a flight controller from position to position in the Space Shuttle environmental systems flight control group⁸⁴. Whenever flight controllers move from one position to another, they must go through another certification process for the new position. Ultimately, this new certification process will not call for a repeat of some training elements such as Training Academy, but it will call for the flight controller to participate in a new curriculum of CBT, FCT, and sim training, culminating in another final certification sim.

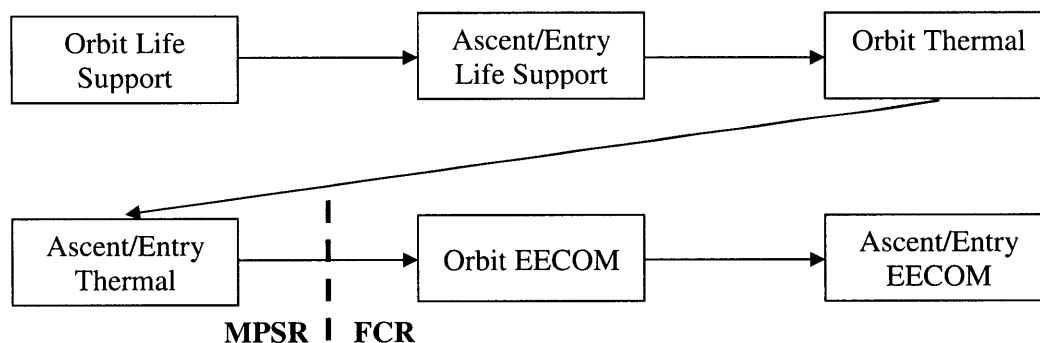


Figure 43. Example certification flow for a flight controller in the Space Shuttle environmental systems group.

⁸⁴ The Space Shuttle environmental systems flight control group has two MPSR positions (Life Support and Thermal) and one FCR position (EECOM). Each position has two levels of certification: Orbit and Ascent/Entry. The Orbit certification allows the flight controller to work only during the phase of the mission where the Space Shuttle is in orbit and it is always achieved before the Ascent/Entry certification. The Ascent/Entry phases of a Space Shuttle flight are much more dynamic than the Orbit phase and therefore require deeper knowledge and capacity for original thought and problem solving relating to the flight control position.

There is no pre-determined amount of time for completing a flight controller training program. It typically takes over a year for flight controller trainees to achieve their first level of certification and may take anywhere from five to fifteen years before they complete every level of certification in their group. Ultimately, the amount of time it takes to complete the progression is dependent on several factors, including: the number of positions and certification levels in their group, the number of people vying for certification or who have certification, the availability of the training facilities, the flight schedule, the time the flight controllers dedicate to training versus working on other assignments, and the flight controllers' individual performance during FCTs and sims. Whenever flight controllers receive a new certification, they may immediately begin training for their next certification or spend some time focusing solely on the responsibilities of their flight control position. Either way, they will be expected to serve a number of shifts at the position that they have become certified for before moving to the next level of certification. Caldwell (2005) estimates that as many as 70% of all flight controllers fail to eventually achieve certification for a FCR position.

Flight Specific Certification Process

In addition to the generic certification process, flight controllers are typically required to go through some kind of separate process to become certified to work on specific missions. This process varies widely among the flight control groups, but can always be completed much faster than the generic certification process. Some groups—especially those that deal directly with mission payloads—have unique responsibilities for each mission and thus require a highly formal process that usually involves flight specific hardware familiarization training. Other groups that have very similar flight responsibilities from mission to mission tend to have a less formal process that consists mainly of participation in the flight specific sims.

Traditions and Foundations of Mission Control

Training programs in Mission Control are fundamentally socialization processes. One aspect of socialization is the adoption of traditions and cultural foundations of a specific group. In professional communities, such traditions and foundations provide indications of how a community views its professional identity. The stated foundations of MOD are as follows (Webb and Smith 2008, Liebergot and Harland 2006, Kranz 2000):

“To instill within ourselves these qualities essential to professional excellence:

***Discipline...**Being able to follow as well as to lead, knowing that we must master ourselves before we can master our task.*

***Competence...**There being no substitute for total preparation and complete dedication, for space will not tolerate the careless or indifferent.*

***Confidence...**Believing in ourselves as well as others, knowing that we must master fear and hesitation before we can succeed.*

Responsibility...*Realizing that it cannot be shifted to others, for it belongs to each of us; we must answer for what we do, or fail to do.*

Toughness...*Taking a stand when we must; to try again, and again, even if it means following a more difficult path.*

Teamwork...*Respecting and utilizing the abilities of others, realizing that we work toward a common goal, for success depends upon the efforts of all.*

Vigilance...*Always attentive to the dangers of spaceflight; Never accepting success as a substitute for rigor in everything we do.*

To always be aware that suddenly and unexpectedly we may find ourselves in a role where our performance has ultimate consequences.

To recognize that the greatest error is not to have tried and failed, but that in the trying, we do not give it our best effort."

These foundations indicate a standard of performance exceeding the mere avoidance of errors. In fact, the only references made to "error" downplay its significance relative to the added value of a sufficiently qualified, accountable, and engaged flight controller. Further reinforcing this view are the "hanging of the plaque" ceremony⁸⁵ and frequent flight controller usage of the following Roosevelt (1910) quote:

"It is not the critic who counts; not the man who points out how the strong man stumbles, or where the doer of deeds could have done them better. The credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood; who strives valiantly; who errs, who comes short again and again, because there is no effort without error and shortcoming; but who does actually strive to do the deeds; who knows great enthusiasms, the great devotions; who spends himself in a worthy cause; who at the best knows in the end the triumph of high achievement, and who at the worst, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who neither know victory nor defeat."

This quote is often referenced in internal flight controller presentations and reference documents, and in the environmental systems group, a flight controller that completes the Ascent/Entry EECOM certification (or otherwise contributes substantially to flight control in the EECOM group over his or her career) receives the "Man in the Arena" award.

⁸⁵ After every mission, the leader of the flight control console team (e.g., ACO, EVA, EECOM, etc.) that is perceived by the Flight Directors and crew to have made contributions to mission success and safety that are most deserving of recognition is invited to physically hang a plaque based on the mission patch in the FCR during a post-flight ceremony.

5.4 Procedure Rework in Space Shuttle Mission Control

Mindell's (2008) description—provided at the beginning of this chapter—of Hugh Blair Smith's reaction to the Apollo 11 program alarms highlights the importance of procedures (and their embedded assumptions) in complex system operation. Procedures are formal descriptions of task execution and disturbance rejection as planned. That being said, it is possible for procedures to be used as a means for control of uncertainty. Procedures can be constructed with an “if-then-else” structure to account for a multitude of possible outcomes that could result from a planned task. Additionally, procedures can be written to detail responses to system disturbances that the system may or may not encounter. Finally, processes can be put in place to remove detrimental inconsistencies in procedures due to design or operational issues that were initially unrecognized or that emerge from system adaptation and the evolution of its operating environment. Inconsistencies in procedures constitute a dynamic hazard in systems with interactive complexity and tight coupling and thus, the rework of procedures is a dynamic, safety risk management process⁸⁶. In accordance with Leveson's (1995) definition of a hazard, the mere existence of inconsistencies in a procedure will not necessarily lead to an accident unless certain contextual conditions are also present (e.g., the procedure executor wishes to execute the procedure as written, etc.). Moreover, the number of inconsistencies in the procedures relevant to a system can change over time as changes occur in the system and its environment and as the procedures themselves are changed. Therefore, it is possible to define system safety constraints that restrict the execution of procedures with inconsistencies, and to design the control authority into the system to allow enforcement of these constraints.

Procedures have traditionally been viewed as rules that must be followed and thus the failure to execute a procedure as written has been viewed as an indication of poor or “unsafe” operator performance (Bourrier 2005, Carroll et al. 2002). Indeed, many accident investigation reports in numerous industries habitually draw attention to the failures of operators to perform the prescribed procedures, and offer recommendations stressing increased training of the procedures and more surveillance of the workers to ensure that the procedures will be followed (Carroll et al. 2002). However, procedures can be ambiguous or outright wrong in many operational situations encountered in complex systems and in such instances it might even be best for the system stakeholders if the procedures are not followed by the operators (Dekker 2005, Bourrier 2005, Leveson 1995)⁸⁷. Such situations require a less commonly held (or at least less commonly discussed) view of procedures: the view of procedures as resources rather than rules.

When viewed as a resource, a procedure is just a medium for communication between the person or group that writes the procedure and the person or group that executes the

⁸⁶ More precisely, inconsistencies in procedures are control flaws—see Figure 33 in Chapter 4—that could instantiate inadequate control actions leading to hazard states (they represent flaws in the controller's model of the process being controlled).

⁸⁷ As noted by Leveson (1995) and others, “working-to-rule” or working in accordance to a procedure as written, regardless of whatever flaws exist in the procedure, is a practice often used as an alternative to formal strikes by workers belonging to labor unions in many industries.

procedure. The writer and the executor of the procedure can either be different people (ideally in such cases the procedure writer will actually be able to provide useful information to the procedure executor) or the same person who, when subjected to time pressure, would benefit from having the procedural information readily available. Every procedure is written for an assumed operational context and when that context applies, the executor of the procedure can use it to free up cognitive resources for thinking more critically about the process they are undertaking (i.e., to think about what's happening rather than trying to remember each step). On the other hand, when the assumed operational context does not apply or the procedure is not internally consistent—due to a mistake in the writing of the procedure or asynchronous system evolution (Leplat 1987)—the executor of the procedure should be given the discretion to delay the procedure in order to discuss it with the procedure writer or deviate from it when delay of the procedure cannot be tolerated. With this view of procedures, there is a burden on the procedure executor(s) to use discretion in executing the procedure and there is a burden on the procedure writer(s) to provide procedures to the executor(s) that are internally consistent and applicable to the actual operational context.

In Mission Control, the burdens of the procedure writer and procedure executor are addressed through a process that is henceforth referred to as *procedure rework*. Procedures are written by the flight controllers in Mission Control and mostly executed by the astronauts on board the spacecraft⁸⁸. The space environment harbors a number of potential disturbances to spacecraft and the spacecraft themselves—being complex and highly coupled—potentially harbor destructive internal inconsistencies in their configuration and thus, uncertainty is recognized in the usage of procedures. While in the months leading up to the mission, the astronauts and flight controllers train extensively on the proper execution of procedures, the foregone assumption throughout training is that the procedures will not be perfect and will need to be continuously updated both before and during the mission. This explicit recognition of uncertainty is perhaps best exemplified by a Mission Control flight rule that states that the Flight Director and the commanding astronaut for the mission have the discretion to resolve any inconsistencies in the flight rules that may be discovered during the mission.

Flight controllers carefully monitor the spacecraft throughout the mission, searching for conditions that may invalidate the assumptions behind the procedures that relate to their domain area. Whenever such conditions are recognized, the flight controllers initiate an update of the procedure through communication over the voice loops and if time permits, a document referred to as a Flight Note. When the procedure change is approved, documents or voice instructions are transmitted to the spacecraft to instruct the crew on how to update their procedure documentation. The astronauts are free to ask questions about procedures and procedure updates and to challenge the rationale for conducting them as written. These challenges present another opportunity to initiate or reiterate rework of a procedure. However, it should be noted that it is a point of pride for most

⁸⁸ As mentioned above, there is limited capability for flight controllers to uplink commands to the spacecraft, thereby executing procedures on their own. The extent to which this commanding capability is possible depends on the spacecraft; the International Space Station, for example, can accept a far greater number of uplinked commands than the Space Shuttle.

flight controllers to discover potential problems with procedures before the astronauts do and thus, procedure rework is usually initiated by flight controllers.

The goal of procedure rework in Mission Control is to induce adaptation of flight controller and astronaut behavior in response to the emergence of inconsistencies in task execution and disturbance rejection as planned. Specifically procedure rework is meant to enforce a safety constraint on the number of potentially harmful inconsistencies and omissions in the procedures. The sources and enablers of this control authority for system adaptation are the knowledge of the flight controllers, MER engineers, and astronauts; the formal processes for procedure rework; and the information systems used for data interpretation and communication.

In the next chapter, this process will be formally analyzed as part of Space Shuttle real-time⁸⁹ operations safety control structure shown in Figure 44. In this safety control structure, the White House and Congress have the responsibility to enable safe operations during emergencies on a national level, while NASA Administration must provide final approval for real-time operations to begin. Of course, both of these components are, by necessity, mostly inactive in real-time operations. The MMT is responsible for most high level real-time operations issues (e.g., redefining mission objectives in flight), while most implementation issues occur on the levels below the MMT. For example, Mission Control (assisted by the MER) is responsible for, among other things, providing safe procedures to the crew to execute in flight.

⁸⁹ The term “real-time” is used in this case study to describe operations occurring from the start of the launch countdown to the safing of the Space Shuttle once it has landed. Maintenance and pre-flight training operations are excluded in the use of this term.

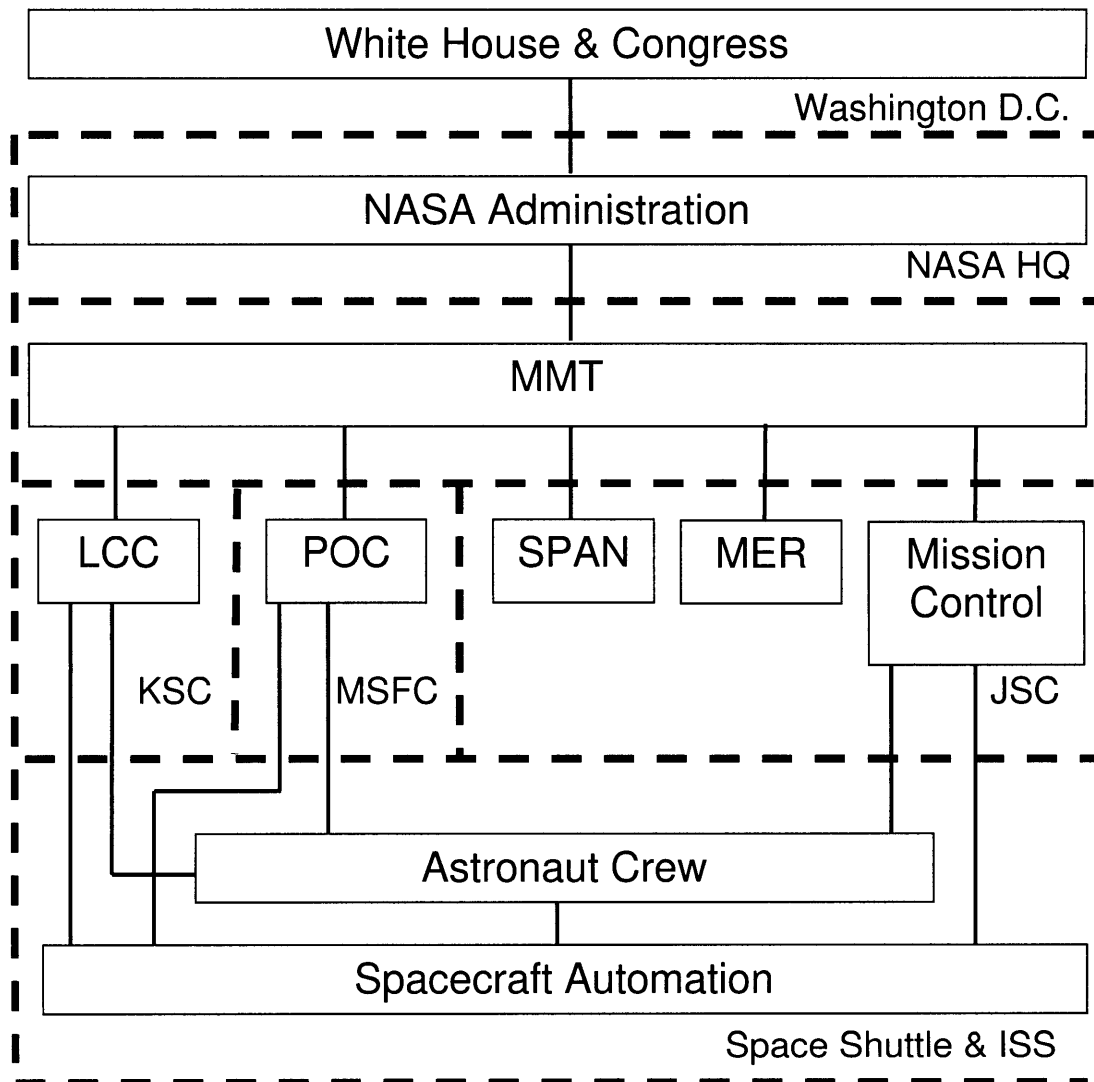


Figure 44. A portion of the Space Shuttle real-time operations safety control structure.

5.5 Mission Control Literature Review

As stated in Chapter 1, the hypothesis of this dissertation is:

“Modeling the output of system safety control structures as phase space attractors with nonlinear, continuous dynamics subject to uncertain initial (or disturbance) conditions will provide useful insights in the design and operation of system safety control structures.”

The discussion in Chapter 4 explains the relationship between phase space attraction and safety control structure evaluation. However, to provide support for the hypothesis’s claim on the usefulness of this relationship it is necessary to briefly summarize what researchers of a specific context have and have not learned without the concepts of this

relationship at their disposal. As stated earlier, the specific context used in this dissertation to demonstrate this usefulness is the Mission Control function. Thus, a brief summary of the Mission Control literature is provided in this section in order to highlight the gaps in knowledge that can be potentially be filled through the application of these safety control structure evaluation concepts. In the next two chapters these concepts are used to begin filling a portion of these gaps.

The amount of data on work in Mission Control that is available to researchers is staggering: the control rooms are continuously videotaped, conversations on the voice loops are recorded and can be monitored with little restriction by anyone with access to any of the hundreds of nodes in the voice loop network, commands uplinked to the spacecraft from flight controller consoles are logged, and official correspondence between flight controllers is saved for future reference. However, even though work in Mission Control is highly visible, unique, and thoroughly documented, relatively few researchers have attempted to study it (Caldwell 2007a) and those who have, did not attempt to perform an integrative, quantitative assessment of the control authority it provides in human spaceflight operations. While Mindell (2008), for example, provides an in-depth historical account of control authority allocation to astronauts and spacecraft automation during the Apollo lunar landings, he only devotes secondary attention to the control authority allocated to Mission Control.

Patterson et al. (1999) provide a detailed qualitative description of voice loop structure and usage in Mission Control that is being followed up by a quantitative network analysis (Caldwell 2007a). Shalin (2005) describes how information displays at two Mission Control consoles (FDO and INCO) are used for planning purposes in order to identify general requirements for developing effective planning representations. Patterson and Woods (2001) observed and describe both nominal and ad hoc shift handovers between flight controllers during a Space Shuttle mission as a means of maintaining flight controller preparedness. Kearney (1987) details the evolution—from the Gemini Era to the Early Space Shuttle Era—of the display and communications systems used in Mission Control. Watts et al. (1996) discuss real-time anomaly response coordination between the flight controllers and the MER. Chow et al. (2000) develop, after reviewing the data collected in previous Mission Control studies (i.e., Watts et al. 1996, Patterson et al. 1999, Patterson and Woods 2001), a descriptive model of the contents of communication among distributed practitioners engaged in anomaly response and re-planning. Garrett and Caldwell (2002) provide a quantitative description of Mission Control Flight Rule Change Request processing between Space Shuttle missions: a key element of flight controller knowledge capture and synchronization. A research group at Purdue University describes the concepts of information flow and synchronization as it relates to Mission Control and the challenges of generically linking these concepts to engineering design contexts in order to improve system reliability and human performance (Caldwell et al. 2007b, Caldwell 2003, Caldwell and Ghosh 2003, Caldwell and Wang 2003). Finally, the memoirs of pre-Shuttle Era flight controllers (Liebergot and Harland 2006, Kraft 2001, Kranz 2000) and “oral histories” recorded by NASA provide personal accounts of work in pre-Shuttle Mission Control. Though these accounts normally describe the technical details of work in Mission Control in a limited manner, they

prominently feature the “war stories” that flight controllers learn during their socialization⁹⁰.

Engineers and flight controllers recently or currently involved in the evolution of Mission Control present additional accounts of tools and processes used for the Mission Control function and potential options for addressing future challenges of space exploration. Webb and Smith (2008) detail MOD’s role in the development of systems for the Constellation Program⁹¹. Sierhuis et al. (2007) describe an agent-based process for simulating tasks performed by flight controllers and propose its use in the design of mission operations work processes. Mishkin et al. (2007) and Korsmeyer et al. (2005) briefly discuss Mission Control as a “locus of control” and mention issues that may necessitate a shift of control authority to the crew and spacecraft automation for Constellation. Esper and Olsen (2007), Leslie (2006), and Jaap et al. (2006) discuss procedure planning for ISS operations and suggest potential improvements for procedure planning in Constellation operations. Rose and Miller (2006) summarize spaceflight training objectives and processes and propose new directions for Constellation operations training. Challis et al. (2007) discuss preflight validation of crew procedures relating to the ISS Columbus Laboratory and the role of these procedures as hazard controls. Brown et al. (2002) describe an automation tool used to simulate astronaut actions during simulations and how it is being used to automate ISS procedures. Finally, Crocker (2005) briefly reviews the role of spacecraft automation vis-à-vis the Mission Control function in current and previous NASA programs and lists considerations and recommendations for the future development of spacecraft autonomy.

All of these publications provide rich descriptions (usually qualitative) of some of the organizational and technical tools in place in Mission Control to enable flight controllers to positively impact human spaceflight. However, researchers have yet to explore, in a rigorous mathematical fashion, how these tools—when used together—allow the alteration of select system states for the purpose of task execution, disturbance rejection, and adaptation. In the remainder of the case study of this dissertation, the concepts for safety control structure evaluation presented in Chapter 4 are applied—for the purpose of demonstrating their potential usefulness in actual socio-technical systems—to an analysis of procedure rework in Mission Control that addresses a portion of this gap in our knowledge of the control authority of Mission Control.

⁹⁰ In the HRO literature, researchers identify vivid stories as a means of enhancing requisite variety (Weick 1987) and preserving heedful interrelation (Weick and Roberts 1993) in a social system.

⁹¹ The Constellation Program is involved in the development of space exploration systems to replace the Space Shuttle, utilize ISS after shuttle retirement, and explore the Moon and beyond.

Chapter 6: Case Study Purpose, Scope, and Methodology

“...an anthropology of space operations would examine skill, training, professional identity, automation, risk, organizations, divisions of power, and other aspects of human-machine relationships. Sources exist for Skylab, the space shuttle, and the International Space Station, as well as for similar endeavors in other countries. What, exactly, are engineers, pilots, and scientists doing in orbit? When are they using judgment, skill, experience, and expertise, and when are they following scripts? What kinds of contingency operations do they perform? How are skills and judgment divided between those in orbit and those on the ground? What kinds of ‘repair’ do humans do (including rework and workarounds) when operating complex systems? Numerous spaceflights have been recorded and transcribed in detail (all of the Apollo flights and at least some of the shuttle flights), allowing such real-time ethnography. Mission transcripts, combined with deep analyses of operations, provide an empirical basis for exploring such questions...Such studies, if rigorously done by disinterested scholars would have implications for engineering design, training, mission planning, and safety in spaceflight...This work will also likely generate insights into other complex technical systems whose operations are rarely as well documented or as accessible as human spaceflight.”—David A. Mindell (2008).

“Principally the discussion of new technologies and tools [for real-time human spaceflight operations] needs to be framed in a manner that identifies and emphasizes the value to the MOD operational flight controller. It is not about replacing ‘man with a machine’, but about augmenting the flight controller or operator to do a better job.”—David J. Korsmeyer and Ernest Smith (2008).

“Every decision is based on an approximation of reality, not reality itself. The question is not, ‘Should models be used?’ but, rather, ‘which is the best model available for the task at hand?’”—Donella “Dana” Meadows et al. (1982).

“A model should always be created for a purpose. The adequacy of the model can only be judged in terms of that purpose. There is no possibility of absolute proof that a model is appropriate for its objective. But the model can be evaluated in several stages. The basic assumptions can be checked against available experience and data. The dynamic behavior of a model can be compared with the real systems it should represent.” —Jay W. Forrester (1969).

6.1 Chapter Overview

The purpose, scope, and methodology of the Space Shuttle Mission Control Procedure Rework Case Study are presented in this chapter. First, the case study purpose and scope are described. Next, the initial actions taken to develop dynamic models of the Procedure Rework Process are discussed along with the actions taken for data collection and

processing. Then, a description is provided of the dynamic models and how they were calibrated.

6.2 Case Study Purpose and Scope

Mindell's (2008) quote at the beginning of this chapter highlights the potential lessons that can be learned about complex system operations in general by studying human spaceflight operations. Of course, not all of what is suggested can be covered in a single dissertation and thus an area of focus is needed. Throughout this dissertation, the author has drawn attention to the management of uncertainty (particularly its downside) and the role of nonlinearity in system accidents. The author has argued—much like Leveson (2004)—that safety is a system property and that the attainment and maintenance of it are best treated as a control problem in complex, socio-technical systems. Specifically, the author has advocated that control authority be designed into systems to enhance and synthesize their adaptability, resilience, flexibility, and robustness to safely counter the effects of uncertainty, and that phase space attractors will emerge from the application of that control authority. Thus, the purpose of this case study is to evaluate how control authority is applied in human spaceflight operations to produce properties of attraction to safe system states and to determine how one would perform such an evaluation.

Mission Control has a number of sources of control authority for task execution, disturbance rejection, and adaptation to affect a number of spaceflight system states. However as alluded to in the Mission Control literature review in the previous chapter, little has been done to quantitatively evaluate this control authority. What has been said recently is that we need to consider augmenting flight controller control authority or transferring it to automated technologies and astronaut crews to confront the challenges—particularly light delay (Korsmeyer and Smith 2008, Landis et al. 2008, Mishkin et al. 2007, Esper and Olsen 2007, Jaap et al. 2006, Korsmeyer et al. 2005, Crocker 2005)⁹²—of future exploration missions. The quote by Korsmeyer and Smith (2008) rightly stresses the importance of identifying the value that such automation technology would provide to the flight controller, but perhaps it is necessary to take a step back and better understand the value of Mission Control's current control authority. After all, Mishkin et al. (2007) pose the following as important issues to pursue:

“What it is to have control authority...What it is to transfer control authority”

Thus, this case study is scoped to evaluate a specific aspect of flight controller control authority in the context of Space Shuttle real-time operations and, to a lesser extent, in the context of a future exploration mission to land on a distant celestial body.

The specific aspect of flight controller control authority analyzed in this study is the control authority that drives the Procedure Rework Process described in the previous chapter. This aspect of flight controller control authority is particularly interesting for two reasons. First, as demonstrated throughout the study, this aspect of flight controller control authority is a key reason for past successes in human spaceflight. Second,

⁹² In fact, some have said that the issue of light delay will necessitate a shift in control authority so dramatic that Mission Control will effectively become “Mission Support.”

procedural issues relate to both the organizational and technical aspects of complex system operations. In other words, they are a subset of the many socio-technical issues that are problematic to address through approaches from the science and engineering science paradigms of research. By contrast, the engineering systems approach taken in this research is intended to provide new insights on exactly these kinds of issues.

6.3 Development of the Dynamic Models for Procedure Rework in Space Shuttle Mission Control

In order to quantitatively identify and evaluate the Space Shuttle Mission Control Procedure Rework Attractor across a range of conditions and human spaceflight mission modes, it was necessary to develop a realistic dynamic model of procedure rework. In this section, the initial steps taken to develop such a model are discussed. These steps initiated an iterative cycle of model-building/refinement, data collection and analysis (described in the next two sections), and model analysis (in other words, deductive-inductive logic cycles). Towards the end of the next chapter, the content of this and the following sections are integrated into a process for safety control structure evaluation and redesign.

Identification of modeling archetypes applicable to procedure rework

As is often the case in modeling efforts, it was possible in this case study to build the core of the model around a set of modeling archetypes in the literature. In this effort, three useful archetypes—described in the following paragraphs—were identified from the System Dynamics literature: the *rework cycle* (Lyneis and Ford 2007, Lyneis et al. 2001, Sterman 2000), *disaster dynamics* (Rudolph and Repenning 2002), and *first-order and pipeline delays* (Sterman 2000, pp. 415-417).

The Rework Cycle

The *rework cycle* is a dynamic structure used in project management modeling. It was developed by Pugh-Roberts Associates (which is now part of PA Consulting Group) in the 1970s and is believed to have appeared with varying degrees of complexity in every project management model created by the System Dynamics community since then (Lyneis and Ford 2007). It has been used in post-project analysis to resolve dozens of contract disputes related to cost and schedule overruns (the total value of these disputes is said to exceed \$4 billion) and in pre-project planning (Lyneis et al. 2001).

The basic structure of the rework cycle is shown in Figure 45 below. Each project that is to be modeled—a project is defined here as a series of tasks that have a specific objective, start and end dates, and funding limits (Lyneis and Ford 2007)—is assumed to be comprised of a certain number of tasks or “Work to Do”. The tasks can either be completed fully and correctly (i.e., they can become “Work Done”) or they can be mistakenly classified as completed fully and correctly (i.e., they can become “Undiscovered Rework”), until it is discovered that they were flawed and need to be redone (i.e., they can go from being “Undiscovered Rework” to “Work to Do”). Thus, the state variables of the system, as shown in Figure 45, are: *Work to Do*, *Undiscovered Rework*, and *Work Done*. The rates at which work is being completed correctly and incorrectly, are affected by the value of *Work to Do* and the *Staff Size*, *Productivity*, and

Work Quality. Similarly, the rate at which rework is discovered and reclassified as work to do is affected by the *Undiscovered Rework* and the *Time to Discover Rework*. In Figure 45, *Staff Size*, *Productivity*, *Work Quality*, and *Time to Discover Rework* are treated as constants (or parameters), which are essentially state variables that remain fixed under the conditions and timescale of the model. However in reality, the parameters in Figure 45 are state variables that are controllable by organizations and thus, they represent the control authority of the organization over the states of *Work to Do*, *Undiscovered Rework*, and *Work Done*. Moreover, there are feedback effects observed and modeled by some that can potentially erode or weaken this control authority (Lyneis and Ford 2007): workforce experience dilution through the addition of workers to a project (i.e., the so-called “Brooks’ Law⁹³”), communication inefficiencies associated with an increase in workforce size, worker burnout associated with prolonged periods of overtime, and higher error rates associated with increased work intensity (i.e., “rushing to get things done”).

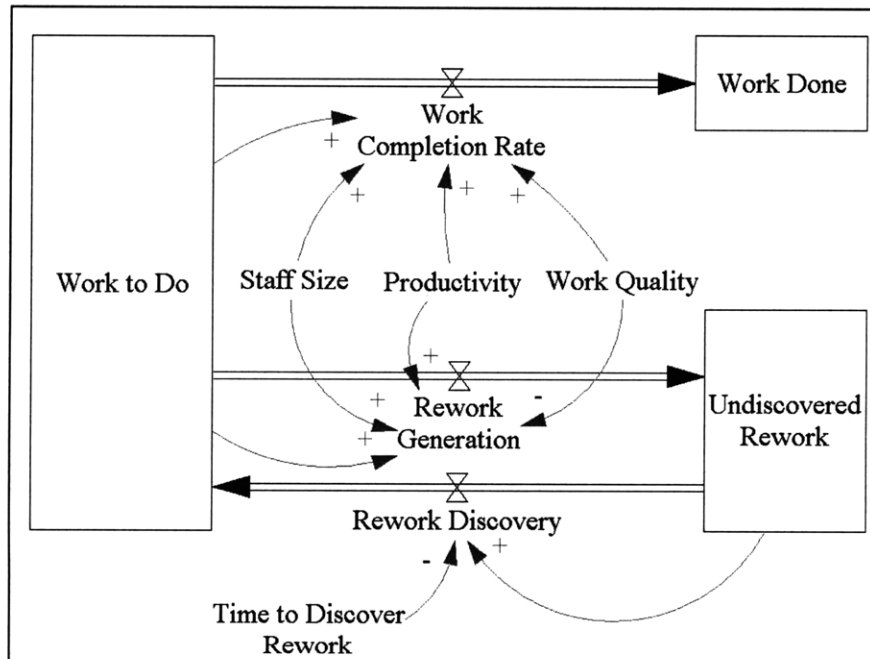


Figure 45. The Rework Cycle dynamic structure (adapted from Lyneis et al. 2001).

The relevance of the rework cycle to safety risk management is that it represents the processes by which “human errors” in system design both occur and are discovered throughout a system development process. The *Work Quality* parameter in Figure 45 implicitly encompasses the inadequate skill-based, rule-based, and knowledge-based behaviors occurring during system design while the *Time to Discover Rework* parameter represents the effectiveness of system reviews and testing in the identification of problems in the design. With several modifications to the basic rework cycle structure in Figure 45, such as those introduced by Dulac (2007) for example, it is possible to demonstrate the effect of organizational decisions on the generation and discovery of

⁹³ See Brooks (1995).

rework during system development and the passage of unresolved rework issues to the operational system.

With that said, the basic rework cycle structure can also be modified to demonstrate how inconsistencies in the planned task executions and disturbance rejections to occur in system operations emerge and are then resolved. Specifically, the behavior associated with the Procedure Rework Process in Mission Control can be captured through modifications to the basic rework cycle structure. Work tasks can be substituted for procedures and the timescale to be modeled can be reduced from the timeframes typical in system development to those of spacecraft flight control. Additionally, detrimental feedback effects relevant to project management such as workforce experience dilution, communication inefficiencies due to increases in workforce size, and workforce burnout would perhaps not need to be modeled due to the short duration of a Space Shuttle flight and the limitations that the flight controller certification process presents to quickly adding flight controllers to the team.

Disaster Dynamics

Rudolph and Repenning (2002) provide a very simple modeling archetype to highlight the potential role of non-novel (i.e., normal and seemingly mundane) disruptions to organizational operations in accidents and organizational collapse. They argue that the link between non-novel disruptions and accidents/organizational collapse are perhaps overlooked due to the attention given to novel disruptions and the naïve assumption that the dynamics associated with non-novel disruptions are intuitive (i.e., “the more there are, the worse things get”). The “central construct” of their model archetype is the concept of an interruption that necessitates a response. Essentially, as the interruptions initially accumulate in a stock of interruptions to be addressed, the outflow of the stock (i.e., the response to the interruptions) is affected. At first, the outflow increases as the level of the stock increases (i.e., the operators increase their performance accordingly), however after a delay, the operators’ ability to perform at the heightened level decreases and thus, the outflow of the stock decreases. Eventually, interruptions accumulate further, leading to a “disaster”.

The obvious analogs for interruptions in the Procedure Rework Process are undiscovered procedures needing rework. As procedures needing rework initially accumulate, the discovery rate of these procedures is likely to increase as well. However, once procedures needing rework have been discovered, the focus of the flight control team must shift (partially at least) to the actual reworking of procedures. As that happens, the ability to discover rework should decrease, leading to the potential accumulation of more undiscovered procedures needing rework, any one of which could potentially be executed, leading to an accident or otherwise adverse incident.

First-Order and Pipeline Delays

First-order delays (Sterman 2000, pp. 415-417) are dynamic structures that regulate the outflow of a stock. Essentially, these structures increase the outflow in proportion to the level of the stock divided by an average outflow or “delay” time (i.e., the stock value will decay exponentially). The fundamental assumption of this structure is that all items in

the stock at any given time will be equally likely to exit the stock, but ultimately some will exit much earlier than the delay time, most will have exited by the delay time, and others will exit much later than the delay time.

In a procedure rework process, the discovery and completion of procedure rework should approximate first-order delayed outflows in operating regimes in which the flight control team's ability to discover and complete rework is not saturated. In such a structure, procedures would flow into stocks of procedures needing rework and procedures being reworked and ultimately remain in those stocks for a certain time on average. Some procedures would exit the stock faster than average while others would exit slower on average, and the overall rates of rework discovery and completion would increase with the overall number of procedures in those stocks.

Pipeline delays (Sterman 2000, pp. 415-416), on the other hand, are structures that regulate the outflow of the stock based on its inflow and a given delay time. Items that enter the stock will remain in it for the given delay time and leave the stock in the same order in which they flowed into it (as if they were moving through a pipe).

For procedure rework processes during missions to Mars or Near-Earth Objects (NEOs) (Landis et al. 2008) with light delays on the order of 10 seconds and higher, the light delay would essentially introduce pipeline delays into the flow of procedures. Changes in spacecraft state that would invalidate certain procedures would not be observable on the ground for the duration of the light delay, and they would become observable in the order that they occur. Additionally, updates transmitted from the ground to the crew would not be observable by the crew for the duration of the light delay and they too would become observable in the order in which they are sent. Thus, for mission types with significant light delays, two pipeline delays would have to be introduced (one for the spacecraft-to-ground flow of information and one for the ground-to-spacecraft flow of information).

Integrating the modeling archetypes applicable to procedure rework

Through integration of the three modeling archetypes described above, the author was able to identify the key state variables and constraints relevant in evaluating the attractor produced by the procedure rework process and to develop a preliminary model of procedure rework. The *Procedures Needing Rework* and *Procedures Being Reworked* stocks were defined as the state variables to be constrained (procedures in these stocks are control flaws that could lead to inadequate control actions during their execution). In a flow structure reminiscent of the standard rework cycle, procedures would flow into the *Procedures Needing Rework* stock from a stock of *Valid Procedures* due to a *Procedure Invalidation Rate*. The procedures in the *Procedures Needing Rework* stock would then flow out of that stock into the *Procedures Being Reworked* stock due to a *Procedure Rework Discovery Rate*. This rate, as stated above, would approximate a first-order delay, however because of the Disaster Dynamics phenomenon, the average outflow or delay time would increase as attention shifts from discovering rework to completing rework (a pair of state variables were thus introduced to track the fraction of resources devoted to each task). Accordingly, the rate of procedures being moved from the *Procedures Being Reworked* to the *Valid Procedures* stock (i.e., the *Procedure Rework*

Completion Rate) would increase as attention shifted from rework discovery to rework completion.

Because of the unpredictable flow of procedures into the *Procedures Needing Rework* stock and the first-order delayed outflow of this stock subject to the Disaster Dynamics phenomenon, it was immediately recognized that the system could not be constrained to the point of zero procedures needing or being reworked at all time. The least hazardous level of constraint that could be hoped for was an equilibrium attractor near values of zero *Procedures Needing Rework* and *Procedures Being Reworked* in the system's phase space.

After preliminary model-building and analysis, the author collected and processed procedure rework data from Space Shuttle missions for model parameter and structure validation. Several key updates to the model structure were made due to discoveries during data processing, and therefore, a full description of the model is provided *after* the data collection and processing summary in the next two sections of this chapter.

6.4 Data Collection

As previously mentioned, there are a number of sources of data to quantitatively characterize procedure rework in Mission Control. Procedure changes occurring during missions and immersive simulations are documented as attachments to flight notes, except in situations in which the procedure changes must be made rapidly and explained to the crew through voice transmission. Once the changes are approved by the Flight Director, the flight note attachment containing the update is taken as written by the FAO and uplinked to the crew as part of an electronic message sent individually or as part of the daily execute package⁹⁴ (Delapp 2008).

With the assistance of a Mission Control FAO (Delapp 2008), the author obtained and processed electronic messages from five Space Shuttle Missions (i.e., STS-97, STS-115, STS-116, STS-117, and STS-120) for procedure update information. Listings of the messages sent to the crew during each mission, along with a record of how (and whether) the author obtained them, are provided in Table 25 to Table 28, Table 48 to Table 53, Table 69 to Table 75, Table 94 to Table 99, and Table 114 to Table 122 of the Appendix 2, respectively. In the remainder of this section, these missions are described.

Brief Overview of the Flights Analyzed

The five Space Shuttle missions analyzed in this case study are described in the paragraphs that follow. Each of these flights involved the deployment or retraction of ISS Solar Array Wings (SAWs). As mentioned in Chapter 5, these deployment and retraction events provide examples of Mission Control's ability to safely⁹⁵ cope with

⁹⁴ Execute packages are sent to the crew at the beginning of each flight day and contain messages produced while the crew was asleep. All execute packages from STS-115 and later missions are available on NASA's website.

⁹⁵ Due to the "unforgiving" environment of low-Earth orbit, the actions taken by Mission Control throughout these missions potentially prevented a number of loss events (e.g., loss of one or more SAWs,

unexpected spaceflight contingencies and they previously had not been mentioned in the literature. Furthermore, due to their relative similarity (when compared to any other group of five missions), these missions, when comparatively analyzed, provide an opportunity to distinguish the effects of high-impact, rare events from the effects of smaller-impact, higher frequency events.

STS-97

The first two of eight ISS SAWs were delivered to the station and deployed on STS-97 in December, 2000. At the time the SAWs were delivered to the space station, the main truss that will ultimately serve as the mounting location of all eight SAWs had yet to be installed—see Figure 46 for a computer rendering of the final ISS configuration and Figure 47 for the ISS configuration as STS-97 first approached the station. Therefore, it was necessary to deploy the first pair of SAWs—referred to as the “P6”⁹⁶ array—at a temporary location.

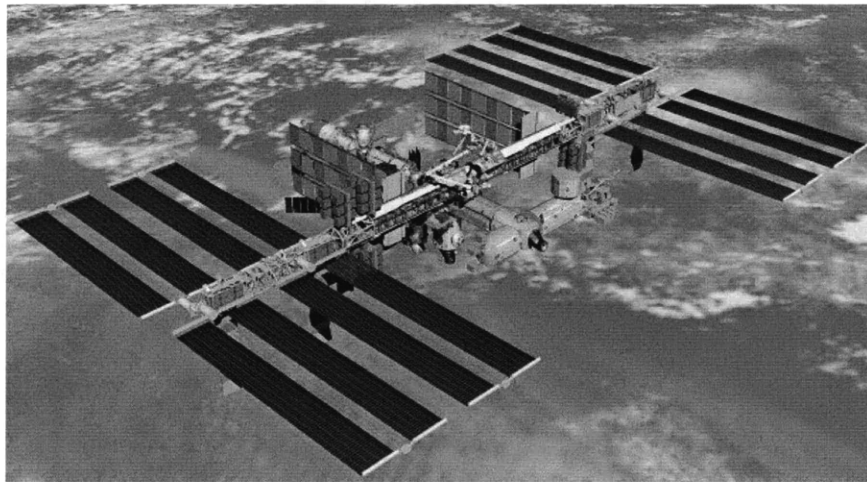


Figure 46. A computer-generated rendering of the anticipated final configuration of the ISS (source: <http://spaceflight.nasa.gov>).

loss of the starboard ISS Solar Alpha Rotary Joint, loss the ISS, loss of a Space Shuttle Orbiter, loss of crew, loss of technical credibility of the human spaceflight program, etc.).

⁹⁶ P6 is an alphanumeric designation of the SAWs' permanent deployment location. The “P” in P6 represents the port side of the space station (with respect to the nominal velocity vector) while the 6 represents six units of measurement from the centerline of the space station.

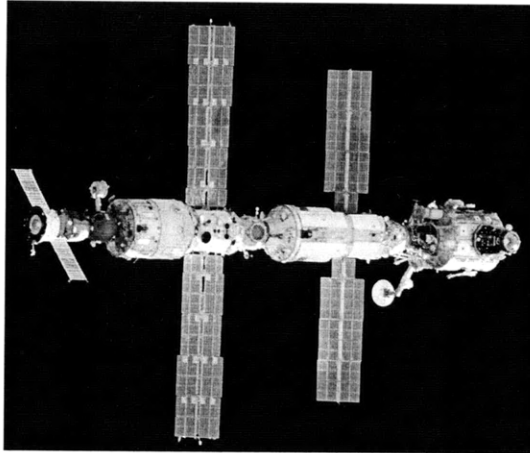


Figure 47. The configuration of the ISS as STS-97 first approached it (source: <http://spaceflight.nasa.gov>).

Deployment of the two SAWs required the unfolding of four 112 foot photovoltaic blanket spans tensioned by wires running the length of each blanket. As the SAWs were deployed, blanket folds stuck together, causing the SAWs to shake dramatically as they unfolded and the tensioning wires jumped off of their guides leaving slack in the tension lines (NASA JSC 2000). Ultimately, the SAWs were successfully deployed after the crew executed modifications to the deployment procedure and manual array tensioning tasks added to the third spacewalk of the mission by flight controllers and MER engineers. The configuration of the ISS once STS-97 left it is shown in Figure 48.

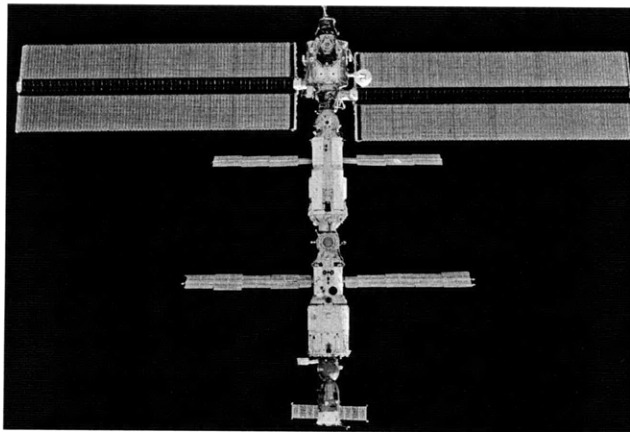


Figure 48. The configuration of the ISS when STS-97 undocked from it (source: <http://spaceflight.nasa.gov>).

STS-115

The second pair of SAWs (i.e., the “P4” array) was delivered to the ISS and deployed on the third post-*Columbia* mission, (i.e., STS-115 in September, 2006). Though STS-97 and STS-115 occurred before and after the *Columbia* Accident, respectively, they shared more similarities than perhaps any pre- and post-*Columbia* mission pair. The primary objective of both missions was delivery and deployment of a pair of SAWs and the same

commander and lead spacewalker participated on the crews of both missions. However, unlike STS-97, STS-115 occurred at a time in the ISS assembly sequence where it could attach a pair of SAWs to their permanent location on the ISS main truss—see Figure 49 for an image of the ISS as STS-115 first approached it. Additionally, STS-115 delivered and activated a Solar Alpha Rotary Joint (SARJ)⁹⁷ on the port side of the truss.

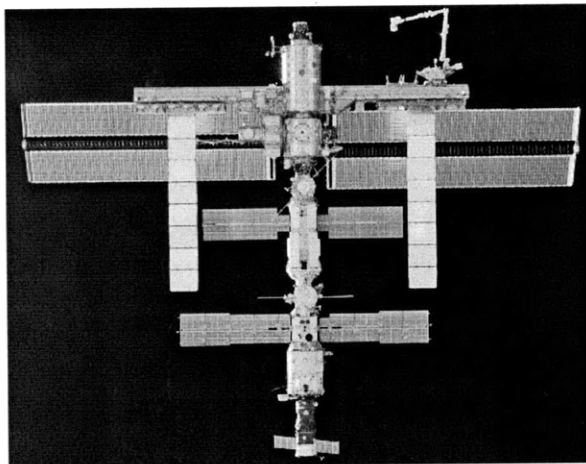


Figure 49. The configuration of the ISS as STS-115 first approached it (source: <http://spaceflight.nasa.gov>).

Though the P4 SAW blanket folds stuck together during deployment as they did on STS-97, modifications to the deployment procedures made during and after the P6 deployment allowed the P4 array deployment to occur much more smoothly. In fact, the spacewalking crew was even able to accomplish a number of “get ahead” tasks (NASA JSC 2006b). The configuration of the ISS when STS-115 undocked from it is shown in Figure 50.

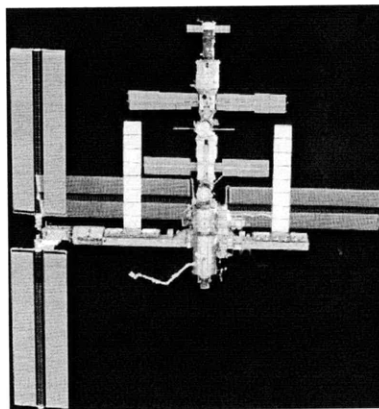


Figure 50. The configuration of the ISS as STS-115 undocked from it (source: <http://spaceflight.nasa.gov>).

⁹⁷ The ISS has a SARJ on each side of the truss. These rotary joints are used to rotate the arrays towards the sun in order to increase the energy output of the arrays.

STS-116

The primary objectives of STS-116—flown in December, 2006—were to reconfigure the ISS power system so that it would accept power from the P4 array instead of P6 array, reconfigure the thermal control system, retract the port side of the P6 array so that the SARJ could rotate the P4 array without obstruction, swap an ISS crewmember with a Shuttle crewmember, and install the P5 truss segment that would ultimately connect the P6 array to the P4 array. When STS-116 arrived at the ISS, the space station's configuration had not changed significantly since STS-115—see Figure 50.

While the crew swap, installation of the P5 segment, and the reconfiguration of the power and thermal systems went relatively smoothly, the retraction of the port side SAW of the P6 array was problematic. As shown in Figure 51, substantial kinks developed in the photovoltaic blankets as they were retracted. Upon recognizing the kinks, Mission Control halted the retraction process and initiated the following actions in an attempt to work the kinks out of the blankets: deploy-retract cycles, Beta Gimbal Assembly (BGA) “wiggles”⁹⁸, and vigorous crew exercise⁹⁹ (NASA JSC 2006d). Because these actions resulted in little progress, Mission Control then instructed the crew of the third spacewalk to physically shake the arrays from one end after they completed their nominally scheduled tasks. A significant portion of the array was retracted through this action; however, full retraction could not be completed before the spacewalk had to be ended. Thus, the MMT extended the mission by one day and added an unscheduled spacewalk to retract the array. During this spacewalk, the crew used makeshift tools that Mission Control instructed them to build to physically manipulate the blanket folds and guide wires until the array was fully retracted—see Figure 52. The configuration of the ISS when STS-116 undocked is shown in Figure 53.

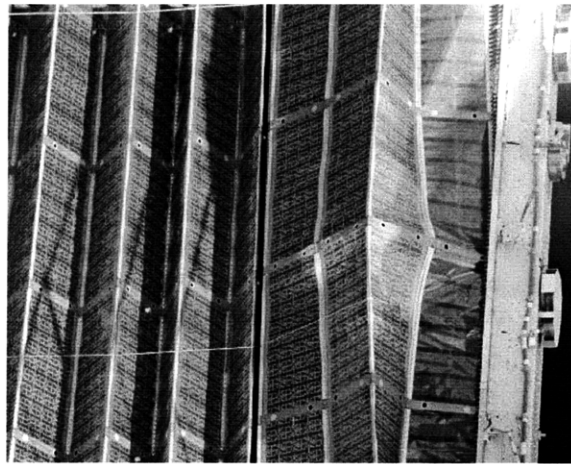


Figure 51. A kink in the port side of the P6 array during retraction (source: <http://spaceflight.nasa.gov>).

⁹⁸ The BGA provides a second axis of SAW rotation—along with the SARJ—for facing the arrays towards the sun. The “wiggles” were small BGA rotations commanded by Mission Control in an attempt to free the kinks.

⁹⁹ It had been noted that the SAWs oscillated slightly whenever the crew exercised on the ISS treadmill. Thus, Mission Control had the crew exercise vigorously in an attempt to remove the kinks.

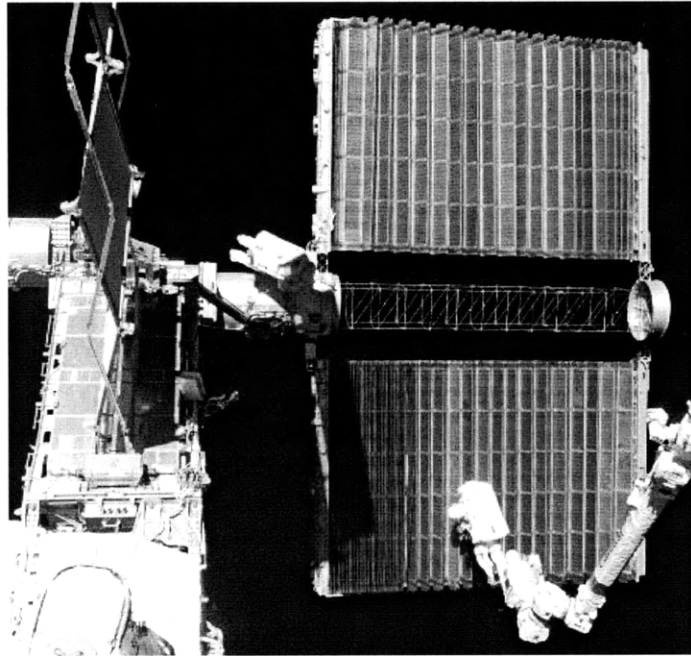


Figure 52. STS-116 astronauts retracting the port side of the P6 SAW during an unscheduled spacewalk (source: <http://spaceflight.nasa.gov>).

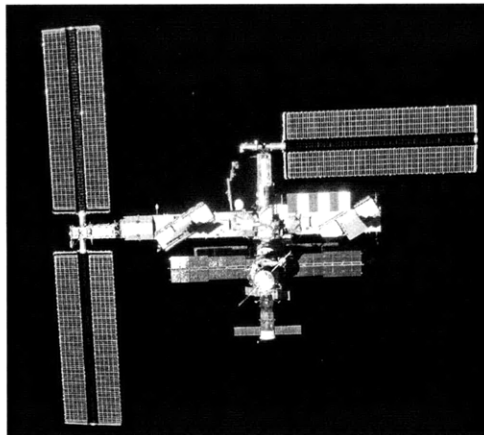


Figure 53. The configuration of the ISS at the conclusion of STS-116 (source: <http://spaceflight.nasa.gov>).

STS-117

The primary objectives of STS-117—flown in June, 2007—were to deliver and activate the starboard SARJ, deliver and deploy the S4 array, swap an ISS crewmember with a Shuttle crewmember, and retract the starboard side of the P6 array. The configuration of the ISS at the beginning of STS-117 was roughly the same as it was at the end of STS-116—see Figure 53. Because Mission Control and the MER had incorporated lessons learned from P6 array problems on STS-97 and STS-116 into the nominal flight plan, all of these objectives were achieved with relatively few problems. However, the mission was not without challenges for flight controllers and MER engineers. A thermal blanket

on the rear of the Orbiter came loose and had to be repaired during a spacewalk, the MMT added an extra spacewalk for ISS “get ahead” tasks, and the ISS developed attitude control problems that led flight controllers to conserve Orbiter consumables so that it could be used for both shuttle and station attitude control for as long as possible (NASA JSC 2007b). The configuration of the ISS at the conclusion of STS-117 is shown in Figure 54.

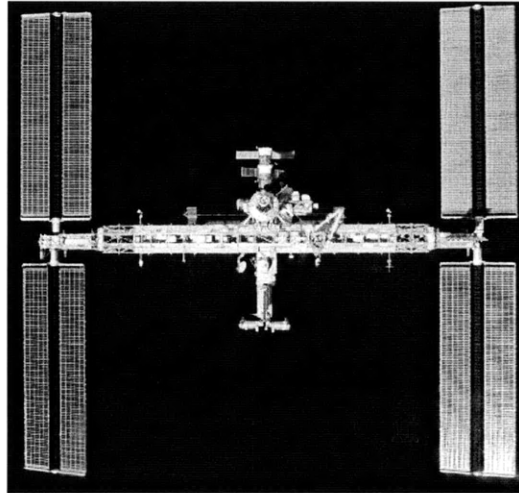


Figure 54. The configuration of the ISS at the conclusion of STS-117 (source: <http://spaceflight.nasa.gov>).

STS-120

The primary objectives of STS-120—flown in October and November of 2007—were to install a new pressurized module on the ISS, move the retracted P6 array to its permanent location on the port side of the main truss and re-deploy it, and swap an ISS crewmember with a Shuttle crewmember. Though STS-118 flew in the interim between STS-117 and STS-120, it did not significantly alter the external configuration of the ISS from the configuration shown in Figure 54¹⁰⁰. In the early stages of the mission, Mission Control decided to have an astronaut inspect the starboard SARJ—which had been vibrating unusually for several weeks—as part of the mission’s second spacewalk. During the inspection, the spacewalker discovered metal shavings in the joint, indicating that the joint was grinding itself. Upon this discovery, Mission Control halted starboard SARJ rotation, added a precautionary inspection of the port SARJ during the third spacewalk, and made plans to do further troubleshooting of the starboard SARJ on the fourth spacewalk (NASA JSC 2007d). While the inspection of the port SARJ uncovered no issues with that joint, additional inspection of the starboard SARJ was canceled after the re-deployment of the P6 SAWs resulted in a tear in one of the photovoltaic blankets¹⁰¹—see Figure 55. After deliberation, Mission Control and the MER re-planned the fourth spacewalk to include a repair of the SAW. For this repair, Mission Control and the MER instructed the crew on how to construct makeshift tools. Additionally, they developed a

¹⁰⁰ STS-118 installed the S5 truss segment that will ultimately connect the S4 and S6 arrays and brought supplies to the ISS. STS-119, which is slated to occur in 2009, is to deliver and deploy the S6 SAWs.

¹⁰¹ Incidentally, the tear occurred in the SAW that was retracted during STS-116.

set of procedures to have a spacewalking astronaut ride on the end of the OBSS attached to the end of the SSRMS in order to reach the tear. Ultimately, the spacewalking astronaut fixed the tear—see Figure 56 and Figure 57—and further troubleshooting of the starboard SARJ was deferred to later missions. The external configuration of the ISS at the conclusion of STS-120 is shown in Figure 58.

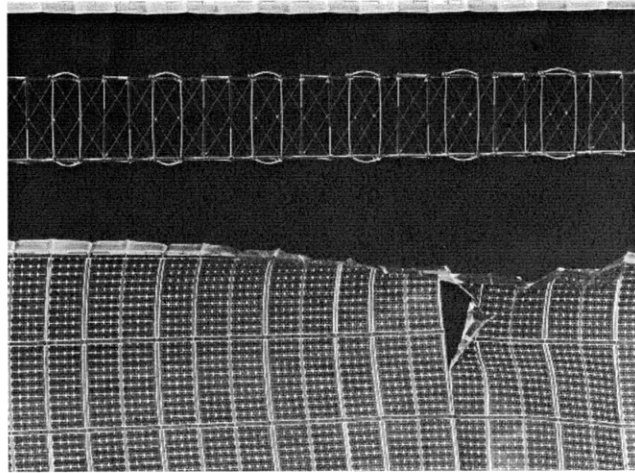


Figure 55. The tear that developed in photovoltaic blanket of the P6 SAW (source: <http://spaceflight.nasa.gov>).

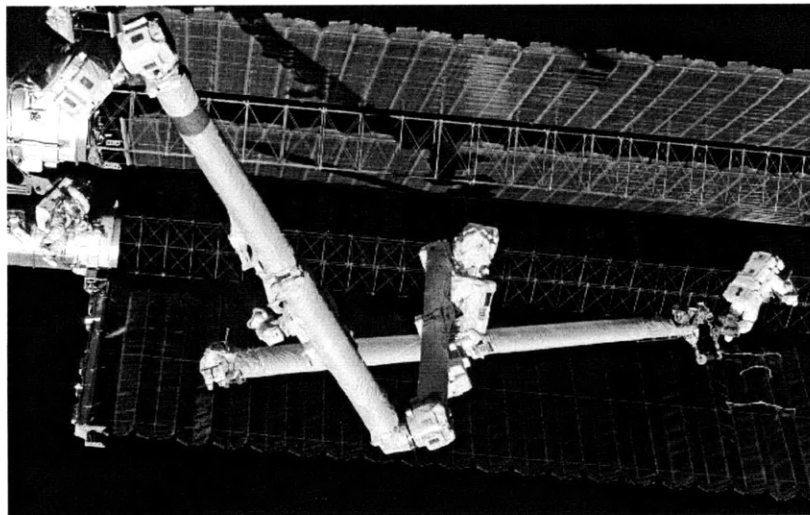


Figure 56. An astronaut "rides" on the end of the OBSS to repair a tear in the P6 SAW (source: <http://spaceflight.nasa.gov>).

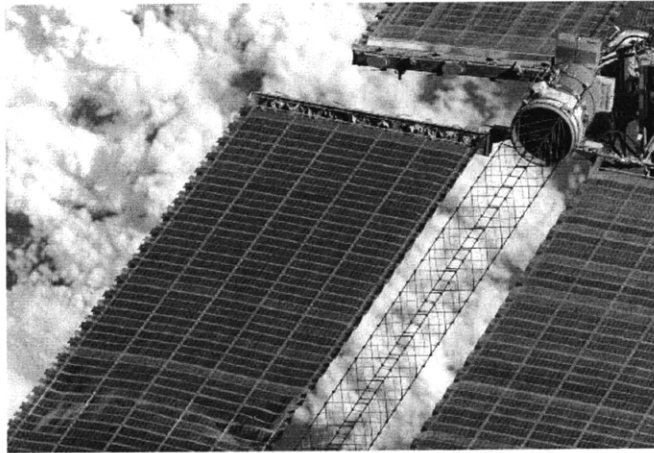


Figure 57. The P6 SAW after the repair of the tear (source: <http://spaceflight.nasa.gov>).

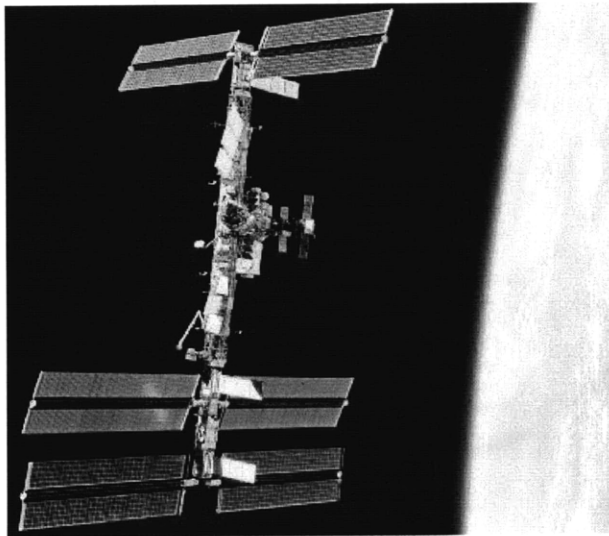


Figure 58. The external configuration of the ISS at the conclusion of STS-120 (source: <http://spaceflight.nasa.gov>).

6.5 Data Processing

In this section, the steps that the author took to investigate the electronic messages from STS-97, STS-115, STS-116, STS-117, and STS-120 are described.

Update Designation

Instances of procedure updating during these missions were identified through several reviews of the electronic messages by the author. The following considerations were relevant in determining what would or would not be classified as an instance of procedure updating:

- Updates that were deemed to have been performed mostly by ISS Mission Control were disregarded in order to keep the focus of the study on the performance of

Space Shuttle Mission Control. However, with that said, updates that were deemed to involve significant contributions from both ISS and Space Shuttle Mission Control were included in the study.

- Updates to the list of items to be transferred between the Space Shuttle and ISS were not considered unless circumstances warranted an “unusual” change to the transfer list. The transfer list is nominally changed dozens, if not hundreds of times over the course of a mission and thus an analysis of these changes, though interesting in its own right, would detract from the analysis of the far less frequent and unexpected changes that occur during a mission.
- Updates to supply water and waste water dumps were not considered unless unexpected events necessitated fundamental changes to the procedure. As is the case with the transfer list, the water dump procedures are executed and updated over a dozen times in a given mission with many “fill-in-the-blank” aspects of the procedure changing as expected from execution to execution.
- Multiple updates of the same procedure at the same time (i.e., in the same electronic message) were counted as a single update unless there were fundamentally different rationales for the various updates in the procedure.

Each instance of procedure updating identified by the author was first designated with an update number and the following information was cataloged: the flight day that the update was issued, the title of the altered procedure, the number of the electronic message in which the update was announced, the rationale for the update, and the console position responsible for the update, all as judged by the author. These designations are provided in Appendix 2 for each respective mission in the following tables: Table 29 to Table 34, Table 54 to Table 58, Table 76 to Table 81, Table 100 to Table 104, and Table 123 to Table 133. A summary of the number of updates identified for these missions is provided below in Table 7.

MISSION	NUMBER OF UPDATES	MISSION DURATION (DAYS)	UPDATES PER DAY
STS-97	93	10.832	8.59
STS-115	63	11.796	5.34
STS-116	86	12.865	6.68
STS-117	66	13.841	4.77
STS-120	135	15.099	8.95
Total	443	64.435 (total) 12.887 (average)	6.88 (average)

Table 7. Procedure update statistics for the Space Shuttle missions analyzed.

Later, the author made and recorded judgments—based on information in the electronic messages and other information available on NASA’s website (e.g., mission status reports, pre-mission flight plans, anomaly briefings, etc.)—of the flight days on which each update was identifiable, issued, and was to be executed. The following considerations were relevant in judging which flight day the procedures were deemed identifiable, issued, and to be executed:

- Updates were deemed to have been issued on the flight day that the electronic message announcing them was sent to the crew.
- Updates that were deemed to have been identifiable at launch were classified as being identifiable on Flight Day 0.
- Refinements and rework of previously sent updates were deemed to have been identifiable on the flight day that the original update was sent.
- The flight day designated for when each update was to be executed is the flight day that the procedure update was expected to be executed when it was issued. These designations usually depended on the flight day the procedures were scheduled in the pre-flight version of the flight plan (NASA JSC 2006a, NASA JSC 2006c, NASA JSC 2007a, NASA JSC 2007c) and did not depend on whether a procedure update's execution time was ultimately delayed or cancelled after the update was issued.
- Whenever there was an update to a contingency procedure that was not planned to be executed, but immediately available for execution if needed, the designation for the execution flight day was the same as the update issue flight day.

These designations are provided in Appendix 2 in Table 35 to Table 37, Table 59 to Table 60, Table 82 to Table 84, Table 105 to Table 106, and Table 134 to Table 137. Additionally these tables include the number of days between when an update was identifiable and when it was updated as well as the number of flight days between when it was updated and when it was to be executed.

This information for the sum of all missions studied is also depicted in Figure 59. The distributions shown in this figure suggest a zero-to-two flight day time horizon on the procedure rework process (i.e., the procedures that are primarily updated are the ones that must be executed within zero-to-two flight days of the current flight day). If the flight control team was attempting to update every procedure that needed updating at all times, then one would expect the distributions to be reversed. The procedural problem would "wait" a short time after becoming identifiable to be discovered, be updated, and then "wait" up to fifteen flight days before being executed. Instead, the procedural problems "wait" for up to fifteen flight days to be updated and then "wait" for only an additionally zero-to-five (but often less than two) flight days to be executed. As hinted at above, this discovery led to a fundamental update in the procedure flow of the model. This model update will be described in the next section.

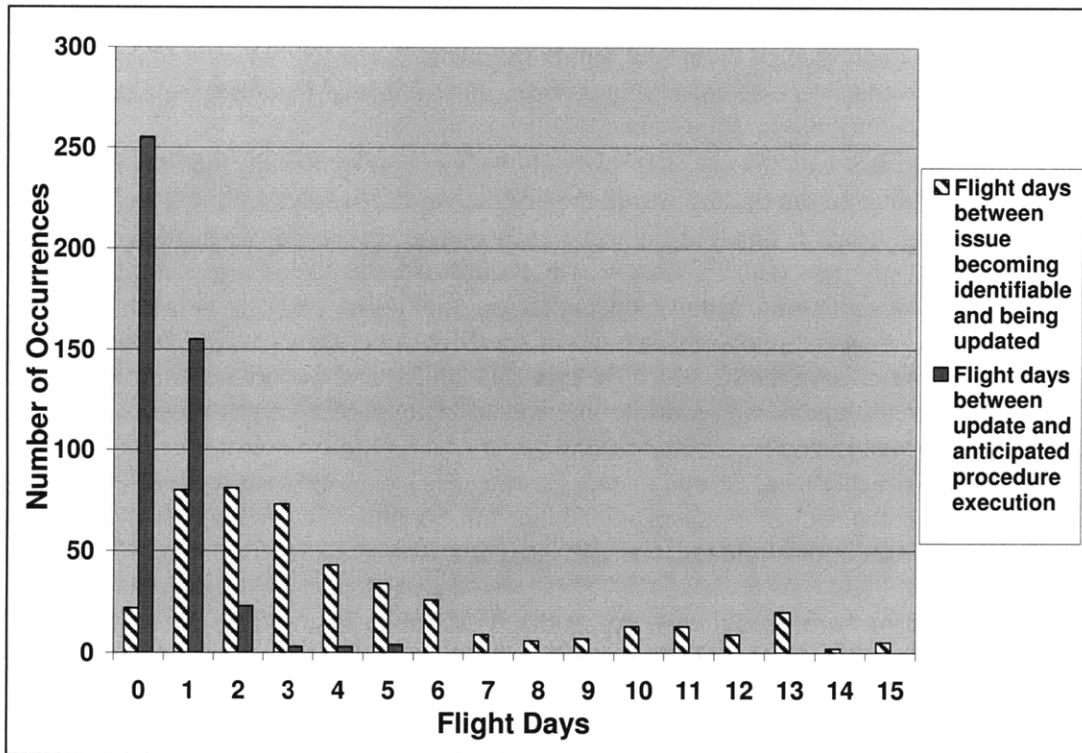


Figure 59. Histogram of time gaps between when updates were identifiable and issued and when updates were issued and expected to be executed.

Rationale Categorization

The author, in addition to providing the specific rationales for each procedure update as mentioned above, developed a set of general update rationale categories for qualitative analysis of the causes of procedure rework. The specific categories chosen by the author are meant to exhaustively capture the updates identified in the case study without: 1) being so general that they “abstract away” useful information on the cause of the update (and its potential remedy) and 2) being so specific that they are too numerous and thus too cumbersome to track. As a result, the categories—though probably not mutually exclusive—should link each update to a particular cause that provides clues on how such an update can be mitigated or avoided in future missions.

The general categories can be broken down into two types of rationale: update rationales due to the downside of uncertainty and update rationales due to the upside of uncertainty (i.e., update rationales due to opportunity exploitation). Recall from Chapter 1 that uncertainty has the potential to lead to undesirable, unexpected events (i.e., risks) as well as the potential to lead to desirable, unexpected events (i.e., opportunities).

The update rationales due to the downside of uncertainty are categorized as follows:

- *Task Deferral or Reprioritization*: Procedures were changed due to the deferral or reprioritization of scheduled tasks.

- *Equipment List Revision*: The equipment list for a procedure was changed or procedures were changed to alter to configuration of equipment to be used for a procedure. For example, the SRMS was required for steps added to a procedure and therefore, procedural steps were added to get the SRMS into the right configuration.
- *Consumable Management Replanning*: A procedure was changed to provide the necessary consumables (e.g., oxygen, water, battery power, etc.) for it. For example, tasks were added to an EVA increasing its duration, necessitating the usage of a different set of batteries or an oxygen recharge from shuttle airlock umbilicals.
- *Unaccounted for Inhibits*: A procedure is changed to add a previously unaccounted for safety inhibit. For example, a step is added to an EVA procedure to ensure that the power to a power connector that a spacewalking astronaut will work with is disabled.
- *Internal Inconsistencies in the Procedure*: The procedure was changed because if it were to be completed from beginning to end as written under the assumed conditions, contradictory steps in the procedure would have prevented the procedural goals from being accomplished or caused other problems.
- *Sensor "Failure" or Bias*: A sensor used to observe Space Shuttle processes "failed" or degraded in a manner that necessitated the procedure update. Failures or degradations of ISS sensors were not covered by this category.
- *Actuator "Failure" or Degradation*: A hardware component used to complete Space Shuttle processes "failed" or degraded in a manner that necessitated procedure updates. Failures or degradations of ISS hardware components (e.g., SARJ) were not covered by this category.
- *Unexpected Software Behavior*: Procedures were changed to cope with unexpected behavior of Space Shuttle software systems. For example, the Payload General Support Computers (PGSCs), which are laptops used for shuttle operations, unexpectedly and repeatedly "crashed," necessitating the procedure updates.
- *Launch Damage (actual or suspected)*: Procedures were updated to inspect or fix damage to the Orbiter or its payloads during launch.
- *Crew Procedural Slips*: An update was due to the astronaut crew's improper execution of a correct procedure.
- *Typos and Omissions*: An update was needed to correct spelling or grammar errors or to insert small procedural items that were mistakenly excluded.
- *Inadvertent Deletion of Steps*: An update was needed to insert procedural steps that were mistakenly deleted in a previous update before or during the mission.
- *Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)*: Procedures had to be updated because an item was in an unexpected stowage location or configuration.
- *Inconsistency between Items Expected to be Launched and Items Actually Launched*: Procedures had to be changed because an item was launched other than what was assumed to be launched in the procedures or an expected item was not launched.

- *Unanticipated Environmental/ISS Conditions (e.g., temperatures)*: Unanticipated environmental or ISS conditions led to changes to the procedures that the Space Shuttle crew must accomplish in order to complete their mission objectives

Similarly, the update rationales due to the upside of uncertainty (i.e., opportunity exploitations) are categorized as follows:

- *“Get-Ahead” Tasks Scheduled*: Procedures were changed to allow the crew to perform tasks beyond what was originally scheduled for them (i.e., tasks to perform when they are "ahead of schedule"). In many instances, "Get-Ahead" tasks are tasks assigned to future crews, however, by having the current crew complete them, the Space Shuttle/ISS programs can "get ahead" of schedule.
- *Consumable Management Optimizations*: Procedures were changed to decrease/increase consumable usage in an advantageous manner.
- *Use of Shuttle Resources to Counteract ISS Problems*: Procedures were changed to allow Space Shuttle resources to be used to address an unexpected problem on the ISS. For example, a procedure was created or changed to allow the Space Shuttle to control the attitude of the docked Space Shuttle/ISS system during ISS attitude control system malfunctions.
- *Proactive Contingency Preparation and/or Hazard Investigation*: Procedures were updated to provide the crew with contingency instructions before they would be needed or procedures were updated to allow the crew to investigate a potentially hazardous condition that does not necessarily interfere with mission priorities (e.g., the port SARJ inspection).
- *Procedure Nominally Updated in Real-time*: Certain procedures were nominally updated during a mission because it is understood that the flight controllers will know the best manner to conduct the procedure at the appropriate time. As an example, a landing procedure required the crew to use one of two or more redundant systems and the flight controllers were only able to determine the best one to use shortly before landing.
- *Crew Comfort Optimizations*: Procedures were changed to make the crew more comfortable.
- *Procedure Efficiency Optimization*: Procedures were changed to increase the efficiency with which they could be completed given the circumstances of the mission.
- *Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch*: Procedural changes were made before launch, but after the procedures had been printed in the procedure books that were loaded onto the Space Shuttle.

Tallies of the number of updates attributed to each categorization are provided in Table 8 and Table 9 for categorization due to the downside and upside of uncertainty, respectively. Furthermore, categorizations of all updates using the above categories are provided in Table 38 to Table 44, Table 61 to Table 65, Table 85 to Table 90, Table 107 to Table 110, and Table 138 to Table 147. These tables also include the author's

interpretation of the detailed rationale for the update as well as the discrete event rationale categorizations (if applicable).

RATIONALE CATEGORIZATION	TOTAL NUMBER OF UPDATES	OVERALL PERCENTAGE OF UPDATES
Task Deferral or Reprioritization	11	2.5%
Equipment List Revision	55	12.4%
Consumable Management Replanning	15	3.4%
Unaccounted for Inhibits	19	4.3%
Internal Inconsistencies in the Procedure	14	3.2%
Sensor "Failure" or Bias	13	2.9%
Actuator "Failure" or Degradation	49	11.1%
Unexpected Software Behavior	18	4.1%
Launch Damage (actual or suspected)	19	4.3%
Crew Procedural Slips	2	0.5%
Typos and Omissions	29	6.5%
Inadvertent Deletion of Steps	1	0.2%
Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)	14	3.2%
Inconsistency between Items Expected to be Launch and Items Actually Launched	5	1.1%
Unanticipated Environmental/ISS Conditions (e.g., temperatures)	49	11.1%
Total updates due to the downside of uncertainty	313	70.7%

Table 8. Number of updates associated with each update rationale categorization relating to the downside of uncertainty.

RATIONALE CATEGORIZATION	TOTAL NUMBER OF UPDATES	OVERALL PERCENTAGE OF UPDATES
"Get-Ahead" Tasks Scheduled	25	5.6%
Consumable Management Optimizations	5	1.1%
Use of Shuttle Resources to Counteract ISS Problems	6	1.4%
Proactive Contingency Preparation and/or Hazard Investigation	20	4.5%
Procedure Nominally Updated in Real-time	20	4.5%
Crew Comfort Optimizations	6	1.4%
Procedure Efficiency Optimization	9	2.0%
Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch	39	8.8%
Total updates due to the upside of uncertainty	130	29.3%

Table 9. Number of updates associated with each update rationale categorization relating to the upside of uncertainty.

The discrete event rationale categorizations identify the updates due to the “novel” or rare (i.e., occurring less than two or three times per mission) events that create the need for a large number of procedure updates at a time. As mentioned earlier, the similarities between the missions studied allow one to distinguish the effects of these discrete events relative to the more frequent events that require fewer updates. As will be shown in the next section, such a distinction is important in characterizing the underlying dynamics of procedure rework. Referring back to Table 7, it is clear that STS-115 and STS-117 have far fewer total updates and updates per day than the other missions even though STS-115 was very similar to (and probably more complex than) STS-97 and despite the fact that STS-117 could be thought of as a hybrid re-enactment of STS-97, STS-115, and STS-116. These differences in update rates are due to the discrete events on STS-97, STS-116, and STS-120. While the ISS SAW deployment, retraction, and redeployment problems were inherent to the design, manufacturing, or pre-flight storage of the SAWs and had to be dealt with during each mission, they respectively were first encountered operationally during STS-97, STS-116, and STS-120, thus leading to the higher updates rates on those missions. As a result of the analysis, the following discrete events were identified:

- *P6 SAW Deploy Problems*: This discrete event designation relates to the SAW deploy problems that began on Flight Day 4 of the STS-97 mission.
- *“Get Aheads”*: Much to the author’s surprise, discrete events related to the ISS SAWs did occur on STS-115 and STS-117. However, these discrete events were not due to problems related to SAW deployment/retraction, but to the opportunities that arose to complete extra tasks after the smoother-than-expected deployment/retraction operations on these flights. On Flight Day 5 of STS-115 a spate of “Get-Ahead” tasks were added to the third spacewalk after the highly successful completion of the first two spacewalks. On Flight Day 4 of STS-117

the MMT instructed Mission Control to perform an additional spacewalk full of “Get-Ahead” tasks after the first spacewalk.

- *P6 SAW Retract Problems*: This discrete event designation relates to the P6 port SAW retraction problems that began on Flight Day 5 of the STS-116 mission.
- *OMS Pod Blanket Tear*: This discrete event designation relates to the tear that developed in an OMS Pod thermal blanket during the launch of STS-117. It includes updates to enable the Orbiter thermal shielding inspection tasks added after the discovery of the tear and updates associated with an EVA task to repair the blanket.
- *ISS Attitude Problems*: This discrete event designation relates to the attitude control problems that the ISS developed during the STS-117 mission. Space Shuttle Mission Control’s response to these problems was to use the Space Shuttle to control attitude of the docked Space Shuttle/ISS system and to conserve consumables so that the Space Shuttle could stay at the ISS and help it maintain attitude control for as long as possible.
- *SARJ Grinding Problems*: This discrete event designation relates to the starboard SARJ grinding problems that the MMT first chose to address on Flight Day 4 of the STS-120 mission (i.e., when the MMT decided that the starboard SARJ would be inspected). Included in this category of updates are updates related to the precautionary inspection of the port SARJ and the troubleshooting tasks that were ultimately cancelled when it was determined that the P6 SAW should be fixed instead.
- *P6 SAW Redeploy Problems*: This discrete event designation relates to the P6 SAW redeployment problems that began on Flight Day 8 of the STS-120 mission.

Table 10 below contains a summary of the number of updates caused by the discrete events.

Flight	Discrete Events	Resulting Updates (without Refinements)	Resulting Updates (including Refinements)
STS-97	P6 SAW Deploy Anomaly	15	17
STS-115	“Get Aheads”	8	8
STS-116	P6 SAW Retract Anomaly	20	26
STS-117	OMS Pod Blanket Tear	10	10
	“Get Aheads”	17	17
	ISS Attitude Anomaly	7	7
STS-120	SARJ Grinding Anomaly	21	23
	SAW Redeploy Anomaly	37	50
Total		135	158
Percent of Total Updates		30.47%	35.67%

Table 10. Summary of the number of procedure updates due to discrete events.

6.6 Model Description

The final versions of the procedure rework models that were developed in this case study are described in this section. Additionally, the model testing and calibration philosophy and approach adopted by the author for this study are detailed.

Model Structure

As alluded to in section 6.3, the core stock and flow structure of the non-light delayed procedure rework model was initially derived from the rework cycle, disaster dynamics, and first-order delay dynamic structure archetypes. However, as mentioned in section 6.5, the discovery of a zero-to-two day time horizon on the Procedure Rework Process led to a significant alteration of the flow structure. The final form of the basic flow structure is shown in Figure 60 and each of the numbered flows is described in Table 11.

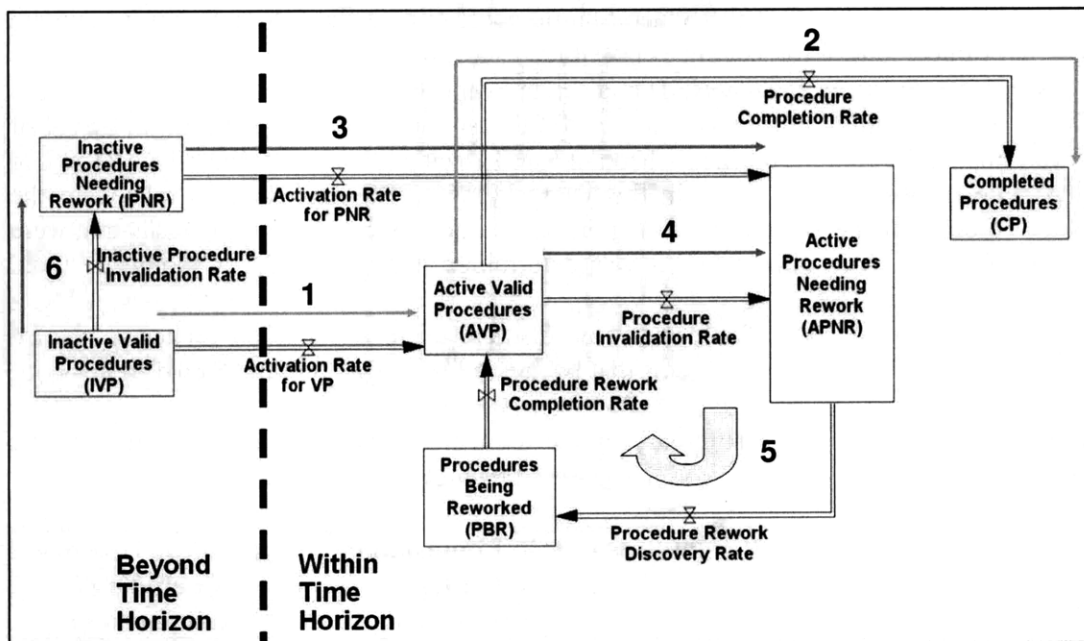


Figure 60. The core stock and flow structure of the procedure rework models.

FLOW NUMBER	DESCRIPTION
1	Before the mission starts, all valid procedures are in the <i>Inactive Valid Procedures</i> stock, which resides beyond the time horizon. As the mission begins and progresses, procedures roll into the time horizon of the procedure rework process (i.e., they flow into the <i>Active Valid Procedures</i> stock due to what the author refers to as an <i>Activation Rate for Valid Procedures</i>). All invalid active procedures (including contingency procedures that are not expected to be used) should become active by the time the end of the mission rolls into the time horizon of the Procedure Rework Process.
2	As the mission progresses, procedures that are to be completed (contingency procedures typically do not fall into this category) move from the <i>Active Valid Procedures</i> stock to the <i>Completed Procedures</i> stock as they are completed.
3	Just as there inactive valid procedures that are activated throughout the flight, so too are there inactive procedures needing rework. These procedures initially reside in the <i>Inactive Procedures Needing Rework</i> stock and flow into the <i>Active Procedures Needing Rework</i> stock as their anticipated execution date rolls into the time horizon.
4	As the mission progresses, a portion of the active valid procedures are invalidated, flowing from the <i>Active Valid Procedures</i> stock to the <i>Active Procedures Needing Rework</i> .
5	Upon recognizing procedures in the <i>Active Procedures Needing Rework</i> stock, the flight controllers move these procedures into the <i>Procedures Being Reworked</i> stock before ultimately reinserting them into the <i>Active Valid Procedures</i> stock. Reworked procedures that ultimately will need to be refined or iterated, effectively work their way into Flow 4 immediately after exiting this flow.
6	Due to the highly coupled nature of the procedures, it is often the case that an incident or even a particular procedure update solution will invalidate multiple procedures. Some of these additional procedures invalidated reside beyond the time horizon at the moment that they are invalidated (e.g., a procedure to be executed on Flight Day 10 is invalidated on Flight Day 3), and thus, they flow from the <i>Inactive Valid Procedures</i> stock to the <i>Inactive Procedures Needing Rework</i> stock.

Table 11. A description of the procedural flows in the core stock and flow structure of the procedure rework models.

Acceptance of this structure requires the following noteworthy assumptions:

- *Procedures needing or being reworked are not executed until they are fully reworked:* While it is reasonable to suggest that procedures needing or being reworked do get executed in reality (and perhaps create problems that lead to more procedure invalidations), it is not clear how one could determine when an invalid procedure is executed and its ultimate impact from the data analyzed by the author (if a procedure is known to be invalid at the time of its

execution, it most likely would not be executed as written). The type of retroactive or experimental study necessary to estimate the number of invalid procedures executed and their tendency to create subsequent procedural invalidations is left to future work. As it is, the effects of the execution of invalid procedures are implicitly addressed by the *Baseline Procedure Invalidation Rate* parameter in the models used for this case study.

- *All procedures created during the procedure rework process exist at the start of the simulation and all other procedures are conserved throughout the simulation:* Though procedures are created¹⁰² and cancelled over the course of the mission, the presence of sources and sinks in the structure (for procedure creation and cancellation, respectively) would have complicated the relevant phase portraits of the system, making it more difficult to interpret the behavior of the procedure rework attractor. Additionally, the alternative to eliminate the sources and sinks by creating extra stocks for procedures to be created and cancelled would have unnecessarily complicated the flow structure. As it is, cancelled procedures, which are not necessarily invalidated, effectively accumulate in the *Active Valid Procedures* stock of the model, and procedures to be created effectively reside beyond the time horizon as inactive procedures before they are created. In both cases, flight controller behavior is not appreciably altered by the presence of procedures yet to be created and cancelled procedures in the structure.
- *Each procedure is equally “important”:* The allocation of resources to rework completion vis-à-vis rework discovery is based purely on the number of procedures in the *Procedures Being Reworked* stock. In reality, some procedures will require more resources than others to rework and therefore lead to a greater attention shift away from rework discovery. This effect could be addressed in future work through numerical weighting of procedures being reworked. As it is, the necessary allocation of resources per procedure being reworked is assumed to average out over the simulation time.
- *Each procedure in a given stock is as likely as any of the other procedures in the same stock to exit the stock at each time step, regardless of its order of entry into the stock (i.e., there are no pipeline delays in this structure):* In reality, there are some aspects of flight control that may affect the order in which procedures are activated, invalidated, identified as needing rework, and corrected (e.g., the order in which the spacecraft automation logs spacecraft faults). However, the priority and complexity of procedures relative to each other will on the whole lead to instances of procedures being activated and reworked much faster or slower than others and instances of certain procedures being reworked in orders other than which they were invalidated (i.e., behavior approximating a first-order delay).

In addition to this core stock and flow structure, each version of the procedure rework model contains a separate flow structure to create the disaster dynamics or “attention shifting” effect that occurs as flight controllers focus more and more heavily on

¹⁰² Refer to Table 46, Table 67, Table 92, Table 112, and Table 149 of Appendix 2 for listings of procedures created during the procedure rework process.

completing rework as more procedures needing rework are discovered. This flow structure contains two stocks with a sum total value of unity: *Fraction of Flight Controller Resources Devoted to Rework Discovery* and *Fraction of Flight Controller Resources Devoted to Procedure Rework*. The values of these two stocks affect the *Time to Discover Procedure Rework* and *Time to Complete Procedure Rework*, respectively.

Finally, each version of the model contains a stock of *Total Procedures Reworked* to track the number of procedure updates issued.

Basic Procedure Rework Model

The Basic Procedure Rework Model was used in this case study to examine the fundamental characteristics of the Space Shuttle Mission Control Procedure Rework Attractor. The complete stock and flow structure of this model is depicted in Figure 61. The parameters used to regulate the flows in this model are described in Table 13. The baseline values for these parameters were derived from the model testing and calibration process. These approaches for parameter baseline value determination are described in the next section. The information necessary to replicate this model fully is documented in Appendix 3.

PARAMETER	DESCRIPTION
Active Procedure Invalidation Rate During Discrete Event	This parameter defines the number of procedures in the <i>Active Valid Procedures</i> stock that would flow in the <i>Active Procedures Needing Rework</i> stock during a discrete event. This parameter was only used for special simulation runs in this case study and thus its baseline value is 0 procedures per minute.
Baseline Flight Controller Rework Recognition Delay	This parameter defines the average rate at which procedures in the <i>Active Procedures Needing Rework</i> stock would be discovered if all available flight controller resources were devoted to rework discovery. The baseline value of this parameter is 30 minutes.
Baseline Procedure Invalidation Rate	This parameter defines the steady state rate (i.e., the rate without discrete events) at which procedures flow from the <i>Active Valid Procedures</i> stock to the <i>Active Procedures Needing Rework</i> stock. Its baseline value is 0.00069 procedures per minute.
Baseline Time to Complete Procedure Rework	This parameter defines the average rate at which procedures in the <i>Procedures Being Reworked</i> stock would be completed if all available flight controller resources were devoted to rework completion. The baseline value for this parameter is 200 minutes.
Inactive Procedure Invalidation Rate During Discrete Event	This parameter defines the number of procedures in the <i>Inactive Valid Procedures</i> stock that would flow in the <i>Inactive Procedures Needing Rework</i> stock during a discrete event. This parameter was only used for special simulation runs in this case study and thus its baseline value is 0 procedures per minute.
Mission Duration (in days)	This parameter defines the length of this mission in days. The baseline value for this parameter is 12.9 days, which was the average mission duration for the flights studied.
Procedure Completion Fraction for Mission	Due to the fact that not all valid procedures are completed in a given mission (e.g., contingency procedures, cancelled procedures, etc.), this parameter is needed to determine what fraction or percentage of procedures will be completed during the mission. The baseline value for this dimensionless parameter is 0.
Procedure Completion Time	This parameter defines the average time it takes to complete procedures. The baseline value for this parameter is 10 minutes.
Procedure Rework Time Horizon	This parameter defines the rate at which inactive procedures (both valid and invalid) are activated. Nearly all inactive procedures should be activated by the time that the simulation time plus this parameter equals the mission duration time. The baseline value for this parameter is 2000 minutes.
Resource Fraction per Procedure Reworked	This parameter defines the desired fraction or percentage of flight controller resources that should be devoted to procedure rework for each procedure in the <i>Procedures Being Reworked</i> stock. The baseline value for this parameter is 20% per procedure.

Table 12. Description of the parameters in the Basic Procedure Rework Model (Part 1 of 2).

PARAMETER	DESCRIPTION
Rework Completion Time Attention Shifting Factor	This parameter defines the factor of increase in average procedure rework completion time that would result from the shifting of all available flight controller resources away from procedure rework. The baseline value for this dimensionless parameter is 1, and thus with this value, procedure rework time would increase by a value equivalent to the <i>Baseline Time to Complete Procedure Rework</i> (i.e., it would double relative to the baseline completion time).
Rework Propagation Factor	This parameter regulates the flow of procedures from the <i>Inactive Valid Procedures</i> stock to the <i>Inactive Procedures Needing Rework</i> stock. It defines the relative proportion of this flow to the flow of procedures from the <i>Procedures Being Reworked</i> stock to the <i>Active Valid Procedures</i> stock (i.e., it defines the proportion of rework propagated beyond the time horizon). The baseline value for this dimensionless parameter is 0.605 or 60.5%.
Rework Recognition Delay Attention Shifting Factor	This parameter defines the factor of increase in average procedure rework discovery time that would result from the shifting of all available flight controller resources away from rework discovery. The baseline value for this dimensionless parameter is 1, and thus with this value, procedure rework time would increase by a value equivalent to the <i>Baseline Flight Controller Rework Recognition Delay</i> (i.e., it would double relative to the baseline rework discovery time).
Startup Delay	This parameter defines the time that the procedure rework process effectively starts after launch. It accounts for key differences between launch/post-launch operations and orbit operations, as well as the time it takes to configure the equipment the crew needs to receive electronic messages from the ground (e.g., printer). The baseline value for this parameter is 520 minutes.
Time of Discrete Event	This parameter defines the time at which a discrete event occurs. This parameter was only used for special simulation runs in this case study and thus its baseline value is 100 minutes.
Time to Shift Focus	This parameter defines the average time that it takes to shift resources to or away from rework discovery. The baseline value for this parameter is 1 minute.

Table 13. Description of the parameters in the Basic Procedure Rework Model (Part 2 of 2).

Flight Specific Procedure Rework Models

The flight specific procedure rework models were used in this case study to calibrate the general procedure rework model with flight specific data. Each of these models is essentially identical to the Basic Procedure Rework Model. The differences between these models and that model mainly relate to the parameter values and simulation timescales used. Additionally, because as many as three discrete events were identified on the Space Shuttle missions, each flight specific procedure rework model included

variables for exogenously initiating up to three discrete invalidation events—generating invalidations both within and beyond the procedure rework time horizon (i.e., flows 4 and 6 in Figure 60)—at the times of the discrete events.

The information necessary to replicate these models fully (including the parameter values used for each model) is documented in Appendix 3.

Flow Controlled Procedure Rework Model

The Flow Controlled Procedure Rework Model is essentially the Basic Procedure Rework Model with several structural elements added to implement flow control as described in Chapter 4. The full stock and flow structure of this model is shown in Figure 63; the variables added to implement flow control are labeled with italicized text. Two different flow control schemes are implemented in this model and can be used individually or in unison.

The first flow control scheme mimics the effect of having a fourth shift of flight controllers working on procedure rework beyond the procedure rework time horizon—this work is done in parallel to the rework done within the time horizon by the first three shifts—or of having one of the first three shifts working primarily on procedure rework beyond the time horizon. This scheme was implemented through the variables added to the left side of the stock and flow structure in Figure 63. These added variables include:

- A flow from *Inactive Procedures Needing Rework* to *Inactive Valid Procedures* to account for the completion of rework beyond the time horizon,
- A small stock and flow structure to account for the resource limitations for procedure rework beyond the time horizon, and
- A stock to record the resource-minutes devoted to rework beyond the time horizon.

The second flow control scheme mimics the effect of suddenly increasing the procedure rework time horizon towards the end of the mission. This scheme was implemented through the variables added to the top of the stock and flow structure in Figure 63. These added variables are:

- An initial value for the procedure rework time horizon,
- A factor of increase to the procedure rework time horizon (relative to the initial value), and
- The time at which the procedure rework time horizon is increased.

The additional parameters needed for this model are described in Table 14. Because there is no data available on these types of flow control and the purpose of this model is to simply demonstrate the types of benefit that can be derived from flow control (precise evaluation of the benefits of flow control is beyond the scope of this study and a potential area for future work), the author's judgment was used to determine notional baseline values for these parameters. The information necessary to replicate this model fully is documented in Appendix 3.

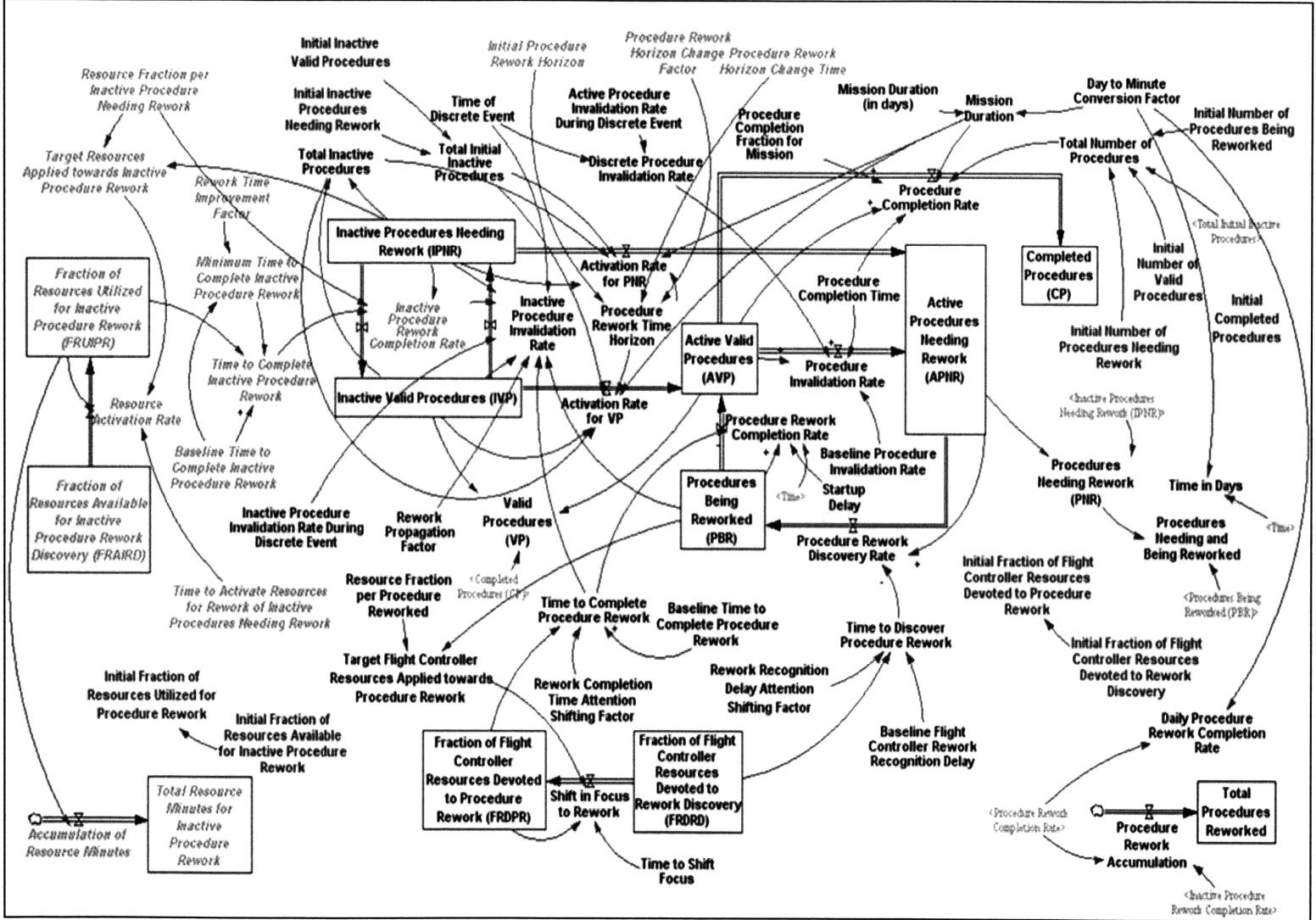


Figure 62. The stock and flow structure of the Flow Controlled Procedure Rework Model.

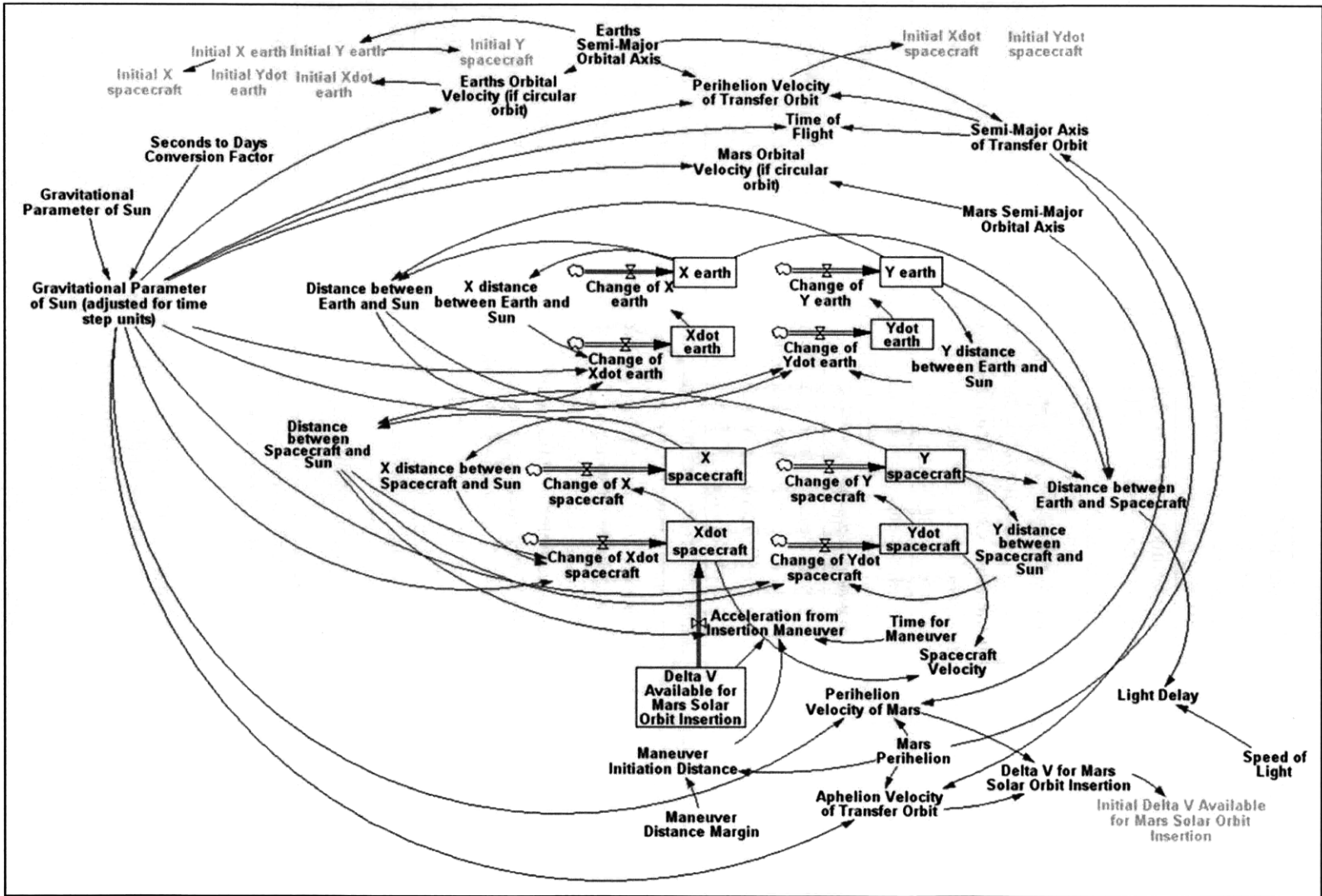
PARAMETER	DESCRIPTION
Baseline Time to Complete Inactive Procedure Rework	This parameter defines the average inactive procedure rework completion time if minimal resources are devoted to rework beyond the time horizon. The baseline value of this parameter is 30,000 minutes.
Initial Procedure Rework Horizon	This parameter defines the procedure rework time horizon at the start of the mission. The baseline value of this parameter is 2,000 minutes.
Procedure Rework Horizon Change Factor	This parameter defines the factor of increase to the procedure rework time horizon (relative to the initial time horizon) at the time of time horizon increase. The baseline value of this dimensionless parameter is 0, which means that the rework time horizon would not increase towards the end of the mission in the baseline scenario.
Procedure Rework Horizon Change Time	This parameter defines the time at which the procedure time horizon is to be increased. The baseline value of this parameter is 14,000 minutes.
Resource Fraction per Inactive Procedure Needing Rework	This parameter defines the desired fraction of resources to be applied to inactive procedure rework for every procedure in the <i>Inactive Procedures Needing Rework</i> stock. The baseline value of this parameter is 0.5 or 50%.
Rework Time Improvement Factor	This parameter defines the factor of improvement of inactive procedure rework time (relative to the <i>Baseline Time to Complete Inactive Procedure Rework</i>) that would be realized if all available resources for inactive procedure rework were devoted to inactive procedure rework. The baseline value of this parameter is 0.02, which means that the inactive procedure rework completion time can be improved to 600 minutes on average. This value makes the shift dedicated to rework beyond the time horizon one-third as effective as the three shifts nominally dedicated to rework within the time horizon.
Time to Activate Resources for Rework of Inactive Procedures Needing Rework	This parameter defines the average amount of time that it takes to activate resources for rework beyond the time horizon. The baseline value of this parameter is 30 minutes.

Table 14. Description of the parameters needed to implement flow control in the Flow Controlled Procedure Rework Model.

Light Delay Model

The light delay model is used in this case study to simulate the light delay as a function of time on a mission to Mars. The full stock and flow structure of the Light Delay Model is shown in Figure 63. In this model, a minimum energy transfer or *Hohmann Transfer* (Bate et al. 1971, pp. 163-166) is assumed from a circular Earth Solar Orbit to Mars Perihelion (i.e., the closest point to the Sun in Mars' orbit). The Sun is assumed to be fixed in inertial space and both the planet and spacecraft trajectories are assumed to be two-dimensional. Once the spacecraft arrives at Mars Perihelion a maneuver is performed

Figure 63. The stock and flow structure of the Light Delay Model.



to insert the spacecraft into Mars' elliptical orbit about the Sun. The information necessary to replicate this model fully is documented in Appendix 3.

Light Delayed Procedure Rework Model

The Light Delayed Procedure Rework Model was used in this case study to evaluate the effect that the light delay associated with a Mars mission would have on the Procedure Rework Process. This model was created through alteration of the Basic Procedure Rework Model and the combination of it with the Light Delay Model. The stock and flow structure of this model minus the elements from the Light Delay Model is shown in Figure 64. The alteration of the Basic Procedure Rework Model consisted of the addition of two pipeline delays to account for the effects of the light delay on the spacecraft-to-ground and ground-to-spacecraft procedure flows. State variable names had to be changed to include these pipeline delays, but no new parameters had to be introduced other than the *Speed of Light* and a control switch to allow the model user to select a *Spacecraft Distance from Earth* parameter to cancel out the light delay on special simulation runs. The time unit of integration for the Light Delay Model was converted from days to minutes and its *Distance between Earth and Spacecraft* variable was used to calculate the light delay. The information necessary to replicate this model fully is documented in Appendix 3.

Light Delayed, Flow Controlled Procedure Rework Model

The Light Delayed, Flow Controlled Procedure Rework Model was used in this case study to identify the effects on flow control on the procedure rework process subject to a significant light delay. It was essentially created through the addition of the flow control elements in the Flow Controlled Procedure Rework Model to the Light Delayed Procedure Rework Model. The information necessary to replicate this model fully is documented in Appendix 3.

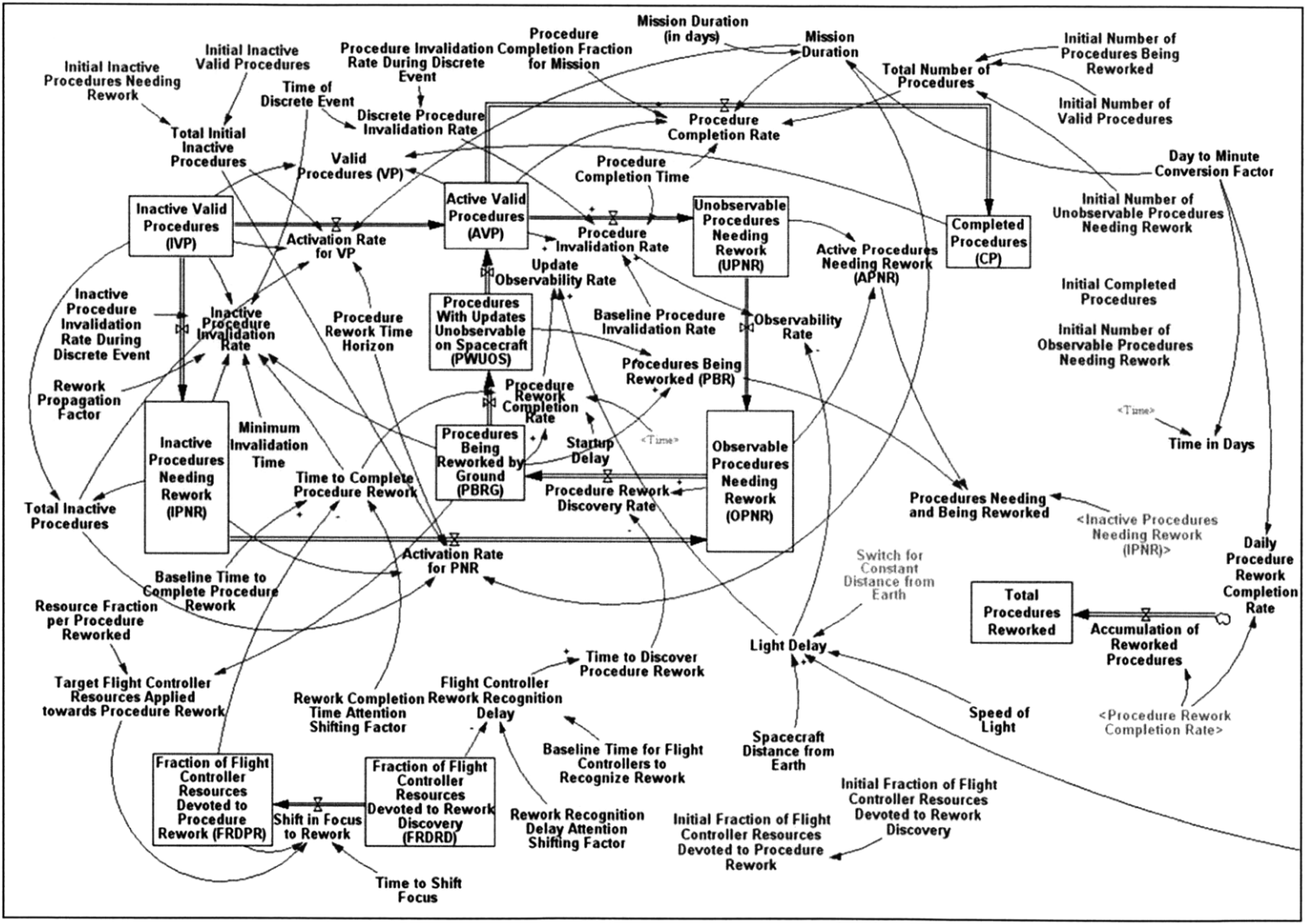


Figure 64. The stock and flow structure of the Light Delayed Procedure Rework Model without the elements from the Light Delay Model.

Model Testing and Calibration

The author subjected the models to the following tests and used the following model building principles in order to establish internal validity (i.e., internal consistency) of the models:

- After each model update, the author verified dimensional consistency of the model using the “Units Check” tool in Vensim®.
- To avoid unrealistic model sensitivity to integration time step size, a minimum delay of 1 minute was used for all first-order delays in accordance with Forrester’s (1968) suggestion that all first order delays should be at least twice as large as the integration time step. This minimum delay time dictated the value of the *Time to Shift Focus* parameter which is more likely to be nearly instantaneous in reality. Furthermore, simulation results were tested for low sensitivity to time step values up to 0.5 minutes.
- Simulations were conducted using various numerical integration techniques (i.e., Euler, Second-order Runge-Kutta with fixed and automatically adjusted time steps, and Fourth-Order Runge-Kutta with fixed and automatically adjusted time steps) to ensure that the results were not sensitive to the method of numerical integration.
- Multiple simulation runs were conducted with extreme parameter values and initial conditions to ensure that the simulation results were consistent with the physical reality that they were trying to represent. Over time, these “extreme conditions tests” enhanced model robustness to the point where only the most absurd parameter values or initial conditions would lead to simulated system states that would suggest a physical impossibility (e.g., negative procedure values in the stocks in the procedure flow).

The data collected in the analysis of the five Space Shuttle missions were used to establish external validity of the models (i.e., to validate them relative to “reality”). As mentioned before, it was the initial analysis of the data that led to the discovery of the procedure rework time horizon and the resulting structural changes to the models. Additionally, the data were used to identify other structural changes to the models and reasonable values for the remaining model parameters.

First, each update had to be classified based on how it would flow through the core procedural flow structure. The categories used for this classification are as follows:

- *Latent updates at launch*: The latent updates at launch (i.e., updates that were judged to be identifiable on Flight Day 0) start at two places in the core procedural flow: the *Inactive Procedures Needing Rework* stock or the *Procedures Being Reworked* stock. These updates thus determine the initial values of these stocks. Most latent updates at launch began in the former stock while a few—judged to most likely have been completed by launch—began in the former stock.
- *Updates within time horizon and due to a discrete event*: While the starting points of these updates are not necessarily relevant, what is relevant is that

they move from the *Active Valid Procedures* stock to the *Active Procedures Needing Rework* stock at the time of the discrete event. Thus, these updates determine the value of the *Active Procedure Invalidation Rate during Discrete Event* parameter in simulations in which a discrete event occurs.

- *Updates propagated beyond time horizon and due to a discrete event:* These updates move from the *Inactive Valid Procedures* stock to the *Inactive Procedures Needing Rework* stock at the time of the discrete event, and because there are no inflows to the *Inactive Valid Procedures* stock, they begin the simulation in the *Inactive Valid Procedures* stock. These updates determine the value of the *Inactive Procedure Invalidation Rate during Discrete Event* parameter in simulations in which a discrete event occurs.
- *Updates due to refinement of an update related to a discrete event:* While the starting points of these updates are not necessarily relevant, what is relevant is that they work their way over time from the *Active Valid Procedures* stock to the *Active Procedures Needing Rework* stock. Thus, if they are to be included in a simulation run, these updates contribute to the value of the *Baseline Procedure Invalidation Rate* parameter. However, because they are due to discrete events, they should not be included in simulation runs without discrete events.
- *Updates propagated beyond time horizon and not due to a discrete event:* These updates flow over time from the *Inactive Valid Procedures* stock to the *Inactive Procedures Needing Rework* stock and therefore determine the value of the *Rework Propagation Factor* parameter.
- *Updates within the time horizon that were not related to a discrete event:* While the starting points of these updates are not necessarily relevant, what is relevant is that they flow over time from the *Active Valid Procedures* stock to the *Active Procedures Needing Rework* stock and they do so without the influence of a discrete event. Thus, these updates determine the value of the *Baseline Procedure Invalidation Rate* parameter in simulation runs in which there are no discrete events and account for most of the value of the parameter in simulation runs in which there are discrete events.

A summary of the update classifications for the five Space Shuttle missions studied is provided in Table 15. The data from which this table is derived is provided in Table 35 to Table 37, Table 46, Table 59 to Table 60, Table 67, Table 82 to Table 84, Table 92, Table 105 to Table 106, Table 112, Table 134 to Table 137, and Table 149 of Appendix 2.

From these classifications, reasonable values for several parameters were determined. For example, because the baseline runs of the Basic Procedure Rework Model exclude discrete events, the baseline values of its *Rework Propagation Factor* and *Baseline Procedure Invalidation Rate* parameters were tuned to contribute 13.2 and 12.6 updates (i.e., the average values in Table 15 for non-discrete event related updates propagated beyond and originating within the time horizon, respectively) to the update total over the average mission duration of 12.9 days. Similarly, the values in Table 15 were used to

determine these parameter values for each of the Flight Specific Procedures Rework Models as well as parameter values associated with discrete events in those models.

	STS-97	STS-115	STS-116	STS-117	STS-120	Total (Average)
Number of latent updates at launch	49	30	35	16	26	156 (31.2)
Number of updates within time horizon and due to a discrete event	3	1	0	3	7	14 (2.8)
Number of updates propagated beyond time horizon and due to a discrete event	12	7	20	31	51	121 (24.2)
Number of updates due to refinement of an update related to a discrete event	2	0	6	0	15	23 (4.6)
Number of updates propagated beyond time horizon and not due to a discrete event	19	13	16	8	10	66 (13.2)
Number of updates within the time horizon that were not related to a discrete event	8	12	9	8	26	63 (12.6)
Total Number of Updates	93	63	86	66	135	443 (88.6)

Table 15. Summary of update classifications for all five Space Shuttle missions studied.

Other structural changes to the models and reasonable values for the remaining parameters were determined through an iterative calibration technique involving the Flight Specific Procedure Rework Models. From the data provided throughout Appendix 2, time histories were developed for all flights studied of the combined values of the *Inactive Procedures Needing Rework*, *Active Procedures Needing Rework*, and *Procedures Being Reworked* stocks. These time histories are provided in Table 45, Table 66, Table 91, Table 111, and Table 148 of Appendix 2, respectively. These time histories were then imported into the Vensim[®] software package for comparison against the simulation results (i.e., the *Procedures Needing and Being Reworked* variable) using the modified Powell Search Algorithm in Vensim[®]. This search algorithm uses a one-parameter-at-a-time (OPAT) routine to identify parameter values that would minimize the difference between the data values and the simulation results. The parameter value constraints placed on the algorithm are listed in Table 16 and were based on the author's judgment of the realistic bounds of these parameters, which was informed by his experience as a member of flight control teams during several Space Shuttle missions between STS-97 and STS-115. Because the algorithm is not guaranteed to find the global minimum if multiple local minima exist, the starting point of the algorithm, which coincides with the baseline parameter values, can affect the result. Therefore, dozens of

experimental baseline values were attempted until the author settled on the values in Table 17, which are shown along with the final calibration run results.

PARAMETER	MINIMUM VALUE	MAXIMUM VALUE
Baseline Flight Controller Rework Recognition Delay	1 minute	120 minutes
Baseline Time to Complete Procedure Rework	30 minutes	360 minutes
Procedure Rework Time Horizon	800 minutes	3,000 minutes
Resource Fraction per Procedure Reworked	0.01	0.5
Rework Completion Time Attention Shifting Factor	0.01	2
Rework Recognition Delay Attention Shifting Factor	0.01	2
Startup Delay	0 minutes	720 minutes

Table 16. Parameter constraints used for calibration runs using the modified Powell Search Algorithm in Vensim®.

The final baseline values represent the author’s best attempt to define a uniform set of parameter values for all of the flights. These parameter values produce simulation results that match the data time histories as closely as possible without disregarding the physical reality that the parameters represent. As stated by Sterman (1984), parameter estimates should be derived from data ‘below the level of aggregation’ of the model, such as engineering data, surveys, or other disaggregate data sources that ‘draw on descriptive knowledge of the system’s structure rather than its aggregate behavior’. The reason for relying on data below the aggregate level of system behavior is that these models, like almost every other model, neglect select behavior modes in the data that are not relevant with regard to the model purpose (otherwise the models would have to be as complex as the system they represent and resources would be wasted on understanding inconsequential behavior modes). By neglecting these behavior modes, two sources of unwanted variability are injected into the results of the calibration runs:

- The results returned by the search algorithm may deviate from physical reality because the algorithm is trying to compensate for the absence of the select behavior modes.
- The results returned by the search algorithm may deviate from flight to flight because an event occurring on a certain flight may excite or amplify a neglected behavior mode on that flight, but not the others.

Thus, the parameter estimates are primarily derived from the author’s judgment of the physical realities represented by the parameters. The calibration run results for the *Baseline Flight Controller Rework Recognition Delay* parameter, for example, were largely neglected because they unrealistically suggested values that coincided with either the upper or lower constraints placed on the search algorithm in all but one case. The results from the calibration runs only factored into the estimates when they suggested an alternative parameter value to the author’s estimate that was physically reasonable *and* capable of significantly improving the fit of the baseline simulation results to the data. For instance, the calibration run results for the *Procedure Rework Time Horizon* parameter suggested that a value of 2,000 minutes would, on average, produce a better fit

than the author's initial estimate of 1,440 minutes (this suggestion represented a realistic and important change to make to the estimate).

More importantly, the calibration runs were used to determine when certain structural changes in the model were justifiable by allowing the author to isolate the effects of parameter values on the simulation results from the effects of model structure. Because the parameter values from each calibration run were optimized for each flight data set, the runs made it clear that any important behavior modes absent from the simulation results during these runs were missing due to the model structure.

PARAMETER	STS-97	STS-115	STS-116	STS-117	STS-120	EXPERIMENTAL BASELINE (AVERAGE)
Baseline Flight Controller Rework Recognition Delay (minutes)	1	60.99	120	120	1	30 (60.6)
Baseline Time to Complete Procedure Rework (minutes)	360	78.51	30	360	360	200 (237.7)
Procedure Rework Time Horizon (minutes)	1264.86	2016	800	2985	3000	2000 (2013.3)
Resource Fraction per Procedure Reworked (dimensionless)	0.5	0.5	0.5	0.01	0.01	0.2 (0.304)
Rework Completion Time Attention Shifting Factor (dimensionless)	0.01	0.01	2	2	0.29	1 (0.862)
Rework Recognition Delay Attention Shifting Factor (dimensionless)	0.01	2	2	2	0.01	1 (1.204)
Startup Delay (minutes)	254.8	459.7	360.0	720	720	520 (502.9)

Table 17. Summary of the results from the final calibration run using the modified Powell Search Algorithm in Vensim®.

Plots of the time histories using the baseline parameter values, final search algorithm results, and flight data for each flight are provided in Figure 65 to Figure 69, respectively. In future work, the baseline parameter estimates can be improved upon by seeking out more data below the aggregation level of in-flight update statistics (e.g., flight controller interviews and survey, experiments conducted with flight controllers, etc.).

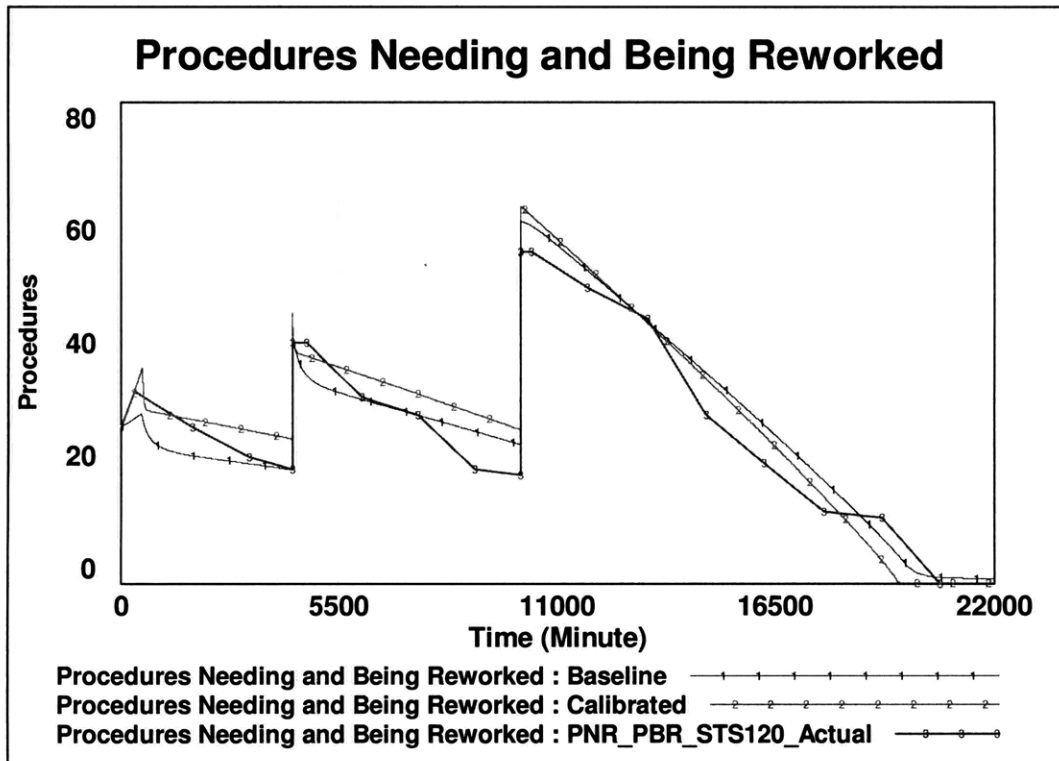


Figure 69. Results of model calibration against STS-120 data.

While visual indications of how well the models replicate the system behavior are provided in Figure 65 through Figure 69, quantitative statistics characterizing the fit are provided in Table 18. The first three columns contain the Mean Absolute Error (MAE), the MAE divided by the mean of the data series, and Root Mean Square (RMS) error—which is derived from the Mean Square Error (MSE)—as defined in the following equations (Sterman 2000):

$$[\text{Eq. 23}] \quad MAE \equiv \frac{1}{n} \sum_{t=1}^n |S_t - A_t|$$

where n = number of observations, S_t = Simulated value at time t , and A_t = Actual value at time t

$$[\text{Eq. 24}] \quad MSE \equiv \frac{1}{n} \sum_{t=1}^n (S_t - A_t)^2$$

$$[\text{Eq. 25}] \quad RMS \equiv \sqrt{MSE}$$

The Theil Inequality Statistics (Sterman 2000 pp. 874-880, Sterman 1984)—shown in the final three columns of Table 18—decompose the mean square error into three

dimensionless components: the bias (U^M), unequal variation (U^S), and unequal covariation (U^C). These terms are mathematically defined in the following equations:

$$[\text{Eq. 26}] \text{MSE} = (\bar{S} - \bar{A})^2 + (S_S - S_A)^2 + 2(1-r)S_S S_A$$

where \bar{S} = mean of the simulated data set, \bar{A} = the mean of the Actual data set, S_S = Standard deviation of the simulated data set, S_A = Standard deviation of the actual data set, and r is the correlation coefficient

$$[\text{Eq. 27}] U^M \equiv \frac{(\bar{S} - \bar{A})^2}{\text{MSE}}$$

$$[\text{Eq. 28}] U^S \equiv \frac{(S_S - S_A)^2}{\text{MSE}}$$

$$[\text{Eq. 29}] U^C \equiv \frac{2(1-r)S_S S_A}{\text{MSE}}$$

From [Eq. 26] through [Eq. 29] it follows that the sum of the Theil Inequality Statistics (U^M , U^S , and U^C) is unity. In other words, these statistics represent a relative distribution of the types of error produced by the model. The following considerations are important in interpreting the distribution of error among these components (Sterman 2000 pp. 874-880, Sterman 1984):

- If the error is largely concentrated in bias (U^M), most of the error is due to the difference in the means of the model results and the data series. This type of error is systematic in that it could undermine what the modeler is trying to accomplish with the model.
- If the error is largely concentrated in unequal variation (U^S), most of the error is due to the difference in the variances of the model results and the data series. This type of error can be due to the different trends in model results and data series, a difference in the amplitude of cycles present in the model results and data series, or the absence of cycles in simulation results that exist in the data series. While each of the causes of this type of error can undermine what the modeler is trying to accomplish, the third cause is only important when the purpose of the model is to study the cycle(s) that has been neglected from the simulation results.
- If the error is largely concentrated in unequal covariation (U^C), the model has a mean and trends that closely match those of the data series. This type of error can be due to an unaccounted for difference in phasing of the results and data series, but is usually due to noise and cycles in the data series that have been neglected. If proper phasing of the model results and data series is vital, then this type of error could undermine what the modeler is trying to accomplish. However, it is more often the case that the phasing, noise, and

cycles are not relevant with regard to the modeler's goal and thus the model should not be faulted for this type of error.

- Because U^S could be affected by unimportant cycles in the data, it is possible that a large concentration of error in U^S and U^C does not necessarily undermine the model's ability to replicate the important system behaviors present in the data series.

As indicated in Table 18 most of the error is concentrated in U^S and U^C for all of the calibration runs and all but one of the baseline runs (which is an accepted consequence of the author's attempt to develop a uniform set of parameters for all missions). This result indicates that the models have means and trends that are very similar to those of the data and most of the difference between the data and the model results are due to cycles and random noise not explicitly represented by the models. In other words, most of the error is due to factors that have little to do with what the modeler was trying to accomplish in this modeling effort.

SIMULATION RUN	RMS (UPDATES)	MAE (UPDATES)	MAE/ \bar{A} (%)	U^M	U^S	U^C
STS-97 Baseline	4.246	3.270	10.98	0.1880	0.2236	0.5884
STS-97 Calibration	2.446	1.929	6.477	0.0866	0.0256	0.8878
STS-115 Baseline	3.218	2.247	10.80	0.2672	0.1981	0.5347
STS-115 Calibration	2.263	1.549	7.447	0.0006	0.0137	0.9856
STS-116 Baseline	7.579	5.761	17.17	0.5626	0.0006	0.4368
STS-116 Calibration	4.514	3.613	10.77	0.0197	0.0051	0.9753
STS-117 Baseline	5.924	4.577	16.78	0.2909	0.4741	0.2349
STS-117 Calibration	5.239	3.985	14.62	0.2022	0.4858	0.3120
STS-120 Baseline	3.994	3.166	11.03	0.0806	0.0178	0.9016
STS-120 Calibration	3.5798	2.820	9.826	$1.45e^{-6}$	0.0640	0.9360

Table 18. Summary statistics for the fit of flight specific model simulation results to the flight data.

Interpretation of the Model Testing and Calibration Process

While the plots in Figure 65 through Figure 69 provide a visual reference of how closely the simulation results “match” the flight data and the summary statistics in Table 18 indicate that the difference is small and primarily due to cycles and noise that are not

relevant to the model purpose, the question of whether the models are “valid” or not requires more contextual grounding than a simple fitting of results to the data. Forrester (1968) provides the following thoughts on model validity:

“Model validity is a relative matter. The usefulness of a mathematical simulation model should be judged in comparison with the mental image or other abstract model which would be used instead...By constructing a formal model, our mental image of the system is clearly exposed...A controversy often develops over whether or not reality is exactly as presented in the model. But such questions miss the first purpose of a model which is to be clear and to provide concrete statements that can be easily communicated. There is nothing in either the physical or social sciences about which we have perfect information. We can never prove that any model is an exact representation of ‘reality.’ Conversely, among those things of which we are aware, there is nothing of which we know absolutely nothing. So we always deal with information which is of intermediate quality—it is better than nothing and short of perfection. Models are then to be judged, not on an absolute scale that condemns them for failure to be perfect, but on a relative scale that approves them if they succeed in clarifying our knowledge and our insights into systems...The value in computer models derives from the differences between them and mental models. When the conflicting results of a mental and a computer model are analyzed, when the underlying causes of the differences are identified, both of the models can be improved.”

Sterman (1991) adds the following:

“By creating a representation of the system in the laboratory [i.e., a simulation model], a modeler can perform experiments that are impossible, unethical, or prohibitively expensive in the real world...In other words, simulation models are ‘what if’ tools.”

Forrester’s argument—which is echoed in the Meadows et al. (1982) and Forrester (1969) quotes provided at the beginning of this chapter—is that we make all of our decisions with models, be they mental or formal. Furthermore, because the process of formalizing a mental model through computer simulation reveals weaknesses in the mental model, it is worth doing even when data is scarce and our knowledge of the mathematical nature of the system severely constrained. Sterman’s comment expands on this argument by identifying the kind of experimentation that is made possible by simulation.

With this argument in mind, questions on the validity of the Procedure Rework Models hinge on the purpose of the models and their usefulness relative to whatever mental or formal models exist on the Procedure Rework Process. As stated above, the purpose of the models are to characterize (and perhaps improve upon) how the Procedure Rework Process attracts human spaceflight systems to safe states under uncertain conditions (i.e., to identify the Procedure Rework Attractor, its bifurcations, and its responses to flow control schemes). The fact that the models produce results that seem to match flight data

is a promising indication towards this end. However, the vast experience of Space Shuttle Mission Control with this process would suggest that its “mental model” of the process should already be rather sophisticated, at least in regards to the standard Space Shuttle mission profile. Thus, most value of the models is likely to come from what they suggest about the attraction properties of the system under conditions that have never been encountered (e.g., long duration flights to land on moons, NEOs, or planets; flights without “novel” or discrete events; flights subject to significant light delays; etc.). What the models have to say about the system under these conditions is discussed in the next chapter. As alluded to in the Mission Control literature review in Chapter 5, this purpose of the models has not been addressed in the scholarly literature and therefore, it is up to the reader to gauge the usefulness and plausibility of the results presented in the next chapter against what would result from his or her mental model of the Procedure Rework Process.

Chapter 7: Case Study Analysis Results and a Process to Use Phase Space Attractors to Evaluate Safety Constraint Enforcement

“The NASA Vision for Space Exploration calls for the return of humans to the Moon, and the eventual human exploration of Mars; the complexity of this range of missions will require an unprecedented use of automation and robotics in support of human crews. The challenges of human Mars missions, including roundtrip communications time delays of 6 to 40 minutes, interplanetary transit times of many months, and the need to manage lifecycle costs, will require the evolution of a new mission operations paradigm far less dependent on real-time monitoring and response by an Earthbound operations team.” –Andrew Mishkin et al. (2007).

“The communications delays [i.e., light delays on missions to distant celestial bodies] will change the way human missions are operated. The crew will be the first responders to emergencies and mundane anomalies; they will attend autonomously to all alarms, switching the troublesome system to a safe mode and/or making quick repairs and reconfigurations. What we now think of as ground control teams will become ground support teams.” –John Jaap et al. (2006).

“Today’s basic paradigm of how to conduct mission operations must change. At their closest approach to Earth, NEOs (particularly PHAs—potentially hazardous asteroids) are 7 to 10 light seconds away. The crew must be very knowledgeable and systems savvy with the vehicle, as the locus of operational decision-making will be upon the crew.” –Rob R. Landis et al. (2008).

“Human missions to the moon and Mars will demand a higher level of spacecraft autonomy than can be demonstrated today. Communications delays induced by long distances render the ground unable to provide the amount or type of support that Mission Control has always provided to crewed spacecraft.” –Alan R. Crocker (2005).

7.1 Chapter Overview

The analysis and results of the Space Shuttle Mission Control Procedure Rework Case Study are presented in this chapter. First, the analyses performed in this case study along with their results and limitations are detailed. These analyses explore a range of flight conditions that, as indicated in the quotes above, NASA is expected to encounter as it executes its vision for space exploration and highlight potential ways in which the Procedure Rework Process can be improved. Then, a general process for using phase

space attractors to evaluate and improve safety control structures is presented with the case study serving as an example application.

7.2 Analysis

Results from the author’s analysis of the Procedure Rework Models and the flight data are presented throughout this section. The Procedure Rework Attractor is characterized across a range of flight conditions (including those that NASA will likely encounter on future human spaceflight missions) and evaluations of bifurcation and flow control schemes to improve it are described. Additionally, limitations of this analysis are discussed.

Rework Propagation Bifurcation

As shown in Figure 70—which was derived from the data in Table 47, Table 68, Table 93, Table 113, and Table 150 of Appendix 2—the “novel” or discrete events during the missions and the latent updates at launch introduce a good deal of noise into the time history of procedure updates, making it difficult to infer trends in procedure update rates over the course of a mission and their causal mechanisms.

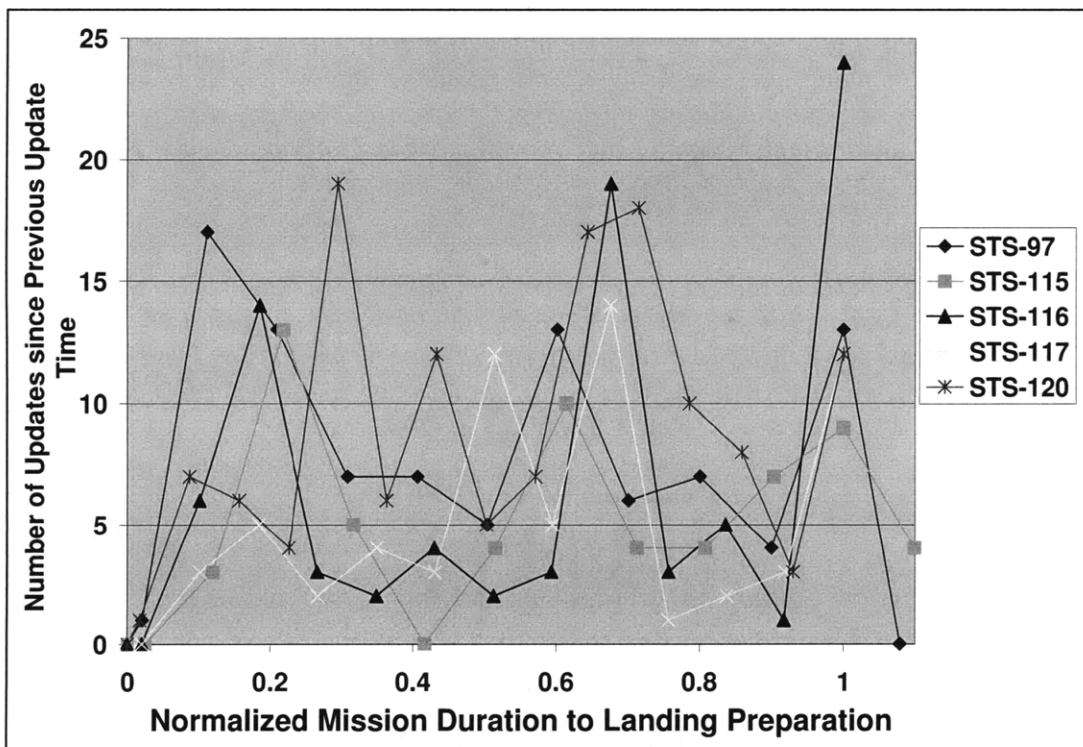


Figure 70. Update times for all missions studied normalized to their time of landing preparation.

The models developed in this case study allow one to remove the latent updates at launch and the discrete events in order to examine the underlying trends of procedure rework and the aspects of the dynamic structure that lead to such behavior. One such dynamic behavior that the author refers to as the *rework propagation end-of-mission effect* is

depicted in Figure 71. When procedure rework is allowed to propagate beyond the time horizon (i.e., when Flow 6 in Table 11 is positive), the procedure rework completion rate increases exponentially throughout the mission until it peaks at the landing preparation time and drops off considerably. Alternatively, when rework propagation is not allowed, the procedure rework rate increases to a steady-state rate that is small (relative to the peak rate when rework propagation occurs) and constant throughout the remainder of the mission.

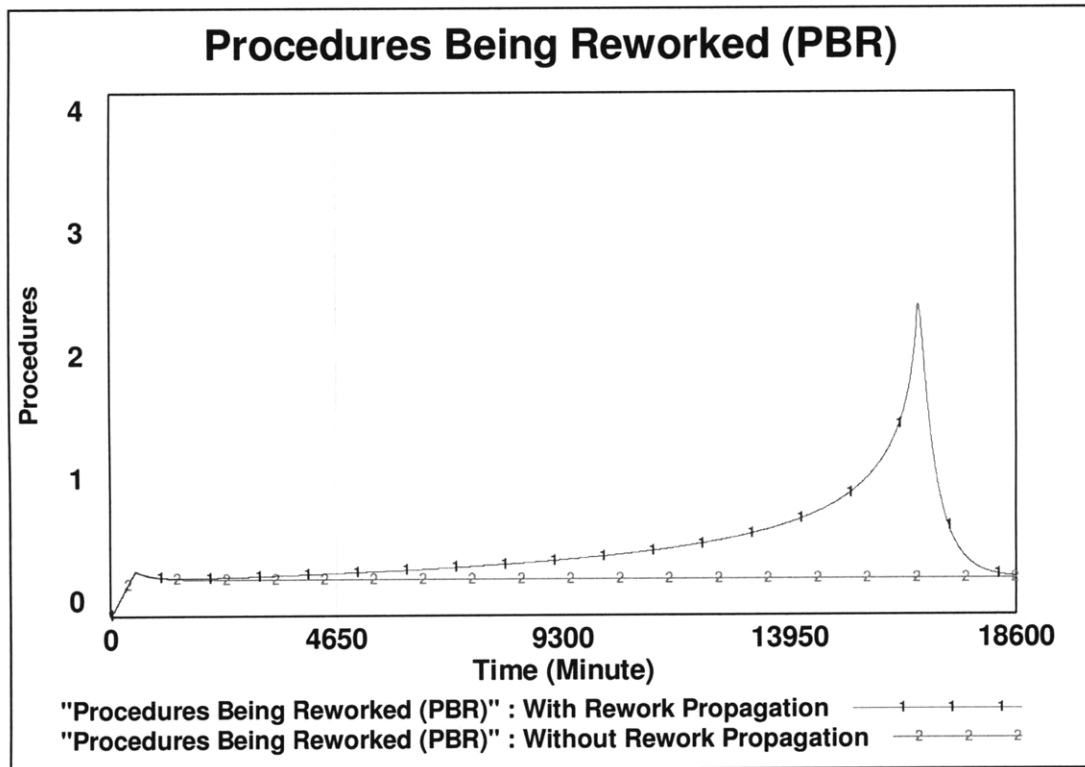


Figure 71. The rate of procedure rework over the course of missions with rework propagation and without rework propagation.

Once this behavior was identified in the model, the author retrospectively examined the data disregarding latent updates at launch and discrete events in order to verify the existence of the rework propagation end-of-mission effect. Figure 72 contains averaged update rates for all procedure rework from all of the missions studied at fourteen update times¹⁰³, each normalized to the landing preparation time of the average (or reference) mission. This figure contains three spikes in the rework completion rate: one towards the beginning of the mission, one in the middle of the mission, and one at the end of the mission (consistent with the notion of the rework propagation end-of-mission effect). When all updates related to discrete events are disregarded—as shown in Figure 73—the second peak disappears and the other two are slightly reduced. This result is consistent with a simulation run—also shown in Figure 73—in which the average number of updates deemed likely to have been finished by launch (i.e., 6.6 updates) was the initial

¹⁰³ See Table 151 in Appendix 2 for these update times and the update rates at these times

value of the *Procedures Being Reworked* stock and the average number of otherwise latent issues at launch (i.e., 24.6 updates) was the initial value of the *Inactive Procedures Needing Rework* stock¹⁰⁴. Finally when the latent updates at launch are also disregarded—as shown in Figure 74—the first peak disappears, leaving only the third peak that would be produced by the rework propagation end-of-mission effect. In fact, the simulation results from using the baseline parameter values for the Basic Procedure Rework Model—also shown in Figure 74—closely match the flight data when latent updates at launch and discrete events updates are disregarded. The closeness of the results in Figure 74—which is quantitatively summarized in Table 19¹⁰⁵—is particularly impressive when one considers the following sources of error in such a comparison:

- The variable considered in this plot (i.e., the procedure update rate) is a rate variable. Rate variables are not measurable unless they are averaged over a period of time (Forrester 1968). The time period used for averaging is thus a potential source of error in the plot (i.e., different time periods used for averaging could lead to better or worse “fits” to the data).
- The effects of the discrete events and latent updates at launch cannot be removed from the data unless they were purely additive or linear. For example, the data shows fewer updates in the third quarter of the mission duration than the model suggests, however, as shown in Figure 72 that was the time period in which most of the discrete event updates were issued. The flight controllers may have been too distracted with discrete event related updates to perform non-discrete event related updates at the rate suggested by the model.
- The model was built on an assumption that the procedure activation and active procedure invalidation rates would be consistent throughout the mission. In reality, the level of procedural activity on a mission varies from day to day. For example, there is typically an “off-duty” day in which the crew performs very few procedures.

Furthermore, it should be noted that Garrett and Caldwell (2002) observed a similar effect in the processing of flight rule change requests between missions (i.e., change requests spiked in the month before a launch). Overall, the analysis provides strong empirical support for the existence of a rework propagation end-of-mission effect.

¹⁰⁴ The value of the *Rework Propagation Factor* parameter was also tuned from the baseline value of 0.605 to 0.185 in order to prevent the model from producing more than 13.2 propagated updates due to the addition of the latent updates at launch.

¹⁰⁵ Note that the error is mostly concentrated in U^C and U^S , indicating that it is likely due to data noise and cycles that are not relevant to the model purpose.

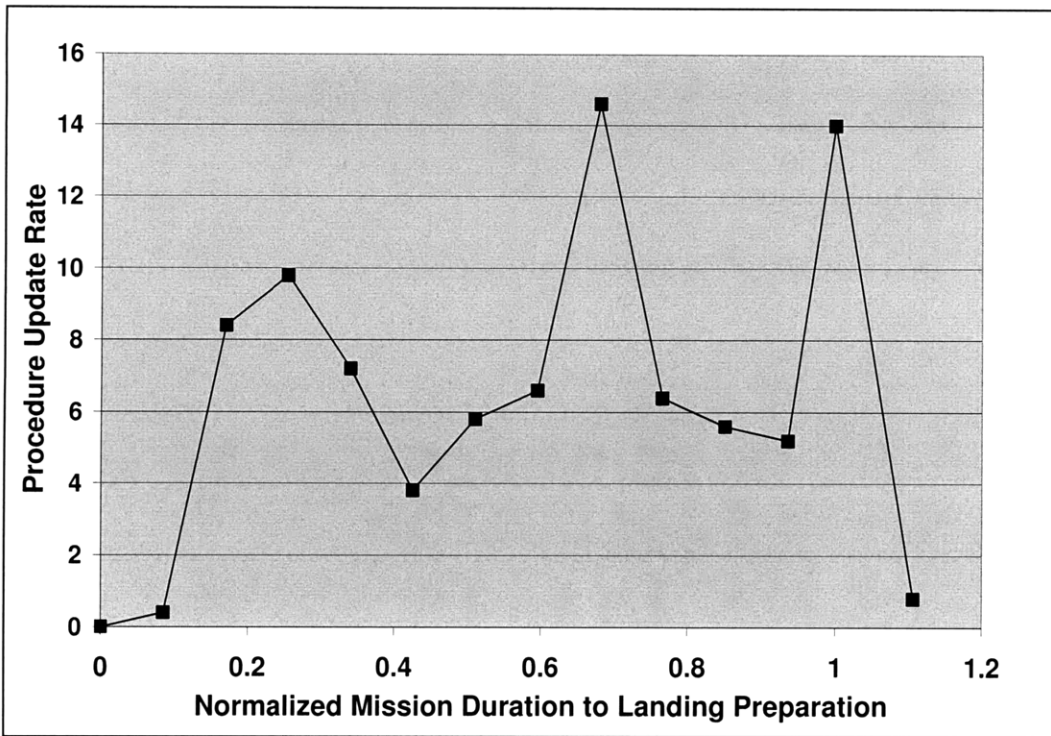


Figure 72. The actual average rate of procedure rework over the missions studied with normalized update times.

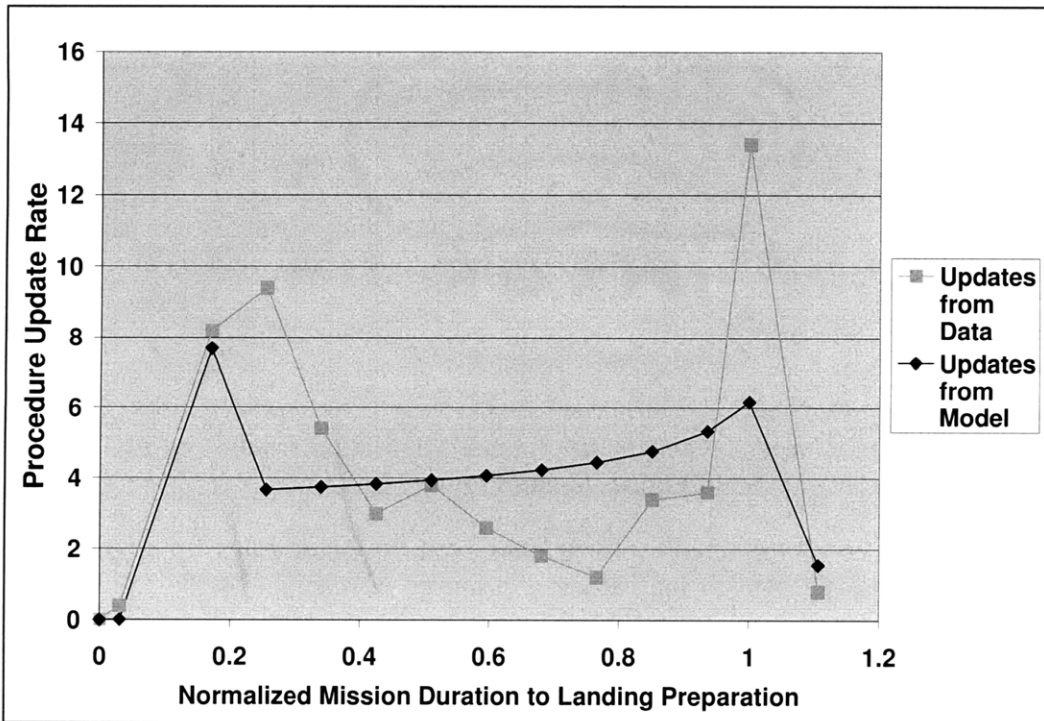


Figure 73. The actual and simulated average rates of procedure rework (excluding discrete event updates) over the missions studied with normalized update times.

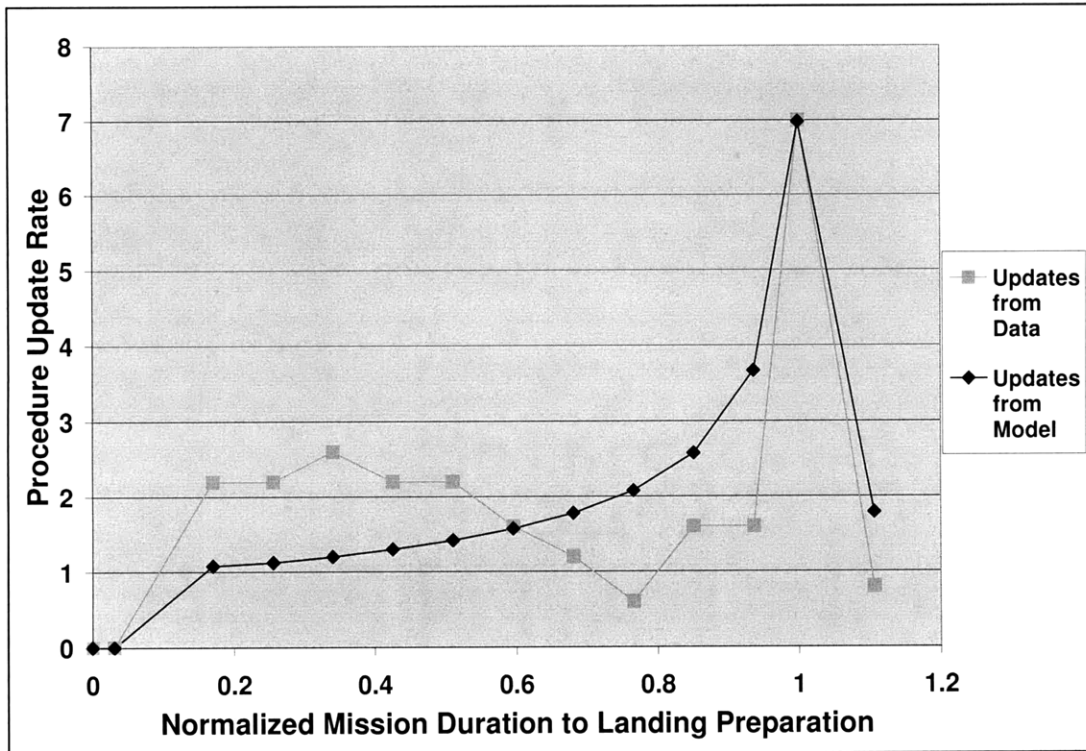


Figure 74. The actual and simulated average rates of procedure rework (excluding latent updates at launch and discrete event updates) over the missions studied with normalized update times.

SIMULATION RUN	RMS (UPDATES)	MAE (UPDATES)	MAE/ \bar{A} (%)	U^M	U^S	U^C
No Discrete Events (see Figure 73)	2.8428	1.9652	48.2691	0.0081	0.3422	0.6497
No Discrete Events or Latent Updates at Launch (see Figure 74)	1.0176	0.8154	44.2454	0.0026	0.0009	0.9965

Table 19. Summary statistics for the fit of model simulation results and flight data in Figure 73 and Figure 74.

Given the existence of the rework propagation end-of-mission effect, questions arise regarding its causal mechanism and its potential impact on safety. As shown in Figure 75, propagated rework (i.e., rework stemming from issues that affected procedures beyond the procedure rework time horizon when they occurred) accumulates throughout the mission until the time comes to “tie up all the loose ends” and prepare for landing. Prior to this time, some of the propagated rework gets activated and resolved. However, because the amount of inactive procedures needing rework is small relative to amount of

valid inactive procedures, they comprise a relatively small proportion of the procedures being activated. Therefore it is not until the point near the end of the mission when all inactive procedures must be activated that the *Inactive Procedures Needing Rework* stock empties faster than it is filled. In describing a similar effect related to flight rule change requests before launch, Garrett and Caldwell (2002) concluded that launch served as a “forcing function” in Mission Control knowledge synchronization (e.g., flight rule change request processing) between missions. Thus, landing can be considered as a forcing function for another type of Mission Control knowledge synchronization (i.e., procedure rework).

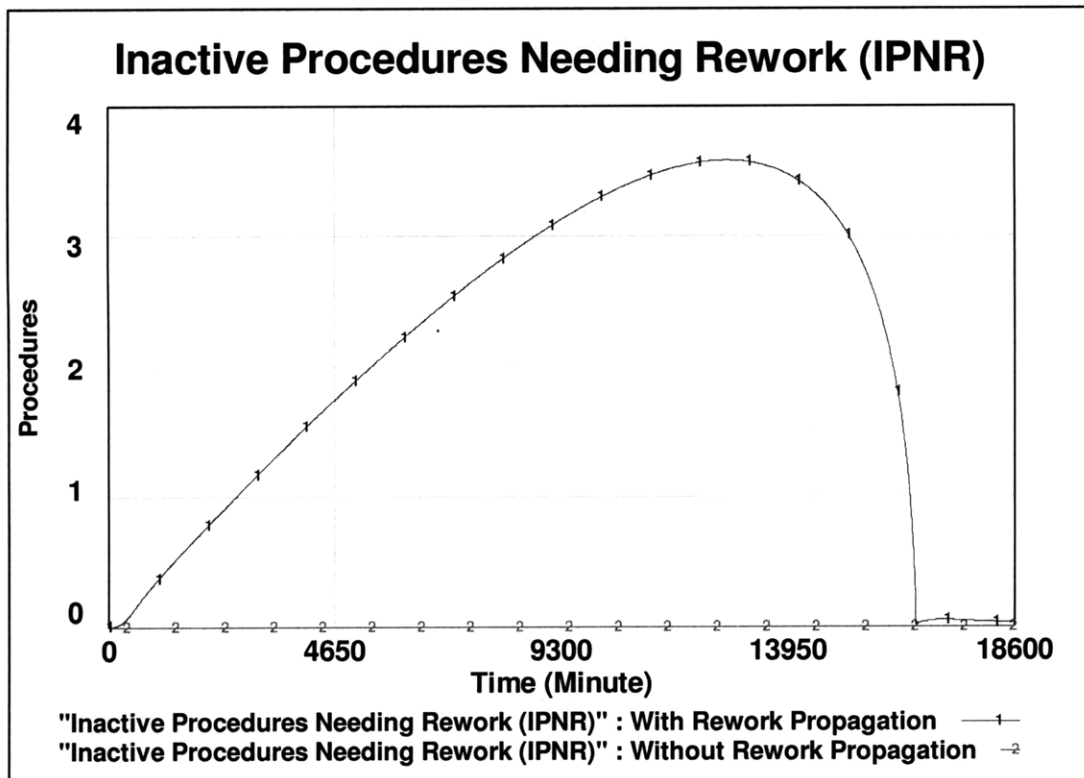


Figure 75. The time history of the *Inactive Procedures Needing Rework* stock for scenarios with and without rework propagation.

As previously mentioned, invalid procedures are control flaws with the potential to lead to inadequate control actions in potentially any safety control process that involves the execution of procedures by astronauts. The Procedure Rework Process is a safety control process to reduce such control flaws, but as shown above, it has its own control flaws. The existence of a procedure rework time horizon that is significantly shorter than mission duration and the tendency of procedures beyond the time horizon to be invalidated almost as frequently as those within time horizon (i.e., rework propagation) are control flaws that lead to the rework propagation end-of-mission effect. Unlike the rework spikes created by the “novel” or discrete events and latent updates at launch, which are typically due to factors outside of the real-time procedure rework process (e.g., SAW design), the rework propagation end-of-mission effect is due to the design of the

Procedure Rework Process and thus, it may be possible to mitigate it through re-design of the process. Furthermore, because discrete events and latent updates at launch also affect procedures beyond the time horizon, such mitigation efforts could improve the system's response to discrete events and latent updates at launch as well.

As suggested throughout this dissertation, one way to characterize such control flaws (so that they may be improved upon) is through evaluation of their effect on system attraction properties in phase space. When viewed in the Valid Procedures¹⁰⁶-Procedures Being Reworked phase space, the Procedure Rework Attractor is an equilibrium point attractor as shown in Figure 76. The two phase portraits in the figure depict simulations with rework propagation and without rework propagation, respectively. In the phase portrait without rework propagation, the system starts on horizontal axis and takes a nearly direct path to the equilibrium point, temporarily overshooting it slightly while the startup delay is in effect. The phase portrait with rework propagation starts in the same spot in phase space, but carries the system away from the equilibrium along both axes of the phase space (i.e., it takes it deeper into the hazardous regions of the phase space) in a path that eventually ends at the equilibrium. Thus, rework propagation changes the path to the equilibrium from a nearly direct path to a pseudo spiral-in trajectory. In other words, rework propagation bifurcates the Procedure Rework Attractor in a hazardous manner. This bifurcation—the *Rework Propagation Bifurcation*—depends on the value of the *Rework Propagation Factor* parameter in the model. When the value of this parameter is zero, no rework propagation occurs. When its value is greater than zero, rework propagation occurs. Finally, when its value is less than zero (a condition that would effectively mean that *Inactive Procedures Needing Rework* are being cancelled or reworked outside of the standard Procedure Rework Process) negative propagation occurs. A phase portrait and time history for a negative propagation scenario, along with the phase portrait of a propagation scenario under identical initial conditions¹⁰⁷ are provided in Figure 77 and Figure 78. It is worth noting that negative propagation eliminates the rework propagation end-of-mission effect in scenarios without discrete events and latent updates at launch and reduces it for scenarios with discrete events and latent updates at launch.

¹⁰⁶ *Valid Procedures* is a state variable derived from summing the values of the *Inactive Valid Procedures*, *Active Valid Procedures*, and *Completed Procedures* stocks.

¹⁰⁷ The dynamics of negative propagation only differ from the dynamics of zero propagation when there are latent updates at launch or when a discrete event invalidates some procedures beyond the time horizon (otherwise the value of the *Inactive Procedures Needing Rework* stock would always be 0 procedures). Thus, the initial value of the *Inactive Procedures Needing Rework* stock is 30 procedures in both simulation runs. The values of the *Rework Propagation Factor* parameter are -0.135 and 0.135 for the negative propagation and positive propagation simulations, respectively.

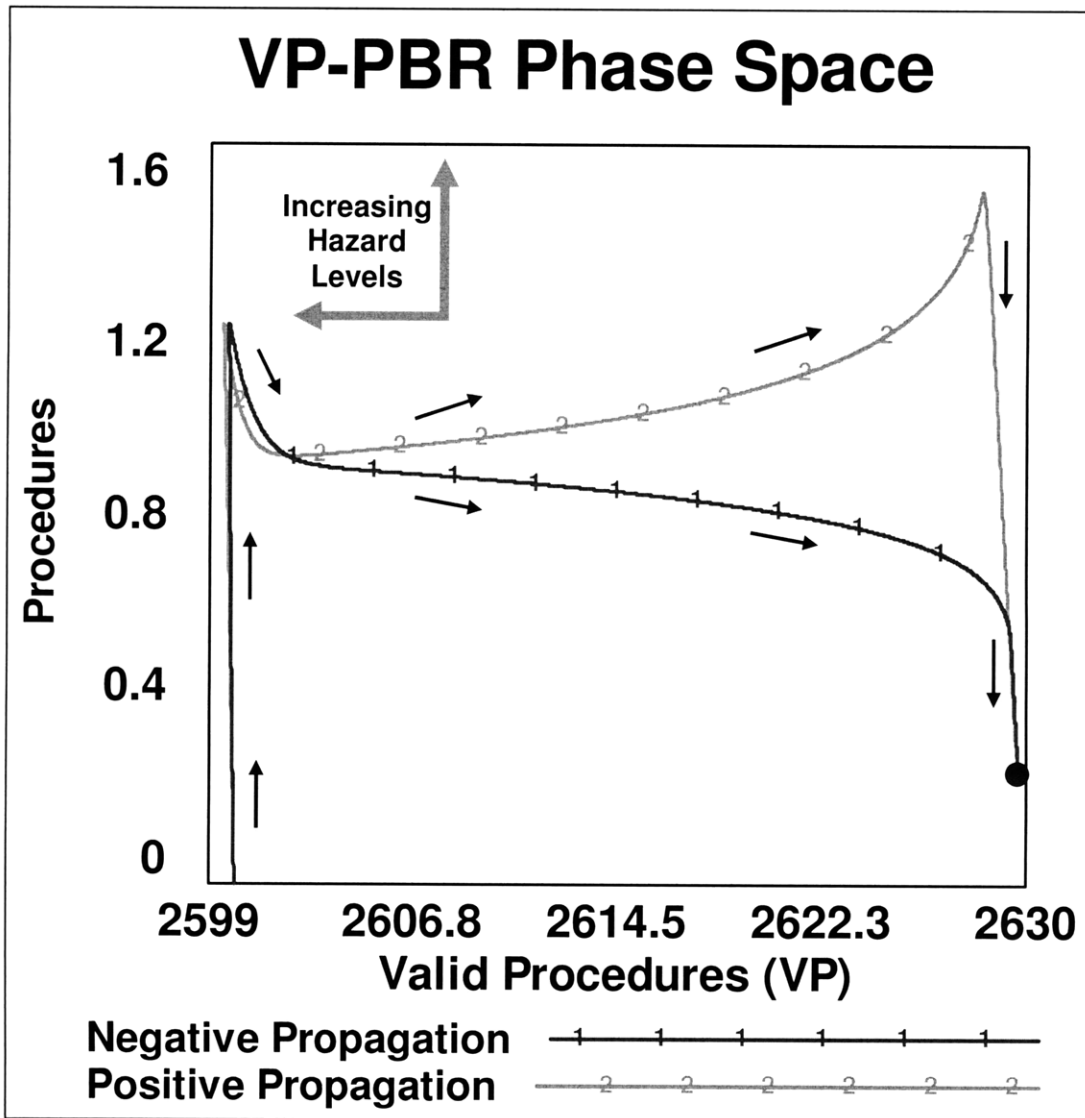


Figure 77. Phase portraits in the *Valid Procedures-Procedures Being Reworked* Phase Space for simulations runs with negative and positive rework propagation.

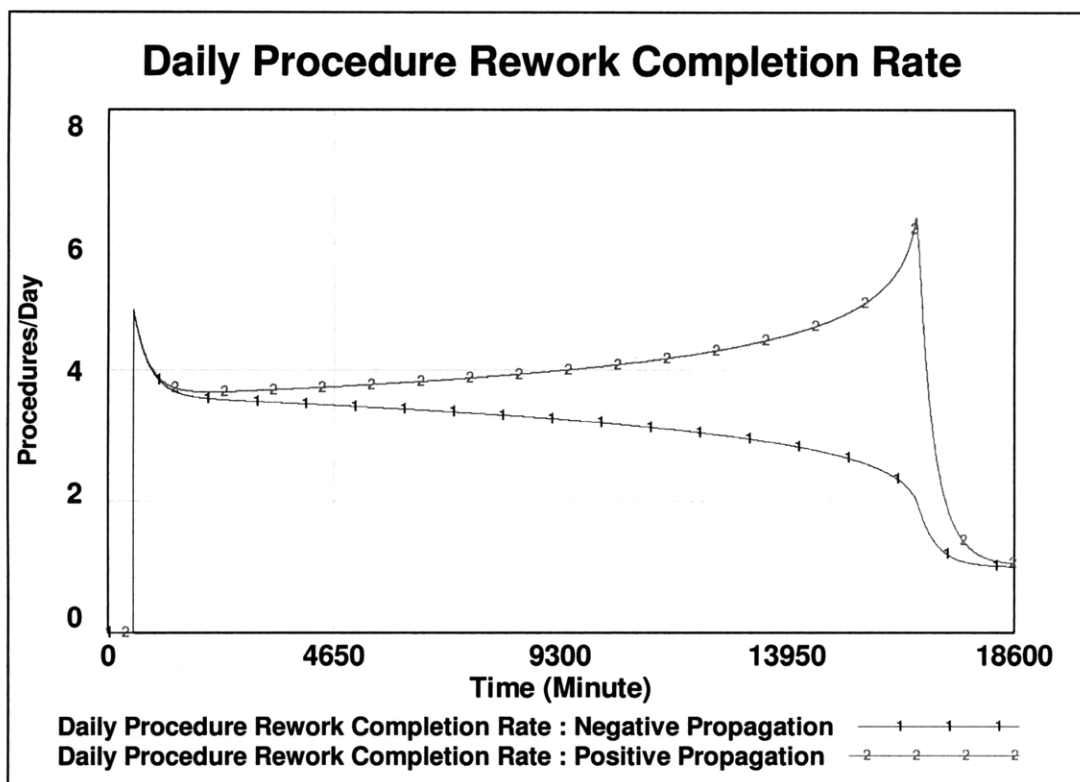


Figure 78. The *Daily Procedure Rework Completion Rate* Time History for simulations with negative and positive rework propagation.

Bifurcation Control of the Rework Propagation Bifurcation

The data seem to indicate that positive propagation occurred on all flights (propagated rework had to be dealt with on each flight through the Procedure Rework Process). Thus, with positive propagation likely to be the norm in the Procedure Rework Process rather than negative propagation, it may be desirable to pursue some bifurcation control techniques in order to reverse this hazardous bifurcation. One set of approaches to such bifurcation control is to identify and alter the factors that affect the *Rework Propagation Factor*.

Table 20 and Table 21 summarize the rationales for all propagated rework. The results in these tables, along with the results in Table 8 and Table 9 suggest that rework (especially propagated rework) is not usually due to human and component reliability issues (i.e., procedure rework is not a reliability problem). The rationale categorizations associated with human/component reliability issues (i.e., Internal Inconsistencies in the Procedure, Sensor “Failure” or Bias, Actuator “Failure” or Degradation, Crew Procedural Slips, Typos and Omissions, Inadvertent Deletion of Steps) only account for 24.4% of the total rework and 20.9% of propagated rework. Rework due to opportunity exploitations (i.e., the upside of certainty) account for more total and propagated rework (29.3% and 21.9%, respectively) than human/component reliability issues. Thus, there appears to be a number of opportunities for rework reduction without necessarily improving human/component reliability:

- *Better inventory management:* Equipment list revisions accounted for the largest number of updates due to a single rationale categorization. Furthermore, there were updates due to inconsistencies between the expected and actual configurations of items launched and between items expected to be launched and items actually launched. While some of these updates were due to the changing equipment requirements for tasks, a portion of these updates were due to an out-of-date listing in the procedure of the item's stowage location and configuration. Thus, it may be possible to reduce such rework by removing procedural references to equipment locations and configurations and instead referring the crew to an electronic database for equipment locations and configurations—such as the Inventory Management System used on ISS (McCallum 2000).
- *Discretion in the pursuit of opportunity exploitations such as “get ahead” tasks and optimizations:* While opportunity exploitations allowed the crews and Mission Control to accomplish more than they expected on these missions, it is important to note that these opportunities exploitations led to significant rework. Ultimately any change to the state of a highly coupled system—be it a change due to bad events that were unexpected or to opportunities that emerged—will have to be accompanied with changes to other parts of the system to prevent hazardous asynchronous system evolution. Thus there is an important lesson for opportunity management to derive from this data: discretion is necessary in the acceptance of opportunity exploitations unless the system is prepared to make the necessary changes to avoid asynchronous system evolution.
- *Task cancellations:* While resisting the temptation to exploit opportunities will lead to a reduction in new rework, the cancellation of tasks can reduce rework that is “waiting” to be resolved (e.g., it can lead to negative rework propagation). However, because the cancellation of a task that other tasks depend on will create procedure rework for those tasks, tasks that are decoupled from other tasks would have to be targeted for cancellation in order to get the desired reduction in rework.
- *Assumptions tracking for improved replanning:* Nearly 11% of propagated rework was due to task deferral, task reprioritization, and consumable management replanning due to the downside of uncertainty. Because the order in which procedures are executed may affect the state of the system when any given procedure is initiated, it is possible for the assumed initial conditions for procedures to be invalidated when procedures are reordered. Thus, if the assumptions are more clearly tracked in the procedures or an electronic database of assumptions, it may be possible to decouple certain procedures from ones that could be reprioritized (i.e., the crew might be able to effectively execute the procedures across a wider range of initial conditions).
- *Reduction of mechanical switch interfaces for the crew:* When one looks more closely at the rework due to actuator/sensor “failure” or degradation/bias, it is often the case that rework is necessary to inform the crew that they should expect a switch to be in another position or that another switch must be used for a procedure. Replacing switch interfaces with software interfaces, for example, could reduce the need for such rework, not because it would alter the change in system state caused by the actuator/sensor problems, but because it would permit the offloading of “switch management” tasks from the crew to the flight

controllers. As mentioned in Chapter 5, ISS flight controllers make use of much more control authority than Space Shuttle flight controllers for commanding subsystem functions due to the relative lack of mechanical switches on ISS. Furthermore, it should be noted that a number of typos were due to mistakes in the descriptions of switch positions, and thus, offloading “switch management” tasks to flight controllers could also reduce the need to initiate updates due to these particular typos.

- *Reduction of planned rework at the end of the mission:* Though technically not a part of rework propagation, procedures that are nominally planned to be updated often occur at the end of the mission, thus weakening the system’s ability to deal with the rework propagation end-of-mission effect.
- *Use of an electronic procedure database:* If the procedures are primarily documented in an electronic database rather than paper books, it would be possible to perform updates without the intervention of the crew. However, such an approach to updating procedures would potentially create three problems: 1) the interaction of the procedure database with other spacecraft databases and software could lead to safety-of-flight issues, 2) the reliability of the procedure database could lead to safety-of-flight issues, and 3) the crew may reject the notion of not being kept aware of all of the updates being made (see Mindell 2008 for an account of astronaut objections to reductions in their control authority in the early U.S. human spaceflight programs).

RATIONALE CATEGORIZATION	TOTAL NUMBER OF UPDATES	OVERALL PERCENTAGE OF UPDATES
"Get-Ahead" Tasks Scheduled	21	11.2%
Consumable Management Optimizations	1	0.5%
Use of Shuttle Resources to Counteract ISS Problems	3	1.6%
Proactive Contingency Preparation and/or Hazard Investigation	10	5.3%
Procedure Nominally Updated in Real-time	0	0.0%
Crew Comfort Optimizations	0	0.0%
Procedure Efficiency Optimization	6	3.2%
Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch	0	0.0%
Total propagated updates due to the upside of uncertainty	41	21.9%

Table 20. Number of propagated updates associated with each update rationale categorization relating to the upside of uncertainty.

RATIONALE CATEGORIZATION	TOTAL NUMBER OF UPDATES	OVERALL PERCENTAGE OF UPDATES
Task Deferral or Reprioritization	5	2.7%
Equipment List Revision	37	19.8%
Consumable Management Replanning	15	8.0%
Unaccounted for Inhibits	10	5.3%
Internal Inconsistencies in the Procedure	2	1.1%
Sensor “Failure” or Bias	7	3.7%
Actuator “Failure” or Degradation	28	15.0%
Unexpected Software Behavior	12	6.4%
Launch Damage (actual or suspected)	15	8.0%
Crew Procedural Slips	1	0.5%
Typos and Omissions	1	0.5%
Inadvertent Deletion of Steps	0	0.0%
Inconsistency between Item’s Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)	2	1.1%
Inconsistency between Items Expected to be Launched and Items Actually Launched	0	0.0%
Unanticipated Environmental/ISS Conditions (e.g., temperatures)	11	5.9%
Total propagated updates due to the downside of uncertainty	146	78.1%

Table 21. Number of propagated updates associated with each update rationale categorization relating to the downside of uncertainty.

Currently, the only mechanism in the Basic Procedure Rework Model for evaluating the effects of such changes is proportional variation of the *Rework Propagation Factor* parameter. Each change can be assumed to reduce the value of that parameter by an amount proportional to the percentage of propagated rework it eliminates. However, because such assumptions would be dubious without further analysis of the causal mechanisms of rework and the specific implementation approaches for these changes, no attempt is made to quantitatively evaluate these solutions in this study. In future work, the *Rework Propagation Factor* variable could be modeled as a state variable rather than a parameter, allowing the modeler to delve deeper into the dynamics of the processes affecting rework propagation. Additionally, researchers can investigate the effectiveness of the ISS Inventory Management System and the predominantly non-mechanical approach to interface design on the ISS in reducing overall procedure rework and rework propagation.

The Effects of Flow Control

Flow control can be used to augment bifurcation control or as an alternative to it in order to cope with the rework propagation end-of-mission effect. The first flow control scheme

examined simply involves the sudden (i.e., step) increase of the procedure rework time horizon towards the end of the mission. As shown in Figure 79, the effect of this scheme is to slightly increase the peak of the rework completion rate and move it to an earlier time in the mission. The advantage of such a scheme is not to reduce the hazard caused by the magnitude of effect, but to improve the timing of the effect (i.e., to make it occur at a more desirable time). Indeed as shown in Figure 80, the effect of this scheme on the Procedure Rework Attractor is to put the system on a path that while taking the system somewhat deeper into the hazardous regions of the phase space, returns the system to the equilibrium more quickly.

The other flow control scheme examined in this case study involves the assignment of a shift of flight controllers and MER engineers to address rework that has propagated beyond the time horizon. This shift could either be an on-call shift that works in parallel to the three primary shifts or it could be one of the three primary shifts. As shown in Figure 79, this scheme creates a sizable reduction in the rework propagation end-of-mission effect. When the performance of this scheme is viewed in phase space—see Figure 81—it is clear that the Procedure Rework Attractor is much stronger with this scheme than without it (i.e., the pseudo spiral-in path to the equilibrium is substantially “shrunk”). However, it is worth noting that fundamental system behavior is the same because the attractor has not been bifurcated. The shift dedicated to rework beyond the time horizon—just like their colleagues in the shifts focused on rework in the time horizon—react to propagated rework accumulation (rather than proactively preventing it as would be done in the bifurcation control approaches) and the changes that they make to the system also introduce propagated rework that they do not immediately realize.

When these two flow control schemes are used together, the rework propagation end-of-mission effect is reduced and occurs at an earlier time in the mission as shown in Figure 79. Additionally, the combined usage of these schemes presents several engineering tradeoffs. Consider the following notional cost function for flow control combining these two schemes:

$$[\text{Eq. 30}] \quad C_{\text{Resources}} = \sum_{i=0}^N 0.0012 \times \text{Total Resource Minutes for Inactive Procedure Rework}_i$$

Where $C_{\text{Resources}}$ is the dimensionless cost of resources applied to inactive procedure rework, i is an index variable denoting the value of the variable at a given time step, and N is the total number of integration steps.

$$[\text{Eq. 31}] \quad C_{\text{TimeHorizon}} = \sum_{i=0}^N 0.0001 \times \text{Procedure Rework Time Horizon}_i$$

Where $C_{\text{TimeHorizon}}$ is the dimensionless cost associated with the value of the procedure rework time horizon, i is an index variable denoting the value of the variable at a given time step, and N is the total number of integration steps.

$$[\text{Eq. 32}] \quad C_{IPNR} = \sum_{i=0}^N 4 \times \left(1 + \frac{\text{Time}}{\text{Mission Duration}}\right)^2 \times \text{Inactive Procedures Needing Rework}_i$$

Where C_{IPNR} is the dimensionless cost associated with the accumulation of inactive procedures needing rework, i is an index variable denoting the value of the variable at a given time step, and N is the total number of integration steps.

$$[\text{Eq. 33}] \quad \text{Overall Cost} = C = C_{\text{Resources}} + C_{\text{TimeHorizon}} + C_{IPNR}$$

This cost function penalizes the system for using resources to address inactive rework with a dedicated shift, increasing the procedure rework time horizon, and allowing inactive procedures needing rework to accumulate. The first two costs are directly proportional to variables in the model while the third has a nonlinear relationship to a variable in the model to account for a desire to address propagated rework early in the mission. These penalties do not complement each other: to reduce one, increases in the other two would most likely have to be accepted. Therefore, it is possible to search for an “optimal” solution as the author has done with the modified Powell Search Algorithm in Vensim[®]. The results of this “optimization” run are shown in Figure 79 and summarized in Table 22.

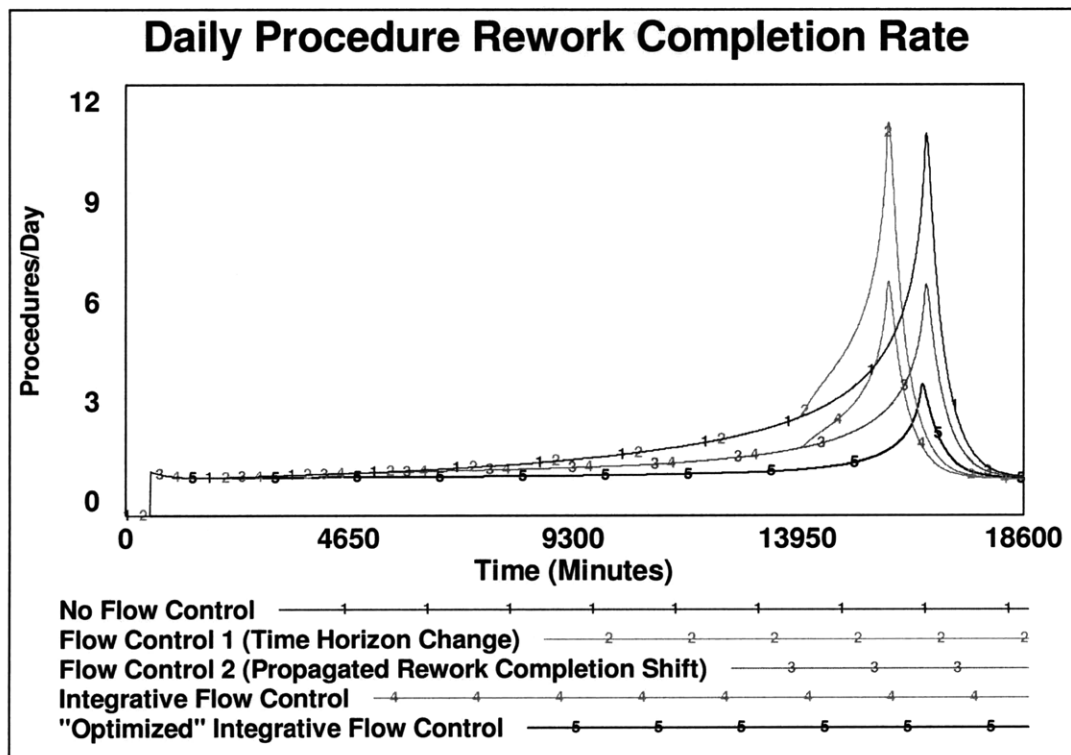


Figure 79. Time history of the Daily Procedure Rework Completion Rate for four simulation runs with flow control and one without flow control.

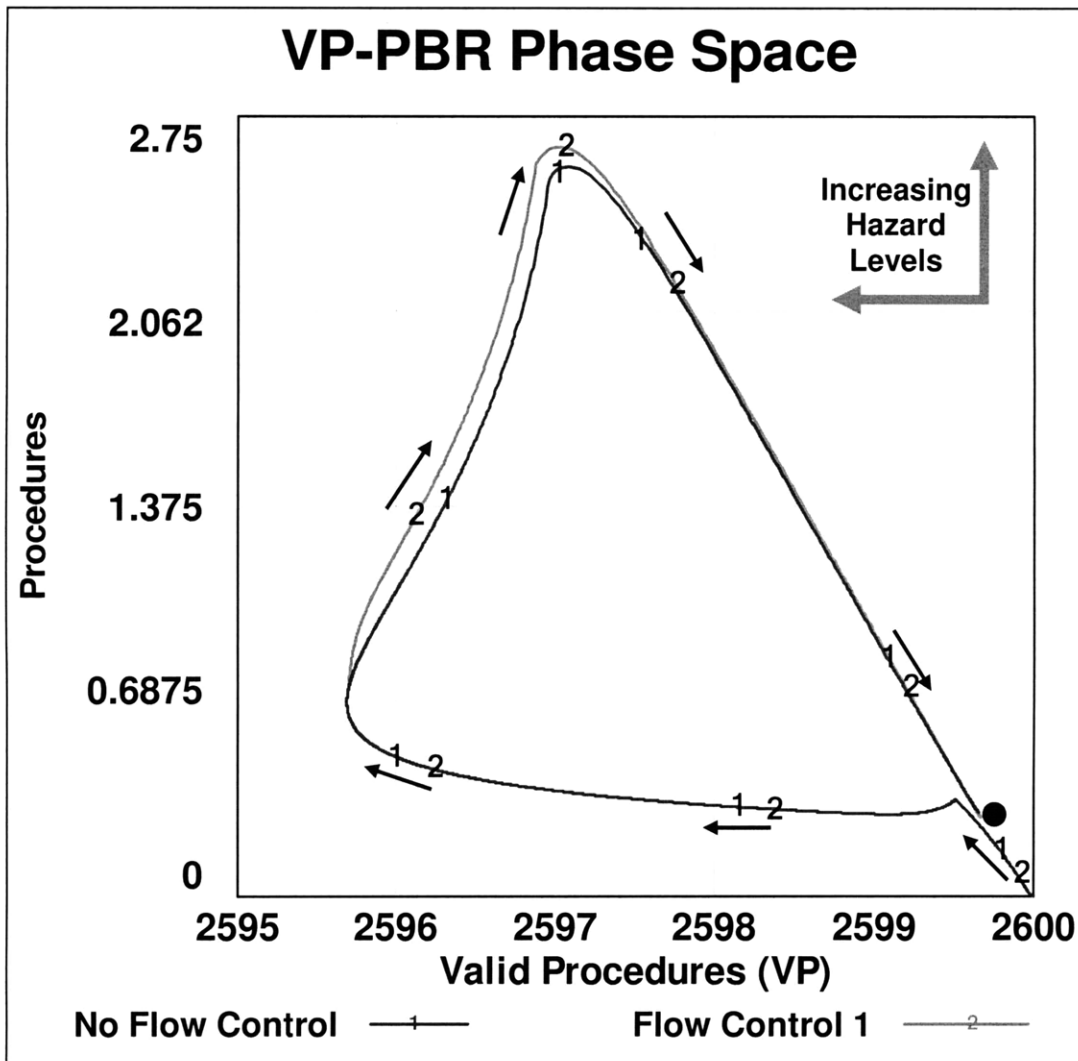


Figure 80. Phase portraits in the *Valid Procedures-Procedures Being Reworked* Phase Space for simulations runs with and without a sudden increase in the procedure rework time horizon.

The reader is advised to consider these results as an example of the type of tradespace involved in developing an integrative flow control scheme rather a statement of the “optimal” parameter values to use for the flow control scheme presented here. If an effort was to be made to identify optimal values for these parameters, the stakeholders involved would have to be more engaged in the definition of the cost function. Furthermore, because the model used for this “optimization” run was built for simulation to understand the system dynamics rather than identification of “optimal” parameter values, it may require some alteration for effective exploration of the tradespace. As stated by Sterman (1991):

“Models can be static or dynamic, mathematical or physical, stochastic or deterministic. One of the most useful classifications, however, divides models into

those that optimize versus those that simulate. The distinction between optimization and simulation models is particularly important since these types of models are suited for fundamentally different purposes...Often such 'what if' information [that can be gained from simulation models] is more important than knowledge of the optimal decision."

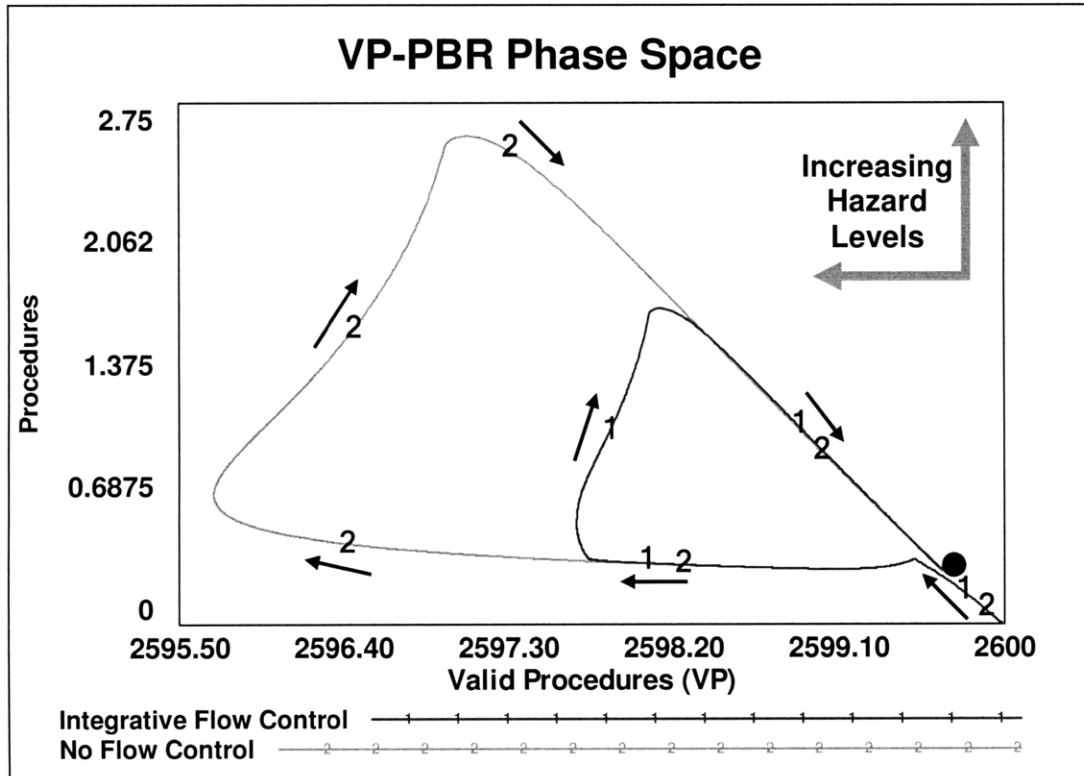


Figure 81. Phase portraits in the *Valid Procedures-Procedures Being Reworked* Phase Space for simulations runs with and without a shift dedicated to rework beyond the time horizon.

PARAMETER	MINIMUM ALLOWABLE VALUE	MAXIMUM ALLOWABLE VALUE	"OPTIMAL" VALUE
Procedure Rework Horizon Change Factor	0	2.5	0.250
Procedure Rework Change Time	14,000 minutes	15,000 minutes	14,000 minutes
Resource Fraction per Inactive Procedure Needing Rework	0.00001	2	1.671

Table 22. Results of the combined flow control scheme "optimization" run.

The Effect of Light Delay

Up until this point, the rework propagation end-of-mission effect has only been discussed in the context of a Space Shuttle mission. Fortunately, because Space Shuttle missions

last for only a few weeks, there is relatively little time for propagated rework to accumulate to the point where it cripples the Procedure Rework Process at the end of the mission. In fact, as shown in Figure 72, the largest peaks in the rate of rework were due to the “novel” or discrete events that occurred on the flights studied. However, the question arises as to how severe the rework propagation end-of-mission effect would be on longer duration missions in which propagated rework will have more time to accumulate.

Because the rework propagation end-of-mission effect requires a mission event in which all of the procedures must be activated by a certain time, one could argue this effect has never been fully encountered on a long duration mission. While there have been many long duration missions on LEO space stations such as the ISS, these space stations are tended by multiple crews and do not land with a crew on board: propagated rework can accumulate, but its activation can always be delayed or ultimately disregarded when the space station is set to be disposed. Furthermore, because crews rotate on these space stations, there is no need to develop the majority of the procedures to be executed over the lifetime of the space station: the procedures that each crew will execute can be developed shortly before that crew launches. On future missions to NEOs, distant moons, and other planets however, there will be points in the mission—such as insertion into the orbit of these celestial bodies—that will require almost all of the outstanding issues to have been addressed. The crew for such events will be the same crew that launched at the start of the mission and therefore, a majority of the necessary procedures will have to have been developed and practiced by this crew before the start of the mission. Furthermore, due to the orbital mechanics of these missions, it will not be possible to significantly delay these events. Additionally, the rework process will be subject to light delay, which—as stressed by the quotes provided at the beginning of this chapter—is expected to change the fundamental nature of human spaceflight operations. Thus, it is necessary to evaluate the rework propagation end-of-mission effect in the context of a long duration mission subject to light delay, such as the one shown in Figure 82.

The results of simulation runs with and without light delay are shown in the time histories provided in Figure 83 and the phase portraits provided in Figure 84. The results from both simulations are nearly identical suggesting that light delay does not significantly alter the rework propagation end-of-mission effect nor weaken the Procedure Rework Attractor. However, the increased mission duration leads to a more pronounced rework propagation end-of-mission effect and severely weakens the Procedure Rework Attractor: the procedure rework completion rate peaks nearly seven times higher than it did for the Space Shuttle mission duration simulations and the system travels deeper into the hazardous regions of the phase space.

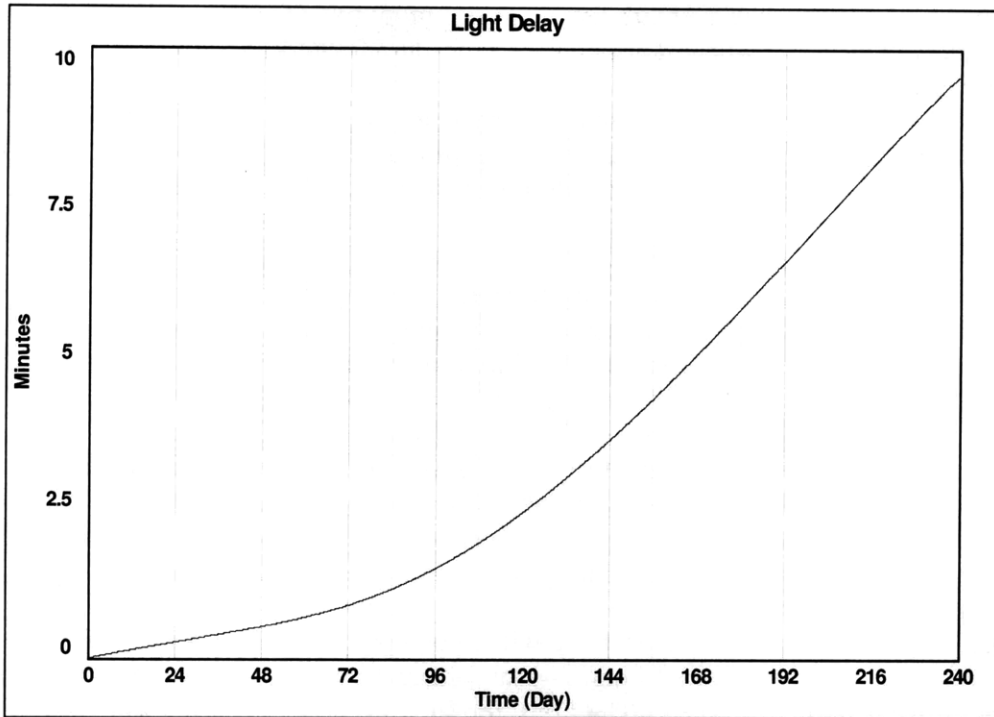


Figure 82. The time history of the light delay affecting a spacecraft on a Hohmann Transfer to Mars perihelion.

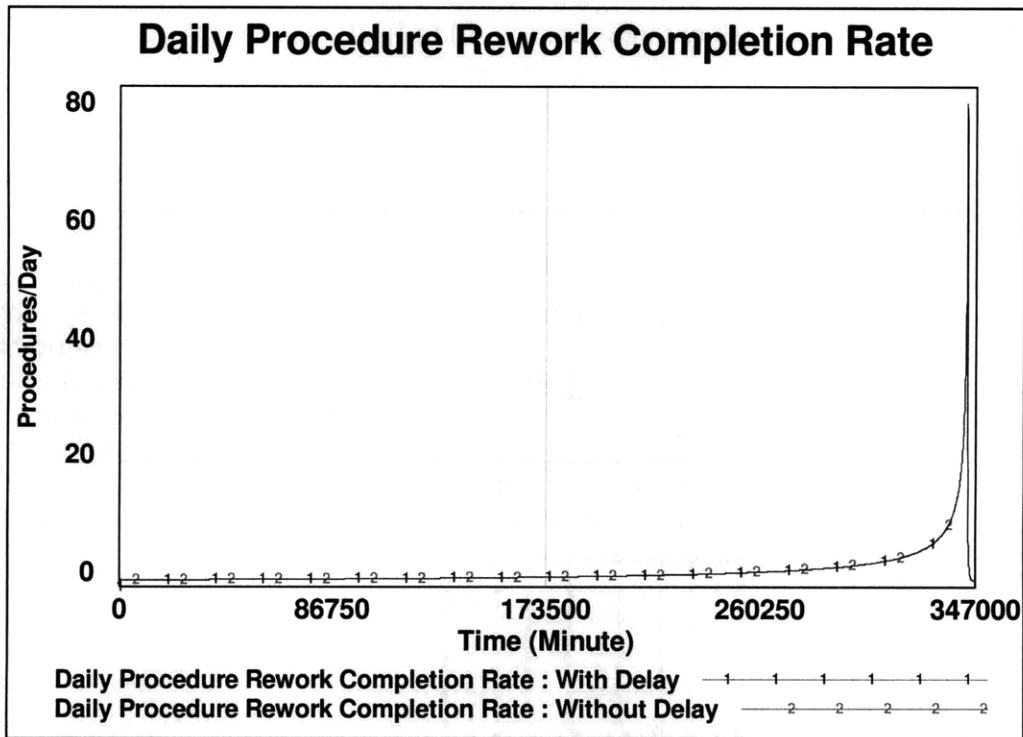


Figure 83. Time history of the *Daily Procedure Rework Completion Rate* for simulation runs of Mars transit duration missions with and without light delay.

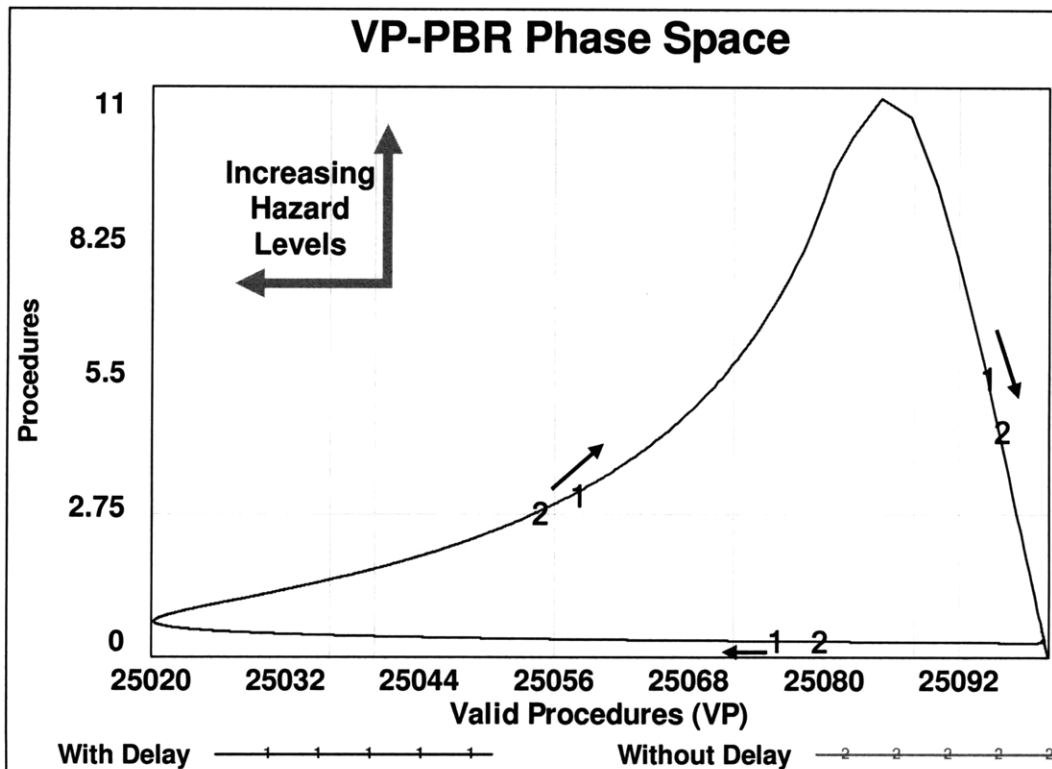


Figure 84. Phase portraits in the *Valid Procedures-Procedures Being Reworked* Phase Space for simulations runs with and without light delay on a Mars transit duration mission.

These simulation runs ended at roughly the time that a Mars-bound crew would be landing on the surface of Mars. Though technically not the end of the mission, such an event would require a substantial fraction of the total mission procedures to be activated. Inserting a spacecraft into the orbit of a distant celestial body and then landing on that body are critical tasks. Indeed, they are so critical that one could perhaps not imagine a worse time for the Procedure Rework Process to be subject to a dramatic rework propagation end-of-mission effect. As noted by Mindell (2008):

“...the landings represented critical moments of each [Apollo lunar landing] mission. Neil Armstrong described them as ‘the hardest for the system and hardest for the crews.’ On a scale of one to ten, Armstrong rated walking around on the moon a one, whereas ‘the lunar descent on a ten scale was probably a thirteen’...An Apollo flight encompassed hundreds of complex operations, but none were as demanding, time-critical, and plagued with uncertainties as the landing, executed in extreme conditions of darkness and cold, far from home...The lunar landings played a microcosm of the entire Apollo program in dramatic ten-minute phases. Here the tensions between human and machine, between manual and automated, between pilots as controllers and pilots as system managers manifested themselves in a string of life- and mission-critical operations, some smooth and some surprising...Like the software itself, the design of the landings embodied the dreams and uncertainties instilled in each mission.”

While the inherent difficulties of orbit insertion and landing are enough to make the timing the rework propagation end-of-mission effect worrisome, it is also worth noting that the effect would occur when the system is subject to a substantial light delay. Though the results suggest that light delay would be a minor factor, the model only treats light delay as a pure information delay. Inefficiencies in astronaut-flight controller communication due to the light delay are not included in the model and would be a major source of uncertainty if they were. If such inefficiencies were to exist, they would probably increase the difficulty of coping with the rework propagation end-of-mission effect. Thus, it would appear from the analysis that the rework propagation end-of-mission effect is more severe for missions to land on celestial bodies than Space Shuttle missions and possibly far more significant in terms of the Procedure Rework Process than the effect of light delay.

Flow control on a mission to land on a distant celestial body

Given the potential severity of the rework propagation end-of-mission effect on missions to land on distant celestial bodies, it is worthwhile to examine some options to mitigate this effect. Of course, many of the bifurcation control techniques mentioned above could potentially be applied to make the effect manageable or to even reverse it. Additionally, at least one of the flow control techniques mentioned above could provide an effective solution to this problem. While the strategy of merely increasing the procedure rework time horizon towards the end of the mission is risky (there is a possibility of not increasing the time horizon soon enough), the use of a shift dedicated to rework beyond the time horizon is likely to substantially decrease the effect. As shown in the time histories in Figure 85 and the phase portraits in Figure 86, a shift dedicated to rework beyond the time horizon substantially reduces the effect. In comparing these plots and phase portraits to those from a Space Shuttle mission duration simulation (i.e., Figure 79 and Figure 81) it is apparent that the relative payoff of flow control increases as mission duration increases.

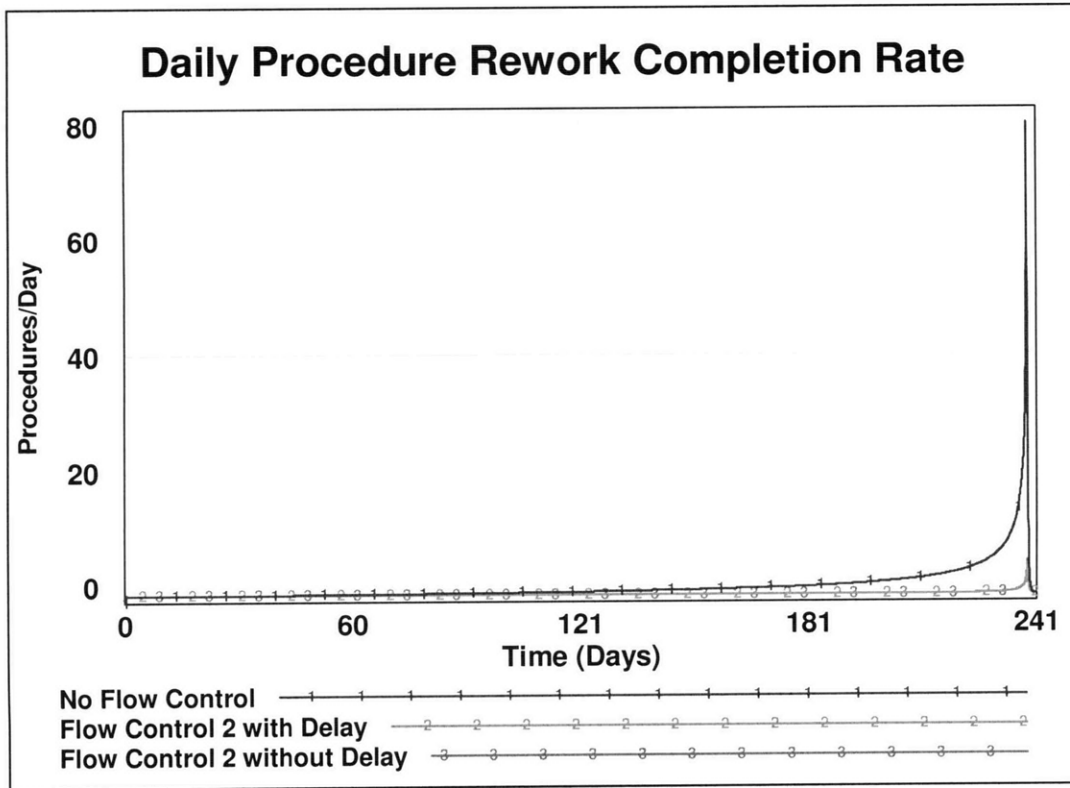


Figure 85. Time history of the *Daily Procedure Rework Completion Rate* for simulation runs of Mars transit duration missions with and without a dedicated shift for flow control.

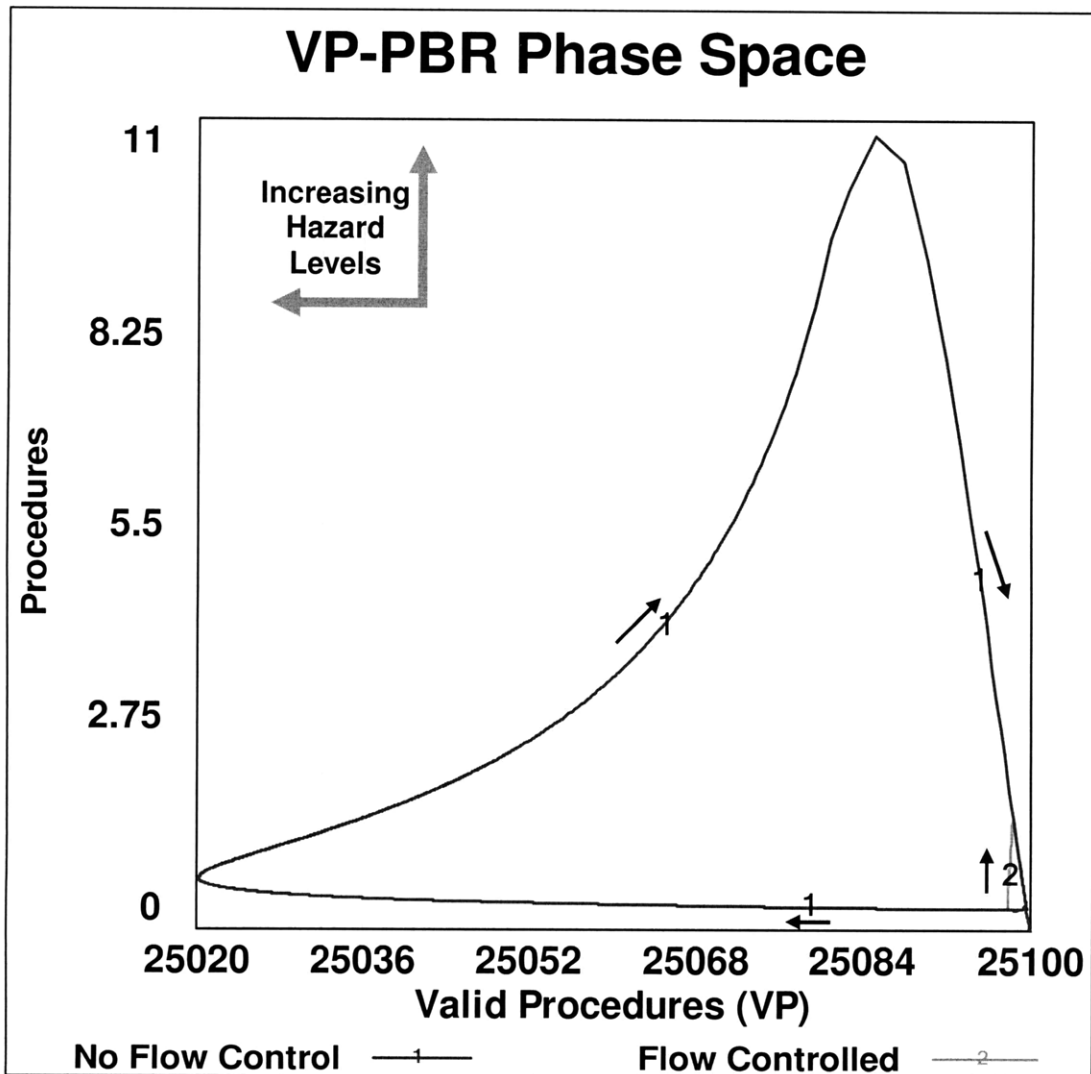


Figure 86. Phase portraits in the *Valid Procedures-Procedures Being Reworked* Phase Space for simulations runs with and without a dedicated shift for flow control on a Mars transit duration mission.

The Disaster Dynamics Bifurcation

The Disaster Dynamics Bifurcation is another bifurcation to which the Procedure Rework Attractor is susceptible. This bifurcation occurs when the shift in flight controller attention from rework discovery to rework completion leads to a situation in which the baseline procedure invalidation rate (i.e., the rate of invalidations due to neither rework propagation nor discrete events) outpaces the procedure rework process. As shown in Figure 87, the rework discovery rate stabilizes at the bifurcation point of the system at a value equivalent to the baseline procedure invalidation rate and thus, procedures needing rework accumulate in the *Active Procedures Needing Rework* stock until all procedures are activated. Beyond the bifurcation point, procedures continue accumulating in the *Active Procedures Needing Rework* stock. In the phase space—see Figure 88 and Figure 89—the pseudo spiral trajectory to an equilibrium point in a relatively safe part of the

phase space is replaced by nearly direct path trajectory to an equilibrium point in a more hazardous part of the phase space.

The parameter that must be varied to create this bifurcation is the *Rework Recognition Delay Attention Shifting Factor*. Fortunately, this bifurcation does not appear to be a threat for Space Shuttle Mission Control as it requires the parameter value to be increased to 7,100 times its baseline value in the baseline scenario. However, the following considerations are noteworthy, as they highlight issues that could make this bifurcation a threat to Space Shuttle Mission Control or in other applications of a procedure rework process:

- As shown in Figure 90, the bifurcation value of the *Rework Recognition Delay Attention Shifting Factor* parameter decays exponentially as the *Baseline Procedure Invalidation Rate* parameter increases.
- The bifurcation is not sudden; the procedure rework process gradually slows as the parameter is varied up to the bifurcation value. Overall the performance of the process can be considered unacceptable for parameter values well below the bifurcation value.
- The rework discovery time is assumed to increase linearly as resources are shifted away from rework discovery. If the increase were nonlinear in reality (e.g., a “square law”), the bifurcation value would be much lower.

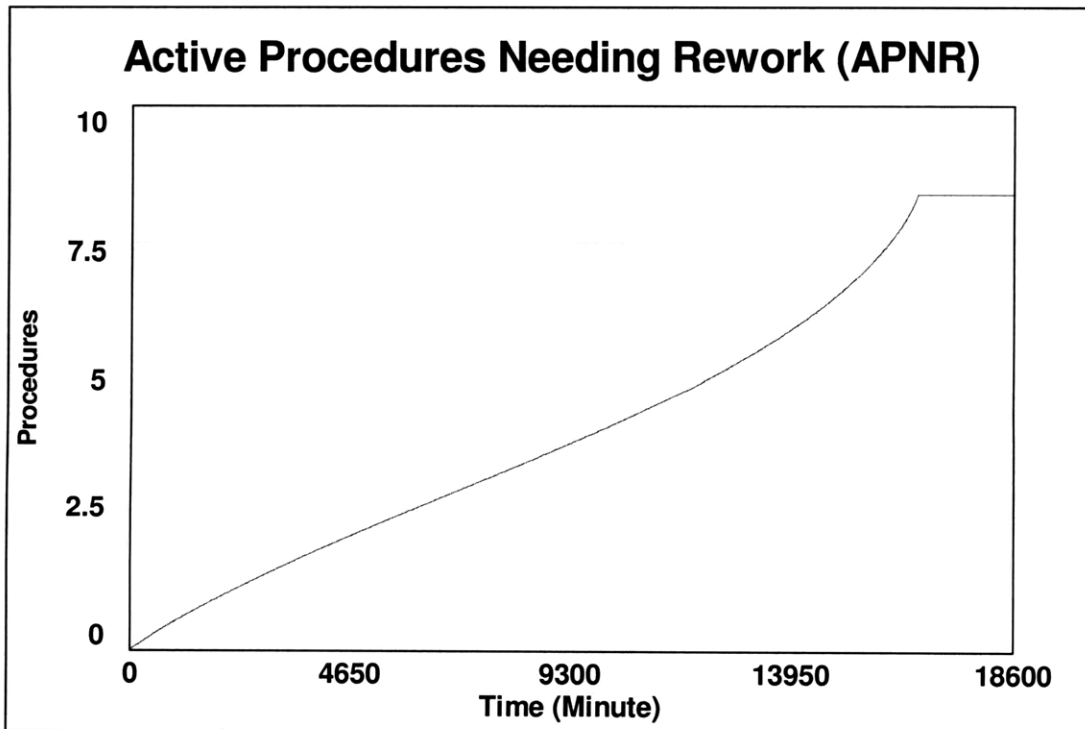


Figure 87. Time history of the value of the *Active Procedures Needing Rework* stock at the Disaster Dynamics bifurcation point of the system.

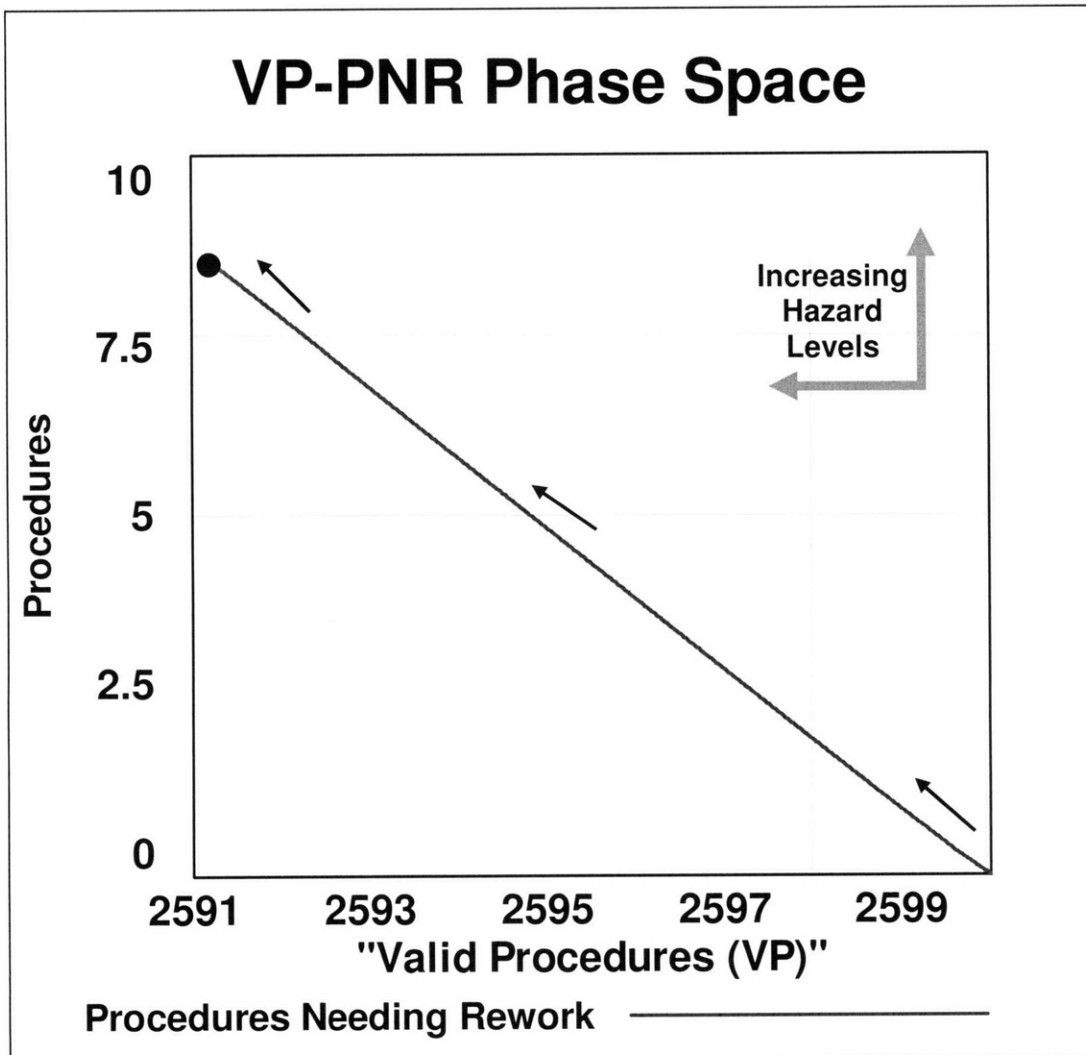


Figure 88. Phase portrait in the *Valid Procedures-Procedures Needing Rework* Phase Space for a simulation at the Disaster Dynamics bifurcation point of the system.

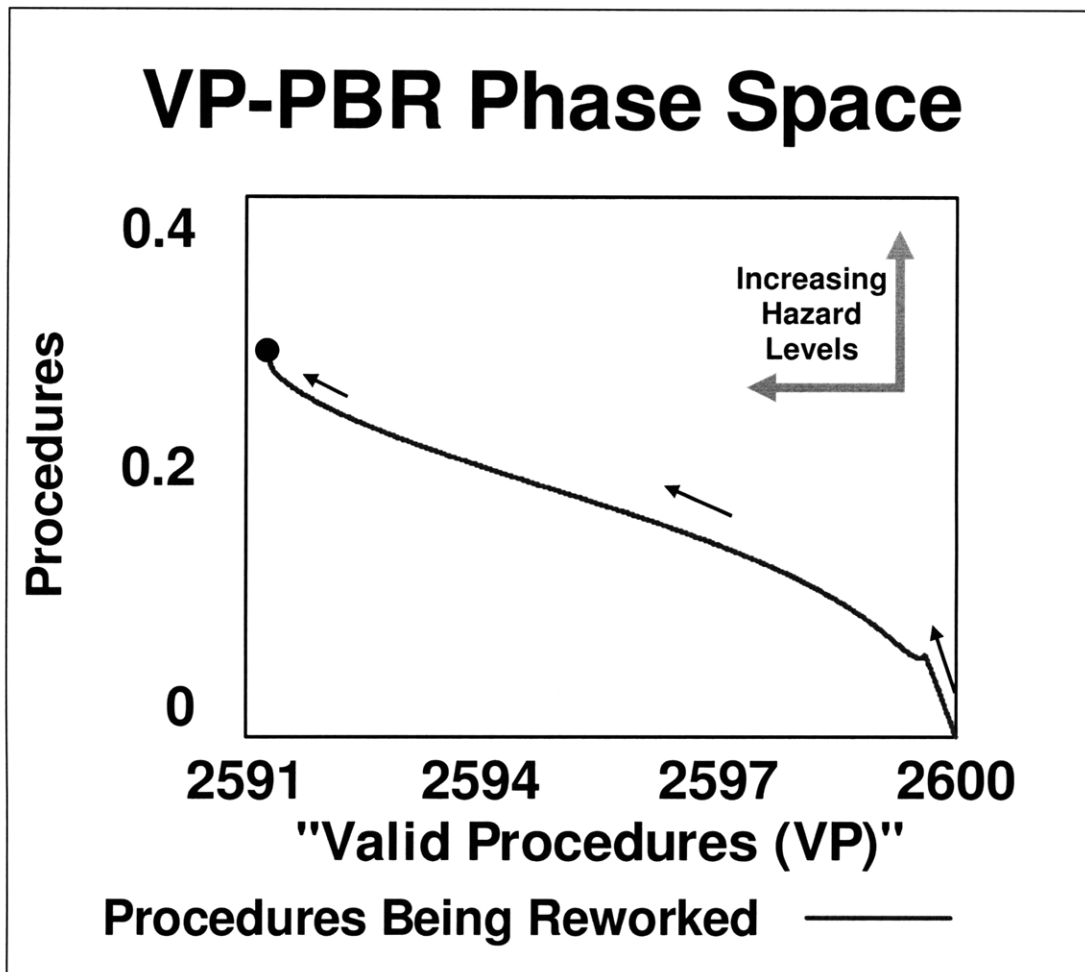


Figure 89. Phase portrait in the *Valid Procedures-Procedures Being Reworked* Phase Space for a simulation at the Disaster Dynamics bifurcation point of the system.

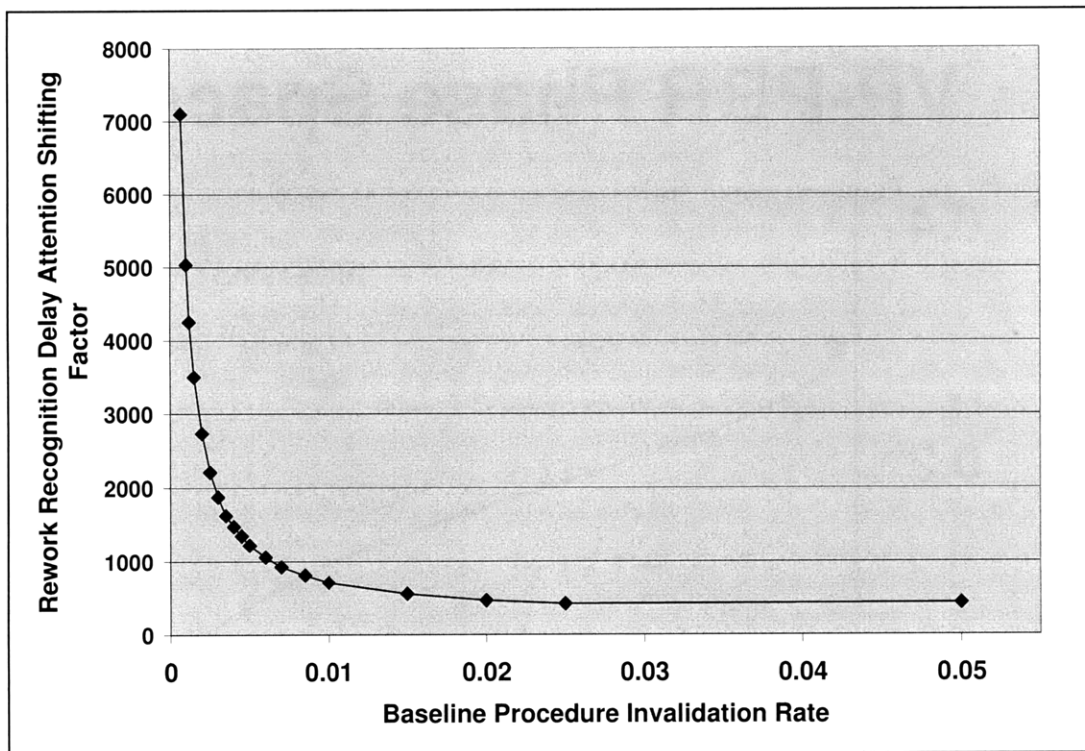


Figure 90. The Disaster Dynamics Bifurcation value of the *Rework Recognition Delay Attention Shifting Factor* parameter as a function of the *Baseline Procedure Invalidation Rate* parameter.

Comments of the usefulness of phase portraits during model development and analysis

As alluded to in the hypothesis of this dissertation, one of the objectives of this case study was to demonstrate the usefulness of evaluating safety control structure performance with phase portraits. Though it can be argued that viewing information in time histories and phase portraits is redundant (the data/simulation results used in each are the same), certain characteristics of the data emerge more readily in phase portraits than they do in time histories and vice versa. For example, consider the time histories in Figure 91 and the phase portrait in Figure 92 for a simulation run in which the dynamics of the system were unintentionally constrained. The constraint—due to a low initial value for the *Inactive Valid Procedures* stock in the Light Delayed Procedure Rework Model¹⁰⁸—flattens the peak of the rework propagation end-of-mission effect and the top of the path that the system takes through phase space as it is returning to the equilibrium point attractor. The flattening is more pronounced in the phase portrait than the time history and thus, it was—not surprisingly—the phase portrait that drew the author’s attention to the unintended constraint on system. Ultimately, it was determined that the initial values used for this simulation allowed the *Inactive Valid Procedures* stock to empty before the rework propagation end-of-mission effect has run its course. Such constraints are particularly important to identify because they could indicate unrealistic behavior or in

¹⁰⁸ The initial value was 3,500 procedures instead of the baseline initial value of 25,000 procedures.

this particular case, they can provide clues on how certain system behaviors can be constrained (i.e., it may be possible to mitigate the rework propagation end-of-mission effect by reducing the overall number of procedures to execute).

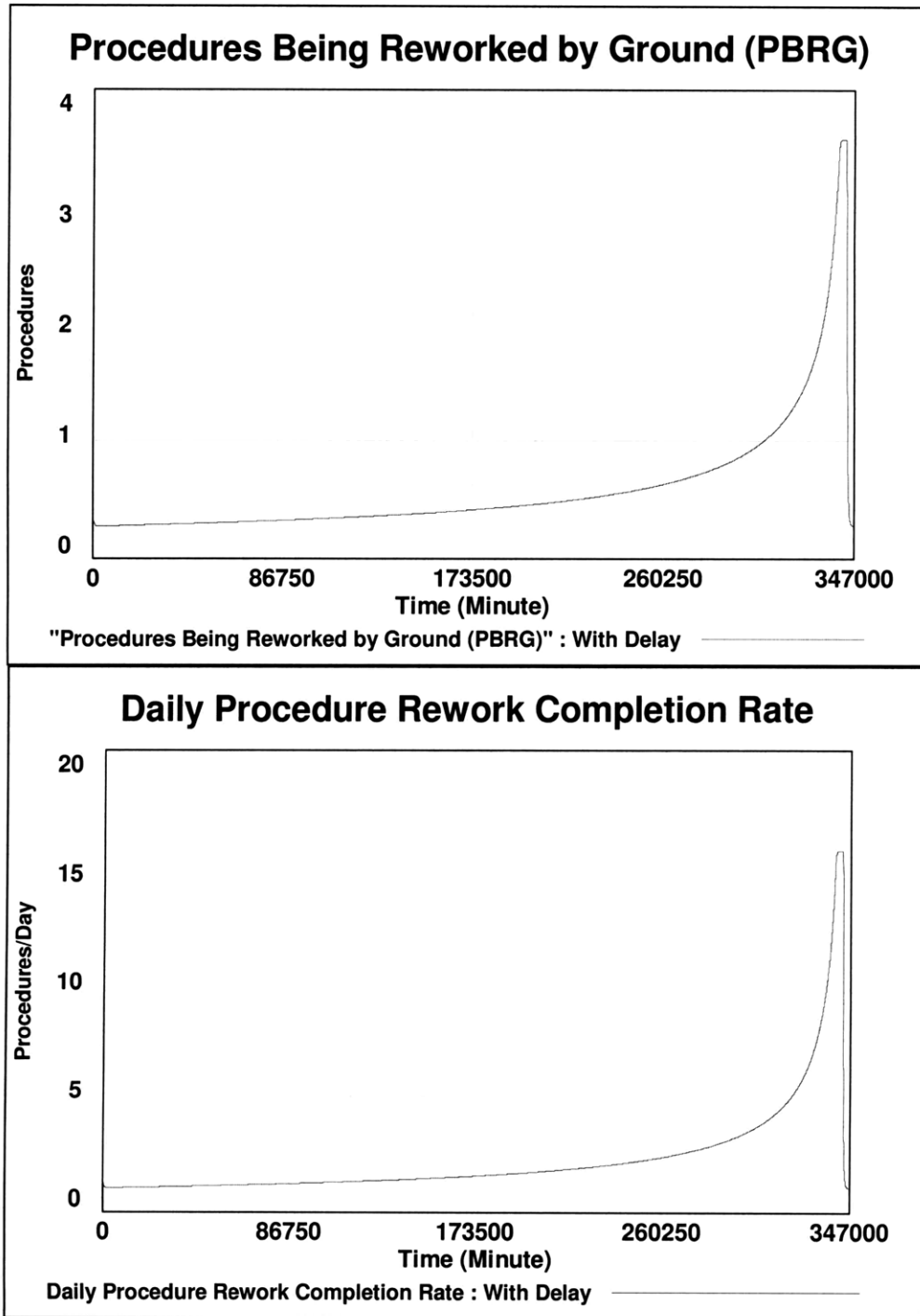


Figure 91. Time histories for a simulation in which the system dynamics were unintentionally constrained.

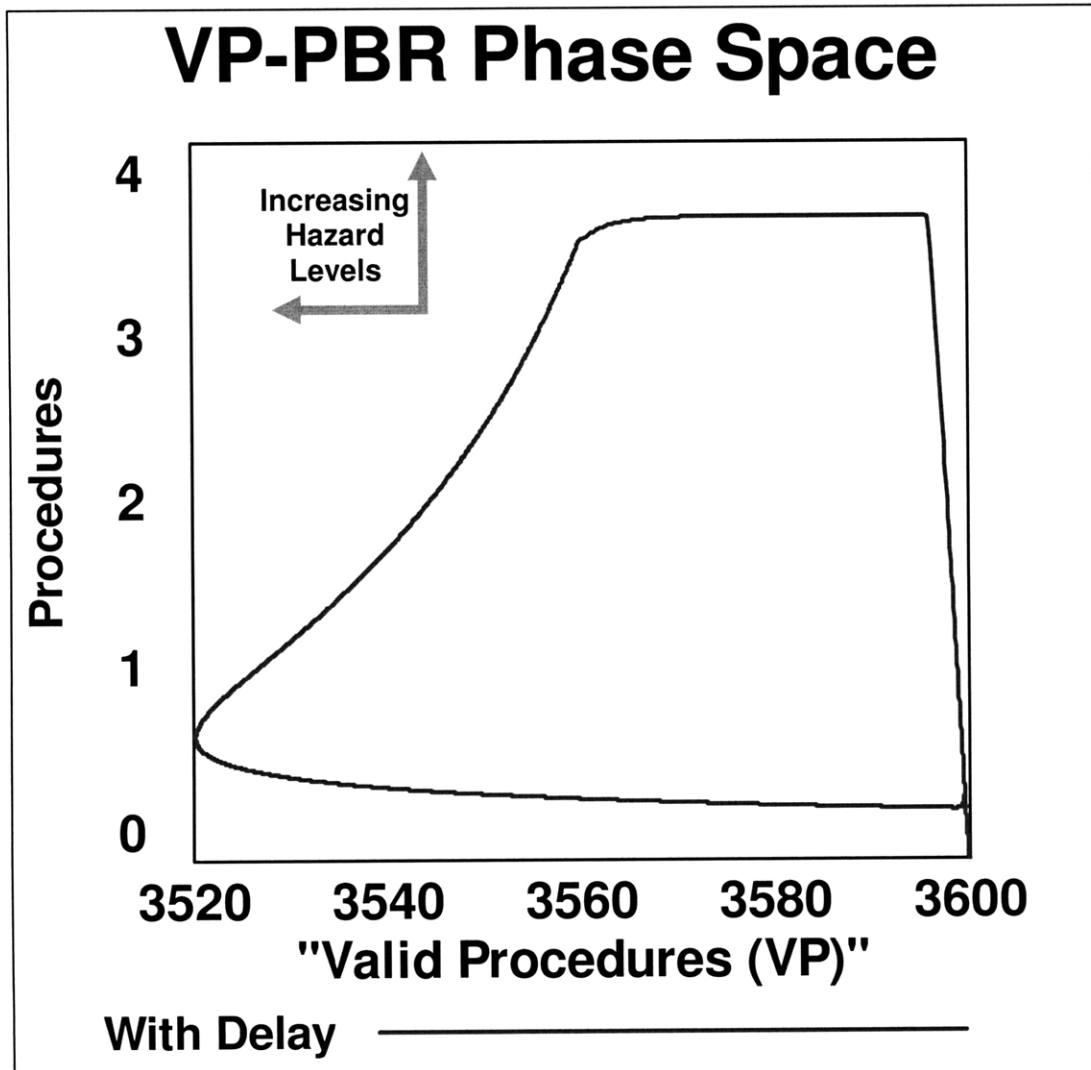


Figure 92. Phase portrait in the *Valid Procedures-Procedures Being Reworked* Phase Space for a simulation in which the system dynamics were unintentionally constrained.

Overall, the author gained insights—in addition to those mentioned in the example above—from both the phase portraits and time histories throughout the model-building and analysis processes. Both types of graphical representations for the simulation results were critical for the identification of logical errors in the model and nuances of the system dynamics.

Summary of analysis results

The key findings of the case study analysis are summarized as follows:

- The Procedure Rework Attractor has a bifurcation (i.e., the Rework Propagation Bifurcation) that leads to a temporary, exponential increase in the rate of procedure rework towards the end of the mission or before any mission event

(e.g., landing on a celestial body) that would require a substantial portion of the unresolved rework to be addressed. This effect—referred to as the rework propagation end-of-mission effect—is due to the slow accumulation of rework beyond the time horizon of the Procedure Rework Process.

- Data from all five of the Space Shuttle missions studied suggests that the rework propagation end-of-mission effect is normal for Space Shuttle missions. In other words, the system typically operates beyond the Rework Propagation bifurcation point. All things being equal, operating on this side of the bifurcation is more hazardous than operating on the other side of it.
- The rationales for procedure rework observed in the five Space Shuttle missions studied indicate that rework is not only necessary to mitigate the effects of negative, unexpected events, but to also prevent asynchronous system evolution when opportunities are exploited. Nearly 30% of all observed procedure rework was due to opportunity exploitations.
- Rework due to human and component reliability issues accounted for less than 30% of all observed procedure rework. The majority of rework was due to opportunity exploitations, logistics issues, and process issues.
- Based on the observed rationales for procedure rework, the following bifurcation control measures might be capable of reducing overall rework and the rework propagation end-of-mission effect: better inventory management, discretion in the pursuit of opportunity exploitations, task cancellations, assumptions tracking for improved replanning, reduction of mechanical switch interfaces for the crew, reduction of planned rework at the end of the mission, and use of an electronic procedure database.
- Increasing the procedure rework time horizon towards the end of the mission will slightly increase the rework propagation end-of-mission effect and move it to an earlier time. It thus, may be possible to use such an approach in certain situations to intentionally make the effect occur at a more desirable time.
- Assigning a dedicated shift of flight controllers and MER engineers—whether they would be an on-call, fourth shift or one of the three primary shifts—to address procedure rework beyond the time horizon will not eliminate the rework propagation end-of-mission effect. However, it will substantially reduce the effect; particularly on long duration missions in which propagated rework has more time to accumulate.
- An integrated flow control scheme in which the procedure rework time horizon is increased towards the end of the mission and a dedicated shift is assigned to address propagated rework is subject to at least three types of penalties: difficulties associated with increasing the time horizon, staffing costs, and risks associated with allowing propagated rework to accumulate. These penalties are not complementary and therefore must be traded against each other.
- If the Procedure Rework Process is applied as it is now on long duration missions to land on celestial bodies, propagated rework accumulation will lead to a larger rework propagation end-of-mission effect than what would be experienced on an average Space Shuttle mission. Moreover, this effect would likely occur shortly before the spacecraft is inserted into the orbit of the celestial body and landed on it (such timing for the effect is probably undesirable given the uncertainties

associated with these mission events). For a mission to Mars, for example, the effect could perhaps be seven (or more) times greater than what has been observed on Space Shuttle missions.

- Light delays on the order of ten minutes, when modeled as pure information delays, will not significantly affect the Procedure Rework Process.
- The Procedure Rework Attractor has a bifurcation (i.e., the Disaster Dynamics Bifurcation) that leads to an inability to discover rework faster than it is being created. This bifurcation is not likely to be a threat to the Space Shuttle Procedure Rework Process, as it occurs well beyond the system's observed operating point. However, if the system's operating point were to migrate towards the bifurcation value, its performance could deteriorate to unacceptable levels well before the bifurcation occurs.

In the next chapter, the implications of these findings relative to the stated hypothesis of the dissertation will be described.

Case Study Limitations

It is impossible to exhaustively address the issues involved in procedure rework in complex, socio-technical systems in a single research study. The research described in this dissertation is not intended to provide universal conclusions on the matter; instead it is intended to draw attention to it and provide a process for further, customizable analysis. The first limitation of the study is that it only looks into procedure rework in one type of organization (i.e., a technical government organization). Procedure rework, which exists in a number of organizations, is sure to vary across organizations in aspects of timescale, formality, and so forth. For example, Mission Control is a component of an organization that primarily exists for safety and technical mission success¹⁰⁹ and thus, the specific insights derived from modeling procedure rework in Mission Control will not necessarily be applicable to organizations where safety conflicts more severely with priorities such cost, schedule, etc. Indeed, as mentioned in Chapter 2, Leveson et al. (2009) have criticized HRO researchers for too broadly generalizing their conclusions following the study of organizations that only or primarily exist for safety (e.g., air traffic control, fire fighting teams, aircraft carrier operations teams during peacetime, etc.). With that said, it is important to reiterate that the aim of the research described in this dissertation was to develop a process for designing and evaluating safety control structures in complex, socio-technical systems while taking into account the unique contextual factors of those systems. The achievement of this goal should make it possible in future studies to apply the methods and modeling archetypes for evaluating procedure rework to organizations that primarily exist for profit, for example, for the purpose of comparing and contrasting the effectiveness and appropriateness of procedure rework in organizations that have different priorities in regards to safety.

¹⁰⁹ Note that Mission Control only takes responsibility for the mission after the spacecraft is launched. Other elements of NASA make spacecraft launch, maintenance, and upgrade decisions and are therefore subject to different pressures (e.g., cost-related pressures, schedule-related pressures, etc.) than Mission Control.

In terms of the application-specific limitations of this case study, there were a few simplifications that should be considered in evaluating the results:

- As mentioned above, flight controller burnout, attrition, and hiring are not considered in the model. While these issues are not likely to be a major problem on short duration Space Shuttle missions, they could potentially have important effects on long duration missions and require corrective action. In fact, ISS Mission Control has developed two “super” console positions (i.e., ATLAS and GEMINI) to perform the Mission Control function at a reduced staffing level during night and weekend shifts so that the flight control team at large will not become burnt out.
- Light delay is modeled as a pure information delay in this case study. In other words, inefficiencies in flight controller/astronaut communications (e.g., the inability to ask clarification questions without delay) are not included in the model.
- The Procedure Rework Process was only evaluated over the timescale of a single mission (though the mission duration was not the same for every simulation). The decision to model certain process factors as parameters rather than state variables hinged on the question, “Do these factors appreciably change over the timescale of a single mission?” Thus, certain parameters in the model may be better treated as state variables if multi-mission timescales are to be considered.

These considerations are mentioned to caution the reader in interpreting the case study results and to highlight potential areas to investigate in future work. As stated by Sterman (1991):

“No one can (or should) make decisions on the basis of computer model results that are simply presented, ‘take ‘em or leave ‘em.’ In fact, the primary function of model building should be educational rather than predictive.”

Accordingly Table 24, which contains the author’s responses to a list of questions from Sterman (1991) for evaluating the validity of a model and its usefulness for solving a specific problem, has been provided to help the reader determine what can be learned from the simulations.

STERMAN'S QUESTION	AUTHOR'S RESPONSE
<i>What is the problem at hand? What is the problem addressed by the model?</i>	The purposes of the models produced in the case study are to identify the Procedure Rework Attractor, its bifurcations, the factors influencing its bifurcations, and its response to flow control schemes under wide range of uncertain conditions in human spaceflight.
<i>What is the boundary of the model? What factors are endogenous? Exogenous? Excluded? Are soft variables included? Are feedback effects properly taken into account? Does the model capture possible side effects, both harmful and beneficial?</i>	The models contain the process variables for procedure rework. The causes of rework are mostly modeled as exogenous factors (the exception being a portion of the propagated rework). As mentioned above, the models can be expanded in future work to capture endogenous side effects of the process that would be relevant on multi-mission timescales. As it is, the models currently capture the endogenous rework propagation end-of-mission effect in a way that closely matches the data.
<i>What is the time horizon relevant to the problem? Does the model include as endogenous components those factors that may change significantly over the time horizon?</i>	The author feels that there is much to be learned by examining the system over both the single-mission and multiple-mission time horizons. The focus of this case study is on the single-mission time horizon, but future work exploring multiple-mission time horizons could be useful.
<i>Are people assumed to act rationally and to optimize their performance? Does the model take non-economic behavior (organizational realities, non-economic motives, political factors, cognitive limitations) into account?</i>	"Non-economic behaviors" are implicitly accounted for in the first order delays in rework discovery/completion and in the <i>Rework Propagation Factor</i> . For example, controllers can create propagated rework by providing rework solutions that will cause rework to propagate to another position or a later time in the mission. The author feels that the explicit modeling of these issues is best left to future work in which the Mission Control stakeholders are further engaged in the modeling process.
<i>Does the model assume people have perfect information about the future and about the way the system works, or does it take into account the limitations, delays, and errors in acquiring information that plague decision makers in the real world?</i>	The flight controllers as represented in the models only react to procedures that are observable to them and within their time horizon for action. Furthermore, they divide their attention between two facets of their job (rework discovery and rework completion) and their performance is affected accordingly.

Table 23. The author's responses to Sterman's (1991) checklist of questions to ask to evaluate the validity of a model and its appropriateness as a tool for a specific problem (Part 1 of 2).

STERMAN'S QUESTION	AUTHOR'S RESPONSE
<i>Are appropriate time delays, constraints, and possible bottlenecks taken into account?</i>	Flight controllers have limited resources for rework discovery/completion and their communications with the spacecraft are subject to light delay.
<i>Is the model robust in the face of extreme variations in input assumptions?</i>	The author subjected the models to a series of extreme conditions tests because of this question. The results of these tests led to numerous model updates to improve model robustness.
<i>Are the policy recommendations derived from the model sensitive to plausible variations in its assumptions?</i>	The rework propagation end-of-mission effect is very robust to parameter and initial condition variation in the model. Furthermore, it is observable in the data.
<i>Are the results of the model reproducible? Or are they adjusted (add factored) by the model builder?</i>	The author has attempted to provide all the information necessary in this chapter, the previous chapter, Appendix 2, and Appendix 3 to replicate the simulation results.
<i>Is the model currently operated by the team that built it? How long does it take for the model team to evaluate a new situation, modify the model, and incorporate new data?</i>	This question is meant to help the reader determine if the people who built the model are available to help the reader use it for some application. The answer to this question depends on the interests of the reader(s) and when this document is being read. For posterity, the author has attempted to describe the models and process used to build and modify them as best as possible so that others can independently use them.
<i>Is the model documented? Is the documentation publicly available? Can third parties use the model and run their own analyses with it?"</i>	The models are documented in Appendix 3.

Table 24. The author's responses to Sterman's (1991) checklist of questions to ask to evaluate the validity of a model and its appropriateness as a tool for a specific problem (Part 2 of 2).

7.3 A Proposed Process for Using Phase Space Attractors to Evaluate System Safety Constraint Enforcement

As mentioned in the dissertation hypothesis and Chapter 4, phase space attractors provide a conceptual construct for the evaluation of safety control structures. In this section, the author proposes a process for using phase space attractors to evaluate system safety constraint enforcement. This process details how he evaluated an actual safety control structure using the concepts of phase space attraction and what others can do to perform a similar evaluation of other control structures. The actions of the process are described both in general (for as broad applicability as possible) and in the specific context of the case study (as a clarifying example).

Process Structure

The process proposed in this dissertation is organized by stages, each representing a maturation level of the evaluation effort to which the process is applied. What it means to be in a stage of the process during an evaluation effort is that the effort involves thought processes and actions of the current stage *and* potentially any or all of those of the previous stages. This structure was chosen instead of a step-by-step (i.e., “cookbook”) structure due to the highly nonlinear nature of an analysis effort occurring within the context of an overall safety-driven design effort. If the overall effort is truly a safety-driven design effort (as opposed to an effort in which safety is added on to the system after it has been designed), then the safety control structure and its presumed operating environment will evolve throughout the process, making linear step-by-step progression through the process difficult, if not impossible.

Over the course of an analysis effort, the effort can progress forward and backward through the stages depending on the evolution of the safety control structure and its presumed operating environment. A successful effort will end on the final stage, leaving the analysis team to focus on other efforts and, when appropriate, to revive the effort in order to make use of new information and resources available for the effort or account for critical changes in the system.

Process Stage 1: Identification of the key state variables relevant to the safety constraints and the hazardous portion of their phase space

In this stage of the process, the key state variables relating to the relevant safety constraints are defined. Additionally, the regions of phase space that the system is allowed (or in more restricted cases, desired) to reside in or visit are determined from the set of relevant constraints. Because system safety constraints are derived from hazards that are defined in STPA in terms of system state, this stage of the process should be straightforward if the constraints are written to provide an unambiguous description of the constrained system state. However, it may be necessary to rework the safety constraints when the allowable phase space implied by the constraints is not viable (e.g., the allowable or desirable phase space is null, physically impractical, etc.). Also, care must be taken to ensure that changes in the key state variables and allowable regions of the phase space due to updates of the safety constraints throughout the safety-driven design effort are incorporated into the process.

The Application of Process Stage 1 in the Space Shuttle Mission Control Procedure Rework Case Study

In the case study presented in this and the previous two chapters, invalidations of procedures were considered to be control flaws that could lead to inadequate control actions in practically any Space Shuttle process that involved the execution of procedures by the astronaut crew. Thus, the number of procedures needing rework (both inactive and active) and number of procedures being reworked were used to define the hazard states associated with these types of control flaws. The model variables *Procedures Needing Rework* (which would eventually become a summation of the *Inactive Procedures Needing Rework* and *Active Procedures Needing Rework* stocks), *Procedures Being Reworked*, and *Valid Procedures* (which would eventually become a summation of

the *Inactive Valid Procedures*, *Active Valid Procedures*, and *Completed Procedures* stocks) were defined for the phase space analysis.

The least hazardous point in the phase space defined above corresponds to a system state in which the value of the *Valid Procedures* variable equals the total number of procedures in the system. The system thus drifts into increasingly hazardous states as the value of the *Valid Procedures* variable decreases and the values of the *Procedures Needing Rework* and *Procedures Being Reworked* variables increase. Ideally one would want to constrain the system so that it would remain at the least hazardous point in the phase space at all times (i.e., the safety constraint would effectively be, “All procedures to be executed by the crew must be valid at all times”). However, this level of constraint is not possible due to the “novel” (i.e., discrete) and “normal” (i.e., effectively continuous) procedure invalidations that occur during Space Shuttle missions and the time delays in rework discovery and completion. Therefore, the safety constraint was initially refined to the following, “All procedures to be executed by the crew must be valid by the time that they are executed.” This constraint immediately implied two things about the Space Shuttle Procedure Rework Attractor: 1) the attractor must attract the system to an equilibrium point near the values of zero procedures needing rework and procedures being reworked and 2) that equilibrium point should be at a spot in which the value of procedures needing rework is no greater than the value of procedures being reworked (procedures needing rework are not known to be invalid and thus they are more likely to be executed). Later—when the rework propagation end-of-mission effect was discovered—it was recognized that this constraint also implied that the attractor must reduce the depth of the end-of-mission excursions into the hazardous regions of phase space or at the very least return the system to the equilibrium point before the affected procedures are executed.

Process Stage 2: Evaluation of the viability of using continuous dynamics to model safety control structure performance

As stated above, the process proposed in this dissertation is meant to increase the depth of the STPA involved in safety-driven design efforts through numerical simulation of the safety control structure’s continuous dynamics. However, this intended purpose raises questions on the usefulness of the process whenever the safety control structure’s behavior is dominated by discontinuous dynamics. Thus, it is necessary in Stage 2 of the process (and later stages) to evaluate whether new and useful information about the safety control structure’s behavior can be derived from simulating its dynamics as being primarily continuous. If it is clear that useful information can potentially be obtained, then the analysis effort can proceed to (or continue in) the later stages of the process. If, on the other hand, the prospect of finding useful information eventually becomes unequivocally doubtful, then the specific process proposed in this dissertation should not be continued further, at least in regards to the specific aspect of the control structure being evaluated. The analysis team should instead focus on other aspects of the control structure or attempt to analyze the aspect of the control structure in question through discontinuous dynamic analysis methods (e.g., State Machine Hazard Analysis).

Unfortunately, there is no simple rule or test for one to invoke in order to determine whether or not useful information will be derivable from a primarily continuous-time dynamic simulation of safety control structure behavior. The following questions were of use in this regard during the dissertation case study and are offered for the reader's discretion:

1. *"Is there a progression or flow of people, material, or information through physical or abstract stages (e.g., experience levels, stations along an assembly line, etc.) that can be modeled with simple conservation laws?"*
2. *"Is the controlled process (or a major part of it) continuous?"*
3. *"Will the control structure's response be more effective if it is (fully or partially) continuous?"*

However, with that said, the reader is cautioned to think beyond these general questions and to perform the evaluation implied in this stage early and often in the analysis effort.

The Application of Process Stage 2 in the Space Shuttle Mission Control Procedure Rework Case Study

The concept of procedures flowing in an approximately continuous manner from states of being valid to being invalidated and ultimately re-validated was identified by the author as soon as the case study was envisioned. However, it was also recognized early on in the case study that many procedure invalidations would be due to events so novel that the accuracy of the model would be affected if they were considered to be continuous in nature. This recognition of discrete or novel events in the data partially led to the selection of the P6 ISS SAW flights as the set of missions to examine. STS-97 and STS-115 in particular, were very similar missions by design, but the former was known beforehand to have encountered a novel event (i.e., the P6 ISS SAW deploy anomaly) while the latter was known to have not encountered this same problem. Thus, by comparing these two missions to each other and ultimately the other three missions, it was possible to qualitatively distinguish novel invalidations from the relatively "normal" deviations and treat them accordingly in the modeling effort. Later on, initial efforts to calibrate the flight data proved encouraging and eventually, useful information was derived from the modeling effort when the rework propagation end-of-mission effect was discovered in the model and then confirmed in the flight data.

Process Stage 3: Identification of state variables, state variable time derivatives, and parameters affecting the key state variables

Stage 3 of the process begins with the qualitative identification of causal (as opposed to simple correlative) relationships between the key state variables, their time derivatives, other state variables and their time derivatives, and parameters. Early work in this stage can involve causal loop diagramming (see Sterman 2000, Ch. 5) or jump straight into the development of the stock and flow structure of the control structure and its operating environment. Later on in the stage (or perhaps in later stages) consideration is given to the division of certain state variables into multiple cohorts (i.e., groups sharing a common trait, such as age) in order to increase the fidelity of the analysis (See Sterman 2000, Ch. 12).

The Application of Process Stage 3 in the Space Shuttle Mission Control Procedure Rework Case Study

As described earlier in this chapter, the initial causal structure of the model was largely derived from three archetypes in the system dynamics literature: the rework cycle (Lyneis and Ford 2007, Lyneis et al. 2001, Sterman 2000), disaster dynamics (Rudolph and Reppenning 2002), and first-order and pipeline delays (Sterman 2000, pp. 415-417). Additionally, variables were added to introduce one-minute-long pulses in the procedure invalidation flows in order to simulate the discrete events during the missions.

Later on when the procedure rework startup delay and procedure rework time horizon were discovered in the flight data, it became necessary to add the *Startup Delay* parameter and divide what were initially the *Valid Procedures* and *Procedures Needing Rework* stocks into two cohorts each to distinguish between the procedures beyond the time horizon and the procedures in the time horizon. With the addition of these two new stocks came the addition of three new flows (two procedure activation flows and an inactive procedure invalidation flow) and the parameters to regulate these flows (e.g., *Rework Propagation Factor*, *Procedure Rework Time Horizon*, etc.). Finally, the causal structure of the basic model was altered to introduce light delay and to implement the flow control schemes in the later model analysis stages of the proposed process.

Process Stage 4: Model construction, iteration, and confidence building

In Stage 4, the analysis team begins to devise and refine the numerical relationships between the state variables, state variable time derivatives, and parameters. The relationships derived are primarily based on conservation laws, decision rules (see Sterman 2000, Ch. 13), control laws, state estimation algorithms, and expert judgment. Parameter values are derived from control set points, resource availability, scientific knowledge (e.g., speed of light), or expert judgment. The dynamics necessary for calculating light delay in the dissertation case study, for example, were based on simple and well established orbital mechanics principles. Once the variable relationships and parameter values are defined, numerical simulation is initiated.

Because the model must be constructed with some degree of subjectivity in quantitative variable relationships, the classification of variables as parameters rather than state variables, and the decisions on which variables to include in the model, it is necessary to build confidence in the model's results before drawing any conclusions from them. First, the model should be checked for dimensional consistency (e.g., that "apples are not added to oranges") and the model's results should be evaluated for sensitivity to the time step of the numerical integration¹¹⁰ and the numerical integration technique. Once dimensional incompatibilities and sensitivity to the numerical integration approach are ruled out, confidence should be increased further by subjecting the model to extreme inputs and initial conditions to ensure that the model's behavior is consistent with the physical reality that it is trying to represent. Only the most absurd inputs or initial conditions should lead to simulated system states that would suggest a physical impossibility (e.g., the dead rising from the grave). Another approach to build confidence in the model is to

¹¹⁰ Forrester (1968) suggests that the time step should be no more than one-half the shortest first-order delay in the system.

perform sensitivity analyses on the model parameters to verify that the model behavior is physically reasonable across a reasonable variation of parameter values. Additionally, confidence in the model can be improved through peer/expert review of the model structure and results. Finally, confidence in the model can be further built through the comparison of simulation results to time history data—preferably through use of metrics such as the Theil Inequality Statistics as described in Sterman (2000, 1984)—provided that an adequate physical incarnation of the model structure, be it heritage or experimental, exists¹¹¹.

Throughout the process of iterating the model and building confidence in it, the analysis team should question the realism of the boundaries and scope of their model. Because the system state modeling in the proposed process is performed on a system level of abstraction, the model is in some sense incomplete until all system states are taken into account. However, such completeness is impossible and thus the modeler(s) is left to decide what level of scope is good enough. This question should be guided by the issue of system coupling. As emphasized throughout this dissertation, complex, socio-technical systems are often nonlinear and thus, a change in one part of the system can lead to disproportionate changes in another part of the system. When developing a safety control structure to produce a specific attractor, the possibility exists that an unaccounted for change in the system could lead to a condition that destroys the attractor over time. Such situations are, in mathematical terms, the coupling that Perrow (1999) and others (Leveson et al. 2006, Woods 2006, Dekker 2005, Leveson 2004, Rasmussen 1997) have identified as a factor in accidents. Thus, the stakes are high to ensure that the model is sufficiently scoped to identify the potential for coupling.

One set of possible starting points in the outward expansion of the model to identify potential sources of coupling are the sources and sinks (i.e., the “clouds” in a stock and flow structure diagram). By “challenging our clouds” (Sterman 2002) or converting a source or sink into a state variable, it is sometimes possible to identify areas in which the safety control structure’s ability to respond to uncertainty could be saturated or eroded. For example, if one were to model the flow of a key resource to the safety control structure (e.g., money, people, etc.) as a source rather than a state variable, he or she would neither recognize the finite limitations of that resource nor the possibility of other parts of the system making that resource unavailable to the safety control structure at an inopportune time. Model parameters are another potential starting point for outward expansion of the model. One way to perform such an expansion would be to convert parameters to state variables with exogenous forcing functions (i.e., inputs that are functions of time rather than system state variables). Alternatively, parameters could be converted into state variables altered by archetypal or unique endogenous dynamic structures (i.e., structures in which all mathematical relationships are functions of system state variables). For example, Marais et al. (2006) described an archetypal dynamic structure—shown in Figure 93—in which safety goals that are widely perceived to be parameters actually erode over time.

¹¹¹ It is also helpful if the attractor produced by the system is not chaotic. Recall from Chapter 4 that time history data of the behavior of the Lorenz Attractor would be quite dubious for inferring system behavior.

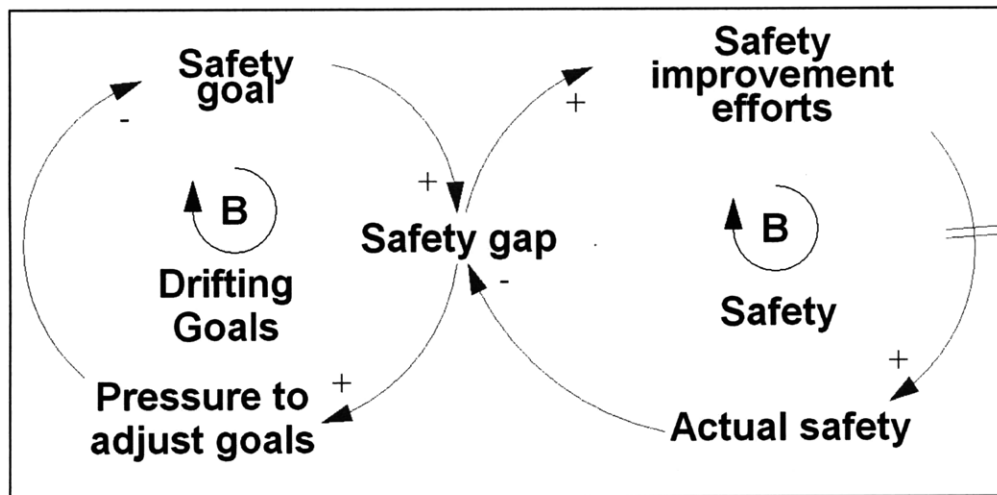


Figure 93. The eroding safety goals archetype (recreated from Marais et al. 2006).

Because outward expansion of the model may uncover system couplings capable of destroying a phase space attractor, it is valuable to monitor the emergence and evolution of phase space attractors appearing in model iterations during Process Stage 4 (and later stages). To perform this monitoring one would create phase portraits of all of the state variables believed to have a feedback relationship and qualitatively evaluate them after every model iteration. Once it appears as though the attractors have stabilized from model iteration to iteration, it may be okay to proceed to the next stage of the process. Such stabilization of the relevant attractors may provide an indication that the attractors are sufficiently decoupled from the rest of the system to proceed or that the modeling effort has begun to focus on aspects of the system that have little effect on the safety control structure dynamics.

The Application of Process Stage 4 in the Space Shuttle Mission Control Procedure Rework Case Study

The descriptions in the literature of the dynamic archetypes from which the qualitative system structure was derived also detail the quantitative structure of these archetypes. Thus, the process of defining the mathematical relations necessary for the initial simulations was relatively straightforward after the initial qualitative structure had been defined. However, early testing of extreme conditions, dimensional consistency, time step sensitivity, and integration technique sensitivity revealed a number of areas in which the mathematical relationships had to be improved to enhance model robustness and realism. These improvements—along with additional rounds of testing and improvement after the introduction of the procedure rework time horizon to model—were made before the model calibration. Then during the model calibration process, further changes were made to the structure of the model to improve the fit of its results to the flight data, and of course, reasonable baseline parameter values were identified.

The phase portraits depicting the Procedure Rework Attractor evolved considerably throughout early model iteration, particularly when the procedure rework time horizon and thus the rework propagation end-of-mission effect were introduced into the model.

However in the later stages of model iteration, the attractor remained relatively unchanged as slight changes were made to the model in order to improve the fit of the simulation results to the flight data. The last noteworthy change in the phase portraits of the attractor occurred when the procedure rework startup delay was introduced into the model, and that change only produced a small kink in the trajectory that the system would take during simulations with rework propagation as it ventured into the more hazardous regions of phase space—see Figure 76, Figure 81, Figure 89, and Figure 92

Ultimately, the Basic Procedure Rework Model and its variants provide a robust and realistic representation of the Procedure Rework Attractor and its rework propagation end-of-mission effect. With that said, there are areas to potentially improve upon in future work. The first area is the treatment of parameters in the model. All of the parameters in the model are state variables in reality and thus, one could explore the possibility of treating some or all of them as such. The key issue in such an effort would be to determine whether they would appreciably change over the relevant operational time period of the system. For example, while the *Baseline Flight Controller Rework Recognition Delay* is probably best treated as a parameter over the time scale of a single Space Shuttle mission, the same may not be true over the time scale of the Space Shuttle Program where flight controller training philosophies could change and operational experience with the Space Shuttle would accumulate. Another area for potential improvement is the treatment of the state variables in the model. While there are no sources or sinks in the core procedure flow structure and thus no “clouds” to challenge, the separation of the procedure stocks into further cohorts may be worth considering in future work.

Process Stage 5: Identification of the phase space attractors produced by the safety control structure and their bifurcations

Process Stage 5 begins with detailed analysis of the phase space attractors produced by the safety control structure. As mentioned above, the phase space attractors can change from one model iteration to the next and thus, it is important (for the sake of reducing wasted effort) to ensure that the model is relatively mature before initiating this stage of the process. Additionally, because discontinuous dynamics tend to make phase portraits more difficult to interpret, it is important to include mechanisms in the model for deactivating discontinuities that have been modeled. For example, suppose that data is available for model calibration and that it contains significant discontinuities. In such an instance, it would be necessary to include the discontinuities while calibrating the model and then deactivate them during the early analysis of the attractors. In doing so, a clearer picture of the underlying continuous dynamics of the safety control structure can be developed before an attempt is made to understand the system dynamics with the discontinuities.

Analysis of the phase space attractors involves two types of model sensitivity analysis: variation of initial/disturbance conditions and variation of model parameters. Initial/disturbance conditions are varied in order to estimate the strength of the attractor while parameters are varied to determine the attractor bifurcation points. Exploration of the parameter space and range of possible initial conditions can be carried out in one-

parameter-at-a-time (OPAT) searches¹¹², adaptive OPAT searches, or through the use of automated search algorithms, if available. However, the reader is advised to perform these kinds of analyses only on relatively mature models because as a model of any given size matures, its potential parameter space and potential range of initial/disturbance conditions is likely to become better defined and thus more manageable.

The Application of Process Stage 5 in the Space Shuttle Mission Control Procedure Rework Case Study

As mentioned above, two bifurcations were discovered in the analysis of the Procedure Rework Attractor: the Rework Propagation Bifurcation and Disaster Dynamics Bifurcation. These bifurcations—caused by variation of the *Rework Propagation Factor* and *Rework Recognition Delay Attention Shifting Factor* parameters, respectively—were found through simple OPAT searches. Furthermore, because the Disaster Dynamics bifurcation point occurred incredibly far (i.e., 7100 times) beyond the baseline operating point of the system, the author analyzed the sensitivity of this bifurcation point to the variation of other model parameters. The plot in Figure 90 is an output of one of these analyses. These sensitivity analyses were conducted by varying a single parameter that might affect the bifurcation point by a fixed amount and then varying the *Rework Recognition Delay Attention Shifting Factor* until the bifurcation occurred.

Ultimately, neither of the two bifurcations occurs suddenly. Increasing the *Rework Propagation Factor* parameter gradually weakens the attractor, leading to further and further excursions into the hazardous regions of the phase space during the rework propagation end-of-mission effect. Increasing the *Rework Recognition Delay Attention Shifting Factor* gradually slides the equilibrium deeper into the hazardous regions of phase space (i.e., to higher equilibrium values of the *Procedures Needing Rework* variable and *Procedures Being Reworked* stock).

Process Stage 6: Evaluation of bifurcation control and flow control options to improve the phase space attractors produced by the safety control structure

Following the analysis in Stage 5, the analysis team may deem the attractor properties of the safety control structure unsatisfactory for effective safety constraint enforcement. Possible reasons for deeming the attractor properties unsatisfactory include:

1. Inability of the attractor to prevent movement of the system into the hazardous regions of the phase space,
2. Inability of the attractor to persist across a wide enough range of initial/disturbance conditions,
3. Slow reaction to undesirable initial/disturbance conditions,
4. Potential for an undesired bifurcation during system operations, or
5. Inefficiency of the attractor.

¹¹² Frey et al. (2003) discuss the advantages of one-parameter-at-a-time experimentation. Though their primary focus is on physical experimentation rather than numerical experimentation, the general concepts apply in both forms of experimentation.

Thus, in Stage 6 of the process, the analysis team can explore possibilities for using bifurcation and flow control to improve the attractor's ability to prevent the system from entering (or lingering too long in) the hazardous regions of the phase space. Options for bifurcation and flow control are identified through a review of the bifurcation analysis results obtained in Stage 5 of the process and an evaluation of the dynamics of the "flows" in the system. The candidate solutions are then implemented in the model through the model-building techniques of the preceding stages of this process.

The Application of Process Stage 6 in the Space Shuttle Mission Control Procedure Rework Case Study

The bifurcation control schemes pursued in the case study were identified from the results of the bifurcation analyses in Process Stage 5. Because the Disaster Dynamics Bifurcation did not appear to be a threat to the Procedure Rework Process in Space Shuttle Mission Control, no action was deemed necessary other than to recommend that the current level of flight controller rework recognition performance be maintained. Additionally, because the Rework Propagation Bifurcation occurs well below the operating point of the system, the author decided to investigate ways in which the operating point could be brought closer to the bifurcation point (i.e., to lower the value of the *Rework Propagation Factor* parameter). After identifying the rationales for procedure rework (particularly propagated rework) the author proposed several technical and process improvements—described earlier in this chapter—to investigate in future work for their effect on the value of the *Rework Propagation Factor* parameter.

Process Stage 7: Reflection, dialogue, and wrap-up

Perhaps, one of the most difficult questions to answer in an analysis effort, particularly when a complex system is being analyzed, is when the analysis is "good enough." In Stage 7 of the process, the analysis team must evaluate whether or not the model developed in the process has served its purpose. Typically, the purpose will center on the identification of control flaws, the recommendation of additional safety constraints on the system, redesign of elements of the control structure, or the addition of new elements to the control structure. The "clients" in these situations will most likely be the managers, engineers, and other stakeholders driving the overall safety-driven design effort.

In Stage 7, a dialogue must be initiated between the analysis team and its "clients" to determine whether or not the model produced has served its initial purpose or is potentially useful towards another purpose. If the model has not quite served its purpose, the analysis team should evaluate what must be done to the model in order to make the model serve its purpose. If the model has been deemed to have served its purpose, the analysis team must determine whether or not an additional purpose can be served by further elaborating the model. Furthermore, they must solicit critiques and advice from individuals outside of the modeling effort and key stakeholders in the effort. If it is found that no further purpose can be served by continuing the modeling effort with the individuals currently involved, the individuals must move on to their next effort while facilitating the transfer of its insights or further effort to the stakeholders¹¹³.

¹¹³ Facilitation of this transfer, in some instances, could involve the development of a version of the model adequate for use by the stakeholders in an operational or developmental setting (e.g., an archetype

Such transfers may be awkward and otherwise difficult, but it is paramount to maintain a clear purpose throughout any modeling effort and to walk away from the effort when no further purpose can be served. In discussing the importance of the purpose that drives a modeling effort, Meadows et al. (1982) pointed out that every member of the *Limits to Growth* global modeling efforts—briefly described in the Chapter 3—had moved on to other modeling efforts by that time because they felt that the purpose for the models had been served. In subsequent years, the *Limits to Growth* team briefly revisited these modeling efforts on occasion, but only when enough new data became available or attitudes towards ecology evolved enough to provide purpose for further effort. As pointed out by Forrester (1985):

“I feel that the emphasis on ‘The’ model is not only unrealistic, but probably also alarming to the reader...I believe we are proposing the ‘Process’ of modeling rather than particular frozen and final models...we are suggesting that models will help to clarify our processes of thought; they will help to make explicit the assumptions we are already making; and they will show the consequences of the assumptions. But as our understanding, our assumptions, and our goals change, so can the models.”

The Application of Process Stage 7 in the Space Shuttle Mission Control Procedure Rework Case Study

The purpose for the case study in this chapter was to develop a process for using the notion of phase space attraction to evaluate safety control structures and to provide the reader with an example application of the process to a “real-world” complex, socio-technical system. An additional purpose was to identify key aspects of the dynamics of procedure rework (i.e., the type of attractor produced, its bifurcations, factors affecting its bifurcations, and its response to flow control schemes). While the solutions provided for bifurcation and flow control of the attractor are not necessarily “optimal”, further development of the case study would not be likely to contribute to the reader’s understanding of the concepts involved in applying this process. Furthermore, the results obtained are worthy of discussion in the appropriate stakeholder community to evaluate their merit and to formulate meaningful goals and strategies for the continuation of this work. In short, the purposes of the case study have been fulfilled and thus the author’s focus in the next chapter is shifted towards reflection on the contributions of this dissertation and proposed possibilities for future research.

contribution to the repository of dynamic structures available to practitioners of Dulac’s methodology, etc.). In other instances, it may be the case that the incumbent modeling team lacks the skill set, financial resources, domain knowledge, access to data, or interest to expand upon the model to serve another purpose while others do possess these attributes. In such instances, the incumbent analysis team would provide the new analysis team the support that they would need to begin pursuing these new purposes.

Chapter 8: Summary of Contributions, Future Work, and Concluding Remarks

8.1 Chapter Overview

In this chapter, the author closes his argument. First, the author's hypothesis is revisited and his contributions to the management of uncertainty in engineering systems are summarized. Next, the author's contributions to procedure rework processes in human spaceflight and in general are reviewed. Then, the author describes possible directions for further research. Finally, the author summarizes the entire dissertation and provides a closing statement.

8.2 The Dissertation Hypothesis Revisited

The hypothesis of this dissertation is as follows:

“Modeling the output of system safety control structures as phase space attractors with nonlinear, continuous dynamics subject to uncertain initial (or disturbance) conditions will provide useful insights in the design and operation of system safety control structures.”

This idea is derived from a desire to improve our understanding of how robustness, adaptability, flexibility, and resilience in complex socio-technical systems can be evaluated and improved for the purpose of opposing unsafe decisions and component behaviors in these systems. If a safety control structure does not have a sufficient blend of robustness, adaptability, flexibility, and resilience to oppose unsafe decisions and component behaviors, it may not successfully attract the system to safe states throughout its lifecycle. What the safety control structure lacks in robustness could allow the system to drift deep into the hazardous regions of its phase space after a disturbance. What it lacks in beneficial adaptability (i.e., adaptability that resists asynchronous or otherwise detrimental system evolution) can allow the attractor to bifurcate over time and draw the system to unsafe states. What it lacks in flexibility can allow its attractive force to be overpowered by changes in the system's environment over time. Finally, what it lacks in resilience can prevent the safety control structure from maintaining (or, in times of crisis, recovering) its desirable attractive properties. In other words, evaluating and improving the attractor produced by a safety control structure can be *one* approach to ensuring that the structure has suitable robustness, adaptability, flexibility, and resilience to oppose unsafe decisions and component behaviors in its uncertain future.

The support provided for this hypothesis throughout the dissertation is summarized in the next three sections. The first of these sections includes a summary of a widely applicable process that emerged from thinking of safety control structure evaluation and design as a phase space attractor engineering problem. Additionally, it describes lessons learned in the application of this process for opportunity management and the treatment of non-novel events in uncertainty management. The second of these sections mentions how an

example application of the process filled gaps in a specific literature. Finally, the third of these sections lists several directions for further research identified while acting on this hypothesis.

8.3 Contributions to the Management of Uncertainty in Engineering Systems

The first class of contributions from this dissertation relates to the management of uncertainty in general. The safety control structure evaluation process proposed and demonstrated in this dissertation holds promise for helping engineers develop better safety control structures to manage the downside of uncertainty. Additionally, in applying this process to an actual system, two interesting nuances of the management of uncertainty were identified. All three contributions are reviewed more fully in the remaining paragraphs of this section.

Development of a process for the quantitative evaluation and improvement of control structures for safety risk (and opportunity) management

By thinking of safety control structure evaluation and design as a phase space attractor engineering problem, the author was able to develop, demonstrate, and describe a process that—though restricted to systems that can be behaviorally represented with continuous dynamics—should be applicable for safety risk (and opportunity¹¹⁴) management in a wide range of situations. The process consists of seven model-building, analysis, and refinement stages that outline an approach for identifying phase space attractors produced by safety control structures. These attractors should attract the system to safe system states despite an onslaught of uncertain events. If such an attraction is not the case or if the attraction is not as good as it should be, the process includes bifurcation and flow control analysis techniques for control structure improvement.

The advantage of such a process over processes involving a linear accident model, for example, is that it does not constrain itself to a linear conception of nonlinear phenomena. Linear accident models rely on a chain of events, which are manifestations of symptoms of the states of the system and its environment. Events depend on confluences of these states that are so complex that they can only be represented by chance. Correctly characterizing these chances becomes an infinitely impossible task in complex systems and thus the task is linearized to the extent possible. In other words, safety risk management is reduced to a linearized “gamble” when the linear accident models are used.

By shifting the focus to system states—as done in the proposed process—our goal changes from the infinitely impossible task of correctly characterizing event chances to the regulation of one or more of the many states that must coincide to allow the undesired events to occur (i.e., to actively control risk rather than gambling on it). Contrary to what one may intuitively think, this shift simplifies the problem to the extent that nonlinearities in system state can be considered. Of course—as demonstrated by even simple chaotic

¹¹⁴ While opportunity management was not the focus of this dissertation, the analysis surprisingly uncovered ways in which safety risk and opportunity are linked. Thus, it is reasonable to speculate that the proposed process can also be used to impact opportunity management directly or indirectly.

systems like the Lorenz Attractor—we will always lack the necessary understanding to determine what specific states the system of concern will be in at all times. This uncertainty is the reason why the concept of phase space attraction is so important. By understanding phase space attraction and how to improve it, we can constrain the system to the safe regions of its phase space without having full certainty of present and future system states and without having to linearize our approach to safety risk management.

Identification of an example of a potential hazard in opportunity exploitation

Though the focus of this dissertation was on safety risk, a contribution to our understanding of opportunity exploitation was nonetheless inferred from the data. Nearly 30% of all instances of procedure rework were due to the upside of uncertainty (i.e., unexpected opportunities that emerged and were exploited). This information has two implications for opportunity exploitation.

The first is that control authority for adaptation can be used to respond to both the upside and downside of uncertainty even if it is predominately in place to manage one side. In other words, having the ability to make changes to the system in response to dangerous, unexpected events may also allow the system to take advantage of unexpected opportunities. This potential for “dual use” of adaptation control authority should be considered when tradeoffs are made as to whether or not to include such capability into the system.

The second implication of these results is that opportunity exploitation can introduce hazards into the system if the exploitations are not accompanied by efforts to coordinate these exploitations with other actions planned for the system. Any unexpected change to the state of the system—even if it is made with the intention of improving system performance—can potentially turn a valid procedure or plan into a hazardous procedure or plan. In implicitly recognizing this potential, Mission Control and the MER routinely “resynchronize” procedures and plans that are desynchronized by opportunity exploitations through the Procedure Rework Process (i.e., they prevent asynchronous system evolution). Such efforts to keep the system synchronized regardless of the positive or negative nature of the desynchronizing “force,” are a reason why Mission Control and the MER are not only very successful in safely guiding the astronaut crew through undesired contingencies, but also in helping the crew safely accomplish more than what is expected of them. Thus, the general lesson for opportunity management is that all opportunity exploitations must be accompanied by efforts to coordinate these exploitations with other actions planned for the system.

Identification of an example of the role of non-novel events in operational hazard emergence

Rudolph and Repenning (2002) used a simple, generic dynamic structure to show that while novel events tend to garner much attention as operational hazards, the effects of non-novel events can accumulate to effectively break down an operational process. By identifying the rework propagation end-of-mission effect, the author has identified a real-world example of such phenomena. This effect is not due to novel events, it is due to the accumulation and sudden activation of procedures invalidated by numerous non-novel

events (i.e., baseline and propagated procedure invalidations) dictated by the system's dynamic structure. Fortunately, this effect has not yet led to a breakdown of the Procedure Rework Process in Space Shuttle Mission Control. However, its presence and the possibility that it could be far more damaging on long duration missions to land on distant celestial bodies serves as a reminder that the way in which non-novel events are handled by the system's dynamic structure is an important aspect of uncertainty management. In fact, one could say that the "normal" nature of system accidents that Perrow (1999) referred to is due to a widespread lack of understanding of how to safely handle non-novel or "normal" events in complex systems (after all, rework propagation is due to system coupling).

8.4 Contributions to Procedure Rework Processes for Human Spaceflight and Other Applications

The second class of contributions from this dissertation relates to procedure rework processes for human spaceflight and other applications. Despite little mention of procedure rework in the literature, the author believes that procedure rework is a primary reason for the success of Mission Control and the MER in guiding astronaut crews safely through spaceflight operations. The qualitative and quantitative aspects of its dynamics that were identified in this dissertation may thus be useful in improving the operational success of Mission Control, the MER, and other operational entities that heed the lessons of this study. In the remaining paragraphs of this section, these contributions are more fully discussed.

Identification of the severity of rework propagation

Rework propagation occurs for two reasons. The first reason is that the procedures are based on assumptions of system states that are in part affected by other procedures (i.e., procedures are coupled and can be invalidated simultaneously). The second reason is that there is a time horizon for the procedure rework process (i.e., procedures are typically reworked less than two flight days before they are to be executed). The result of rework propagation is an exponential increase in the amount of rework before the end of the mission or any other event that would require "all loose ends to be tied up" (i.e., the rework propagation end-of-mission effect)¹¹⁵. The data indicate that this effect commonly occurs on Space Shuttle missions and may not be as much of a problem as the "novel" events that occur on many Space Shuttle missions (in fact, it may not even be noticeable relative to the novel events).

However, the analysis in this dissertation has revealed that the procedure rework process could significantly increase in severity on a long duration mission to land on a distant celestial body. Furthermore, the analysis suggests that the effect of rework propagation on the Procedure Rework Process will be much more severe than the effect of light delay—an unavoidable issue often cited in the literature as a primary challenge to overcome on such missions. On a Mars mission, for example, the Procedure Rework Process would be most stressed when the spacecraft is about to enter Mars orbit and land.

¹¹⁵ A prior study by Garrett and Caldwell (2002) noted a similar effect in the processing of flight rule change requests in the month before each Space Shuttle launch. However, no attempt was made in that study to simulate that effect.

However, this stress would *not* necessarily be due to the intuitive and unavoidable problem of light delay; it would be due to the less intuitive and preventable problem of procedure rework propagation. The identification of this problem thus highlights a key gap in the literature on (and perhaps stakeholder mental models of) the future of crewed spaceflight mission flight control.

Identification of rationales for procedure rework

In order to anticipate, fix, and prevent instances of procedure rework, an understanding or model of procedure rework causality is necessary. Procedure rework is necessary in human spaceflight (and other domains) for a number of reasons and barring a clear record of these reasons, flight controllers and MER engineers are left to develop their mental models of procedure rework through experience. Such a reliance on experience takes time, subjecting the system to additional levels of hazard while the flight controller or MER engineer learns, and subjects the eventual mental model to biases that people often make in informal inference of past experience.

By explicitly identifying the rationales of procedure rework observed in this study, the author has provided information to aid flight controllers and MER engineers in the anticipation, completion, and prevention of procedure rework (indeed the author provides several recommendations based on this analysis to prevent instances of rework). One could look at the data and identify rationales that they previously overlooked or rationales that were falsely attributed to be the cause of most rework. For example, one who attributes most rework to unpreventable component or human reliability issues may instead realize from the data that most rework is due to more manageable logistics and process issues.

Characterization of strategies for using flow control to mitigate the effect of rework propagation

Two distinct and one integrative flow control schemes to mitigate rework propagation were demonstrated in this dissertation. The first involved either the use of a fourth shift of flight controllers and MER engineers to work on propagated rework in parallel to the three primary shifts or the use of one of the primary shifts to work on propagated rework as needed throughout the flight. The second scheme involved the sudden increase in the time horizon of the procedure rework process as the mission neared its end. The first scheme significantly reduced the rework propagation end-of-mission effect (particularly on the long duration missions) falling somewhat short of eliminating it while the second scheme merely moved the effect to an earlier (and perhaps more desirable) time in the mission. Each of these schemes has their costs and benefits and thus, an integrative scheme and notional cost function were defined to synthesize these two schemes. Though these schemes cannot be said to be “optimal,” they provide a set of options for Mission Control and the MER to consider as they prepare for future human spaceflight missions.

Qualitative and quantitative description of the Procedure Rework Process in Space Shuttle Mission Control

The ways in which procedures are created, updated, and ultimately executed are key issues in the interface of humans and technology. The Procedure Rework Process relies on a view of procedures as resources rather than rigid rules and a dual responsibility in procedure development and execution (i.e., the procedure developer has a responsibility to provide the procedure executor with a useful procedure and the procedure executor must use discretion in executing the procedure). The qualitative and quantitative description of the process provided in this dissertation should promote the concepts and merit of such a view to operational environments in which procedures are viewed as rigid rules and the operator's responsibility is merely to follow them. In particular, the explicit identification of the capacity for original thought and problem solving as a flight controller training objective and the results that follow from that objective should speak to the usefulness of harnessing the potential of human operators in complex system operation vis-à-vis treating them as components that must be regulated by inflexible procedures for "reliable" performance. Furthermore, the overall description of the process should provide indications of tangible human contributions to complex system operation for those seeking to understand how control authority should be split between humans and automation (many instances of rework are examples of contingencies or opportunity exploitations that require a human's ability for original thought).

As far as Mission Control is concerned, the description of the Procedure Rework Process provided in this dissertation should be useful for flight controller training. Because procedure rework is an important part of a flight controller's job, the qualitative description of the process, documented procedure rationales, and simulation model could be used in flight controller training—perhaps in a CBT or Training Academy lecture—to help trainees understand their role in the process and the strengths and weaknesses of its dynamic structure.

Finally, the generic dynamic structure of procedure rework developed in this study can be added to the repository of generic dynamic models available to practitioners of Dulac's (2007) method, discussed in Chapter 4.

8.5 Future Work

Further research can proceed along three directions: 1) additional development of the proposed process for using phase space attractors to evaluate safety constraint enforcement, 2) additional investigation of procedure rework, and 3) application of the process to other systems. These directions are discussed in the paragraphs below.

Additional development of the proposed process for using phase space attractors to evaluate system safety constraint enforcement

The process proposed in this dissertation takes some of the abstract mathematical notions of phase space attraction and applies them to the practical system safety problem of safety control structure evaluation and design. However, the author has admittedly only "scratched the surface" of the established knowledge of phase space attraction and much work could be done to determine uses for it in the process. Mathematicians have studied

bifurcations and attractors for decades and as mentioned in Chapter 4, bifurcation control is an emerging subfield of nonlinear control theory. Review of this work and perhaps collaboration with researchers in these areas of study are likely to yield augmentations to the process that will help process users better understand how bifurcations form and can be controlled. Such an understanding would not only lead to better schemes for bifurcation control, but also provide more clarity as to what dynamic structures should be created in the model-building process to reveal the relevant bifurcations of the system.

Similarly, the approaches taken to flow control in this dissertation are derived from some of the simplest control schemes known today (e.g., proportional control). Further research could be applied towards identifying far more sophisticated and useful schemes for flow control in the nonlinear control literatures.

Moreover, work can be done to better enable the use of phase space attractors for the evaluation of safety constraint enforcement in systems dominated by discrete or hybrid dynamics. Such efforts would likely be aimed at augmenting the current process with analysis techniques from discrete mathematics or developing a complementary process focused on discrete or hybrid systems.

Additional investigation of procedure rework

In this dissertation, procedure rework was identified as a key process to the success of Space Shuttle operations and several important aspects of its dynamics were described. Given its importance, it is possible that stakeholders in Mission Control, the MER, the Astronaut Office, or even completely different industries will want to know more about it. Thus, there are several opportunities for further investigation of procedure rework.

The first potential area of investigation could involve refinement and expansion of the model to further validate the long duration mission rework propagation concerns raised in the initial analysis or to identify other issues. The following considerations could apply to such analysis:

- The analysis in this dissertation was baselined from Space Shuttle data. When long duration missions to land on distant celestial bodies do occur, they will be performed with other spacecraft architectures and potentially a new Mission Control architecture. Thus, the model might have to be altered to account for the architectural difference between these systems and the current one.
- Only a portion of the safety control structure was analyzed in this dissertation. By expanding the model to include other components of the safety control structure, it may be possible to show that while procedure rework is sufficiently decoupled from other system processes over the duration of a single Space Shuttle mission, there are safety control and cost minimization processes in other parts of the control structure that could weaken or destroy the Procedure Rework Attractor over a multi-mission timescale.
- During the analysis, light delay was not shown to be a major issue for the Procedure Rework Process. However, the models used represent the effect of light delay in an optimistic manner (i.e., light delay is only treated as a pure

information delay). Investigation of potential nonlinear effects of light delay on flight controller performance could potentially reveal problems that would have to be addressed.

- Flight controller and MER engineer burnout, attrition, and hiring were not accounted for in the model. While these issues are probably irrelevant over the duration of a Space Shuttle mission, they may have a significant effect on long duration missions. Thus, it may be worthwhile to model these effects in future work.
- Rework propagation is caused by a number of issues. While the model currently treats the *Rework Propagation Factor* as a parameter, further modeling efforts can expand upon the processes affecting rework propagation and perhaps allow for better analysis of bifurcation control options.

The next potential area of investigation could involve refinement of the flow control tradespace exploration. As stated in Chapters 6 and 7, the purpose of the model developed in this dissertation was to simulate procedure rework rather than optimize it. However, there are bound to be optimization considerations in the development of a flight control strategy for future human spaceflight missions. According to Webb and Smith (2008) and Korsmeyer and Smith (2008), MOD has a goal of staffing flight support for the proposed Orion Crew Exploration Vehicle with approximately 50% of the staff currently required for Shuttle. Future work could be geared towards making the necessary refinements to the model and notional cost functions presented in Chapter 7 to evaluate the impact of such a strategy. Furthermore, multiple flow control schemes could be identified and traded against each other.

Additionally, procedure rework can be evaluated in the operation of other spacecraft to identify potential ways in which its practice may differ in future human spaceflight missions from how it is done during Space Shuttle missions. As mentioned in Chapter 7, studying procedure rework for the ISS may reveal the advantages and disadvantages of some of the bifurcation control techniques proposed in this dissertation (e.g., reduction of mechanical interfaces for the crew, use of an electronic inventory management database, etc.). However, care would have to be taken to ensure that some of the fundamental differences between ISS-style missions and Space Shuttle-style missions are properly accounted for in the evaluation of these techniques. For example, in studying rework propagation on ISS, one may be led to believe that rework propagates more slowly because there are no mission events to force the completion of all unaddressed rework (i.e., propagated rework could be delayed beyond the time period studied). Similarly, when evaluating procedure rework for uncrewed spacecraft missions, one would have to account for the fact that procedures written for humans differ from procedures written for automation (in fact, this study only considered procedures written for humans), and that the humans executing procedures in such missions are executing them from a control room on Earth. In other words, comparisons of procedure rework data for crewed and uncrewed spacecraft missions could easily be as invalid as the comparisons between “apples and orangutans” (*double pun intended*) if such differences are not taken into account.

Finally, procedure rework in the operation of other complex systems can be evaluated to develop a better understanding of how it can (or perhaps cannot) be more universally applied.

Application of the proposed process to other engineering systems

The process is meant to be applicable to any engineering system in which useful information can be derived by treating some aspect of the system's dynamics as continuous. Thus, there are sure to be countless opportunities to apply the process to other systems in order to evaluate and improve the performance of their safety control structures whether they are already in existence or being engineered.

8.6 Concluding Remarks

This dissertation began with what the author intended to be a provocative discussion on the role of nonlinearity in two complex system accidents and one near accident. The interactions of components in such systems can cause some components to compensate for the “failings” of others or to degrade: the behavior of the system as a whole differs from the sum of the behaviors of its parts. The reason for bringing this role to the attention of the reader is a not-so-subtle emphasis in traditional science and engineering research to fit linear reasoning to even the most complex phenomena as mentioned in Chapter 1. As discussed in Chapter 2, this emphasis has left us with linear, event-based accident models that are problematic to use for safety risk management in complex, socio-technical systems.

However, the situation was not said to be entirely grim as several works were highlighted that have begun to draw attention to the nonlinearity of system accidents and to stress the importance of system-level properties like resilience, robustness, flexibility, adaptability, and safety in managing the positive and negative aspects of uncertainty. Among these works, an idea has arisen—promoted mostly by Leveson and her research group—to explicitly treat safety as a control problem. Thus, some fundamentals of control theory were presented in Chapter 3 to help the reader understand what treating safety as a control problem would mean. Then in Chapter 4, the author introduced the mathematical concept of phase space attractors and laid the conceptual groundwork for a process to use them to evaluate how well safety is being controlled in a system and how this control can be improved. Finally, in Chapters 5, 6, and 7, the author used a case study of a real-world safety control application—the Space Shuttle Mission Control Procedure Rework Process—to describe and demonstrate the proposed process while drawing attention to the aspects that make this application successful in a complex, uncertain environment. Accordingly, the contributions of this work have implications for the management of uncertainty in general and in reworking procedures in Mission Control and elsewhere.

In treating safety control structure evaluation and design as a phase space attractor engineering problem, the author has taken steps to better foster the resilience, adaptability, flexibility, and robustness of safety constraint enforcement in one particular engineering system. Moreover, this work identifies a path for future steps to be taken with regards to safety constraint enforcement in this and other engineering systems.

Appendix 1: List of Acronyms and Abbreviations

AA	Associate Administrator
AAE	Aeronautical and Astronautical Engineering
ACM	Association for Computing Machinery
ACO	Assembly and Checkout Officer
AIAA	American Institute of Aeronautics and Astronautics
B.S.	Bachelor of Science
BGA	Beta Gimbal Assembly
BOOSTER	Booster Systems Engineer
CAIB	<i>Columbia</i> Accident Investigation Board
CAPCOM	Spacecraft Communicator
CSA	Canadian Space Agency
CSM	Command and Service Module
CSRL	Complex Systems Research Laboratory
DfC	Design for Changeability
DoD	Department of Defense
DPS	Data Processing Systems Engineer
EECOM	Emergency, Environmental, Consumables Manager
EGIL	Electrical Generation and Illumination Engineer
ESD	Engineering Systems Division
ESMD	Exploration Systems Mission Directorate
ET	External Tank
EVA	Extravehicular Activities Officer
FAO	Flight Activities Officer
FCR	Flight Control Room
FCT	Flight Controller Trainer
FD	Flight Day
FDO	Flight Dynamics Officer
FLIGHT	Flight Director
GC	Ground Controller
GDO- Rendezvous	Rendezvous Guidance and Procedures Officer
GNC	Guidance, Navigation, and Control Systems Engineer
GP-B	Gravity Probe B
HRO	High Reliability Organization
IAASS	International Association for the Advancement of Space Safety
IEEE	Institute of Electrical and Electronics Engineers
IL	Instrumentation Laboratory
INCO	Integrated and Communications Officer
ISS	International Space Station
ITA	Independent Technical Authority

JSC	Johnson Space Center
JPL	Jet Propulsion Laboratory
KBB	Knowledge Based Behavior
KSC	Kennedy Space Center
LCC	Launch Control Center
LEO	Low-Earth Orbit
LiOH	Lithium Hydroxide
M.S.	Master of Science
MAE	Mean Absolute Error
MBE	Multiple Bit Error
MBU	Multiple Bit Upset
MCC	Mission Control Center
MER	Mission Evaluation Room
MIT	Massachusetts Institute of Technology
MMACS	Maintenance, Mechanical, Arm, and Crew Systems Officer
MMT	Mission Management Team
MOCR	Mission Operations Control Room
MOD	Mission Operations Directorate
MPSR	Multi-Purpose Support Room
MSE	Mean Square Error
MSFC	Marshall Space Flight Center
MSG	Message
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NAT	Normal Accident Theory
NEO	Near-Earth Object
OJT	On-the-Job-Trainee
OMS	Orbital Maneuvering System
OPAT	One-Parameter-At-a-Time
PAO	Public Affairs Officer
PAYLOADS	Payloads Officer
PC	Personal Computer
PDRS	Payload Deployment and Retrieval Systems
PGSC	Payload General Support Computer
PGT	Pistol Grip Tool
PI	Principle Investigator
PRA	Probabilistic Risk Assessment
PROP	Propulsion
PSA	Probabilistic Safety Assessment
Ph.D.	Doctor of Philosophy
RBB	Rule Based Behavior
RCC	Reinforced Carbon-Carbon
RF	Radio-Frequency
RMS	Root Mean Square
S.M.	Master of Science (Latin Abbreviation)

SARJ	Solar Alpha Rotary Joint
SAW	Solar Array Wing
SBB	Skill Based Behavior
SBE	Single Bit Error
SBU	Single Bit Upsets
SE	Spiral-in Equilibrium
SRB	Solid Rocket Booster
SRMS	Shuttle Remote Manipulator System
SSME	Space Shuttle Main Engine
SSRMS	Space Station Remote Manipulator System
STAMP	Systems Theoretic Accident Model and Processes
STPA	STAMP-based Analysis
STS	Space Transportation System
SURGEON	Flight Surgeon
WHO	World Health Organization

Appendix 2: Detailed Space Shuttle Flight Data Tables

This appendix contains the necessary documentation for an independent evaluation of the author's data analysis for each Space Shuttle mission studied. The first set of tables shown for each mission include a listing of the electronic messages sent to the crews during those flights and how (or whether) the author obtained them for the case study. The second set of tables provided for each mission includes a numerical code for each update (e.g., Procedure Update 1, Procedure Update 2, etc.), the flight days on which the updates occurred, the title of the altered procedure, the number of the electronic message in which the update was announced, the rationale for the update, and console position responsible for the update as judged by the author. The third set of tables include the author's judgment of the flight days on which each update was identifiable, issued, and was to be executed. Additionally the third set of tables include the number of days between when an update was identifiable and when it was updated as well as the number of flight days between when it was updated and when it was to be executed. The fourth set of tables for each mission include the author's interpretation of the detailed rationale for the update as well as the more general rationale categorization and discrete event rationale categorization (if applicable). The fifth set of tables for each mission include the data time history of the *Procedures Needing and Being Reworked* variable used in the calibration of the procedure rework model. The information in the fifth set of tables was derived from an integration of the values in the third set of tables and an evaluation of the mission timelines that yielded the mission elapsed time when each flight day ended and when the discrete events effectively occurred. The next to last table provided for each mission identifies which updates the author judged as originating within/beyond the time horizon, attributable to specific discrete events (within/beyond the time horizon or due to refinements of prior updates), and being created as a result of the procedure rework process. These evaluations largely dictated the parameter values used in the model calibration. The last table for each mission lists the update times and totals normalized to the landing preparation time. Finally, the last table of this appendix list the update times and totals for all missions normalized to a standard landing preparation time.

STS-97 Data Tables

MSG #	MSG Title	FD	Status for Case Study
157C	EDW Entry Summary	12	Disregarded
156B	KSC Entry Summary	12	Disregarded
155	FD11 - FD13 Summary Pages	11	Requested & Delivered by JSC on 7/2/08
154B	Entry C/L Deltas	11	Requested & Delivered by JSC on 7/2/08
153C	D/O Prep Deltas	11	Requested & Delivered by JSC on 7/2/08
152	Entry Day Fluid Loading and Anti-G Suit Operations	11	Disregarded
151	FD11 Internet Questions	11	Disregarded
150A	SWIS Network RF Comm Sensitivity Check	11	Requested & Delivered by JSC on 7/2/08
149	FD11 PAO Event Summary	11	Disregarded
148	FD11 Earth Obs Image	11	Disregarded
147	FD11 Earth Obs Text	11	Disregarded
146	FD11 Mission Summary	11	Requested & Delivered by JSC on 7/2/08
145B	FD11 Flight Plan Revision	11	Requested & Delivered by JSC on 7/2/08
144	FD11 Summary Timeline	10	Disregarded
143	Middeck Stowage Configuration	10	Disregarded
142	FD10 Internet Questions	10	Disregarded
141A	FD10 Transfer Message (ACFN585A)	10	Requested & Delivered by JSC on 7/2/08
140	Joint Ops Update Summary	10	Requested & Delivered by JSC on 7/2/08
139A	FD10 PAO Event Summary	10	Disregarded
138	Conjunction Viewing (FAIN338)	09	Requested & Delivered by JSC on 7/2/08
137A	(OCA_0510B) Joint PMA3 Egress Procedure Deltas	10	Requested & Delivered by JSC on 7/2/08
136	FD10 Mission Summary	10	Requested & Delivered by JSC on 7/2/08
135D	FD10 Flight Plan Revision	10	Requested & Delivered by JSC on 7/2/08
134	FD10 Earth Obs Image	10	Disregarded
133	FD10 Earth Obs Text	10	Disregarded
132	Cancelled	10	Disregarded
131	FD10 Summary Timeline	09	Disregarded
130	Transfer Message (ACFN562A)	09	Requested & Delivered by JSC on 7/2/08
129	Undocking Plan (GPFN558)	09	Requested & Delivered by JSC on 7/2/08
128	OCA Jumper build with Shuttle Resources (ISS Get A)	09	Requested & Delivered by JSC on 7/2/08
127	FD09 Internet Questions	09	Disregarded
126	Assembly Ops Update Summary	09	Requested & Delivered by JSC on 7/2/08
125A	DTO261 Alt Test Ops Updates (ACFN550)	09	Requested & Delivered by JSC on 7/2/08
124	(OCA_0490) IWIS Abbreviated Setup	09	Requested & Delivered by JSC on 7/2/08
123A	(OCA_0496A)FD09 PAO Event	09	Disregarded
122A	SAFER Equipment Stow For ISS Transfer (EVFN524)	09	Requested & Delivered by JSC on 7/2/08
121A	EVA Crew Hook Lock Attachment Procedure (EVFN516)	09	Requested & Delivered by JSC on 7/2/08
120A	EVA Equipment Hook Changeout Procedure (EVFN515)	09	Requested & Delivered by JSC on 7/2/08
119	FD09 Transfer Message	08	Requested & Delivered by JSC on 7/2/08
118	(OCA_0493) CBCS Install Mods - Missing Video Cable	09	Requested & Delivered by JSC on 7/2/08
117	FD09 Earth Obs Image	09	Disregarded

Table 25. Listing of the electronic messages sent to the STS-97 crew (Part 1 of 4).

MSG #	MSG Title	FD	Status for Case Study
116	FD09 Earth Obs Text	09	Disregarded
115A	FD09 Mission Summary	09	Requested & Delivered by JSC on 7/2/08
114D	FD09 Flight Plan Revision	09	Requested & Delivered by JSC on 7/2/08
113	FD09 Summary Timeline	08	Disregarded
112	ISS Flyaround Procedures	09	Requested & Delivered by JSC on 7/2/08
111	REBA/EMU TV Power Cable Check (EVFN483)	08	Requested & Delivered by JSC on 7/2/08
110	EVA Tool Config Deltas (EVFN490)	08	Requested & Delivered by JSC on 7/2/08
109	Cable Slack Wrench Photo (EVFN495)	08	Requested & Delivered by JSC on 7/2/08
108	FD08 Internet Questions	08	Disregarded
107A	Manual SABB Latch Cycle (EVFN487B)	08	Requested & Delivered by JSC on 7/2/08
106B	PDRS PMA2 Connector Survey (PDFN457)	08	Requested & Delivered by JSC on 7/2/08
105	Solar Array Mast Retraction Update (PHFN434A)	08	Requested & Delivered by JSC on 7/2/08
104B	Final EVA Timeline	08	Disregarded
103B	SA Tension Cable Slack Take-up (Wrench B/U Procedure)	08	Requested & Delivered by JSC on 7/2/08
102B	EVA3 Big Picture	08	Disregarded
101	FD08 Earth Obs Image	08	Disregarded
100	FD08 Earth Obs Text	08	Disregarded
099A	(OCA_0468) CMG Procedure Deltas	08	Requested & Delivered by JSC on 7/2/08
098B	FD08 Mission Summary	08	Requested & Delivered by JSC on 7/2/08
097C	FD08 Flight Plan Revision	08	Requested & Delivered by JSC on 7/2/08
096	FD08 Summary Timeline	07	Disregarded
095	EVA 3 Procedure Deltas (EVFN459)	07	Requested & Delivered by JSC on 7/2/08
094	EVA Picture #2	07	Disregarded
093A	EVA Picture #1	07	Disregarded
092B	EVA 3 Tool Config (EVFN431)	07	Requested & Delivered by JSC on 7/2/08
091	Solar Array Mast Retraction (PHFN434)	07	Requested & Delivered by JSC on 7/2/08
090C	2B Maintenance Summary (FDFN433)	07	Requested & Delivered by JSC on 7/2/08
089	FD07 Internet Questions	07	Disregarded
088A	WVS Troubleshoot Procedure	07	Requested & Delivered by JSC on 7/2/08
087A	Preliminary EVA3 Procedures	07	Requested & Delivered by JSC on 7/2/08
086	Tension Solar Array (PHFN436)	07	Requested & Delivered by JSC on 7/2/08
085	Latch Cycle Procedure (PHFN435)	07	Requested & Delivered by JSC on 7/2/08
084	Assembly Ops Update Summary	07	Requested & Delivered by JSC on 7/2/08
083	(OCA_0453) DTO-261 Test Ops (VRCS) & IWIS ACT	07	Requested & Delivered by JSC on 7/2/08
082	(OCA_0452) IWIS Software File Update	07	Requested & Delivered by JSC on 7/2/08
081	FD07 Earth Obs Image	07	Disregarded
080	FD07 Earth Obs Text	07	Disregarded
079	FD07 PAO Event	07	Disregarded
078	FD07 Mission Summary	07	Requested & Delivered by JSC on 7/2/08
077C	FD07 Flight Plan Revision	07	Requested & Delivered by JSC on 7/2/08
076	FD07 Summary Timeline	06	Disregard
075	FD06 PMA 3 Ingress Procedure (EEFN406A)	06	Requested & Delivered by JSC on 7/2/08
074	Assembly Ops Update Summary	06	Requested & Delivered by JSC on 7/2/08

Table 26. Listing of the electronic messages sent to the STS-97 crew (Part 2 of 4).

MSG #	MSG Title	FD	Status for Case Study
073	(OCA_0444)Node 1 Ingress for Node 1 Patch Panel Re	06	Requested & Delivered by JSC on 7/2/08
072	Z1 Patch Panel Reconfig Procedure Updates (OPFN394	06	Requested & Delivered by JSC on 7/2/08
071	FD06 Internet Questions	06	Disregarded
070	EVA Picture #5	06	Disregarded
069	EVA Picture #4	06	Disregarded
068	EVA Picture #3	06	Disregarded
067	EVA Picture #2	06	Disregarded
066	EVA Picture #1	06	Disregarded
065	FD06 Earth Obs Image	06	Disregarded
064	FD06 Earth Obs Text	06	Disregarded
063B	Updated LiOH Cue Card for FD06	06	Requested & Delivered by JSC on 7/2/08
062A	FD06 Mission Summary	06	Requested & Delivered by JSC on 7/2/08
061C	FD06 Flight Plan Revision	06	Requested & Delivered by JSC on 7/2/08
060	FD06 Summary Timeline	05	Disregarded
059	EVA WVS Survey of Stbd Wing(2B) Right SABB	05	Requested & Delivered by JSC on 7/2/08
058	Updates to EVA 2 H-Jumper Inhibits (ACFN339A)	05	Requested & Delivered by JSC on 7/2/08
057A	4B SAW Deploy Ops Update (PHFN354A)	05	Requested & Delivered by JSC on 7/2/08
056	RMS SAW Survey (PDFN342)	05	Requested & Delivered by JSC on 7/2/08
055	FD05 Earth Obs Image	05	Disregarded
054	FD05 Earth Obs Text	05	Disregarded
053	FD05 Internet Questions	05	Disregarded
052B	FD05 PAO Event Summary	05	Disregarded
051B	FD05 Mission Summary	05	Requested & Delivered by JSC on 7/2/08
050C	FD05 Flight Plan Revision	05	Requested & Delivered by JSC on 7/2/08
049D	FD05 Summary Timeline	04	Disregarded
048	Assembly Ops Update Summary	04	Requested & Delivered by JSC on 7/2/08
047	Z1 Keel Target Blockage	04	Requested & Delivered by JSC on 7/2/08
046	FD04 Internet Questions	04	Disregarded
045	IMAX/ICBC3D Troubleshooting (ACFN276)	03	Requested & Delivered by JSC on 7/2/08
044	Mast Canister Thermal Blanket Re-Install (EVFN270)	03	Requested & Delivered by JSC on 7/2/08
043	FD04 Earth Obs Image	04	Disregarded
042	FD04 Earth Obs Text	04	Disregarded
041A	FD04 Mission Summary	04	Requested & Delivered by JSC on 7/2/08
040B	FD04 Flight Plan Revision	04	Requested & Delivered by JSC on 7/2/08
039	FD04 Summary Timeline	03	Disregarded
038A	EVA Workarounds Cribsheet Updates (EVFN266)	03	Requested & Delivered by JSC on 7/2/08
037	IEA Keel Pin Nut Plate Removal (EVFN274)	03	Requested & Delivered by JSC on 7/2/08
036	Cancelled	03	Disregarded
035A	FD03 Transfer Message (ACFN250)	03	Requested & Delivered by JSC on 7/2/08
034	Final IMAX Scene List (ACFN205A)	03	Requested & Delivered by JSC on 7/2/08
033	Audio Config Cue Card Input (INFN247)	03	Requested & Delivered by JSC on 7/2/08
032A	(OCA_386) BGA Position Plan	03	Requested & Delivered by JSC on 7/2/08

Table 27. Listing of the electronic messages sent to the STS-97 crew (Part 3 of 4).

MSG #	MSG Title	FD	Status for Case Study
031	Preliminary Orbital Maneuver Pad for Ti	03	Requested & Delivered by JSC on 7/2/08
030	Progress Relmo Plot	03	Disregarded
029	Relmo Plot	03	Disregarded
028	Preliminary Orbital Maneuver Pad for NC4	03	Requested & Delivered by JSC on 7/2/08
027	Joint Ops Update Summary	03	Requested & Delivered by JSC on 7/2/08
026	(OCA_0384) Failure to Unlatch SABB Remotely	04	Requested & Delivered by JSC on 7/2/08
025	(OCA_0383) Failure to Tension SABB Remotely	04	Requested & Delivered by JSC on 7/2/08
024	(OCA_0382) Failure to Extend Mast Remotely	04	Requested & Delivered by JSC on 7/2/08
023A	Assembly Ops Update Summary	03	Requested & Delivered by JSC on 7/2/08
022C	(OCA_0381C) EPS Deltas to Assembly Ops	03	Requested & Delivered by JSC on 7/2/08
021B	(OCA_0380B) P6 PVR Retract	03	Requested & Delivered by JSC on 7/2/08
020	Cancelled	03	Disregarded
019	ISS Radiogram 204	03	Requested & Delivered by JSC on 7/2/08
018	Updated Proc For ODS Vestibule Depress (EEFN218)	03	Requested & Delivered by JSC on 7/2/08
017	FD03 Mission Summary	03	Requested & Delivered by JSC on 7/2/08
016B	FD03 Flight Plan Revision	03	Requested & Delivered by JSC on 7/2/08
015	DTO 257 Changes (GNFN202)	03	Requested & Delivered by JSC on 7/2/08
014	FD03 Earth Obs Image	03	Disregarded
013A	FD03 Earth Obs Text	03	Disregarded
012A	FD03 Summary Timeline	02	Disregarded
011	Rendezvous Updates	02	Requested & Delivered by JSC on 7/2/08
010	ODS C/L Camera Misalignment Workaround	02	Requested & Delivered by JSC on 7/2/08
009	FD02 News From Home	02	Disregarded
008A	EVA C/L Updates (FN181)	02	Requested & Delivered by JSC on 7/2/08
007	EVA Warm Restart Procedure (FN176)	02	Requested & Delivered by JSC on 7/2/08
006	SWIS SETUP Procedure Updates (FN165)	01	Requested & Delivered by JSC on 7/2/08
005	FD02 Earth Obs Image	02	Disregarded
004	FD02 Earth Obs Text	02	Disregarded
003	Z1 RSU Networking Procedure (FN161)	02	Requested & Delivered by JSC on 7/2/08
002	FD02 Mission Summary	02	Requested & Delivered by JSC on 7/2/08
001A	FD02 Flight Plan Revision	02	Requested & Delivered by JSC on 7/2/08

Table 28. Listing of the electronic messages sent to the STS-97 crew (Part 4 of 4).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
1	2	OIU ACTIVATION	1	Change of OIU 2 to primary unit (OIU 1 was primary unit for the previous flight, but was tripped due to an under-rated circuit breaker)	ACO/EGIL
2	2	EMU SWAP	1	Battery Swap due to improper charging of battery	EVA
3	2	EMU C/O	1	Removal of step to close external airlock heaters due to warm attitudes of STS-97	EVA
4	2	Z1 RSU Networking Procedure	3	Procedural Flaws Discovered on FD 1	ACO
5	1	SWIS SETUP	6	Procedural Flaws Discovered on FD 1	ACO
6	2	DISPLAY LOSS DURING POWER TRANSFER	7	EMU display anomaly during testing corrected	EVA
7	2	UNSTOW PORT SAW BLANKET BOXES, RELEASE MAST TIP FITTINGS	8	Change to ensure that there will be no interference between STBD SSU and APFR	EVA
8	2	EVA 2 TOOL CONFIG	8	Change to ensure that there will be no interference between STBD SSU and APFR	EVA
9	2	EVA 2 TOOL CONFIG	8	Last minute addition of protective covers	EVA
10	2	EVA 2 SORTIE SETUP	8	Last minute addition of protective covers	EVA
11	2	ATTACH Z1 TO P6 QD	8	Last minute addition of a release ring snap back test to avoid leaking and/or hose whipping hazard to EVA crew	EVA
12	2	UNSTOW STARBOARD SAW BLANKET BOXES	8	Change to bolt torque settings due to Boeing analysis	EVA
13	2	UNSTOW PORT SAW BLANKET BOXES	8	Change to bolt torque settings due to Boeing analysis	EVA
14	2	ATTACH P6 TO Z1 USING CONTINGENCY FASTENERS	8	Change to bolt torque settings due to Boeing analysis	EVA
15	2	MANUAL OVERRIDE TO EXTEND RADIATOR	8	Change to bolt torque settings due to Boeing analysis	EVA
16	2	WORKAROUNDS CRIBSHEET	8	Change to bolt torque settings due to Boeing analysis	EVA
17	2	ODS C/L CAMERA MISALIGNMENT WORKAROUND	10	Contingency procedure (there was a misalignment on the previous flight: STS-92)	MMACS/RNDZ

Table 29. Procedure update designations for STS-97 (Part 1 of 6).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
18	2	RNDZ Timeline	11	Time of callouts changed due to potential packet conflict	RNDZ
19	3	DTO 257 PRCS TEST	15	Changes possibly due to RCS problems on FD 1	PROP
20	3	ACBM TO PCBM GROUND STRAP INSTALLATION	16	Logistical Changes	ACO
21	3	ODS VEST/PMA3 PRESSURIZATION	16	Minor Omissions	ACO
22	3	SWIS SETUP	16	Missing step	ACO
23	3	Z1 RSU Networking Procedure	16	Typo	ACO
24	3	UPDATED PROC FOR ODS VESTIBULE DEPRESS	18	Changes to procedure after print deadline	ACO/EECOM
25	3	P6/Z1 UTILITY CONNECTION POWERDOWN AND RECOVERY	22	Previously unaccounted for PVCU Switchover inhibit	ACO
26	3	P6 CH 4B/2B BGA ACTIVATION AND SAW DEPLOY	22	Inadvertent deletion of a step call out to ensure that attitude control is handed over	ACO
27	3	P6 PVR DEPLOY	22	Previously unaccounted for PVR Turnoff inhibit	ACO
28	3	EETCS RADIATOR DEPLOY	22	Auto Off function must be re-enabled in order for the power off command to successfully execute	ACO
29	3	IEA KEEL PIN NUT PLATE REMOVAL	37	Contingency procedure to be performed if the crew cannot break torque on the IEA Keel Pin Bolt	EVA
30	4	DEPRESS/REPRESS CC	40	Typo	EVA
31	4	POST EVA	40	Step Incompatible with EMU PREBREATHE procedures for EVA 2 and EVA 3	EVA
32	4	POST EVA	40	Incompatible steps deleted	EVA
33	4	POST DEPRESS CC	40	Airlock External Heater Steps Removed due to warm attitudes of STS-97	EVA
34	4	POST EVA	40	Airlock External Heater Steps Removed due to warm attitudes of STS-97	EVA

Table 30. Procedure update designations for STS-97 (Part 2 of 6).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
35	4	RMS IMAX OPS	40	New RMS position to view IMAX camera shutter (probably to ensure that IMAX camera is functioning properly after ICBC3D camera failure)	ACO/ PDRS
36	3	MAST CANISTER THERMAL BLANKET RE-INSTALLATION	44	Procedure added to re-install thermal blankets that became partially detached (possibly during launch)	EVA
37	3	IMAX/ICBC3D Troubleshooting	45	Problems with ICBC3D camera	ACO/ INCO
38	4	P6 INSTALL SCRIPT	47	A PAD tethered to the Z1 Keel was floating into and out of the line of sight to a target	PDRS
39	5	HEATER RECONFIG-CONFIG B	50	Steps deleted (possibly due to warm attitude of STS-97)	EGIL/ MMACS
40	5	RELEASE EETCS STATION STARBOARD CINCHES AND WINCH	50	Steps deleted to meet requirement for STS-98	EVA
41	5	SAW VIEWING	56	Steps added due to SAW Deploy Anomaly	PDRS
42	5	4B SAW DEPLOY OPS	57A	Added due to SAW Deploy Anomaly	ACO
43	5	H-JUMPER INSTALLATION	58	Previously unaccounted for inhibits	EVA
44	5	EVA WVS SURVEY OF STBD WING (2B) RIGHT SABB	59	Added due to SAW Deploy Anomaly	EVA
45	5	LDRI Troubleshooting	61	LDRI problems on FD 3	INCO
46	6	LiOH Cue Card	63	Update made to save a LiOH canister (i.e., optimize usage)	EECOM
47	6	Z1 PATCH PANEL RECONFIGURATION	72	Temperature checks added, typos fixed, and procedure updated to reflect ISS config.	ACO
48	6	NODE 1 PATCH PANEL RECONFIGURATION	73	Procedure updated to reflect ISS configuration	EVA/ACO
49	6	EARLY PMA3 INGRESS	75	Steps changed to prevent excess pressure during transfer ops in PMA3 (i.e., the crew would break EVA prebreathe protocol if the pressure exceeded 10.6 psi)	ACO/ EECOM

Table 31. Procedure update designations for STS-97 (Part 3 of 6).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
50	6	EARLY PMA3 EGRESS	75	Steps changed to prevent excess pressure during transfer ops in PMA3 (i.e., the crew would break EVA prebreathe protocol if the pressure exceeded 10.6 psi)	ACO/EECOM
51	7	FPP ASSEMBLY	77	Step added due to SAW Deploy anomaly	ACO
52	7	IWIS SOFTWARE FILE UPDATE	82	Procedure added to command IWIS to take data properly	ACO
53	7	IWIS ACTIVATION	83	Unaccounted for delay	ACO
54	7	DTO-261 TEST OPS (VRCS)	83	Procedure changed due to rescheduling of Test 1 and Test 2	ACO
55	7	LATCH CYCLE PROCEDURE	85	Procedure added due to SAW Deploy anomaly	EVA/ACO
56	7	TENSION SOLAR ARRAY	86	Procedure added due to SAW Deploy anomaly	EVA/ACO
57	7	STBD SAW SABB Tensioning	87	Procedure added due to SAW Deploy anomaly	EVA/ACO
58	7	WVS TROUBLESHOOTING PROCEDURE	88A	Added to recover EV 1's EMU Camera (which failed on FD6)	EVA
59	7	SOLAR ARRAY MAST RETRACTION	91	Procedure added due to SAW Deploy anomaly	EVA/ACO
60	7	EVA 3 TOOL CONFIG	92B	Logistical changes due to SAW Deploy anomaly	EVA
61	7	INSTALL FPP ANTENNA	95	Changes due to SAW Deploy anomaly	EVA
62	7	EVA 3 SORTIE SETUP	95	Changes due to SAW Deploy anomaly	EVA
63	7	EVA 3 SORTIE CLEANUP	95	Changes due to SAW Deploy anomaly	EVA
64	8	CMG Procedure Deltas	99A	Changes to activate CMG heaters	ACO
65	8	SA REEL TENSION CABLE SLACK TAKEUP	103B	Contingency procedure added due to SAW Deploy Anomaly	EVA
66	8	SOLAR ARRAY MAST RETRACTION	105	Procedure refined	EVA/ACO
67	8	PDRS PMA2 CONNECTOR SURVEY	106B	Procedure added to gather more information on a problem that occurred during STS-92	PDRS
68	8	MANUAL SABB LATCH CYCLE	107A	Contingency procedure added due to SAW Deploy Anomaly	EVA/ACO
69	8	EVA 3 TOOL CONFIG	110	Procedure refined	EVA
70	9	NODE 1 FWD CBCS INSTALL	118	Potentially missing Video In/Out Cable	ACO

Table 32. Procedure update designations for STS-97 (Part 4 of 6).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
71	9	EVA EQUIPMENT HOOK CHANGEOUT PROCEDURE	120A	The appropriate hooks apparently were not stowed for launch	EVA
72	9	SAFER EQUIPMENT STOW FOR ISS TRANSFER	122A	This transfer function was done in order to accommodate change in STS-98 manifest following the deferral of 3P	ACO
73	9	NODE 1 IWIS SETUP	124	Contingency update due to possible addition of crew to procedure in order to get it done on time	ACO
74	9	DTO-261 TEST OPS (ALT)	125A	Procedure updated to save propellant after the separation of Tests 1 and 2	ACO/ PROP
75	9	OCA JUMPER BUILD WITH SHUTTLE RESOURCES	128	Task added as an ISS get ahead	MMACS
76	9	Undocking Plan	129	Changed due to ICBC3D camera failure on FD 3	RNDZ
77	10	UNDOCK AND FLYAROUND	135	Changes due to SAW Deploy Anomaly	INCO
78	10	UNDOCK AND FLYAROUND	135	Changes due to LDRI problems on FD 3	INCO
79	10	DOCKING MECHANISM POWERUP	135	Changes due to changes made in ODS vestibule depress procedure on FD 3 (ref. MSG 018)	MMACS
80	10	JOINT PMA3 EGRESS	137A	Logistical Changes	ACO
81	11	SWIS NETWORK RF COMM SENSITIVITY CHECK	150A	Procedure added to test sensitivity of SWIS network to RF communication	ACO
82	11	PAYLOAD ENTRY SWITCH LIST CONFIGURATION	153C	PRI MNC switch position typo	ACO
83	11	DEORBIT PREP	153C	Changes due to LDRI problems on FD 3	INCO
84	11	DEORBIT PREP	153C	Change in PL BAY Flood light configuration due to DTO-261	EGIL
85	11	ENTRY SWITCH LIST/ VERIFICATION	153C	Change in Cabin Temperature Controller Configuration due to stuck pip pin on FD 5	EECOM
86	11	ENTRY SWITCH LIST/ VERIFICATION	153C	Different configuration of external airlock heaters due to warm attitudes of STS-97	EECOM

Table 33. Procedure update designations for STS-97 (Part 5 of 6).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
87	11	ENTRY SWITCH LIST/ VERIFICATION	153C	Reverses change in RMS Wireless Video Config made after the FD 5 discovery that the LDRI will respond to an array of camera commands issued by ground	PDRS
88	11	DEORBIT PREP BACKOUT	153C	Change in Cabin Temperature Controller Configuration due to stuck pip pin on FD 5	EECOM
89	11	DEORBIT PREP BACKOUT	153C	Change in PL BAY Flood light configuration due to DTO-261	EGIL
90	11	DEORBIT PREP BACKOUT	153C	Reverses change in RMS Wireless Video Config made after the FD 5 discovery that the LDRI will respond to an array of camera commands issued by ground	PDRS
91	11	DEORBIT BURN (2ENG)	154	Typo	PROP
92	11	NH3 ACT	154	NH3 boiler configuration	EECOM
93	11	NH3 RECONFIG	154	NH3 boiler configuration	EECOM

Table 34. Procedure update designations for STS-97 (Part 6 of 6).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
1	2	0*	2	0	2
2	2	0*	2	0	2
3	2	0	2	0	2
4	2	0	3	1	2
5	1	0	2	1	1
6	2	0*	2	0	2
7	2	0*	4	2	2
8	2	0	5	3	2
9	2	0*	5	3	2
10	2	0*	6	4	2
11	2	0*	6	4	2
12	2	0*	4	2	2
13	2	0*	4	2	2
14	2	0*	4	2	2
15	2	0*	4	2	2
16	2	0*	4	2	2
17	2	0*	3	1	2
18	2	0*	3	1	2
19	3	1	3	0	2

Table 35. Key flight days for each STS-97 procedure update (Part 1 of 3).

Procedure Update	FD	FD when issue identifiable	FD when update was to be executed	Number of FD between issue of update and anticipated execution	Number of FD between when issue was identifiable and when it was updated
20	3	0	3	0	3
21	3	0	3	0	3
22	3	1	3	0	2
23	3	2	3	0	1
24	3	0*	3	0	3
25	3	0	4	1	3
26	3	0	4	1	3
27	3	0	4	1	3
28	3	0	7	4	3
29	3	0	4	1	3
30	4	0	4	0	4
31	4	0	4	0	4
32	4	0	4	0	4
33	4	0	4	0	4
34	4	0	4	0	4
35	4	3	4	0	1
36	3	1	4	1	2
37	3	3	3	0	0
38	4	0	4	0	4
39	5	0	5	0	5
40	5	0	6	1	5
41	5	4	5	0	1
42	5	4	5	0	1
43	5	0	6	1	5
44	5	4	6	1	1
45	5	3	5	0	2
46	6	6	6	0	0
47	6	0	6	0	6
48	6	0	6	0	6
49	6	3	6	0	3
50	6	3	6	0	3
51	7	4	7	0	3
52	7	4	7	0	3
53	7	0	7	0	7
54	7	7	7	0	0
55	7	4	8	1	3
56	7	4	8	1	3
57	7	4	8	1	3
58	7	6	7	0	1
59	7	4	8	1	3
60	7	4	7	0	3
61	7	4	8	1	3
62	7	4	8	1	3
63	7	4	8	1	3
64	8	0	9	1	8

Table 36. Key flight days for each STS-97 procedure update (Part 2 of 3).

Procedure Update	FD	FD when issue identifiable	FD when update was to be executed	Number of FD between issue of update and anticipated execution	Number of FD between when issue was identifiable and when it was updated
65	8	4	8	0	4
66	8	7	8	0	1
67	8	0	8	0	8
68	8	4	8	0	4
69	8	7	8	0	1
70	9	0	9	0	9
71	9	0	9	0	9
72	9	0	9	0	9
73	9	7	9	0	2
74	9	7	9	0	2
75	9	8	9	0	1
76	9	3	10	1	6
77	10	4	10	0	6
78	10	3	10	0	7
79	10	0	10	0	10
80	10	9	10	0	1
81	11	9	11	0	2
82	11	0	12	1	11
83	11	3	12	1	8
84	11	7	12	1	4
85	11	5	12	1	6
86	11	0	12	1	11
87	11	5	12	1	6
88	11	5	12	1	6
89	11	7	12	1	4
90	11	5	12	1	6
91	11	0	12	1	11
92	11	0	12	1	11
93	11	0	12	1	11

*Likely being reworked or already finished at launch

Table 37. Key flight days for each STS-97 procedure update (Part 3 of 3).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
1	Change of OIU 2 to primary unit (OIU 1 was primary unit for the previous flight, but was tripped due to an under-rated circuit breaker)	N/A	Actuator "Failure" or Degradation
2	Battery Swap due to improper charging of battery	N/A	Actuator "Failure" or Degradation
3	Removal of step to close external airlock heaters due to warm attitudes of STS-97	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
4	Procedural Flaws Discovered on FD 1	N/A	Internal Inconsistencies in the Procedure
5	Procedural Flaws Discovered on FD 1	N/A	Internal Inconsistencies in the Procedure
6	EMU display anomaly during testing corrected	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
7	Change to ensure that there will be no interference between STBD SSU and APFR	N/A	Internal Inconsistencies in the Procedure
8	Change to ensure that there will be no interference between STBD SSU and APFR	N/A	Internal Inconsistencies in the Procedure
9	Last minute addition of protective covers	N/A	Inconsistency between Items Expected to be Launched and Items Actually Launched
10	Last minute addition of protective covers	N/A	Inconsistency between Items Expected to be Launched and Items Actually Launched
11	Last minute addition of a release ring snap back test to avoid leaking and/or hose whipping hazard to EVA crew	N/A	Proactive Contingency Preparation and/or Hazard Investigation
12	Change to bolt torque settings due to Boeing analysis	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
13	Change to bolt torque settings due to Boeing analysis	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch

Table 38. STS-97 update rationales (Part 1 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
14	Change to bolt torque settings due to Boeing analysis	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
15	Change to bolt torque settings due to Boeing analysis	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
16	Change to bolt torque settings due to Boeing analysis	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
17	Contingency procedure (there was a misalignment on the previous flight: STS-92)	N/A	Proactive Contingency Preparation and/or Hazard Investigation
18	Time of callouts changed due to potential packet conflict	N/A	Internal Inconsistencies in the Procedure
19	Changes possibly due to RCS problems on FD 1	N/A	Actuator "Failure" or Degradation
20	Logistical Changes	N/A	Equipment List Revision
21	Minor Omissions	N/A	Typos and Omissions
22	Missing step	N/A	Typos and Omissions
23	Typo	N/A	Typos and Omissions
24	Changes to procedure after print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
25	Previously unaccounted for PVCU Switchover inhibit	N/A	Unaccounted for Inhibits
26	Inadvertent deletion of a step call out to ensure that attitude control is handed over	N/A	Inadvertent Deletion of Steps
27	Previously unaccounted for PVR Turnoff inhibit	N/A	Unaccounted for Inhibits
28	Auto Off function must be re-enabled in order for the power off command to successfully execute	N/A	Internal Inconsistencies in the Procedure
29	Contingency procedure to be performed if the crew cannot break torque on the IEA Keel Pin Bolt	N/A	Proactive Contingency Preparation and/or Hazard Investigation
30	Typo	N/A	Typos and Omissions

Table 39. STS-97 update rationales (Part 2 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
31	Step Incompatible with EMU PREBREATHE procedures for EVA 2 and EVA 3	N/A	Internal Inconsistencies in the Procedure
32	Incompatible steps deleted	N/A	Internal Inconsistencies in the Procedure
33	Airlock External Heater Steps Removed due to warm attitudes of STS-97	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
34	Airlock External Heater Steps Removed due to warm attitudes of STS-97	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
35	New RMS position to view IMAX camera shutter (probably to ensure that IMAX camera is functioning properly after ICBC3D camera failure)	N/A	Actuator "Failure" or Degradation
36	Procedure added to re-install thermal blankets that became partially detached (possibly during launch)	N/A	Launch Damage (actual or suspected)
37	Problems with ICBC3D camera	N/A	Actuator "Failure" or Degradation
38	A PAD tethered to the Z1 Keel was floating into and out of the line of sight to a target	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
39	Steps deleted (possibly due to warm attitude of STS-97)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
40	Steps deleted to meet requirement for STS-98	N/A	Internal Inconsistencies in the Procedure
41	Steps added due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
42	Added due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
43	Previously unaccounted for inhibits	N/A	Unaccounted for Inhibits
44	Added due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)

Table 40. STS-97 update rationales (Part 3 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
45	LDRI problems on FD 3	N/A	Unexpected Software Behavior
46	Update made to save a LiOH canister (i.e., optimize usage)	N/A	Consumable Management Optimizations
47	Temperature checks added, typos fixed, and procedure updated to reflect ISS configuration.	N/A	Typos and Omissions
48	Procedure updated to reflect ISS configuration	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
49	Steps changed to prevent excess pressure during transfer ops in PMA3 (i.e., the crew would break EVA prebreathe protocol if the pressure exceeded 10.6 psi)	N/A	Internal Inconsistencies in the Procedure
50	Steps changed to prevent excess pressure during transfer ops in PMA3 (i.e., the crew would break EVA prebreathe protocol if the pressure exceeded 10.6 psi)	N/A	Internal Inconsistencies in the Procedure
51	Step added due to SAW Deploy anomaly	P6 SAW Deploy Problems	Task Deferral or Reprioritization
52	Procedure added to command IWIS to take data properly	N/A	Unexpected Software Behavior
53	Unaccounted for delay	N/A	Unexpected Software Behavior
54	Procedure changed due to rescheduling of Test 1 and Test 2	N/A	Task Deferral or Reprioritization
55	Procedure added due to SAW Deploy anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
56	Procedure added due to SAW Deploy anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
57	Procedure added due to SAW Deploy anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
58	Added to recover EV 1's EMU Camera (which failed on FD6)	N/A	Sensor "Failure" or Bias

Table 41. STS-97 update rationales (Part 4 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
59	Procedure added due to SAW Deploy anomaly	P6 SAW Deploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
60	Logistical changes due to SAW Deploy anomaly	P6 SAW Deploy Problems	Equipment List Revision
61	Changes due to SAW Deploy anomaly	P6 SAW Deploy Problems	Task Deferral or Reprioritization
62	Changes due to SAW Deploy anomaly	P6 SAW Deploy Problems	Equipment List Revision
63	Changes due to SAW Deploy anomaly	P6 SAW Deploy Problems	Equipment List Revision
64	Changes to activate CMG heaters	N/A	Internal Inconsistencies in the Procedure
65	Contingency procedure added due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Proactive Contingency Preparation and/or Hazard Investigation
66	Procedure refined	P6 SAW Deploy Problems	Internal Inconsistencies in the Procedure
67	Procedure added to gather more information on a problem that occurred during STS-92	N/A	Proactive Contingency Preparation and/or Hazard Investigation
68	Contingency procedure added due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Proactive Contingency Preparation and/or Hazard Investigation
69	Procedure refined	P6 SAW Deploy Problems	Equipment List Revision
70	Potentially missing Video In/Out Cable	N/A	Inconsistency between Items Expected to be Launched and Items Actually Launched
71	The appropriate hooks apparently were not stowed for launch	N/A	Inconsistency between Items Expected to be Launched and Items Actually Launched
72	This transfer function was done in order to accommodate change in STS-98 manifest following the deferral of 3P	N/A	"Get-Ahead" Tasks Scheduled
73	Contingency update due to possible addition of crew to procedure in order to get it done on time	N/A	Procedure Efficiency Optimization
74	Procedure updated to save propellant after the separation of Tests 1 and 2	N/A	Consumable Management Optimizations
75	Task added as an ISS get ahead	N/A	"Get-Ahead" Tasks Scheduled

Table 42. STS-97 update rationales (Part 5 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
76	Changed due to ICBC3D camera failure on FD 3	N/A	Actuator "Failure" or Degradation
77	Changes due to SAW Deploy Anomaly	P6 SAW Deploy Problems	Proactive Contingency Preparation and/or Hazard Investigation
78	Changes due to LDRI problems on FD 3	N/A	Unexpected Software Behavior
79	Changes due to changes made in ODS vestibule depress procedure on FD 3 (ref. MSG 018)	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
80	Logistical Changes	N/A	Equipment List Revision
81	Procedure added to test sensitivity of SWIS network to RF communication	N/A	"Get-Ahead" Tasks Scheduled
82	PRI MNC switch position typo	N/A	Typos and Omissions
83	Changes due to LDRI problems on FD 3	N/A	Unexpected Software Behavior
84	Change in PL BAY Flood light configuration due to DTO-261	N/A	Procedure Efficiency Optimization
85	Change in Cabin Temperature Controller Configuration due to stuck pip pin on FD 5	N/A	Actuator "Failure" or Degradation
86	Different configuration of external airlock heaters due to warm attitudes of STS-97	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
87	Reverses change in RMS Wireless Video Config made after the FD 5 discovery that the LDRI will respond to an array of camera commands issued by ground	N/A	Procedure Efficiency Optimization
88	Change in Cabin Temperature Controller Configuration due to stuck pip pin on FD 5	N/A	Actuator "Failure" or Degradation
89	Change in PL BAY Flood light configuration due to DTO-261	N/A	Procedure Efficiency Optimization
90	Reverses change in RMS Wireless Video Config made after the FD 5 discovery that the LDRI will respond to an array of camera commands issued by ground	N/A	Procedure Efficiency Optimization

Table 43. STS-97 update rationales (Part 6 of 7).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
91	Typo	N/A	Typos and Omissions
92	NH3 boiler configuration	N/A	Procedure Nominally Updated in Real-time
93	NH3 boiler configuration	N/A	Procedure Nominally Updated in Real-time

Table 44. STS-97 update rationales (Part 7 of 7).

DATA POINT	MISSION ELAPSED TIME (MINUTES)	NUMBER OF PROCEDURES NEEDING AND BEING REWORKED
Launch	0	49
End of FD 1	300	51
End of FD 2	1620	35
End of FD 3	3030	30
Instant before SAW Deploy Anomaly	4200	25
Instant after SAW Deploy Anomaly	4201	40
End of FD 4	4470	39
End of FD 5	5880	36
End of FD 6	7290	33
End of FD 7	8700	27
End of FD 8	10140	22
End of FD 9	11580	17
End of FD 10	13020	13
End of FD 11	14460	0

Table 45. The STS-97 data time history for the variable *Number of Procedures Needing and Being Reworked*.

TYPES OF PROCEDURE UPDATES	PROCEDURE UPDATE NUMBERS
Due to SAW Deploy Anomaly and in Time Horizon	41, 42, and 44
Due to SAW Deploy Anomaly and Beyond Time Horizon (i.e., propagated reworks due to the SAW Deploy Anomaly)	51, 55, 56, 57, 59, 60, 61, 62, 63, 65, 68, and 77
Outside Time Horizon and Not Latent at Launch (i.e., propagated reworks not due to a discrete event)	19, 22, 36, 45, 49, 50, 52, 73, 74, 76, 78, 81, 83, 84, 85, 87, 88, 89, and 90
Due to refinements of previously submitted SAW Deploy Anomaly related updates	66 and 69
Procedures developed as a result of the rework process	29, 36, 37, 42, 44, 45, 52, 55, 56, 57, 59, 65, 67, 68, 71, 72, 74, 75, and 81

Table 46. List of specially designated STS-97 procedure updates.

FLIGHT DAY	MISSION ELAPSED TIME AT END OF FLIGHT DAY (MINUTES)	NORMALIZED TIME TO LANDING PREPARATION AT THE END OF FD 11	UPDATES SINCE PREVIOUS FLIGHT DAY
0	0	0	0
1	300	0.02075	1
2	1620	0.11203	17
3	3030	0.2095	13
4	4470	0.3091	7
5	5880	0.4066	7
6	7290	0.5041	5
7	8700	0.6017	13
8	10140	0.7012	6
9	11580	0.8008	7
10	13020	0.9004	4
11	14460	1	13
12	15598	1.0787	0

Table 47. STS-97 update times normalized to landing preparation time.

STS-115 Data Tables

MSG #	MSG Title	FD	Status for Case Study
139	Attitudes for OBSS Inspections sources: F012928	12	Requested & Delivered by JSC on 7/2/08
138	EOM+1 Entry Summary Message sources: N015286	12	Disregarded
137	FD13 EOM+1 - EOM+3 Summary Timeline	12	Disregarded
136	FD13 EOM+1 Detail Timeline	12	Disregarded
135	FD12 OBSS INSPECTIONS sources: F012925	12	Requested & Delivered by JSC on 7/2/08
134A	RMS EE ORBITER SURVEY sources: F012918	12	Retrieved from FD12 Execute Package
133	FD12 Water Summary Message sources: F012909	12	Retrieved from FD12 Execute Package
132A	FD12 Summary Timeline	12	Retrieved from FD12 Execute Package
131A	FD12 Mission Summary sources: N015267, F012907, N015280	12	Retrieved from FD12 Execute Package
130A	FD12 Flight Plan Revision sources: F012904	12	Retrieved from FD12 Execute Package
129A	Entry Summary Template	11	Disregarded
128A	Entry Summary sources: N015231	11	Disregarded
127C	Entry FIW Summary sources: FD02-11 Ex Pkg, F012884	11	Requested & Delivered by JSC on 7/2/08
126	Entry Day Fluid Loading sources: N015160	11	Disregarded
125	Entry Checklist Deltas sources: F012872, F012864A	11	Requested & Delivered by JSC on 7/2/08
124A	Deorbit Prep Updates sources: F012864A, F012865	11	Requested & Delivered by JSC on 7/2/08
123	Sunday Funnies	11	Disregarded
122	FD10 MMT Summary sources: F012878	11	Retrieved from FD11 Execute Package
121	FD11 Water Summary Message sources: F012863	11	Retrieved from FD11 Execute Package
120	FD11 PAO Events - Inflight Interviews with KYW-TV, KARE-TV and WGN-TV sources: F012866	11	Disregarded
119	Deltas to FCS Checkout Procedure sources: F012843	11	Retrieved from FD11 Execute Package
118A	FD11 Summary Timeline	11	Retrieved from FD11 Execute Package
117	FD11 Mission Summary sources: N015170, F012870, N015218, N015224	11	Retrieved from FD11 Execute Package
116A	FD11 Flight Plan Revision sources: F012862, N015211, N015209, N015212, N015222	11	Retrieved from FD11 Execute Package
115	FD11 Preliminary Summary Timeline	11	Disregarded

Table 48. Listing of the electronic messages sent to the STS-115 crew (Part 1 of 6).

MSG #	MSG Title	FD	Status for Case Study
114	FD09 MMT Summary sources: F012822	10	Retrieved from FD10 Execute Package
113	PLBD Troubleshooting for Loss of Port FWD CL A Indication sources: F012711	10	Retrieved from FD10 Execute Package
112	MICROBE/Yeast - GAP Updates sources: F012812	10	Retrieved from FD10 Execute Package
111A	FD10 Water Summary Message sources: F012808	10	Retrieved from FD10 Execute Package
110	FD10 Summary Timeline	10	Retrieved from FD10 Execute Package
109	FD10 Mission Summary sources: N015145, N015154	10	Retrieved from FD10 Execute Package
108	FD10 Preliminary Summary Timeline	09	Disregarded
107A	FD10 Flight Plan Revision sources: F012821, F012804, F012805, N015110, N015151	10	Retrieved from FD10 Execute Package
106	FD08 MMT Summary (13-1260) sources: F012800	09	Retrieved from FD9 Execute Package
105	Docked Audio Troubleshooting (13-1259) sources: F012775	09	Retrieved from FD9 Execute Package
104	Undocking Camera Change sources: F012719	09	Retrieved from FD9 Execute Package
103A	FD09 LiOH Transfer sources: F012791	09	Retrieved from FD9 Execute Package
102	LiOH Cue Card sources: F012790	09	Retrieved from FD9 Execute Package
101	FD09 Water Summary Message sources: F012793	09	Retrieved from FD9 Execute Package
100	FD09 Transfer Message (13-1254) sources: F012797	09	Retrieved from FD9 Execute Package
099	FD09 Summary Timeline	09	Retrieved from FD9 Execute Package
098A	FD09 Mission Summary (13-1253A) sources: N015075, N015092	09	Retrieved from FD9 Execute Package
097A	FD09 Flight Plan Revision sources: F012792, F012798, N015067, F012794, N015084	09	Retrieved from FD9 Execute Package
096	Undocking Pad and Event Summary (13- 1252) sources: F012769	08	Requested & Delivered by JSC on 7/2/08
095	FD09 Preliminary Summary Timeline	08	Disregarded
094	FD07 MMT Summary (13-1247) sources: F012749	08	Retrieved from FD8 Execute Package
093	12A SODF Transfer List sources: F012743	08	Retrieved from FD8 Execute Package
092	External Airlock Return Bag Change sources: F012742	08	Retrieved from FD8 Execute Package

Table 49. Listing of the electronic messages sent to the STS-115 crew (Part 2 of 6).

MSG #	MSG Title	FD	Status for Case Study
091	Updates to Pre-Undock EVA Reconfig and Xfer sources: F012741	08	Retrieved from FD8 Execute Package
090	Atlantis/ISS Joint Crew News Conference (13-1239) sources: F012723	08	Disregarded
089	Atlantis PAO Event w/CBS, NBC, and ABC sources: F012723	08	Disregarded
088	FD08 Water Summary Message sources: F012740	08	Retrieved from FD8 Execute Package
087	FD08 Transfer Message (13-1237) sources: F012739	08	Retrieved from FD8 Execute Package
086A	FD08 Summary Timeline	08	Retrieved from FD8 Execute Package
085	FD08 Mission Summary (13-1236) sources: N015011, N015014	08	Retrieved from FD8 Execute Package
084A	FD08 Flight Plan Revision sources: F012737, F012735, F012738, F012743, F012746, F012748, F012747, F012751	08	Retrieved from FD8 Execute Package
083A	FD08 Preliminary Summary Timeline	07	Disregarded
082	FD06 MMT Summary (13-1233) sources: F012700	07	Retrieved from FD7 Execute Package
081	EVA 3 Changeout Pages (13-1232) sources: F012698	07	Retrieved from FD7 Execute Package
080	Updated Middeck Bag A Layout and Entry Locker Layout sources: F012692, N014941	07	Retrieved from FD7 Execute Package
079	EVA 3 Detailed Timeline Pen and Inks (13-1231) sources: F012690	07	Retrieved from FD7 Execute Package
078	PRLA Close With OBSS Safing sources: F012684	07	Retrieved from FD7 Execute Package
077	FD07 Water Summary Message sources: F012693	07	Retrieved from FD7 Execute Package
076	FD07 Summary Timeline	07	Retrieved from FD7 Execute Package
075	FD07 Mission Summary (13-1228) sources: N014952, N014944	07	Retrieved from FD7 Execute Package
074A	FD07 Flight Plan Revision sources: F012697, F012696, N014943, N014947	07	Retrieved from FD7 Execute Package
073	FD07 Preliminary Summary Timeline	06	Disregarded
072	12A PRE EVA 3 TOOL CONFIG Pen&Ink Updates (13-1227)	06	Requested & Delivered by JSC on 7/2/08
071	12A EVA Tool Restow (13-1226) sources: F012758A	08	FD8 Execute Package
070	EVA3 Replanned Summary Timeline (13-1225)	06	Disregarded

Table 50. Listing of the electronic messages sent to the STS-115 crew (Part 3 of 6).

MSG #	MSG Title	FD	Status for Case Study
069	FD 6 Activities to Move Earlier - Part 1 (13-1224) sources: F012633	06	Requested & Delivered by JSC on 7/2/08
068	ERCA Troubleshooting Procedure (13-1223) sources: F012662B	06	Requested & Delivered by JSC on 7/2/08
067	STS-115 Middeck Bag Layouts sources: F012639	06	Retrieved from FD6 Execute Package
066	Atlantis / ISS PAO Event with National Public Radio and CNN (13-1222) sources: F012636	06	Disregarded
065	Atlantis Canadian Space Agency PAO Event (13-1221) sources: F012636	06	Disregarded
064	SASA, BSP and XPDR Tie Down Plan (13-1217)	06	Retrieved from FD6 Execute Package
063A	FD05 MMT Summary (13-1216A) sources: F012656	06	Requested & Delivered by JSC on 7/2/08
062	FD06 Water Summary Message sources: F012651	06	Retrieved from FD6 Execute Package
061	FD06 Transfer Message (13-1214) sources: F012646	06	Retrieved from FD6 Execute Package
060A	FD06 Summary Timeline	06	Retrieved from FD6 Execute Package
059	FD06 Mission Summary (13-1213) sources: F012648, N014867	06	Retrieved from FD6 Execute Package
058A	FD06 Flight Plan Revision sources: F012569, F012628, N014865, F012653	06	Retrieved from FD6 Execute Package
057	FD06 Preliminary Summary Timeline	05	Disregarded
056	Bag C Layout sources: F012620	05	Requested & Delivered by JSC on 7/2/08
055	ORCA Outlet Hose Checkout (13-1211)	06	Retrieved from FD6 Execute Package
054	FD04 MMT Summary (13-1208) sources: F012606	05	Retrieved from FD5 Execute Package
053	EVA 2 Summary Timeline Updates (13-1207) sources: F012593	05	Retrieved from FD5 Execute Package
052	FD05 Monitor Ops sources: N014785	05	Retrieved from FD5 Execute Package
051	EVA 2 Big Picture (13-1206) sources: F012593	05	Disregarded
050	FD05 Water Summary Message sources: F012601	05	Retrieved from FD5 Execute Package
049	FD05 Transfer Message (13-1203) sources: F012597	05	Retrieved from FD5 Execute Package
048	FD05 Summary Timeline	05	Retrieved from FD5 Execute Package
047	FD05 Mission Summary (13-1202) sources: N014787, N014798	05	Retrieved from FD5 Execute Package
046	FD05 Flight Plan Revision sources: F012594	05	Retrieved from FD5 Execute Package

Table 51. Listing of the electronic messages sent to the STS-115 crew (Part 4 of 6).

MSG #	MSG Title	FD	Status for Case Study
045	Preliminary FD05 Summary Timeline	04	Disregarded
044	FD03 MMT Summary (13-1201) sources: F012568	04	Retrieved from FD4 Execute Package
043	BPSMU Audio Config sources: F012566	04	Retrieved from FD4 Execute Package
042	Robotics Procedure Update Rationale for FD04 sources: F012503	04	Retrieved from FD4 Execute Package
041	FD4 Lighting Predicts for AVU Operations (13-1199)	04	Retrieved from FD4 Execute Package
040	FD04 Monitor Ops sources: F012535	04	Retrieved from FD4 Execute Package
039	P3 Activation Procedure Updates sources: F012532	04	Retrieved from FD4 Execute Package
038	FD04 Water Activity Summary sources: F012549	04	Retrieved from FD4 Execute Package
037	Loose SARJ Thermal Blanket Troubleshooting (13-1196) sources: F012563	04	Retrieved from FD4 Execute Package
036	FD04 Summary Timeline	04	Retrieved from FD4 Execute Package
035	FD04 Mission Summary (13-1195) sources: F012541, N014723, F012556, N014739	04	Retrieved from FD4 Execute Package
034	FD04 Flight Plan Revision sources: F012564, N014728, W010290, F012567, N014737	04	Retrieved from FD4 Execute Package
033	FD04 Preliminary Summary Timeline	03	Disregarded
032	1.301 AVU SPEE CAM P3 Truss Install (13-1194)	04	Retrieved from FD4 Execute Package
031	Unberth Hand CNTRL Test Results sources: F012528A	03	Requested & Delivered by JSC on 7/2/08
030	RelMo Plots and Burn Pads sources: N014671	03	Retrieved from FD3 Execute Package
029	FD03 MMT Summary (13-1189) sources: F012517B	03	Retrieved from FD3 Execute Package
028	Contingency RTL Loss After WR Limping (13-1187)	04	Retrieved from FD4 Execute Package
027	Contingency P3/4 Installation with Failed SSAS RTL (13-1186) sources: F012479	04	Retrieved from FD4 Execute Package
026	OPCL and EPCL P&I Deltas sources: F012486	03	Retrieved from FD3 Execute Package
025A	EVA Changeout Pages (13-1185A) sources: F012493A	03	Retrieved from FD3 Execute Package
024A	EVA Procedure P&I Deltas (13-1184A) sources: F012493A	03	Retrieved from FD3 Execute Package
023	EVA SAFER Latch Taping (13-1183) sources: F012494	03	Retrieved from FD3 Execute Package

Table 52. Listing of the electronic messages sent to the STS-115 crew (Part 5 of 6).

MSG #	MSG Title	FD	Status for Case Study
022	FD03 Water Activity Summary sources: F012512	03	Retrieved from FD3 Execute Package
021	FD03 Transfer Message (13-1182) sources: F012511	03	Retrieved from FD3 Execute Package
020A	FD03 Summary Timeline	03	Retrieved from FD3 Execute Package
019	FD03 Mission Summary (13-1181) sources: F012514, N014670, N014673	03	Retrieved from FD3 Execute Package
018A	FD03 Flight Plan Revision sources: F012513, F012515	03	Retrieved from FD3 Execute Package
017A	FD03 Preliminary Summary Timeline	02	Disregarded
016	Rendezvous Event and Lighting Info sources: F012942	02	Disregarded
015A	6.113 CUP(LAB) Artificial Vision Unit (AVU) Hard Disk Drive (HDD) Changeout (13-0907A)	03	Retrieved from FD3 Execute Package
014A	6.210 MT Generic Auto Translation Using String A(B) IMCAS (13-0555A)	03	Retrieved from FD3 Execute Package
013	7.001 MSS Failure Response and Recovery (13-1104)	03	Retrieved from FD3 Execute Package
012	7.201 MSS COMM Failure (13-1103)	03	Retrieved from FD3 Execute Package
011A	Ref Data Flight Supplement Updates sources: F012451	02	Retrieved from FD2 Execute Package
010A	FD02 Water Activity Summary sources: F012472	02	Retrieved from FD2 Execute Package
009	FD02 OBSS LDRI RCC SURVEY - STBD UNDOCKED Procedure Update sources: F012470	02	Retrieved from FD2 Execute Package
008	FD02 Flat Fields Procedure sources: F012468	02	Retrieved from FD2 Execute Package
007	RCS Jet Reprioritization sources: F012466	02	Retrieved from FD2 Execute Package
006	5.501 Attitude Control Constraints for P3P4 Install (13-1176)	02	Retrieved from FD2 Execute Package
005B	12A Photo/TV Stowage Matrix (13-1060B)	02	Retrieved from FD2 Execute Package
004A	FD02 Summary Timeline	02	Retrieved from FD2 Execute Package
003A	FD02 Mission Summary (13-1175A) sources: F012461, F012462, F012475, N014608	02	Retrieved from FD2 Execute Package
002A	FD02 Flight Plan Revision sources: N014604, F012469, F012476	02	Retrieved from FD2 Execute Package
001	Star Pairs Pad Update sources: Pointing	01	Requested & Delivered by JSC on 7/2/08

Table 53. Listing of the electronic messages sent to the STS-115 crew (Part 6 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
1	2	OBSS UNBERTH	002A	Typo	PDRS
2	2	OBSS ITVC/LDRI FLAT FIELDS	8	Procedure updates after the print deadline	PDRS
3	2	OBSS LDRI RCC SURVEY-STBD UNDOCKED	9	Procedure updates after the print deadline	PDRS
4	3	LiOH Cue Card	018A	Change made in order to save a LiOH can	EECOM
5	3	EMU PREBREATHE	23	Steps added for IV crew member to tape a SAFER latch that has had a tendency to jam	EVA
6	3	AIRLOCK CONFIG	024A	Missing steps	EVA
7	3	PRE EVA 1 TOOL CONFIG	024A	Logistical Changes	EVA
8	3	12A WORKAROUND CRIBSHEET	024A	New PGT settings	EVA
9	3	12A EMU/AIRLOCK CONSUMABLES CUE CARD	024A	Logistical Changes and Typos	EVA
10	3	EVA 2 Inhibit Pad	25	Previously unaccounted for inhibit and typos	EVA
11	3	12A WORKAROUND CRIBSHEET	25	Added QD workarounds for vent tool on Z1-M5	EVA
12	3	P1-P3 CAPTURE LATCH OVERRIDE	25	New PGT settings	EVA
13	3	P1-P3 MBA BOLT OVERRIDE	25	New PGT settings	EVA
14	3	OPCL	26	Changes due to loss of AC 1 Phase A for Fuel Cell 1	EGIL
15	3	EPCL	26	Changes due to loss of AC 1 Phase A for Fuel Cell 1	EGIL
16	3	CUP(LAB) ARTIFICIAL VISION UNIT (AVU) HARD DISK DRIVE (HDD) CHANGEOUT	15A	Procedure to replace "failed" hard drive disk	ROBO
17	4	AVU SPEE CAM P3 TRUSS INSTALL	32	Logistical changes and other changes due to obstructed view of P1 targets discovered on FD3	PDRS/ROBO
18	4	LOOSE SARJ THERMAL BLANKET TROUBLESHOOTING	37	Blanket came loose during launch	EVA

Table 54. Procedure update designations for STS-115 (Part 1 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
19	4	P3 ACTIVATION AND S0, S1, AND P1 POWERDOWN/POWERUP	39	Missing RPC position checks	ACO
20	4	PRE-SLEEP	40	Steps added to configure ISS Loopback capability from CVIU 6 to VTR2 using the shuttle's Monitor 2 and VPU capability	INCO
21	4	BPSMU AUDIO CONFIG	43	Alternative to BPSMU Audio Only string referenced in P/TV05 INTERNAL OPS scene (BPSMU cable was accidentally returned on STS-121)	INCO
22	6	ORCA OUTLET HOSE with CHECK VALVE TRANSFER AND CHECKOUT	55	This procedure was added to check for trapped air in the ORCA hose (discovered in ground testing)	ACO/EGIL
23	6	SASA, BSP and XPDR Tie Down Plan	64	Contingency Procedure	EVA
24	6	ERCA TROUBLESHOOTING PROCEDURE	68	Procedure to recover an ERCA that failed during EVA 2	EVA
25	6	PRE EVA 3 TOOL CONFIG	72	Equipment added for get ahead tasks and typos fixed	EVA
26	7	POST-SLEEP	74A	New Cryo Config due to unexpected heating conditions	EGIL
27	7	PRLA CLOSE	78	Updated to safe OBSS in response to a STBD Manipulator Retention Latch microswitch failure	ACO/PDRS
28	7	RELEASE P4 PV RADIATOR CINCHES/WINCHES	79	Changes due to the addition of get ahead tasks	EVA
29	7	MISSE 5 RETRIEVAL	79	Logistical changes due to the addition of get ahead tasks	EVA
30	7	DTO 861 IR CAMERA - WLE IMAGERY	79	Logistical changes due to the addition of get ahead tasks	EVA
31	7	EVA 3 INHIBIT PAD	81	Addition of callout	EVA

Table 55. Procedure update designations for STS-115 (Part 2 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
32	7	EVA 3 EGRESS/SETUP	81	Logistical changes due to the addition of get ahead tasks	EVA
33	7	P3 CLEANUP	81	Logistical changes due to the addition of get ahead tasks	EVA
34	7	INSTALL SGANT AGIT HEAD SHIELD	81	Steps added to indicate desired photograph areas	EVA
35	7	EWIS ANTENNA INSTALLATION	81	Changed steps due to DAIU failure	EVA
36	8	POST-SLEEP	84	New Cryo Config due to unexpected heating conditions (refinement of update in msg 74A)	EGIL
37	8	LiOH Cue Card	84	Changes made to save a canister	EECOM
38	8	EVA PREP FOR TRANSFER TO SHUTTLE	91	Logistical Changes	EVA
39	8	UNDOCKING PAD AND EVENT SUMMARY	96	Changes due to newly planned ISS maneuver during flyaround (the maneuver was added because of high beta magnitudes)	RNDZ
40	9	POST-SLEEP	97	New Cryo Config due to unexpected heating conditions (refinement of update in msg 84)	EGIL
41	9	HEATER RECONFIG-CONFIG B(CONFIG A)	97	Potentially due to unexpected heating at the given attitude	EECOM
42	9	P/TV03 UNDOCK	104	Undocking Camera Change	INCO
43	9	DOCKED AUDIO TROUBLESHOOTING	105	Changed steps due to DAIU failure	INCO
44	10	POST-SLEEP	107A	New Cryo Config due to unexpected heating conditions (refinement of update in msg 97)	EGIL
45	10	EMU INSTALLATION	107A	Changed made to ensure that proper loads are transferred to Airlock Adapter Plate	EVA

Table 56. Procedure update designations for STS-115 (Part 3 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
46	10	OBSS UNBERTH	107A	Typo (same as the one noted in msg 002A)	PDRS
47	10	OBSS LDRI RCC SURVEY-STBD UNDOCKED	107A	Same as msg 9	PDRS
48	10	SSV Troubleshooting	107A	SSV stopped generating video	PDRS
49	10	PLBD TROUBLESHOOTING FOR LOSS OF PORT FWD CL A INDICATION	113	Contingency Procedure added due to microswitch problems on FD1	MMACS
50	10	MICROBE ACTIVATION	112	Leak mitigation steps added	ACO
51	11	POST-SLEEP	116A	New Cryo Config due to unexpected heating conditions (refinement of update in msg 107A)	EGIL
52	11	DEACTIVATION AND TEARDOWN	116A	New stowage location for WLES	ACO
53	11	FCS CHECKOUT	119	Changes due to Speedbrake Channel 3 degradation on FD1	GNC
54	11	NOMINAL DEORBIT PREP	124	Step added due to FD1 failure of AC Phase A failure of Fuel Cell Pump	EGIL
55	11	ENTRY SWITCH LIST VERIFICATION	124	Step changed due to FD1 failure of AC Phase A failure of Fuel Cell Pump	EGIL
56	11	ENTRY SWITCH LIST VERIFICATION	124	Step changed due to Supply H2O Dump Valve leakage observed on FD 10	EECOM
57	11	DEORBIT PREP BACKOUT	124	PCS configuration	EECOM
58	11	NH3 ACT	125	NH3 boiler config	EECOM
59	11	NH3 RECONFIG	125	NH3 boiler config	EECOM
60	12	POST-SLEEP	130A	New Cryo Config due to unexpected heating conditions (refinement of update in msg 116A)	EGIL
61	12	SUPPLY/WASTE WATER DUMP	133	Step changed due to Supply H2O Dump Valve leakage observed on FD 10	EECOM

Table 57. Procedure update designations for STS-115 (Part 4 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
62	12	RMS EE ORBITER SURVEY	134	Contingency survey of Orbiter to verify that OD object seen on FD 11 did not come off of the Orbiter	PDRS
63	12	FD 12 OBSS INSPECTIONS	135	Refinement of MSG 134	PDRS

Table 58. Procedure update designations for STS-115 (Part 5 of 5).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
1	2	0	2	0	2
2	2	0*	2	0	2
3	2	0*	2	0	2
4	3	0*	3	0	3
5	3	0*	4	1	3
6	3	0	4	1	3
7	3	0*	3	0	3
8	3	0*	4	1	3
9	3	0	4	1	3
10	3	0	5	2	3
11	3	0	5	2	3
12	3	0*	5	2	3
13	3	0*	5	2	3
14	3	1	3	0	2
15	3	1	3	0	2
16	3	0	4	1	3
17	4	3	4	0	1
18	4	1	5	1	3
19	4	0	4	0	4
20	4	0	4	0	4
21	4	0	4	0	4
22	6	0*	6	0	6
23	6	0	7	1	6
24	6	5	6	0	1
25	6	5	6	0	1
26	7	0	7	0	7
27	7	2	7	0	5
28	7	5	7	0	2
29	7	5	7	0	2
30	7	5	7	0	2
31	7	5	7	0	2
32	7	5	7	0	2

Table 59. Key flight days for each STS-115 procedure update (Part 1 of 2).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
33	7	5	7	0	2
34	7	0	7	0	7
35	7	3	7	0	4
36	8	7	8	0	1
37	8	7	8	0	1
38	8	5	8	0	3
39	8	7	9	1	1
40	9	8	9	0	1
41	9	0	9	0	9
42	9	0	9	0	9
43	9	3	9	0	6
44	10	9	10	0	1
45	10	0	10	0	10
46	10	0	10	0	10
47	10	0	10	0	10
48	10	9	10	0	1
49	10	1	12	2	9
50	10	0	10	0	10
51	11	10	11	0	1
52	11	9	12	1	2
53	11	1	11	0	10
54	11	1	12	1	10
55	11	1	12	1	10
56	11	10	12	1	1
57	11	0	12	1	11
58	11	0	12	1	11
59	11	0	12	1	11
60	12	11	12	0	1
61	12	10	12	0	2
62	12	10	12	0	2
63	12	12	12	0	0

*Likely being reworked or already finished at launch

Table 60. Key flight days for each STS-115 procedure update (Part 2 of 2).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
1	Typo	N/A	Typos and Omissions
2	Procedure updates after the print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
3	Procedure updates after the print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
4	Change made in order to save a LiOH can	N/A	Consumable Management Optimizations
5	Steps added for IV crew member to tape a SAFER latch that has had a tendency to jam	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
6	Missing steps	N/A	Typos and Omissions
7	Logistical Changes	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
8	New PGT settings	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
9	Logistical Changes and Typos	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
10	Previously unaccounted for inhibit and typos	N/A	Unaccounted for Inhibits
11	Added QD workarounds for vent tool on Z1-M5	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
12	New PGT settings	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch

Table 61. STS-115 update rationales (Part 1 of 5).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
13	New PGT settings	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
14	Changes due to loss of AC 1 Phase A for Fuel Cell 1	N/A	Actuator "Failure" or Degradation
15	Changes due to loss of AC 1 Phase A for Fuel Cell 1	N/A	Actuator "Failure" or Degradation
16	Procedure to replace "failed" hard drive disk	N/A	Actuator "Failure" or Degradation
17	Logistical changes and other changes due to obstructed view of P1 targets discovered on FD3	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
18	Blanket came loose during launch	N/A	Launch Damage (actual or suspected)
19	Missing RPC position checks	N/A	Typos and Omissions
20	Steps added to configure ISS Loopback capability from CVIU 6 to VTR2 using the shuttle's Monitor 2 and VPU capability	N/A	Use of Shuttle Resources to Counteract ISS Problems
21	Alternative to BPSMU Audio Only string referenced in P/TV05 INTERNAL OPS scene (BPSMU cable was accidentally returned on STS-121)	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
22	This procedure was added to check for trapped air in the ORCA hose (discovered in ground testing)	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
23	Contingency Procedure	N/A	Proactive Contingency Preparation and/or Hazard Investigation
24	Procedure to recover an ERCA that failed during EVA 2	N/A	Sensor "Failure" or Bias
25	Equipment added for get ahead tasks and typos fixed	"Get Aheads"	"Get-Ahead" Tasks Scheduled
26	New Cryo Config due to unexpected heating conditions	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)

Table 62. STS-115 update rationales (Part 2 of 5).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
27	Updated to safe OBSS in response to a STBD Manipulator Retention Latch microswitch failure	N/A	Sensor "Failure" or Bias
28	Changes due to the addition of get ahead tasks	"Get Aheads"	"Get-Ahead" Tasks Scheduled
29	Logistical changes due to the addition of get ahead tasks	"Get Aheads"	"Get-Ahead" Tasks Scheduled
30	Logistical changes due to the addition of get ahead tasks	"Get Aheads"	"Get-Ahead" Tasks Scheduled
31	Addition of callout	"Get Aheads"	"Get-Ahead" Tasks Scheduled
32	Logistical changes due to the addition of get ahead tasks	"Get Aheads"	"Get-Ahead" Tasks Scheduled
33	Logistical changes due to the addition of get ahead tasks	"Get Aheads"	"Get-Ahead" Tasks Scheduled
34	Steps added to indicate desired photograph areas	N/A	"Get-Ahead" Tasks Scheduled
35	Changed steps due to DAIU failure	N/A	Actuator "Failure" or Degradation
36	New Cryo Config due to unexpected heating conditions (refinement of update in msg 74A)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
37	Changes made to save a canister	N/A	Consumable Management Optimizations
38	Logistical Changes	"Get Aheads"	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
39	Changes due to newly planned ISS maneuver during flyaround (the maneuver was added because of high beta magnitudes)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
40	New Cryo Config due to unexpected heating conditions (refinement of update in msg 84)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
41	Potentially due to unexpected heating at the the given attitude	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)

Table 63. STS-115 update rationales (Part 3 of 5).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
42	Undocking Camera Change	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
43	Changed steps due to DAIU failure	N/A	Actuator "Failure" or Degradation
44	New Cryo Config due to unexpected heating conditions (refinement of update in msg 97)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
45	Changed made to ensure that proper loads are transferred to Airlock Adapter Plate	N/A	Internal Inconsistencies in the Procedure
46	Typo (same as the one noted in msg 002A)	N/A	Typos and Omissions
47	Same as msg 9	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
48	SSV stopped generating video	N/A	Unexpected Software Behavior
49	Contingency Procedure added due to microswitch problems on FD1	N/A	Sensor "Failure" or Bias
50	Leak mitigation steps added	N/A	Proactive Contingency Preparation and/or Hazard Investigation
51	New Cryo Config due to unexpected heating conditions (refinement of update in msg 107A)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
52	New stowage location for WLES	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
53	Changes due to Speedbrake Channel 3 degradation on FD1	N/A	Sensor "Failure" or Bias
54	Step added due to FD1 failure of AC Phase A failure of Fuel Cell Pump	N/A	Actuator "Failure" or Degradation
55	Step changed due to FD1 failure of AC Phase A failure of Fuel Cell Pump	N/A	Actuator "Failure" or Degradation

Table 64. STS-115 update rationales (Part 4 of 5).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
56	Step changed due to Supply H2O Dump Valve leakage observed on FD 10	N/A	Actuator "Failure" or Degradation
57	PCS configuration	N/A	Procedure Nominally Updated in Real-time
58	NH3 boiler config	N/A	Procedure Nominally Updated in Real-time
59	NH3 boiler config	N/A	Procedure Nominally Updated in Real-time
60	New Cryo Config due to unexpected heating conditions (refinement of update in msg 116A)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
61	Step changed due to Supply H2O Dump Valve leakage observed on FD 10	N/A	Actuator "Failure" or Degradation
62	Contingency survey of Orbiter to verify that OD object seen on FD 11 did not come off of the Orbiter	N/A	Launch Damage (actual or suspected)
63	Refinement of MSG 134	N/A	Launch Damage (actual or suspected)

Table 65. STS-115 update rationales (Part 5 of 5).

DATA POINT	MISSION ELAPSED TIME (MINUTES)	NUMBER OF PROCEDURES NEEDING AND BEING REWORKED
Launch	0	30
End of FD 1	360	37
End of FD 2	1740	35
End of FD 3	3180	25
End of FD 4	4620	20
Instant before "Get Aheads"	5640	21
Instant after "Get Aheads"	5641	29
End of FD 5	6060	29
End of FD 6	7500	25
End of FD 7	8940	18
End of FD 8	10380	15
End of FD 9	11760	14
End of FD 10	13140	11
End of FD 11	14550	3
End of FD 12	15990	0

Table 66. The STS-115 data time history for the variable *Number of Procedures Needing and Being Reworked*.

TYPES OF PROCEDURE UPDATES	PROCEDURE UPDATE NUMBERS
Due to "Get Aheads" and in Time Horizon	25
Due to "Get Aheads" and Beyond Time Horizon (i.e., propagated reworks due to the "Get Aheads")	28, 29, 30, 31, 32, 33, and 38
Outside Time Horizon and Not Latent at Launch (i.e., propagated reworks not due to a discrete event)	14, 15, 18, 27, 35, 43, 49, 52, 53, 54, 55, 61, and 62
Due to refinements of previously submitted "Get Ahead" related updates	None
Procedures developed as a result of the rework process	16, 18, 21, 22, 23, 24, 43, 48, 49, and 62

Table 67. List of specially designated STS-115 procedure updates.

FLIGHT DAY	MISSION ELAPSED TIME AT END OF FLIGHT DAY (MINUTES)	NORMALIZED TIME TO LANDING PREPARATION AT THE END OF FD 11	UPDATES SINCE PREVIOUS FLIGHT DAY
0	0	0	0
1	360	0.02474	0
2	1740	0.1196	3
3	3180	0.2186	13
4	4620	0.3175	5
5	6060	0.4165	0
6	7500	0.5155	4
7	8940	0.6144	10
8	10380	0.7134	4
9	11760	0.8082	4
10	13140	0.9031	7
11	14550	1	9
12	15990	1.0990	4

Table 68. STS-115 update times normalized to landing preparation time.

STS-116 Data Tables

MSG #	Message Title	FD	Status for Case Study
152	FD13 MMT Summary sources: Flight Director	13	Disregarded
151A	Northrup Updates to Entry Checklist sources: F014485	13	Requested & Delivered by JSC on 7/2/08
150A	DPS Entry Message for BFS --> PASS DK Assignment sources: F014464C	13	Requested & Delivered by JSC on 7/2/08
149	SHAB Entry Prep sources: F014475A	13	Requested & Delivered by JSC on 7/2/08
148A	Entry Summary Template sources: MATS	13	Disregarded
147A	Entry Summary sources: N017342	13	Disregarded
146B	Entry Checklist Deltas sources: F014462,F014478,N017335	13	Requested & Delivered by JSC on 7/2/08
145	Payload Deact Procedure Deltas sources: N017283D	13	Requested & Delivered by JSC on 7/2/08
144B	Deorbit Prep Updates sources: F014458, F014470,F014478, F014481	13	Requested & Delivered by JSC on 7/2/08
143	Entry FIW Summary	13	Requested & Delivered by JSC on 7/2/08
142	Entry Day Fluid Loading sources: F014434B	13	Disregarded
141	Sunday Funnies	13	Retrieved from FD13 Execute Package
140	FD13 SpaceHab Viewport Violations sources: F014472	13	Retrieved from FD13 Execute Package
139	FD13 PAO Event Summary sources: F014463	13	Disregarded
138B	FD13 EECOM Updates sources: F014450, F014451, F014452, F014466A	13	Retrieved from FD13 Execute Package
137	FD13 Water Summary Message sources: F014469	13	Retrieved from FD13 Execute Package
136	FD12 MMT Summary sources: Flight Director	13	Retrieved from FD13 Execute Package
135A	FD13 Mission Summary sources: N017316A, N017307	13	Retrieved from FD13 Execute Package
134A	FD13 - EOM+1 Flight Plan Revision sources: F014472, F014468, F014465	13	Retrieved from FD13 Execute Package
133A	FD13 Preliminary Summary Timeline	12	Disregarded
132	FD12 SpaceHab Viewport Violations sources: F014432	12	Retrieved from FD12 Execute Package
131	Updates to LCS Cue Card sources: MSG028	12	Retrieved from FD12 Execute Package
130	FD12 Water Summary Message sources: F014425	12	Retrieved from FD12 Execute Package
129	FD11 MMT Summary sources: Flight Director	12	Retrieved from FD12 Execute Package

Table 69. Listing of the electronic messages sent to the STS-116 crew (Part 1 of 6).

MSG #	Message Title	FD	Status for Case Study
128	FD12 Mission Summary sources: N017263, N017273	12	Retrieved from FD12 Execute Package
127A	FD12 Flight Plan Revision sources: F014432, F014431, F014428, F014419	12	Retrieved from FD12 Execute Package
126	FD12 Preliminary Summary Timeline	12	Disregarded
125	Undock With Fly around Updates sources: F014400	11	Requested & Delivered by JSC on 7/2/08
124	Docked Audio Hardline Voice Test (14-0643) sources: F014389	11	Retrieved from FD11 Execute Package
123	Middeck Stowage Updates sources: F014371	11	Retrieved from FD11 Execute Package
122	Spacehab Inlet Duct Screen Check sources: F014370	11	Retrieved from FD11 Execute Package
121	FD10 MMT Summary (14-0637) sources: Flight Director	11	Retrieved from FD11 Execute Package
120	PMA 2 X3 Connector Photography Procedure sources: F014360A	11	Retrieved from FD11 Execute Package
119A	FD11 Water Summary Message sources: F014831	11	Retrieved from FD11 Execute Package
118	FD11 Transfer Message (14-0636) sources: F014394	11	Retrieved from FD11 Execute Package
117	FD11 Mission Summary (14-0635) sources: N017165, N017189	11	Retrieved from FD11 Execute Package
116A	FD11 Flight Plan Revision sources: F014362C, F014379, F014391	11	Retrieved from FD11 Execute Package
115	FD11 Preliminary Summary Timeline	10	Disregarded
114	EMU Reconfig & Transfer Update (14-0634) sources: F014365	10	Requested & Delivered by JSC on 7/2/08
113	Undock Message and Sep Burn Revision sources: F014358A	10	Requested & Delivered by JSC on 7/2/08
112	Middeck Stowage Bag Drawings sources: F014340A	10	Retrieved from FD10 Execute Package
111A	FD10 Water Summary Message sources: F014342	10	Retrieved from FD10 Execute Package
110A	FD10 Transfer Message (14-0628A) sources: F014348, N017123	10	Retrieved from FD10 Execute Package
109	FD09 MMT Summary (14-0627) sources: Flight Director	10	Retrieved from FD10 Execute Package
108	FD10 Mission Summary (14-0626) sources: N017106, N017124	10	Retrieved from FD10 Execute Package
107C	FD10 Flight Plan Revision sources: F014335, F014345, F014350	10	Retrieved from FD10 Execute Package
105	Deltas to EVA PREP to checkout EMU 3015 (14-0624) sources: F014329	09	Requested & Delivered by JSC on 7/2/08
104	FD10 Preliminary Summary Timeline	09	Disregarded
103	Additional SAW Inspections for EVA 4 (14-0623) sources: F014327	09	Requested & Delivered by JSC on 7/2/08

Table 70. Listing of the electronic messages sent to the STS-116 crew (Part 2 of 6).

MSG #	Message Title	FD	Status for Case Study
102	EVA 4 Procedures (14-0622) sources: F014326	09	Available online
101	EVA 4 Tool Stowage Locations and EMU Wrist Disconnect Taping (14-0620) sources: F014317, F014318	09	Requested & Delivered by JSC on 7/2/08
100	FD10-EOM Overview Timeline (14-0618)	09	Disregarded
099	EVA 4 Briefing Package (14-0617) sources: F014312	09	Disregarded
098	Preliminary EVA 4 Procedures (14-0615) sources: F014300A	09	Retrieved from FD9 Execute Package
097	EMU SWAP for EVA 4 (14-0614) sources: F014297	09	Retrieved from FD9 Execute Package
096	FD9 and FD10 Big Picture words for Robotics Ops (14-0613) sources: F014299	09	Retrieved from FD9 Execute Package
095	Updated LiOH CC sources: F014296	09	Retrieved from FD9 Execute Package
094	FD09 PAO Event Summary Message sources: F014291	09	Disregarded
093	ISS HAM KENWOOD MANUAL FREQUENCY INPUT sources: ISS MSG 14-0193	09	Retrieved from FD9 Execute Package
092	Logistics Cue Card (14-0611) sources: F014297	09	Retrieved from FD9 Execute Package
091A	P6 4B Solar Array Retract EVA Support (14-0610A) sources: F014282	09	Retrieved from FD9 Execute Package
090A	EVA 12A.1: SSRMS DOUG Setup Notes for 12A.1 EVA 4 (14-0609A)	09	Retrieved from FD9 Execute Package
089	EVA4 Support Setup (14-0608) sources: F014276	09	Retrieved from FD9 Execute Package
088A	FD08 MMT Summary (14-0607A) sources: Flight Director	09	Retrieved from FD9 Execute Package
087A	FD09 Water Summary Message sources: F014292	09	Retrieved from FD9 Execute Package
086	FD09 Transfer Message (14-0606) sources: F014302	09	Retrieved from FD9 Execute Package
085	FD09 Mission Summary (14-0605) sources: N017034, N017051	09	Retrieved from FD9 Execute Package
084A	FD09 Flight Plan Revision sources: F014279, F014293, N017052	09	Retrieved from FD9 Execute Package
083	FD09 Preliminary Summary Timeline	08	Disregarded
082	Maneuver to MT Translate Config WS3 to WS5 from P6 Retract Viewing (14-0604) sources: F014271		Requested & Delivered by JSC on 7/2/08
081	EVA 4 SAW SRMS Viewing sources: F014267A	10	Retrieved from FD10 Execute Package
080	Big Picture Words for Channel (1/4) for Power Reconfiguration (14-0600)	08	Retrieved from FD8 Execute Package

Table 71. Listing of the electronic messages sent to the STS-116 crew (Part 3 of 6).

MSG #	Message Title	FD	Status for Case Study
079	Updated LiOH CC sources: F014254	08	Retrieved from FD8 Execute Package
078	FD08 Water Summary Message sources: F014252	08	Retrieved from FD8 Execute Package
077	FD08 Transfer Message (14-0599) sources: F014260	08	Retrieved from FD8 Execute Package
076A	FD07 MMT Summary (14-0598A) sources: Flight Director	08	Retrieved from FD8 Execute Package
075	FD08 Mission Summary (14-0597) sources: N016982, N016999	08	Retrieved from FD8 Execute Package
074	FD08 Flight Plan Revision sources: F014257	08	Retrieved from FD8 Execute Package
073	STS-116 EVA#3 Agreements for SAW Retraction (14-0595) sources: F014237	07	Requested & Delivered by JSC on 7/2/08
072	EVA 3 SAW Troubleshooting (14-0596) sources: F014235	07	Requested & Delivered by JSC on 7/2/08
071A	FD08 Preliminary Summary Timeline	07	Disregarded
070	Channel 1/4 Ground/Crew Interaction Table (14-0594) sources: F014238	08	Retrieved from FD8 Execute Package
069	Channel 1/4 Power Reconfiguration Definitions Table (14-0593) sources: F014071	08	Retrieved from FD8 Execute Package
068	Channel 1/4 Flow Chart Update (14-0592) sources: F014071	08	Retrieved from FD8 Execute Package
067	HAM Pass for GMT 351 - Thunmanskolan, Knivsta, Sweden (14-0589)	08	Retrieved from FD8 Execute Package
066	Crew News Conference Event (14-0583) sources: F014207	07	Disregarded
065	FD07 ESA PAO EVENT (14-0582) sources: F014205A	07	Disregarded
064	2.3.402 N14B Y-Jumper Installation/Removal sources: ODF	07	Retrieved from FD7 Execute Package
063A	EVA Questions and Deltas to FD7 EMU Resize sources: F014200A, F014201A, N016921A	07	Retrieved from FD7 Execute Package
062	FD07 Water Summary Message sources: F014212	07	Retrieved from FD7 Execute Package
061	FD06 MMT Summary (14-0580) sources: Flight Director	07	Retrieved from FD7 Execute Package
060	FD07 Transfer Message (14-0579) sources: F014219	07	Retrieved from FD7 Execute Package
059	FD07 Mission Summary (14-0578) sources: N016894, F014125, N016916	07	Retrieved from FD7 Execute Package
058A	FD07 Flight Plan Revision sources: F014208, F014216, F014218	07	Retrieved from FD7 Execute Package

Table 72. Listing of the electronic messages sent to the STS-116 crew (Part 3 of 6).

MSG #	Message Title	FD	Status for Case Study
057	2.600 Unknown EPS 12A.1 EVA 2 through EVA 3 (14-0577) sources: F014190	06	Disregarded
056	FD07 Preliminary Summary Timeline	06	Disregarded
055	EVA #4 Discussion with Crew sources: F014186A	06	Disregarded
054	Excerpts from FD06 Daily Summary sources: F014154	06	Retrieved from FD6 Execute Package
053	FD06 Water Summary Message sources: F014166	06	Retrieved from FD6 Execute Package
052	FD06 Transfer Message (14-0572) sources: F014171	06	Retrieved from FD6 Execute Package
051	FD05 MMT Summary (14-0571) sources: Flight Director	06	Retrieved from FD6 Execute Package
050	FD06 Ceta Cart Relocation Viewing sources: F014148	06	Retrieved from FD6 Execute Package
049	FD06 Mission Summary (14-0570) sources: N016834, N016849	06	Retrieved from FD6 Execute Package
048A	FD06 Flight Plan Revision sources: F014149, F014165, F014168	06	Retrieved from FD6 Execute Package
047	Preliminary FD06 Summary Timeline	05	Disregarded
046	Channel 2-3 Ground/Crew Interaction Table (14-0569) sources: F014152	06	Retrieved from FD6 Execute Package
045	Channel 2/3 Power Reconfiguration Definitions Table Update (14-0568) sources: F014072	06	Retrieved from FD6 Execute Package
044	Channel 2-3 Power Reconfiguration Flowchart Update (14-0567) sources: F014072	06	Retrieved from FD6 Execute Package
043	ROBO Procedure Updates for EVA2 (14-0566) sources: F014150	06	Retrieved from FD6 Execute Package
042	Z1 Tray QD U-Jumper Nutplate Caps Imagery (14-0561)	05	Retrieved from FD5 Execute Package
041A	FD05 PAO Event Summary Message (14-0560A) sources: F014121B	05	Disregarded
040	FD05 Water Summary Message sources: F014122	05	Retrieved from FD5 Execute Package
039	FD05 Transfer Message (14-0558) sources: F014130	05	Retrieved from FD5 Execute Package
038	FD04 MMT Summary (14-0557) sources: Flight Director	05	Disregarded
037	FD05 Mission Summary (14-0556) sources: N016769, N016785	05	Retrieved from FD5 Execute Package
036B	FD05 Flight Plan Revision sources: N016746, F014128, N016779C, F014131	05	Retrieved from FD5 Execute Package
035	FD05 Preliminary Summary Timeline	04	Disregarded

Table 73. Listing of the electronic messages sent to the STS-116 crew (Part 4 of 6).

MSG #	Message Title	FD	Status for Case Study
034A	Panel 19 Viewing with SRMS EE sources: F014109	04	Requested & Delivered by JSC on 7/2/08
033C	FD05 Mnvr to 4B SAW Retract Viewing Position sources: F014113	05	Retrieved from FD5 Execute Package
032	FN03 DAT Review (14-0551) sources: F014092A. ET DOORS IMPACT.ppt (e-mail)	04	Disregarded
031	FD04 Water Summary Message sources: F014076	04	Retrieved from FD4 Execute Package
030	FD03 MMT Summary (14-0549) sources: Flight Director	04	Disregarded
029	FD04 Transfer Message (14-0548) sources: F014093A	04	Retrieved from FD4 Execute Package
028	Updates to LCS Cue Card sources: F014066	04	Retrieved from FD4 Execute Package
027	Desktop Video Downlink Test sources: F014064	04	Retrieved from FD4 Execute Package
026	FD04 Mission Summary (14-0547) sources: F014077, N016706, N016722	04	Retrieved from FD4 Execute Package
025B	FD04 Flight Plan Revision sources: F014058, N016719	04	Retrieved from FD4 Execute Package
024	FD04 Preliminary Summary Timeline	04	Disregarded
023	Orbiter Port RCC Panel Inspection (14-0546) sources: F014055	03	Requested & Delivered by JSC on 7/2/08
022	SODF Book Transfer (14-0534)	03	Retrieved from FD3 Execute Package
021	FD03 RELMO AND MNVR PADS sources: N016650	03	Retrieved from FD3 Execute Package
020	9.101 JOINT EXPEDITED UNDOCKING AND SEPARATION Procedure Update (14- 0542) sources: F014031A	03	Retrieved from FD3 Execute Package
019	FD03 Transfer Message (14-0541) sources: F014039	03	Retrieved from FD3 Execute Package
018A	FD02 MMT Summary (14-0537A) sources: Flight Director	03	Retrieved from FD3 Execute Package
017B	FD03 EVA Updates (14-0538B) sources: F013994, F014022, F014023	03	Retrieved from FD3 Execute Package
016	FD03 Mission Summary (14-0539) sources: N016646A, F014036, F014020	03	Retrieved from FD3 Execute Package
015B	FD03 Flight Plan Revision sources: F014006, F014015	03	Retrieved from FD3 Execute Package
014	FD03 Preliminary Summary Timeline	02	Disregarded
013	DOUG Setup Notes for 12A.1 (14-0535) sources: F014006	03	Requested & Delivered by JSC on 7/2/08
012	FD03 Events and Lighting Summary sources: F013993	02	Disregarded
011	FD03 Water Summary Message sources: F014035	03	Retrieved from FD3 Execute Package

Table 74. Listing of the electronic messages sent to the STS-116 crew (Part 5 of 6).

MSG #	Message Title	FD	Status for Case Study
010	FD02 SpaceHab Viewport Violations sources: N016591	02	FD2 Execute Package
009	FD02 Summary Timeline	02	Retrieved from FD2 Execute Package
008A	FD02 Transfer Message (14-0528A) sources: F013983, F013984	02	Retrieved from FD2 Execute Package
007A	FD02 Water Summary Message sources: F013976	02	Retrieved from FD2 Execute Package
006	Port Upper Carrier Tile ITVC Survey sources: F013971	02	Retrieved from FD2 Execute Package
005A	PL PWRDWN UPDATES sources: F014012	03	Retrieved from FD3 Execute Package
004A	FD02 Mission Summary (14-0529A) sources: F013977, F013967, N016590, N016596	02	Retrieved from FD2 Execute Package
003B	FD02 Flight Plan Revision sources: F013964, F013963, F013974, F013980A	02	Retrieved from FD2 Execute Package
002	FLIGHT NIGHT 01 ATTITUDES sources: F013957	01	Requested & Delivered by JSC on 7/2/08
001	OCA PRINTER TEST MESSAGE sources: MATS	01	Disregarded

Table 75. Listing of the electronic messages sent to the STS-116 crew (Part 6 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
1	2	RCS JET REPRIORITIZATION	3	Tin Whisker mitigations determined pre-flight	GNC/PROP
2	2	P5 Ungrapple	3	Changes due to RHC 10V Failure	PDRS
3	2	OBSS Berth	3	Changes due to RHC 10V Failure	PDRS
4	2	OBSS Handoff From SRMS to SSRMS	3	Changes due to RHC 10V Failure	PDRS
5	2	POST SLEEP	3	Step added for FES PRI B troubleshooting	EECOM
6	2	PORT UPPER TILE ITVC SURVEY	6	Changes due to RHC 10V Failure	PDRS
7	3	DOUG Setup for FD4	13	Typo	PDRS
8	3	LCH DEACT	15B	Checkmark added and callout deleted	PDRS
9	3	PL PWRDWN	005A	Modified SpaceHab steps	ACO
10	3	PL SAFING	005A	Modified SpaceHab steps	ACO
11	3	S0/N1 PWR CABLE INSTALL	017B	Logistical Changes	EVA
12	3	UIA HANDRAILS	017B	Typo	EVA
13	3	EVA 3 TOOLS AND STOWAGE	017B	Missing PGT SETTINGS TABLE	EVA

Table 76. Procedure update designations for STS-116 (Part 1 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
14	3	EVA 3 UNSCH/CONT EVA TASK	017B	Logistical Changes	EVA
15	3	STS-116 Logistics Cue Card	017B	Changed Serial Numbers for LiOH canisters	EVA
16	3	EMU AND EVA TOOL TRANSFER AND RECONFIGURATION	017B	Changed Serial Numbers for LiOH canisters	EVA
17	3	EMU PREBREATHE	017B	Typo	EVA
18	3	EMU PREBREATHE	017B	SAFER LATCH GUARD Steps Added (they did a variant of these steps on STS-115 also)	EVA
19	3	JOINT EXPEDITED UNDOCKING AND SEPARATION PROCEDURE	20	Typos and extra instructions	ACO
20	3	ORBITER PORT RCC PANEL INSPECTION	23	Added due to port wing leading edge sensor indications during launch	PDRS/ROBO
21	4	DESKTOP VIDEO DOWNLINK TEST	27	Added due to FD2 LCC Desktop malfunction	INCO
22	4	LCS Cue Card	28	Changes due to FD2 LCC Desktop malfunction	INCO
23	4	PORT PANEL 19 VIEWING	34A	Added due to port wing leading edge sensor indications during launch	PDRS
24	5	4B SAW RETRACT VIEWING	33C	Added to put the SRMS in the desired config for SAW viewing after the extra inspection on FD3	PDRS
25	5	CHANNEL 2/3 POWER RECONFIGURATION	42	Steps added to inspect Z1 U-jumper nutplates for sharp edge hazard	EVA
26	6	PRLA CLOSE	048A	Improper config of OBSS MRL Logic	ACO/PDRS
27	6	STBD CETA CART 2 RELOCATION	43	Typos	PDRS/ROBO
28	6	STBD CETA CART 1 RELOCATION	43	Extra Instructions Added	PDRS/ROBO
29	6	CETA CART RELOCATION VIEWING	50	Procedure intended to be updated in real-time	PDRS/ROBO
30	7	PRE EVA 3 EMU RESIZE	063A	Steps added to make the procedure outcome more efficient	EVA
31	7	SSRMS STOW TO P6 RETRACT VIEWING	59	Maneuver added in anticipation of viewing SAW retraction after BGA wiggle test	PDRS

Table 77. Procedure update designations for STS-116 (Part 2 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
32	8	LiOH Cue Card	79	Updated to account for recovery of ISS CDRA	EECOM
33	8	EVA 3 SAW Troubleshooting	72	Procedure added due to SAW Retract Anomaly	EVA
34	8	MANEUVER TO MT TRANSLATE CONFIG WS3 TO WS5 FROM P6 RETRACT VIEWING	82	Maneuver added in anticipation of viewing SAW retraction during EVA 3	ROBO
35	9	EVA4 SUPPORT SETUP	89	Maneuver added in anticipation of viewing SAW retraction during EVA 4	ROBO
36	9	DOUG Setup for EVA 4	90	Added for support of EVA 4	PDRS/ ROBO
37	9	P6 4B SOLAR ARRAY RETRACT EVA SUPPORT	91	Added for support of EVA 4	ROBO
38	9	STS-116 Logistics Cue Card	92	Updated for newly added EVA 4	EVA
39	9	EMU SWAP for EVA 4	97	Added to swap an EMU for EVA 4	EVA
40	9	EVA 4 NOTES, CAUTIONS, & WARNINGS	98	Added for EVA 4	EVA
41	9	EVA 4 INHIBIT PAD	98	Added for EVA 4	EVA
42	9	EVA 4 TOOL CONFIG	98	Added for EVA 4	EVA
43	9	EGRESS	98	Added for EVA 4	EVA
44	9	INGRESS	98	Added for EVA 4	EVA
45	9	EMU WRIST DISCONNECT TAPING	98	Added to reduce electrocution hazard on EVA 4	EVA
46	9	EVA 4 NOTES, CAUTIONS, & WARNINGS	102	Refinement of EVA 4 Procedure	EVA
47	9	EVA 4 INHIBIT PAD	102	Refinement of EVA 4 Procedure	EVA
48	9	EVA 4 TOOL CONFIG	102	Refinement of EVA 4 Procedure	EVA
49	9	EGRESS	102	Refinement of EVA 4 Procedure	EVA
50	9	P6 4B SOLAR ARRAY WING RETRACT TROUBLESHOOTING	102	Added for EVA 4	EVA
51	9	INGRESS	102	Refinement of EVA 4 Procedure	EVA
52	9	P6 4B SOLAR ARRAY WING RETRACT TROUBLESHOOTING	103	Addition of steps to inspect SABB	EVA

Table 78. Procedure update designations for STS-116 (Part 3 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
53	9	10.2 PSIA CAMPOUT EVA PREP	105	Addition of steps to inspect EV 2's EMU (which had not been through a complete checkout)	EVA
54	10	EVA 4 SAW SRMS VIEWING	81	Added for EVA 4	PDRS
55	10	SEP BURN	113	Changes due to possibility of SAW not retracting	RNDZ
56	10	EMU RECONFIGURATION FOR TRANSFER	114	Added for EVA 4	EVA/ACO
57	11	APU HEATER RECONFIG	116A	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
58	11	HEATER RECONFIG- CONFIG B(CONFIG A)	116A	Possibly due to warm attitude	EECOM
59	11	PMA 2 X3 CONNECTOR PHOTOGRAPHY PROCEDURE	120	Added to inspect PMA audio interface for damage	INCO
60	11	DOCKED AUDIO HARDLINE VOICE TEST	124	Audio problem troubleshooting	INCO
61	11	SEP BURN	125	Updated to re-insert flyaround	RNDZ
62	12	LCS Cue Card	131	Additional changes resulting from the LCC problem on FD2	INCO
63	13	WASTE H2O DUMP TERMINATION	137	Steps changed to perform a purge of the Waste H2O Dump Line	EECOM
64	13	Ext Airlock Heater Reconfig	138B	Steps added to return Ext Airlock Heaters to nominal config for D/O Prep	EECOM
65	13	PRE-SLEEP	138B	Steps changed due to the discovery of a bias in O2 Sys 2 flow sensor during PCS configuration on FD11	EECOM
66	13	POST SLEEP	138B	Steps changed due to the discovery of a bias in O2 Sys 2 flow sensor during PCS configuration on FD11	EECOM
67	13	RAD BYPASS/FES C/O	144B	Switch positions changed due to FES PRI B Controller on FD 1	EECOM
68	13	NOMINAL DEORBIT PREP C/L	144B	Switch positions changed due to FES PRI B Controller on FD 1	EECOM

Table 79. Procedure update designations for STS-116 (Part 4 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
69	13	NOMINAL DEORBIT PREP C/L	144B	Switch positions changed due to failure of a Mid Port Payload Bay Floodlight on FD3	EGIL
70	13	ENTRY SWITCH LIST VERIFICATION	144B	Switch positions changed due to FES PRI B Controller on FD 1	EECOM
71	13	ENTRY SWITCH LIST VERIFICATION	144B	Switch positions changed due to waste water line purge	EECOM
72	13	ENTRY SWITCH LIST VERIFICATION	144B	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
73	13	DEORBIT PREP BACKOUT	144B	Switch positions changed due to FES PRI B Controller on FD 1	EECOM
74	13	DEORBIT PREP BACKOUT	144B	Switch positions changed due to failure of a Mid Port Payload Bay Floodlight on FD3	EGIL
75	13	DEORBIT PREP BACKOUT	144B	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
76	13	PAYLOAD DEACTIVATION	145	Additional steps required	ACO
77	13	MNVR to D/O BURN	146B	Switch position changed due to APU heater reconfig	EGIL/ MMACS
78	13	NH3 ACT	146B	NH3 Boiler Config	EECOM
79	13	MS SYS DEACT F/ EXTENDED PWR UP	146B	Step not required for this flight	ACO
80	13	APU HTR DEACT	146B	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
81	13	NH3 RECONFIG	146B	NH3 Boiler Config	EECOM
82	13	1-Orbit Late D/O Procedure	146B	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
83	13	MNVR to 1-ORB LATE D/O ATT	146B	Switch position changed due to APU heater reconfig according to preflight plan	EGIL/ MMACS
84	13	TUNNEL CONFIG	149	Improper installation of caps on air circulation ducts during SHAB prep for docking	ACO

Table 80. Procedure update designations for STS-116 (Part 5 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
85	13	BFS --> PASS DK ASSIGNMENT	150A	New procedure due to single-hit I/O error on IDP4 during Post Insertion	DPS
86	13	OMS/RCS VALVE TEST	151A	New steps added due to the possibility of landing at White Sands (this possibility was considered due to the extra docked day at ISS to accommodate EVA 4)	PROP

Table 81. Procedure update designations for STS-116 (Part 6 of 6).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
1	2	0*	2	0	2
2	2	1	3	1	1
3	2	1	2	0	1
4	2	1	3	1	1
5	2	1	2	0	1
6	2	1	2	0	1
7	3	0	4	1	3
8	3	0	3	0	3
9	3	0*	3	0	3
10	3	0*	3	0	3
11	3	0	6	3	3
12	3	0	8	5	3
13	3	0	8	5	3
14	3	0	8	5	3
15	3	0	3	0	3
16	3	0	3	0	3
17	3	0	4	1	3
18	3	0*	4	1	3
19	3	0	3	0	3
20	3	1	3	0	2
21	4	2	4	0	2
22	4	2	4	0	2
23	4	1	4	0	3
24	5	1	5	0	4
25	5	0	6	1	5
26	6	0	6	0	6
27	6	0	6	0	6
28	6	0	6	0	6

Table 82. Key flight days for each STS-116 procedure update (Part 1 of 3).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
29	6	0	6	0	6
30	7	0	7	0	7
31	7	5	7	0	2
32	8	8	8	0	0
33	8	5	8	0	3
34	8	5	8	0	3
35	9	5	10	1	4
36	9	5	10	1	4
37	9	5	10	1	4
38	9	5	10	1	4
39	9	5	9	0	4
40	9	5	10	1	4
41	9	5	10	1	4
42	9	5	9	0	4
43	9	5	10	1	4
44	9	5	10	1	4
45	9	5	10	1	4
46	9	9	10	1	0
47	9	9	10	1	0
48	9	9	9	0	0
49	9	9	10	1	0
50	9	5	10	1	4
51	9	9	10	1	0
52	9	9	10	1	0
53	9	9	9	0	0
54	10	10	10	0	0
55	10	5	11	1	5
56	10	5	11	1	5
57	11	0	11	0	11
58	11	0	11	0	11
59	11	0	11	0	11
60	11	0	11	0	11
61	11	10	11	0	1
62	12	2	12	0	10
63	13	12	13	0	1
64	13	0	13	0	13
65	13	11	13	0	2
66	13	11	13	0	2
67	13	1	13	0	12
68	13	1	13	0	12
69	13	3	13	0	10
70	13	1	13	0	12
71	13	12	13	0	1
72	13	0	13	0	13

Table 83. Key flight days for each STS-116 procedure update (Part 2 of 3).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
73	13	1	13	0	12
74	13	3	13	0	10
75	13	0	13	0	13
76	13	0	13	0	13
77	13	0	13	0	13
78	13	0	13	0	13
79	13	0	13	0	13
80	13	0	13	0	13
81	13	0	13	0	13
82	13	0	13	0	13
83	13	0	13	0	13
84	13	3	13	0	10
85	13	1	13	0	12
86	13	5	13	0	8

*Likely being reworked or already finished at launch

Table 84. Key flight days for each STS-116 procedure update (Part 3 of 3).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
1	Tin Whisker mitigations determined pre-flight	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
2	Changes due to RHC 10V Failure	N/A	Actuator "Failure" or Degradation
3	Changes due to RHC 10V Failure	N/A	Actuator "Failure" or Degradation
4	Changes due to RHC 10V Failure	N/A	Actuator "Failure" or Degradation
5	Step added for FES PRI B troubleshooting	N/A	Actuator "Failure" or Degradation
6	Changes due to RHC 10V Failure	N/A	Actuator "Failure" or Degradation
7	Typo	N/A	Typos and Omissions
8	Checkmark added and callout deleted	N/A	Typos and Omissions
9	Modified SpaceHab steps	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch

Table 85. STS-116 update rationales (Part 1 of 6).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
10	Modified SpaceHab steps	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
11	Logistical Changes	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
12	Typo	N/A	Typos and Omissions
13	Missing PGT SETTINGS TABLE	N/A	Typos and Omissions
14	Logistical Changes	N/A	Equipment List Revision
15	Changed Serial Numbers for LiOH canisters	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
16	Changed Serial Numbers for LiOH canisters	N/A	Inconsistency between Items Expected to be Launched and Items Actually Launched
17	Typo	N/A	Typos and Omissions
18	SAFER LATCH GUARD Steps Added (they did a variant of these steps on STS-115 also)	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
19	Typos and extra instructions	N/A	Typos and Omissions
20	Added due to port wing leading edge sensor indications during launch	N/A	Launch Damage (actual or suspected)
21	Added due to FD2 LCC Desktop malfunction	N/A	Unexpected Software Behavior
22	Changes due to FD2 LCC Desktop malfunction	N/A	Unexpected Software Behavior
23	Added due to port wing leading edge sensor indications during launch	N/A	Launch Damage (actual or suspected)
24	Added to put the SRMS in the desired config for SAW viewing after the extra inspection on FD3	N/A	Launch Damage (actual or suspected)

Table 86. STS-116 update rationales (Part 2 of 6).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
25	Steps added to inspect Z1 U-jumper nutplates for sharp edge hazard	N/A	Proactive Contingency Preparation and/or Hazard Investigation
26	Improper config of OBSS MRL Logic	N/A	Unexpected Software Behavior
27	Typos	N/A	Typos and Omissions
28	Extra Instructions Added	N/A	Typos and Omissions
29	Procedure intended to be updated in real-time	N/A	Procedure Nominally Updated in Real-time
30	Steps added to make the procedure outcome more efficient	N/A	Procedure Efficiency Optimization
31	Maneuver added in anticipation of viewing SAW retraction after BGA wiggle test	P6 SAW Retract Problems	Equipment List Revision
32	Updated to account for recovery of ISS CDRA	N/A	Consumable Management Optimizations
33	Procedure added due to SAW Retract Anomaly	P6 SAW Retract Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
34	Maneuver added in anticipation of viewing SAW retraction during EVA 3	P6 SAW Retract Problems	Equipment List Revision
35	Maneuver added in anticipation of viewing SAW retraction during EVA 4	P6 SAW Retract Problems	Equipment List Revision
36	Added for support of EVA 4	P6 SAW Retract Problems	Equipment List Revision
37	Added for support of EVA 4	P6 SAW Retract Problems	Equipment List Revision
38	Updated for newly added EVA 4	P6 SAW Retract Problems	Consumable Management Replanning
39	Added to swap an EMU for EVA 4	P6 SAW Retract Problems	Equipment List Revision
40	Added for EVA 4	P6 SAW Retract Problems	Unaccounted for Inhibits
41	Added for EVA 4	P6 SAW Retract Problems	Unaccounted for Inhibits
42	Added for EVA 4	P6 SAW Retract Problems	Equipment List Revision
43	Added for EVA 4	P6 SAW Retract Problems	Task Deferral or Reprioritization
44	Added for EVA 4	P6 SAW Retract Problems	Task Deferral or Reprioritization
45	Added to reduce electrocution hazard on EVA 4	P6 SAW Retract Problems	Unaccounted for Inhibits

Table 87. STS-116 update rationales (Part 3 of 6).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
46	Refinement of EVA 4 Procedure	P6 SAW Retract Problems	Unaccounted for Inhibits
47	Refinement of EVA 4 Procedure	P6 SAW Retract Problems	Unaccounted for Inhibits
48	Refinement of EVA 4 Procedure	P6 SAW Retract Problems	Equipment List Revision
49	Refinement of EVA 4 Procedure	P6 SAW Retract Problems	Task Deferral or Reprioritization
50	Added for EVA 4	P6 SAW Retract Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
51	Refinement of EVA 4 Procedure	P6 SAW Retract Problems	Task Deferral or Reprioritization
52	Addition of steps to inspect SABB	P6 SAW Retract Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
53	Addition of steps to inspect EV 2's EMU (which had not been through a complete checkout)	P6 SAW Retract Problems	Unaccounted for Inhibits
54	Added for EVA 4	P6 SAW Retract Problems	Equipment List Revision
55	Changes due to possibility of SAW not retracting	P6 SAW Retract Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
56	Added for EVA 4	P6 SAW Retract Problems	Equipment List Revision
57	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
58	Possibly due to warm attitude	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
59	Added to inspect PMA audio interface for damage	N/A	Proactive Contingency Preparation and/or Hazard Investigation
60	Audio problem troubleshooting	N/A	Actuator "Failure" or Degradation
61	Updated to re-insert flyaround	N/A	Procedure Efficiency Optimization

Table 88. STS-116 update rationales (Part 4 of 6).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
62	Additional changes resulting from the LCC problem on FD2	N/A	Unexpected Software Behavior
63	Steps changed to perform a purge of the Waste H2O Dump Line	N/A	Actuator "Failure" or Degradation
64	Steps added to return Ext Airlock Heaters to nominal config for D/O Prep	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
65	Steps changed due to the discovery of a bias in O2 Sys 2 flow sensor during PCS configuration on FD11	N/A	Sensor "Failure" or Bias
66	Steps changed due to the discovery of a bias in O2 Sys 2 flow sensor during PCS configuration on FD11	N/A	Sensor "Failure" or Bias
67	Switch positions changed due to FES PRI B Controller on FD 1	N/A	Actuator "Failure" or Degradation
68	Switch positions changed due to FES PRI B Controller on FD 1	N/A	Actuator "Failure" or Degradation
69	Switch positions changed due to failure of a Mid Port Payload Bay Floodlight on FD3	N/A	Actuator "Failure" or Degradation
70	Switch positions changed due to FES PRI B Controller on FD 1	N/A	Actuator "Failure" or Degradation
71	Switch positions changed due to waste water line purge	N/A	Actuator "Failure" or Degradation
72	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
73	Switch positions changed due to FES PRI B Controller on FD 1	N/A	Actuator "Failure" or Degradation
74	Switch positions changed due to failure of a Mid Port Payload Bay Floodlight on FD3	N/A	Actuator "Failure" or Degradation

Table 89. STS-116 update rationales (Part 5 of 6).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
75	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
76	Additional steps required	N/A	Typos and Omissions
77	Switch position changed due to APU heater reconfig	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
78	NH3 Boiler Config	N/A	Procedure Nominally Updated in Real-time
79	Step not required for this flight	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
80	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
81	NH3 Boiler Config	N/A	Procedure Nominally Updated in Real-time
82	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
83	Switch position changed due to APU heater reconfig according to preflight plan	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
84	Improper installation of caps on air circulation ducts during SHAB prep for docking	N/A	Crew Procedural Slips
85	New procedure due to single-hit I/O error on IDP4 during Post Insertion	N/A	Unexpected Software Behavior
86	New steps added due to the possibility of landing at White Sands (this possibility was considered due to the extra docked day at ISS to accommodate EVA 4)	P6 SAW Retract Problems	Consumable Management Replanning

Table 90. STS-116 update rationales (Part 6 of 6).

DATA POINT	MISSION ELAPSED TIME (MINUTES)	NUMBER OF PROCEDURES NEEDING AND BEING REWORKED
Launch	0	35
End of FD 1	360	48
End of FD 2	1770	45
End of FD 3	3240	34
End of FD 4	4650	31
Instant before SAW Retract Anomaly	5325	27
Instant after SAW Retract Anomaly	5326	47
End of FD 5	6090	47
End of FD 6	7500	43
End of FD 7	8940	41
End of FD 8	10350	39
End of FD 9	11790	27
End of FD 10	13200	26
End of FD 11	14580	23
End of FD 12	15990	24
End of FD 13	17430	0

Table 91. The STS-116 data time history for the variable *Number of Procedures Needing and Being Reworked*.

TYPES OF PROCEDURE UPDATES	PROCEDURE UPDATE NUMBERS
Due to SAW Retract Anomaly and in Time Horizon	None
Due to SAW Retract Anomaly and Beyond Time Horizon (i.e., propagated reworks due to the SAW Retract Anomaly)	31, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 50, 53, 54, 55, 56, and 86
Due to refinements of previously submitted SAW Retract Anomaly related updates	46, 47, 48, 49, 51 and 52
Outside Time Horizon and Not Latent at Launch (i.e., propagated reworks not due to a discrete event)	20, 21, 22, 23, 24, 62, 65, 66, 67, 68, 69, 70, 73, 74, 84, and 85
Procedures developed as a result of the rework process	1, 20, 21, 23, 24, 31, 33, 34, 35, 36, 37, 39, 40, 41, 42, 43, 44, 45, 50, 54, 59, 60, and 85

Table 92. List of specially designated STS-116 procedure updates.

FLIGHT DAY	MISSION ELAPSED TIME AT END OF FLIGHT DAY (MINUTES)	NORMALIZED TIME TO LANDING PREPARATION AT THE END OF FD 13	UPDATES SINCE PREVIOUS FLIGHT DAY
0	0	0	0
1	360	0.02065	0
2	1770	0.1016	6
3	3240	0.1859	14
4	4650	0.2668	3
5	6090	0.3494	2
6	7500	0.4303	4
7	8940	0.5129	2
8	10350	0.5938	3
9	11790	0.6764	19
10	13200	0.7573	3
11	14580	0.8365	5
12	15990	0.9174	1
13	17430	1	24

Table 93. STS-116 update times normalized to the landing preparation time.

STS-117 Data Tables

MSG #	MSG Title	FD	Status for Case Study
120	Blank Star Pairs Pad	13	Requested & Delivered by JSC on 7/2/08
119B	Waveoff Summary Timeline	13	Disregarded
118A	Entry Notes sources: FN020557	13	Requested & Delivered by JSC on 7/2/08
117A	Entry Summary Template	13	Disregarded
116A	Entry Summary sources: N020550A	13	Disregarded
115A	Entry Checklist Deltas sources: N020545, N020559	13	Requested & Delivered by JSC on 7/2/08
114A	Deorbit Prep Updates sources: F017102, F017113, N020545	13	Requested & Delivered by JSC on 7/2/08
113A	Entry FIW Summary sources: F017059, F017106, F016565	13	Requested & Delivered by JSC on 7/2/08
112	Entry Day Fluid Loading and Anti-G Suit Operations sources: F017097	13	Disregarded
111	Sunday Funnies	13	Disregarded
110	FD13 PAO Event Summary sources: F17095	13	Disregarded
109A	FD12 MMT Summary sources: F017094A	13	Retrieved from FD13 Execute Package
108	FD13 Mission Summary sources: N020539, N020540	13	Retrieved from FD13 Execute Package
107A	FD13 and FD14 Flight Plan Revision sources: F017104A, F017107A, N020535	13	Retrieved from FD13 Execute Package
106	MDM OA2 Card 5 Impacts for FCS C/O and Entry	12	Requested & Delivered by JSC on 7/2/08
105	Late Inspection Playback Times sources: F017096	12	Disregarded
104A	FD13 Preliminary Summary Timeline	12	Disregarded
103	Modified Group C Powerup sources: F017042	12	Retrieved from FD12 Execute Package
102C	FD11 MMT Summary (15-0494C) sources: F17043	12	Retrieved from FD12 Execute Package
101	FD12 Mission Summary (15-0493) sources: N020476, N020477, F017059	12	Retrieved from FD12 Execute Package
100B	FD12 Flight Plan Revision sources: F017058, F017067, F017068A, N020464	12	Retrieved from FD12 Execute Package
099B	FD12 Preliminary Summary Timeline	11	Disregarded
098B	Undocking PAD and Event Summary sources: N20461, N20466	11	Requested & Delivered by JSC on 7/2/08
097	Handover Attitude Control Orbiter to CMG-Only Without RS SMTc (15-0487) sources: F016955	11	Retrieved from FD11 Execute Package
096A	FD10 MMT Summary (15-0482A) sources: F017006	11	Retrieved from FD11 Execute Package

Table 94. Listing of the electronic messages sent to the STS-117 crew (Part 1 of 6).

MSG #	MSG Title	FD	Status for Case Study
095	FD11 Transfer Message (15-0481) sources: F017033	11	Retrieved from FD11 Execute Package
094	FD11 Mission Summary (15-0480) sources: F017017, N020428, N020420	11	Retrieved from FD11 Execute Package
093A	FD11 Flight Plan Revision sources: F016946, F017001A, F017013, F017018, F017019, F017029, N020438	11	Retrieved from FD11 Execute Package
092C	FD11 Preliminary Summary Timeline	10	Disregarded
091	Updated H2O Activities Cue Card sources: F016976	10	Retrieved from FD10 Execute Package
090	13A EVA-4: MMOD Shield Instructions (15-0475) sources: F016962	09	Requested & Delivered by JSC on 7/2/08
089	FD09 MMT Summary (15-0473) sources: F016958	10	Retrieved from FD10 Execute Package
088	FD10 Transfer Message (15-0472) sources: F016985	10	Retrieved from FD10 Execute Package
087	FD10 Mission Summary (15-0471) sources: N020359, N020366	10	Retrieved from FD10 Execute Package
086B	FD10 Flight Plan Revision sources: F016946, F016972A, F016986, F016987	10	Retrieved from FD10 Execute Package
085D	FD10 Preliminary Summary Timeline	09	Disregarded
084	13A EVA-4: ESP-2 Instructions (15-0468) sources: F016956	09	Requested & Delivered by JSC on 7/2/08
083	Detailed EVA 4 Procedures (15-0467)	09	Requested & Delivered by JSC on 7/2/08
082	EVA 4 Summary Timeline (15-0463) sources: F016930	09	Retrieved from FD9 Execute Package
081	EVA Transfer and Reconfig Update (15- 0462) sources: F016926	09	Retrieved from FD9 Execute Package
080	PAO Event Summary Message Joint Crew News Conference (15-0460) sources: F016919	09	Disregarded
079	Question for Crew Regarding EVA 3 (15- 0458)	08	Disregarded
078	FD08 MMT Summary (15-0457) sources: F016916A	09	Retrieved from FD9 Execute Package
077	FD09 Transfer Message (15-0456) sources: F016936	09	Retrieved from FD9 Execute Package
076	FD09 Mission Summary (15-0455) sources: N020308, N020311	09	Retrieved from FD9 Execute Package
075B	FD09 Flight Plan Revision sources: F016925, F016928, F016930, F016932, F016935, N020300	09	Retrieved from FD9 Execute Package
074A	FD08 Pre-Sleep Powerdowns sources: F016905A	08	Requested & Delivered by JSC on 7/2/08
073A	Words from Lindsey (15-0459A) sources: F016904	09	Retrieved from FD9 Execute Package

Table 95. Listing of the electronic messages sent to the STS-117 crew (Part 2 of 6).

MSG #	MSG Title	FD	Status for Case Study
072	EVA 3 Procedure Pen and Inks (15-0453) sources: F016879	08	Retrieved from FD8 Execute Package
071	Updated LiOH Cue Card sources: F016881	08	Retrieved from FD8 Execute Package
070A	FD07 MMT Summary (15-0451A) sources: F016867	08	Retrieved from FD8 Execute Package
069B	FD08 Flight Plan Revision sources: F016819, F016869, F016871, F016880, F016882A, F016884, F016887, N020213	08	Retrieved from FD8 Execute Package
068B	FD08 Preliminary Summary Timeline	07	Disregarded
066	EVA 3 Detailed Procedures (15-0447) sources: F016858	07	Requested & Delivered by JSC on 7/2/08
065	EVA 3 Cuff Checklist Pages (15-0445) sources: F016855	07	Disregarded
064	FD08 Mission Summary (15-0443) sources: N020233, N020232	08	Retrieved from FD8 Execute Package
063	Broken Stapler sources: F016838	07	Requested & Delivered by JSC on 7/2/08
062	OMS Pod Repair Stowage Matrix (15-0440) sources: F016832B	07	Requested & Delivered by JSC on 7/2/08
061A	Modified Group C Powerdown Procedure sources: F016825A	07	Retrieved from FD7 Execute Package
060	SRMS OMS Pod Blanket Repair Procedure sources: F016801, F016813	07	Retrieved from FD7 Execute Package
059	Detailed EVA Repair Procedure (15-0438) sources: F016830	07	Retrieved from FD7 Execute Package
058A	Updated EVA 3 Tool Config (15-0437A) sources: F016834A	07	Requested & Delivered by JSC on 7/2/08
057	Updated EVA 3 Inhibit Pad (15-0435) sources: F016821A	07	Retrieved from FD7 Execute Package
056	Space to Ground EVA 3 Tagup Outline (15-0434) sources: F016822	07	Retrieved from FD7 Execute Package
055	OMS Pod Blanket Repair Practice Session Procedure (15-0433) sources: F016799A	07	Retrieved from FD7 Execute Package
054	OMS Pod Blanket Repair Tool Prep Procedure (15-0432) sources: F016823A	07	Retrieved from FD7 Execute Package
053	EVA Tool Gather Procedure (15-0431) sources: F016831	07	Retrieved from FD7 Execute Package
052	Blanket Repair Briefing Package (15-0430) sources: F016826	07	Retrieved from FD7 Execute Package
051	EVA 3 Summary Timeline (15-0429) sources: F016816	07	Retrieved from FD7 Execute Package
050B	FD07 EVA Summary (15-0436B) sources: F016820	07	Retrieved from FD7 Execute Package

Table 96. Listing of the electronic messages sent to the STS-117 crew (Part 3 of 6).

MSG #	MSG Title	FD	Status for Case Study
049A	MEDS Power Savings Cue Card sources: F016804A	07	Retrieved from FD7 Execute Package
048	Updated H2O Activities Cue Card sources: F016806	07	Retrieved from FD7 Execute Package
047	2B SAW Retract Lighting Information (15-0428) sources: F016794	07	Retrieved from FD7 Execute Package
046	PAO Event Summary Message Fox News Radio, KMGH-TV, KUSA-TV (15-0427) sources: F016798	07	Disregarded
045	Parameters Affected By OA2 Card 5 MDM Failure sources: INCO, N020143	07	Requested & Delivered by JSC on 7/2/08
044	FD06 MMT Summary (15-0425) sources: F016788A	07	Retrieved from FD7 Execute Package
043	FD07 Transfer Message (15-0424) sources: F016824	07	Retrieved from FD7 Execute Package
042	FD07 Mission Summary (15-0423) sources: F016810, N020165, N020168	07	Retrieved from FD7 Execute Package
041A	FD07 Flight Plan Revision sources: F016800, F016811	07	Retrieved from FD7 Execute Package
040B	FD07 Preliminary Summary Timeline	06	Disregarded
039	2B SAW Retract Lighting Information (15-0419) sources: F016763B	06	Retrieved from FD6 Execute Package
038	EVA Assessment of OMS Pod Blanket Repair (15-0417) sources: F016726B	06	Retrieved from FD6 Execute Package
037	EMU Water Recharge Troubleshooting for Post EVA 2 (15-0416) sources: F016758	06	Retrieved from FD6 Execute Package
036	FD05 MMT Summary (15-0415) sources: F016744	06	Retrieved from FD6 Execute Package
035	FD06 Transfer Message (15-0414) sources: F016769A	06	Retrieved from FD6 Execute Package
034	FD06 Mission Summary (15-0413) sources: N020099, N020092	06	Retrieved from FD6 Execute Package
033A	FD06 Flight Plan Revision sources: F016742, F016760, F016767, F016768, N020094A	06	Retrieved from FD6 Execute Package
032B	FD06 Preliminary Summary Timeline	05	Disregarded
031	EVA 2 Tool Updates (15-0410)	05	Requested & Delivered by JSC on 7/2/08
030A	FD5 EVA Status Items (15-0406A) sources: F016713	05	
029	PAO Event Summary Message CBS News, KFOX-TV, KTSM-TV (15-0405) sources: F016703	05	Disregarded
028A	FD04 MMT Summary (15-0404A) sources: F016693	05	Retrieved from FD5 Execute Package

Table 97. Listing of the electronic messages sent to the STS-117 crew (Part 4 of 6).

MSG #	MSG Title	FD	Status for Case Study
027	FD05 Transfer Message (15-0403) sources: F016717	05	Retrieved from FD5 Execute Package
026	FD05 Mission Summary (15-0402) sources: F016709, F016710, N020018, N020017	05	Retrieved from FD5 Execute Package
025A	FD05 Flight Plan Revision sources: F016708, F016712	05	Retrieved from FD5 Execute Package
024	FD05 Preliminary Summary Timeline	04	Disregarded
023	Status of Regions of Interest (15-0398) sources: F016670A	04	Retrieved from FD4 Execute Package
022	FD03 MMT Summary (15-0396) sources: F016649	04	Retrieved from FD4 Execute Package
021	FD4 SVS S3S4 VIEWING LIGHTING PREDICTIONS (15-0395) sources: F016660	04	Retrieved from FD4 Execute Package
020B	FD04 Flight Plan Revision sources: F016673, F016665, F016668, F016671, N019926A	04	Retrieved from FD4 Execute Package
019A	FD04 Preliminary Summary Timeline	03	Disregarded
018	FD04 Mission Summary (15-0392) sources: N019955, N019956	04	Retrieved from FD4 Execute Package
017A	Port OMS Pod Survey sources: F016629	03	Retrieved from FD3 Execute Package
016	FD03 RELMO and MNVR PADS sources: N019907	03	Retrieved from FD3 Execute Package
015	FD02 MMT Summary (15-0390) sources: F016613	03	Retrieved from FD3 Execute Package
014B	FD03 Preliminary Summary Timeline	02	Disregarded
013	FD03 Transfer Message (15-0387) sources: F016626	03	Retrieved from FD3 Execute Package
012A	FD03 Mission Summary (15-0386A) sources: N019905, N019902A	03	Retrieved from FD3 Execute Package
011C	FD03 Flight Plan Revision sources: F016597, F016607, F016620, F016627	03	Retrieved from FD3 Execute Package
010	FD02 Inspection Playback Times sources: N19887	02	Disregarded
009	OMS Pod Blanket Survey sources: F016598	02	Requested & Delivered by JSC on 7/2/08
008	WLES Recovery on STS7 sources: FN16594	02	Requested & Delivered by JSC on 7/2/08
007	Rendezvous Events and Lighting Info sources: F016593	02	Disregarded
006	IWIS Big Picture Words for 13A (15-0361) sources: F016584	03	Retrieved from FD3 Execute Package
005	IWIS INSTALLATION IN SHUTTLE AIRLOCK (15-0374) sources: F016552B	03	Retrieved from FD3 Execute Package

Table 98. Listing of the electronic messages sent to the STS-117 crew (Part 5 of 6).

MSG #	MSG Title	FD	Status for Case Study
004	H2O Activities Cue Card sources: F016566	02	Retrieved from FD2 Execute Package
003	FD02 Mission Summary (15-0371) sources: F016565, F016560B, N019847B, N019849	02	Retrieved from FD2 Execute Package
002	FD02 Flight Plan Revision sources: F016527, F0165662, N019839, F016574	02	Retrieved from FD2 Execute Package
001	FD1 Test Message	01	Disregarded

Table 99. Listing of the electronic messages sent to the STS-117 crew (Part 6 of 6).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
1	2	OBSS LDRI/IDC RCC SURVEY - STBD	2	Changes to prevent the Sun from coming into the field of view of the IDC	PDRS
2	2	WLES RECOVERY ON STS7	8	Problems with STS7	FAO
3	2	OBSS LDRI/IDC RCC SURVEY - PORT	9	Procedure changed to allow more detailed inspection of the thermal blanket tear on the port OMS Pod	PDRS
4	3	POST SLEEP	11C	Reconfiguration of the OMS POD heaters (perhaps due to the tear in the thermal blanket)	PROP
5	3	N2 REPRESS USING PAYLOAD N2 VALVES	11C	Non-functional N2 Flow Sensor	EECOM
6	3	Switch Guard	11C	Switch guard placed over switch for a failed PL Bay Flood light	EGIL
7	3	IWIS INSTALLATION IN SHUTTLE AIRLOCK	5	Procedure not ready by print deadline	ACO
8	3	P/TV08 EXTERNAL SURVEY S/U	17A	Procedure changed to allow more detailed inspection of the thermal blanket tear on the port OMS Pod	PDRS
9	4	N2 REPRESS USING PAYLOAD N2 VALVES	20	Update sent to correct a step that had been done incorrectly on FD3	EECOM

Table 100. Procedure update designations for STS-117 (Part 1 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
10	4	PRE-SLEEP	20	Update to configure cameras for monitoring SAW deploy (per request from ROBO)	INCO
11	5	PRE-SLEEP	25	Refinement of the Update from Message 20	INCO
12	5	STS-117 Consumables Tracking Cue Card	30A	PGT battery logistics changed due to PGT power off anomaly during EVA 1	EVA
13	5	STS-117 Battery Recharge Plan	30A	PGT battery logistics changed due to PGT power off anomaly during EVA 1	EVA
14	5	EVA 2 Tool Config	31	Addition of a tool to cut the 2B leader (the fact that it still had a spring attached was reported on EVA 1)	EVA
15	6	FUEL CELL PURGE - MANUAL	33A	Change due to MDM OA2 Card 5 failure	EGIL
16	6	EMU WATER RECHARGE POST UIA CAP and PLUG	37	Changes due to poor EMU water recharging after EVA 1	EVA
17	6	2B SAW Retract Lighting Information	39	Provides the necessary camera pan/tilt angles for viewing SAW retract	PDRS/ROBO
18	7	PRE-SLEEP	41A	Refinement of update from Msg. 25. Changes made to support transfer of Shuttle camera images to ISS overnight	INCO
19	7	2B SAW Retract Lighting Information	47	Provides the necessary camera pan/tilt angles for viewing SAW retract	PDRS/ROBO
20	7	H2O ACTIVITIES CUE CARD	48	Changes due to poor EMU water recharging after EVA 1	EECOM

Table 101. Procedure update designations for STS-117 (Part 2 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
21	7	MEDS POWER SAVINGS CUE CARD	49A	Added to save power in order to potentially support extra days in orbit due to ISS attitude control problems	DPS
22	7	EVA 3 TOOL GATHER	53	Updated to accommodate OMS Pod Blanket Repair	EVA
23	7	OMS POD BLANKET REPAIR TOOL PREP	54	Added to prepare tools for OMS Pod Blanket Repair on EVA 3	EVA
24	7	OMS POD BLANKET REPAIR PRACTICE SESSION	55	Added to construct a platform to simulate OMS POD TPS Blanket material and to practice repair method	EVA
25	7	EVA 3 INHIBIT PAD	57	Updated to accommodate OMS Pod Blanket Repair	EVA
26	7	EVA 3 TOOL CONFIG	58A	Updated to accommodate OMS Pod Blanket Repair	EVA
27	7	OMS POD REPAIR	59	Added to accommodate OMS Pod Blanket Repair	EVA
28	7	SRMS OMS POD BLANKET REPAIR	60	Added to accommodate OMS Pod Blanket Repair	PDRS
29	7	GROUP C POWERDOWN	61A	Added save power in order to potentially support extra days in orbit due to ISS attitude control problems	ACO/ EECOM/ EGIL/GNC
30	8	SRMS OMS POD BLANKET REPAIR	69B	Changes due to ISS attitude problems	PDRS
31	8	POST EVA RCS RECONFIGURATION	69B	Changes due to ISS attitude problems	GNC/PROP
32	8	LiOH CUE CARD	71	Updated to accommodate extra days in orbit	EECOM
33	8	DLA 2 VERIFICATIONS/SARJ LAUNCH RESTRAINT REMOVAL	72	New PGT Settings	EVA

Table 102. Procedure update designations for STS-117 (Part 3 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
34	8	PRE-SLEEP	74A	New powerdowns to accommodate extra days in orbit	EGIL
35	9	POST EVA RECONFIGURATION AND TRANSFER	81	Changes due to addition of 4th EVA	EVA
36	9	EVA 4 INHIBIT PAD	83	Added to accommodate 4th EVA	EVA
37	9	EVA 4 EGRESS	83	Added to accommodate 4th EVA	EVA
38	9	CP1 ETVCG STANCHION INSTALLATION	83	Added to accommodate 4th EVA	EVA
39	9	DLA 2 VERIFICATIONS/SARJ LAUNCH RESTRAINT REMOVAL	83	Updated to be completed in 4th EVA	EVA
40	9	S3 KEEL PIN/Drag Link STOW	83	Added to accommodate 4th EVA	EVA
41	9	APFR RELOCATE/S4 MMOD SHIELD BOLT RELEASE	83	Added to accommodate 4th EVA	EVA
42	9	MT/CETA PATH/S3 CLEANUP	83	Added to accommodate 4th EVA	EVA
43	9	NODE/SM LAN CABLE ROUTING	83	Added to accommodate 4th EVA	EVA
44	9	SASA GIMBAL LOCKS	83	Added to accommodate 4th EVA	EVA
45	9	GPS ANTENNA #4 REMOVAL	83	Added to accommodate 4th EVA	EVA
46	9	VENT VALVE OPEN/MMOD SHIELD	83	Added to accommodate 4th EVA	EVA
47	9	EVA 4 CLEANUP/INGRESS	83	Added to accommodate 4th EVA	EVA
48	9	POST EVA 4 TOOL CONFIG	83	Added to accommodate 4th EVA	EVA
49	10	H2O ACTIVITIES CUE CARD	91	Updated to reflect extra docked days	EECOM

Table 103. Procedure update designations for STS-117 (Part 4 of 5).

Procedure Update	FD	Procedure Name	MSG #	Rationale	Console Position
50	11	POST EVA RECONFIGURATION AND TRANSFER	93A	Items added	EVA/ACO
51	11	HANDOVER ATTITUDE CONTROL ORBITER TO CMG-ONLY WITHOUT RS SMTC	97	Added as contingency procedure in response to ISS attitude problems	ADCO/GNC
52	12	HEATER RECONFIG - CONFIG B	100B	Possibly due to warm attitude	EECOM
53	12	OBSS LDRI/IDC RCC SURVEY - STBD	100B	Changes to prevent the Sun from coming into the field of view of the IDC	PDRS
54	12	GROUP C POWERUP	103	Changed due to earlier powerdowns to preserve power while ISS attitude problems were worked out	ACO/EECOM/EGIL/GNC
55	13	PAYLOAD DEACTIVATION	114A	Removes unnecessary step and adds a missing step to open AC1 MAR 3 phase circuit breaker	ACO
56	13	PAYLOAD ENTRY SWITCH LIST/ VERIFICATION	114A	Adds two missing circuit breaker checks (including a check to ensure that AC1 MAR 3 phase is open)	ACO
57	13	NOMINAL DEORBIT PREP CHECKLIST	114A	Different coldsoak initiation	EECOM
58	13	NOMINAL DEORBIT PREP CHECKLIST	114A	Change due to MDM OA2 Card 5 failure	INCO
59	13	NOMINAL DEORBIT PREP CHECKLIST	114A	Change due to failed PL Bay Flood light	EGIL
60	13	NOMINAL DEORBIT PREP CHECKLIST	114A	Change to high pitch noise from A6U ANNUN BUS	EGIL
61	13	ENTRY SWITCH LIST VERIFICATION	114A	New cabin temp controller config	EECOM
62	13	DEORBIT PREP BACKOUT	114A	Change due to failed PL Bay Flood light	EGIL
63	13	DEORBIT PREP BACKOUT	114A	New cabin temp controller config	EECOM
64	13	DEORBIT PREP BACKOUT	114A	PCS config	EECOM
65	13	NH3 ACT	115	NH3 boiler config	EECOM
66	13	NH3 RECONFIG	115	NH3 boiler config	EECOM

Table 104. Procedure update designations for STS-117 (Part 5 of 5).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
1	2	0	2	0	2
2	2	2	2	0	0
3	2	1	2	0	1
4	3	1	3	0	2
5	3	0	3	0	3
6	3	1	3	0	2
7	3	0*	3	0	3
8	3	1	3	0	2
9	4	3	4	0	1
10	4	0	4	0	4
11	5	4	5	0	1
12	5	4	6	1	1
13	5	4	6	1	1
14	5	4	6	1	1
15	6	5	6	0	1
16	6	4	6	0	2
17	6	0	6	0	6
18	7	5	7	0	2
19	7	6	7	0	1
20	7	4	7	0	3
21	7	6	7	0	1
22	7	1	8	1	6
23	7	1	8	1	6
24	7	1	7	0	6
25	7	1	8	1	6
26	7	1	7	0	6
27	7	1	8	1	6
28	7	1	8	1	6
29	7	6	7	0	1
30	8	6	8	0	2
31	8	6	8	0	2
32	8	4	8	0	4
33	8	0	8	0	8
34	8	6	8	0	2
35	9	4	9	0	5
36	9	4	10	1	5
37	9	4	10	1	5
38	9	4	10	1	5
39	9	4	10	1	5
40	9	4	10	1	5
41	9	4	10	1	5
42	9	4	10	1	5
43	9	4	10	1	5

Table 105. Key flight days for each STS-117 procedure update (Part 1 of 2).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
44	9	4	10	1	5
45	9	4	10	1	5
46	9	4	10	1	5
47	9	4	10	1	5
48	9	4	10	1	5
49	10	4	10	0	6
50	11	4	11	0	7
51	11	6	11	0	5
52	12	0	12	0	12
53	12	0	12	0	12
54	12	6	12	0	6
55	13	0	14	1	13
56	13	0	14	1	13
57	13	0	14	1	13
58	13	5	14	1	8
59	13	1	14	1	12
60	13	10	14	1	3
61	13	0	14	1	13
62	13	1	14	1	12
63	13	0	14	1	13
64	13	0	14	1	13
65	13	0	14	1	13
66	13	0	14	1	13

*Likely being reworked or already finished at launch

Table 106. Key flight days for each STS-117 procedure update (Part 2 of 2).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
1	Changes to prevent the Sun from coming into the field of view of the IDC	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
2	Problems with STS7	N/A	Unexpected Software Behavior
3	Procedure changed to allow more detailed inspection of the thermal blanket tear on the port OMS Pod	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
4	Reconfiguration of the OMS POD heaters (perhaps due to the tear in the thermal blanket)	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
5	Non-functional N2 Flow Sensor	N/A	Sensor "Failure" or Bias
6	Switch guard placed over switch for a failed PL Bay Flood light	N/A	Actuator "Failure" or Degradation
7	Procedure not ready by print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
8	Procedure changed to allow more detailed inspection of the thermal blanket tear on the port OMS Pod	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
9	Update sent to correct a step that had been done incorrectly on FD3	N/A	Crew Procedural Slips
10	Update to configure cameras for monitoring SAW deploy (per request from ROBO)	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
11	Refinement of the Update from Message 20	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
12	PGT battery logistics changed due to PGT power off anomaly during EVA 1	N/A	Actuator "Failure" or Degradation
13	PGT battery logistics changed due to PGT power off anomaly during EVA 1	N/A	Actuator "Failure" or Degradation

Table 107. STS-117 update rationales (Part 1 of 4).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
14	Addition of a tool to cut the 2B leader (the fact that it still had a spring attached was reported on EVA 1)	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
15	Change due to MDM OA2 Card 5 failure	N/A	Sensor "Failure" or Bias
16	Changes due to poor EMU water recharging after EVA 1	N/A	Actuator "Failure" or Degradation
17	Provides the necessary camera pan/tilt angles for viewing SAW retract	N/A	Procedure Nominally Updated in Real-time
18	Refinement of update from Msg. 25. Changes made to support transfer of Shuttle camera images to ISS overnight	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
19	Provides the necessary camera pan/tilt angles for viewing SAW retract	N/A	Procedure Nominally Updated in Real-time
20	Changes due to poor EMU water recharging after EVA 1	N/A	Actuator "Failure" or Degradation
21	Added to save power in order to potentially support extra days in orbit due to ISS attitude control problems	ISS Attitude Problems	Use of Shuttle Resources to Counteract ISS Problems
22	Updated to accommodate OMS Pod Blanket Repair	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
23	Added to prepare tools for OMS Pod Blanket Repair on EVA 3	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
24	Added to construct a platform to simulate OMS POD TPS Blanket material and to practice repair method	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
25	Updated to accommodate OMS Pod Blanket Repair	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
26	Updated to accommodate OMS Pod Blanket Repair	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
27	Added to accommodate OMS Pod Blanket Repair	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
28	Added to accommodate OMS Pod Blanket Repair	OMS Pod Blanket Tear	Launch Damage (actual or suspected)
29	Added save power in order to potentially support extra days in orbit due to ISS attitude control problems	ISS Attitude Problems	Use of Shuttle Resources to Counteract ISS Problems

Table 108. STS-117 update rationales (Part 2 of 4).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
30	Changes due to ISS attitude problems	ISS Attitude Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
31	Changes due to ISS attitude problems	ISS Attitude Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
32	Updated to accommodate extra days in orbit	"Get Aheads"	Consumable Management Replanning
33	New PGT Settings	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
34	New powerdowns to accommodate extra days in orbit	ISS Attitude Problems	Use of Shuttle Resources to Counteract ISS Problems
35	Changes due to addition of 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
36	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
37	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
38	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
39	Updated to be completed in 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
40	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
41	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
42	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
43	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
44	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
45	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
46	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
47	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
48	Added to accommodate 4th EVA	"Get Aheads"	"Get-Ahead" Tasks Scheduled
49	Updated to reflect extra docked days	"Get Aheads"	Consumable Management Replanning

Table 109. STS-117 update rationales (Part 3 of 4).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
50	Items added	"Get Aheads"	Equipment List Revision
51	Added as contingency procedure in response to ISS attitude problems	ISS Attitude Problems	Use of Shuttle Resources to Counteract ISS Problems
52	Possibly due to warm attitude	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
53	Changes to prevent the Sun from coming into the field of view of the IDC	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
54	Changed due to earlier powerdowns to preserve power while ISS attitude problems were worked out	ISS Attitude Problems	Use of Shuttle Resources to Counteract ISS Problems
55	Removes unnecessary step and adds a missing step to open AC1 MAR 3 phase circuit breaker	N/A	Typos and Omissions
56	Adds two missing circuit breaker checks (including a check to ensure that AC1 MAR 3 phase is open)	N/A	Typos and Omissions
57	Different coldsoak initiation	N/A	Procedure Nominally Updated in Real-time
58	Change due to MDM OA2 Card 5 failure	N/A	Sensor "Failure" or Bias
59	Change due to failed PL Bay Flood light	N/A	Actuator "Failure" or Degradation
60	Change to high pitch noise from A6U ANNUN BUS	N/A	Actuator "Failure" or Degradation
61	New cabin temp controller config	N/A	Procedure Nominally Updated in Real-time
62	Change due to failed PL Bay Flood light	N/A	Actuator "Failure" or Degradation
63	New cabin temp controller config	N/A	Procedure Nominally Updated in Real-time
64	PCS config	N/A	Procedure Nominally Updated in Real-time
65	NH3 boiler config	N/A	Procedure Nominally Updated in Real-time
66	NH3 boiler config	N/A	Procedure Nominally Updated in Real-time

Table 110. STS-117 update rationales (Part 4 of 4).

DATA POINT	MISSION ELAPSED TIME (MINUTES)	NUMBER OF PROCEDURES NEEDING AND BEING REWORKED
Launch	0	16
Instant before OMS Pod Thermal Blanket Tear	8	16
Instant after OMS Pod Thermal Blanket Tear	9	26
End of FD 1	360	29
End of FD 2	1770	27
End of FD 3	3210	23
Instant before ISS "Get Aheads"	4650	27
Instant after ISS "Get Aheads"/ End of FD 4	4651	44
End of FD 5	6090	43
Instant before ISS Attitude Problems	7320	42
Instant after ISS Attitude Problems	7321	49
End of FD 6	7500	48
End of FD 7	8940	36
End of FD 8	10350	31
End of FD 9	11760	17
End of FD 10	13170	17
End of FD 11	14580	15
End of FD 12	15990	12
End of FD 13	17400	0

Table 111. The STS-117 data time history for the variable *Number of Procedures Needing and Being Reworked*.

TYPES OF PROCEDURE UPDATES	PROCEDURE UPDATE NUMBERS
Due to OMS Pod Blanket Tear and in Time Horizon	3
Due to OMS Pod Blanket Tear and Beyond Time Horizon (i.e., propagated reworks due to the OMS Pod Blanket Tear)	4, 8, 22, 23, 24, 25, 26, 27, and 28
Due to refinements of previously submitted OMS Pod Blanket Tear related updates	None
Due to "Get Aheads" and in Time Horizon	None
Due to "Get Aheads" and Beyond Time Horizon (i.e., propagated reworks due to the "Get Aheads")	32, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50
Due to refinements of previously submitted "Get Aheads" related updates	None
Due to ISS Attitude Problems and in Time Horizon	21 and 29
Due to ISS Attitude Problems and Beyond Time Horizon (i.e., propagated reworks due to ISS Attitude Problems)	30, 31, 34, 51, 54,
Due to refinements of previously submitted ISS Attitude Problems related updates	None
Outside Time Horizon and Not Latent at Launch (i.e., propagated reworks not due to a discrete event)	6, 16, 18, 20, 58, 59, 60, and 62
Procedures developed as a result of the rework process	2, 6, 7, 17, 21, 23, 24, 27, 28, 31, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 47, 48, and 51

Table 112. List of specially designated STS-117 procedure updates.

FLIGHT DAY	MISSION ELAPSED TIME AT END OF FLIGHT DAY (MINUTES)	NORMALIZED TIME TO LANDING PREPARATION AT THE END OF FD 13	UPDATES SINCE PREVIOUS FLIGHT DAY
0	0	0	0
1	360	0.02069	0
2	1770	0.1017	3
3	3210	0.1845	5
4	4650	0.2672	2
5	6090	0.35	4
6	7500	0.4310	3
7	8940	0.5138	12
8	10350	0.5948	5
9	11760	0.6759	14
10	13170	0.7569	1
11	14580	0.8379	2
12	15990	0.9190	3
13	17400	1	12

Table 113. STS-117 update times normalized to the landing preparation time.

STS-120 Data Tables

MSG #	MSG Title	FD	Status for Case Study
184	FD16 - EOM+3 Flight Plan Revision sources: F019885	15	Requested & Delivered by JSC on 6/30/08
183A	Entry Summary Template sources: N023866A, N023872	15	Disregarded
182B	Entry Summary Message sources: N023866A	15	Disregarded
181A	FIW Summary sources: F019281, F019821, F019908	15	Disregarded
180A	Entry C/L Deltas sources: N023849, F019897, F019903A	15	Requested & Delivered by JSC on 6/16/08
179D	Deorbit Prep Updates sources: N023854, F019906, F019907	15	Requested & Delivered by JSC on 6/16/08
178	Sunday Funnies	15	Disregarded
177	Entry Day Fluid Loading and Anti-G Suit Ops sources: F019880	15	Retrieved from FD15 Execute Package
176A	Increased Middeck Air Circulation sources: N023865	15	Retrieved from FD15 Execute Package
175	FD15 PAO Event Summary sources: F19887	15	Disregarded
174	FD14 MMT Summary sources: F019890	15	Retrieved from FD15 Execute Package
173	FD15 Mission Summary sources: N23858, N23867	15	Retrieved from FD15 Execute Package
172B	FD15 Flight Plan Revision sources: N023863, N023865	15	Retrieved from FD15 Execute Package
171	FD15 Preliminary Summary Timelines	15	Disregarded
170	FD13 MMT Summary sources: F019857A	14	Retrieved from FD14 Execute Package
169	Starboard Survey Page 7-16 Update sources: F19855	14	Retrieved from FD14 Execute Package
168	OBSS Maneuver to Hover sources: F019837C	14	Retrieved from FD14 Execute Package
167	FD14 Mission Summary (16-0228) sources: N23798, N23802	14	Retrieved from FD14 Execute Package
166B	FD14 Flight Plan Revision sources: F019839, N023776, N023800	14	Retrieved from FD14 Execute Package
165	FD14 Preliminary Summary Timeline	13	Disregarded
164	Undocking PAD and Event Summary sources: F019827	13	Requested & Delivered by JSC on 6/30/08
163	FD13 Sensor Checkout sources: F19801B	13	Retrieved from FD13 Execute Package
162	FD13 ISS Stowage Info sources: F019809	13	Retrieved from FD13 Execute Package
161A	ESA-ASI PAO Event Summary Message: Sky News Italia sources: F19806A	13	Disregarded

Table 114. Listing of the electronic messages sent to the STS-120 crew (Part 1 of 9).

MSG #	MSG Title	FD	Status for Case Study
160	FD13 Transfer Message (16-0220) sources: F19816	13	Retrieved from FD13 Execute Package
159	EVA Stow Procedure (16-0219)	14	Requested & Delivered by JSC on 6/16/08
158	Post EVA 4 BSA Battery Recharge Graphic (16-0218) sources: F019803	13	Retrieved from FD13 Execute Package
157	EVA Prep for Transfer to Shuttle (16-0217)	13	Retrieved from FD13 Execute Package
156	FD 13 EVA DELTAS (16-0216) sources: F019810A	13	Retrieved from FD13 Execute Package
155B	Handover Attitude Control Procedure Update (16-0214B) sources: F019140, N23742, N23746	13	Retrieved from FD13 Execute Package
154	FD12 MMT Summary (16-0213) sources: F019814	13	Retrieved from FD13 Execute Package
153	FD13 Mission Summary (16-0212) sources: N23756, N23751, F19821	13	Retrieved from FD13 Execute Package
152B	FD13 Flight Plan Revision sources: F019766, FD019809, N023716, N023717, N023737, N023747	13	Retrieved from FD13 Execute Package
151A	FD13 Preliminary Summary Timeline	12	Disregarded
150	Revised Overview Timeline (16-0209)	12	Disregarded
149	Updated LiOH Cue Card sources: F019744	12	Retrieved from FD12 Execute Package
148	EVA 4 Frame of Reference (16-0208) sources: F019769	12	Retrieved from FD12 Execute Package
147	Middeck Stowage Maps sources: F019750	12	Retrieved from FD12 Execute Package
146	FD12 Transfer Message (16-0205) sources: F019771	12	Requested & Delivered by JSC on 6/16/08
145A	FD12 Post-EVA OBSS Handoff to SRMS (16-0202A) sources: F019749	12	Retrieved from FD12 Execute Package
144A	FD12 Port OBSS Handoff to SSRMS (16-0201A) sources: F019748D	12	Retrieved from FD12 Execute Package
143	FD12 OBSS Maneuver From Undock to Handoff (16-0200) sources: F019747	12	Retrieved from FD12 Execute Package
142	10A EVA4 SAW Damage Diagram (16-0196)	12	Requested & Delivered by JSC on 6/16/08
141	10A EVA4 Updated Detailed Timeline (16-0195) sources: F019745	11	Requested & Delivered by JSC on 6/16/08
140	Post EVA4 EMU Resize (16-0193)	12	Retrieved from FD12 Execute Package
139	FD12 EVA DELTAS (16-0192) sources: F019765	12	Retrieved from FD12 Execute Package
138	FD11 MMT Summary (16-0191) sources: F19764	12	Retrieved from FD12 Execute Package

Table 115. Listing of the electronic messages sent to the STS-120 crew (Part 2 of 9).

MSG #	MSG Title	FD	Status for Case Study
137	FD12 Mission Summary (16-0190) sources: N023677, N023678	12	Retrieved from FD12 Execute Package
136B	FD12 Flight Plan Revision (16-0189B) sources: N23652A, N23673	12	Retrieved from FD12 Execute Package
135A	FD12 Preliminary Summary Timeline	11	Disregarded
134	EVA4: Safety tethering to OBSS - Procedure Deltas (16-0188) sources: F019733	11	Requested & Delivered by JSC on 6/16/08
133	EVA S/G Tagup Agenda (16-0186) sources: F019731	11	Disregarded
132	Russian Dino Taping Procedure (16-0185) sources: F019730	11	Requested & Delivered by JSC on 6/16/08
131	Exercise Protocol (16-0184) sources: F019728	11	Requested & Delivered by JSC on 6/30/08
130A	DOUG Setup Notes (16-0183A) sources: F019727	11	Requested & Delivered by JSC on 6/30/08
129A	SSRMS Support of P6 4B Blanket Repair (16-0182A) sources: F019722	12	Requested & Delivered by JSC on 6/16/08
128A	SSRMS OBSS Grapple at WS 8 (16-0181A) sources: F019725	12	Requested & Delivered by JSC on 6/16/08
127	OBSS Unberth, Handoff, and MNVR to Pre-Grapple at WS8 (16-0180) sources: F019710A	11	Requested & Delivered by JSC on 6/16/08
126	EVA Tool Taping Procedures (16-0178) sources: F019711	11	Retrieved from FD11 Execute Package
125	SAW Repair Nomenclature and Cuff Pictures (16-0177) sources: F019713	11	Disregarded
124	EVA 4 SAW Repair Detailed Procedures (16-0176) sources: F019724B	11	Requested & Delivered by JSC on 6/16/08
123A	FD11 WS3 OBSS Handoff to SRMS sources: F019703A	11	Retrieved from FD11 Execute Package
122	Date/Time Set for DCS 760 S/N1016 sources: F19697	11	Retrieved from FD11 Execute Package
121A	FD10 MMT Summary (16-0175A) sources: F019700A	11	Retrieved from FD11 Execute Package
120	FD11 Transfer Message (16-0171) sources: F019702	11	Retrieved from FD11 Execute Package
119	FD11 Mission Summary (16-0169) sources: N023576	11	Retrieved from FD11 Execute Package
118B	FD11 Flight Plan Revision sources: N23551, N23569, N23567, N23577, F19698	11	Retrieved from FD11 Execute Package
117	Trash/Stowage Management for Extension Days sources: F019677A	10	Requested & Delivered by JSC on 6/16/08

Table 116. Listing of the electronic messages sent to the STS-120 crew (Part 3 of 9).

MSG #	MSG Title	FD	Status for Case Study
116A	Preliminary FD11 Summary Timeline	10	Disregarded
115	FD11 EVA Summary (16-0168) sources: F019717	11	Requested & Delivered by JSC on 6/30/08
114	EVA 4 Translation Path (16-0165) sources: F019720	11	Requested & Delivered by JSC on 6/30/08
113	Needle Nose Pliers Modification (16-0164) sources: F019721	11	Disregarded
112	FD11 and 12 Robotics - EVA Operations Sequence (16-0162) sources: F019664		Requested & Delivered by JSC on 6/30/08
111	EVA Get-Aheads FD10 (16-0161) sources: F019656	10	Requested & Delivered by JSC on 6/16/08
110	SSRMS MNVR to OBSS Pre-Grapple (16-0159) sources: F019663		Requested & Delivered by JSC on 6/16/08
109	SSRMS OBSS Unberth (16-0158) sources: F019663		Requested & Delivered by JSC on 6/16/08
108	Berthed OBSS Grapple From WS3 (16-0157) sources: F019663		Requested & Delivered by JSC on 6/16/08
107	Stowage Locations For Thu Plan (GMT 305, FD10) (16-0150)	10	Disregarded
106	Solar Array Hinge Stabilizer Construction (16-0156) sources: F019650	10	Requested & Delivered by JSC on 6/16/08
105B	15 Day Overview Timeline (FD12 EVA 4) (16-0160B) sources: W017421B	10	Disregarded
104A	10A EVA 4 Solar Array No Touch Briefing (16-0154A) sources: F019646A	10	Disregarded
103	EMU Wrist Disconnect Taping Procedure (16-0153) sources: F019643	10	Requested & Delivered by JSC on 6/16/08
102	EVA 4 SAW Repair Procedures (16-0152) sources: F19641	10	Requested & Delivered by JSC on 6/16/08
101	FD09 MMT Summary (16-0151) sources: F19637	10	Retrieved from FD10 Execute Package
100	10A EVA 4 Summary Timeline and Tool Config (16-0149)	10	Disregarded
099	FD10 EVA Deltas (16-0148)	10	Requested & Delivered by JSC on 6/16/08
098	FD10 Transfer Message (16-0144) sources: F019633	10	Retrieved from FD10 Execute Package
097	FD10 Mission Summary (16-0143) sources: N023493, N023497	10	Retrieved from FD10 Execute Package
096B	FD10 Flight Plan Revision sources: F19614, N23484, N23486	10	Retrieved from FD10 Execute Package
095	FD10 Preliminary Summary Timeline	09	Disregarded

Table 117. Listing of the electronic messages sent to the STS-120 crew (Part 4 of 9).

MSG #	MSG Title	FD	Status for Case Study
094	EMU Glove Recommendation For Parzynski (16-0136)	09	Requested & Delivered by JSC on 6/16/08
093	Initial Crew Package (16-0134)	09	Disregarded
092	Photo Technique for SARJ EVA 4 (16-0139) sources: F019587	09	Requested & Delivered by JSC on 6/16/08
091	FD08 MMT Summary (16-0135) sources: F019582	09	Retrieved from FD09 Execute Package
090	10A EVA 4 SARJ Briefing Package (16-0133) sources: F019589	09	Disregarded
089	10A EVA 4 Preliminary Detailed Timeline (16-0132)		Disregarded
088	Wheelock EMU Glove Reconfiguration (16-0131)	09	Requested & Delivered by JSC on 6/16/08
087	10A EVA Tool Buildup (16-0130)	09	Requested & Delivered by JSC on 6/30/08
086	Event Summary Message - ESA-ASI VIP Call sources: F019575	09	Disregarded
085	Event Summary Message - Discovery/Alpha Joint Crew News Conference (16-0128) sources: F019576	09	Disregarded
084	FD09 HAM Pass with Liceo Scientifico G.Galilei (16-0127) sources: N023042	09	Disregarded
083	FD09 Transfer Message (16-0126) sources: F019585	09	Retrieved from FD09 Execute Package
082	FD09 Mission Summary (16-0125) sources: N023414, N023427	09	Retrieved from FD09 Execute Package
081	FD9 EVA Deltas (16-0123) sources: F019588A	09	Requested & Delivered by JSC on 6/16/08
080B	FD09 Flight Plan Revision sources: F19579A, W17293, N23409, N23412, N23429	09	Retrieved from FD09 Execute Package
079	Mission Overview 15 DAY TIMELINE	08	Disregarded
078A	FD09 Preliminary Summary Timeline	08	Disregarded
077	10A EVA3 Detailed Timeline - NO MBSU (16-0115)	08	Retrieved from FD08 Execute Package
076	FD8 EVA DELTAS (16-0114)	08	Retrieved from FD08 Execute Package
075	FD07 MMT Summary (16-0112) sources: F019522	08	Retrieved from FD08 Execute Package
074A	FD08 Mission Summary (16-0111A) sources: N023343, N023348, N023356	08	Retrieved from FD08 Execute Package
073B	FD08 Flight Plan Revision sources: F19523, N23341	08	Retrieved from FD08 Execute Package
072A	PGSC Reconfig Due to STS6 Monitor Problems sources: FAO-F01956B	07	Requested & Delivered by JSC on 6/16/08

Table 118. Listing of the electronic messages sent to the STS-120 crew (Part 5 of 9).

MSG #	MSG Title	FD	Status for Case Study
071	EVA 3 Options for MBSU Time (16-0110) sources: EVA-F019510	07	Requested & Delivered by JSC on 6/16/08
070	FD08 Preliminary Summary Timeline	07	Disregarded
069	EVA 3 Summary Timeline (Reflects Port SARJ Inspection) (16-0106) sources: F019494	07	Disregarded
068	10A EVA3 Port SARJ Inspect (16-0103) sources: F019492	07	Requested & Delivered by JSC on 6/16/08
067	FD07 PAO Event Summary (16-0102) sources: F019478	07	Disregarded
066A	FD07 Flight Plan Revision sources: F019465, F019281, N023259, N023268, N023280, N023285	07	Retrieved from FD07 Execute Package
065	FD07 Mission Summary (16-0099) sources: N023294, N023286	07	Retrieved from FD07 Execute Package
064	FD07 MS4 Ham Pass with IIS Deambrosis-Natta & University of L'Aquila (16-0098) sources: N023041	07	Disregarded
063	FD7 EVA DELTAS (16-0096) sources: F019486A	07	Retrieved from FD07 Execute Package
062B	FD06 MMT Summary (16-0094B) sources: F019480	07	Retrieved from FD07 Execute Package
061	Post EVA2 SARJ inspect questions (16-0095)	06	Disregarded
060	FD07 Preliminary Summary Timeline	06	Disregarded
059	SRMS Mnvr to Pre-Cradle Position sources: F019438	06	Retrieved from FD06 Execute Package
058	FD6 EVA DELTAS (16-0090) sources: F019442	06	Retrieved from FD06 Execute Package
057	FD06 Transfer Message (16-0085) sources: F019437	06	Retrieved from FD06 Execute Package
056	FD05 MMT Summary (16-0084) sources: F019440	06	Retrieved from FD06 Execute Package
055	FD06 Mission Summary (16-0083) sources: F019439, N023232, N023237	06	Retrieved from FD06 Execute Package
054B	FD06 Flight Plan Revision sources: F019433, F019434, F019435, F019441, F019444, F019445A, N023223, N023229	06	Retrieved from FD06 Execute Package
053	SRMS MANEUVER TO NODE 2 VIEWING (16-0082) sources: PDRS -F019425	05	Requested & Delivered by JSC on 6/16/08
052	FD06 Preliminary Summary Timeline	05	Disregarded
051	EVA 2 Notes and Updates (16-0080) sources: EVA - F019421	05	Requested & Delivered by JSC on 6/16/08
050	EVA 2 Summary Timeline (16-0079)	05	Disregarded
049	10A EVA SARJ Cribsheet (16-0077)	05	Disregarded
048	10A EVA2 Detail Timeline Deltas (16-0076)	05	Requested & Delivered by JSC on 6/16/08

Table 119. Listing of the electronic messages sent to the STS-120 crew (Part 6 of 9).

MSG #	MSG Title	FD	Status for Case Study
047	10A EVA SARJ Inspection Briefing Package (16-0075)	05	Disregarded
046	FD05 PGSC Network Cabling Replacement sources: F019404	05	Retrieved from FD05 Execute Package
045B	Node 2 Equipment Prep sources: F019401	05	Retrieved from FD05 Execute Package
044A	FD05 FCMS Trouble Shooting sources: N023166	05	Retrieved from FD05 Execute Package
043A	PAO Event Summary Message - CBS News, FOX News, WHAM-TV, Rochester, NY (16-0073A) sources: F019393	05	Disregarded
042	Handover Attitude Control Orbiter to CMG-Only Without RS SMTc (16-0072) sources: F019366	05	Retrieved from FD05 Execute Package
041	RCC PLUG HOUSING REPLACEMENT (16-0070) sources: F019384	05	Retrieved from FD05 Execute Package
040	FD05 EVA DELTAS (16-0069) sources: F019407A	05	Requested & Delivered by JSC on 6/30/08
039	FD05 Transfer Message (16-0067) sources: F019400	05	Retrieved from FD05 Execute Package
038	FD04 MMT Summary (16-0066) sources: F019396	05	Retrieved from FD05 Execute Package
037A	FD05 Mission Summary (16-0065A) sources: F019391, F019390, F019394, N023195	05	Retrieved from FD05 Execute Package
036A	FD05 Flight Plan Revision sources: F019371, F019386, F019395, N023112A; N023140B, N023152, N023159, N023164, N023184	05	Retrieved from FD05 Execute Package
035	DCS760 Camera Issues sources: MMACS - F019376	04	Requested & Delivered by JSC on 6/16/08
034	FD5 Preliminary Summary Timeline	04	Disregarded
033B	Manual WinDecom SpOC Update Procedure sources: F019357	04	Retrieved from FD04 Execute Package
032A	FD04 EVA DELTAS (16-0056A) sources: F019347B	04	Retrieved from FD04 Execute Package
031	Background Information on the Naming of "Harmony" (16-0055) sources: F019345	04	Retrieved from FD04 Execute Package
030	FD03 MMT Summary (16-0054) sources: F019346	04	Retrieved from FD04 Execute Package
029A	Water Ops Cue Card sources: N023139	04	Retrieved from FD04 Execute Package
028	FD04 Transfer Message (16-0052) sources: F019356	04	Retrieved from FD04 Execute Package

Table 120. Listing of the electronic messages sent to the STS-120 crew (Part 7 of 9).

MSG #	MSG Title	FD	Status for Case Study
027A	FD04 Mission Summary (16-0051A) sources: N023134, N023135	04	Retrieved from FD04 Execute Package
026B	FD04 Flight Plan Revision sources: F019344, F019352, N023113, N023114, N023129, N023130, N023140	04	Retrieved from FD04 Execute Package
025	EMU Prebreathe Updates (16-0049)	03	Requested & Delivered by JSC on 6/16/08
024	FD04 Preliminary Summary Timeline	03	Disregarded
023	TCS Troubleshooting Procedure sources: F019311B	03	Retrieved from FD03 Execute Package
022	SODF Transfer Activity (16-0031)		Requested & Delivered by JSC on 6/16/08
021	FD03 RELMO and Maneuver Pads sources: N023061	03	Retrieved from FD03 Execute Package
020A	FD03 EVA Deltas sources: F019294B	03	Retrieved from FD03 Execute Package
019	FD02 MMT Summary sources: F019306	03	Disregarded
018	Stowage Locations For IWIS Accelerometer Install sources: F019302	03	Retrieved from FD03 Execute Package
016	FD03 Transfer Message (16-0037) sources: F019310	03	Retrieved from FD03 Execute Package
014	IWIS Installation Near Shuttle Ergometer (16-0035) sources: F019275A	03	Retrieved from FD03 Execute Package
013	FD03 Mission Summary sources: F019281, N023056, N023071	03	Retrieved from FD03 Execute Package
012A	FD03 Flight Plan Revision sources: F019300, F019302, F019305, N023027, N023047, N023057	03	Retrieved from FD03 Execute Package
011	FD3 Preliminary Summary Timeline	02	Disregarded
010	FD2 Survey Times for Playback sources: INCO- F0197276A	02	Requested & Delivered by JSC on 6/16/08
009	Rendezvous Event and Lighting Information Summary sources: F019267	02	Requested & Delivered by JSC on 6/30/08
008	FD02 EVA C/L and ISS EVA Systems C/L Deltas sources: F019259	02	Retrieved from FD02 Execute Package
007	Post EVA EMU Glove Photo Reference Procedures (16-0030) sources: F019261	02	Retrieved from FD02 Execute Package
006	FD02 Survey Deltas sources: F019248A	02	Retrieved from FD02 Execute Package
005	FD02 Transfer Message sources: F019255	02	Retrieved from FD02 Execute Package

Table 121. Listing of the electronic messages sent to the STS-120 crew (Part 8 of 9).

MSG #	MSG Title	FD	Status for Case Study
004	FD02 Mission Summary sources: F019258, N02292, N022989	02	Retrieved from FD02 Execute Package
003B	FD02 Flight Plan Revision sources: F019207, F019239A, F019254, F019257, F019260, N022986, N022988	02	Retrieved from FD02 Execute Package
002	FD1 Timeline Updates	01	Requested & Delivered by JSC on 6/16/08
001	Test Message	01	Disregarded

Table 122. Listing of the electronic messages sent to the STS-120 crew (Part 9 of 9).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
1	1	DON ACTIWATCH	2	Mistakenly Omitted from timeline for MS5 (Typo)	ACO/ SURGEON
2	2	FC Purge - Manual	003B	Failed Flowmeter (Failure occurred on STS-116)	EGIL
3	2	OBSS LDRI/IDC RCC Survey - STBD	6	Improving IDC coverage of panels 9R, 13R, 9L, and 12L	PDRS
4	2	OBSS LDRI/IDC RCC Survey - PORT	6	Improving IDC coverage of panels 9R, 13R, 9L, and 12L	PDRS
5	2	Post EVA Glove Photos - Required	7	New procedure developed in response to glove damage on STS-118. This procedure was not completed in time to make it into the ISS EVA Systems C/L before the print deadline	EVA
6	2	EVA PREP FOR TRANSFER TO ISS	8	Logistical Changes	EVA
7	2	EVA PREP FOR TRANSFER TO SHUTTLE	8	Logistical Changes	EVA
8	2	EVA STOW	8	Logistical Changes	EVA
9	3	IWIS INSTALLATION NEAR SHUTTLE ERGOMETER	14	Details of this procedure were not finalized until after print deadline	ACO
10	3	FD03_TRANSFERLIST_STS120	16	PGSC Power cable failure	ACO
11	3	PRE EVA 1 TOOL CONFIG	020A	Tasks simplified by ISS crew item prepositioning	EVA

Table 123. Procedure update designations for STS-120 (Part 1 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
12	3	STS-120/10A Consumables Tracking Cue Card	020A	Serial numbers called down by crew and recorded on the cue card. Also, there was a typo	EVA
13	3	TCS TROUBLE SHOOTING PROCEDURE	23	Bad TCS data cable or improper assignment of the COM Port within the Windows operating system.	FAO
14	3	EMU PREBREATHE	25	Details of this procedure were not finalized until after print deadline	EVA
15	4	EVA 1 INHIBIT PAD LOCATION DEPENDENT INHIBITS	032A	The lab window shutter being closed throughout the mission eliminated the need for several steps	EVA
16	4	EVA1 INHIBIT PAD EVA 1 SPECIFIC INHIBITS - SSPTS DEACTIVATION	032A	Messages Omitted	EVA
17	4	MANUAL WINDECOM SPOC UPDATE PROCEDURE	033B	PGSC Network problems	FAO
18	4	DCS SETUP Cue Card	35	Overexposed images from DCS760 cameras (Note: this may not be a procedure update as much as a compliance verification)	MMACS
19	5	POST EVA 1/PRE EVA 2 TOOL CONFIG	40	Confusion over whether to leave a tool on ISS or bring it back	EVA
20	5	PRE EVA 2 TOOL CONFIG	40	Added tools for SARJ inspection	EVA
21	5	POST EVA 2 TOOL CONFIG	40	Added tools for SARJ inspection	EVA
22	5	EVA 2 CLEANUP AND A/L INGRESS	40	Added steps to inspect the APFR (it was thought that the glove damage on STS-118 and EVA 1 may be due to poor performance by the APFR)	EVA

Table 124. Procedure update designations for STS-120 (Part 2 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
23	5	S1 SFU CONFIG CINCH FIRING	40	Changed due to addition of SARJ Inspection	EVA
24	5	PDGF INSTALL ON NODE 2	40	Removed inhibits and step 1 due to task reordering to accommodate the addition of SARJ Inspection	EVA
25	5	RCC PLUG HOUSING REPLACEMENT	41	Details of this procedure were not finalized until after print deadline	MMACS
26	5	HANDOVER ATTITUDE CONTROL ORBITER TO CMG-ONLY WITHOUT RS SMTC	42	This new procedure is in response to the ISS attitude control problems encountered on STS-117. It probably did not make its way into the procedure books before the print deadline	ADCO/ GNC
27	5	FD05 FCMS TROUBLE SHOOTING	044A	PGSC Network Problems	FAO
28	5	NODE 2 EQUIPMENT PREP	045B	IMS update	ACO
29	5	FD05 PGSC NETWORK CABLING REPLACEMENT	46	PGSC Network Problems	FAO
30	5	NODE 2 OUTFITTING	48	Step reprioritized and reordered due to addition of SARJ Inspection	EVA
31	5	AIRLOCK OPS AND CETA HANDRAIL INSPECTION	48	CETA Rail damage from MMOD believed to be related to EMU glove damage on STS-118 and EVA 1	EVA
32	5	SARJ INSPECTION	48	SARJ vibrations	EVA
33	5	EVA 2 Tool Config	51	Removal of hardware added in MSG 40 from the EVA	EVA
34	5	SARJ Inspection cribsheet	51	Removal of hardware added in MSG 40 from the EVA	EVA
35	5	SARJ INSPECTION	51	Typo	EVA
36	5	EVA 2 Inhibit Pad	51	New translation path necessitated a new inhibit.	EVA

Table 125. Procedure update designations for STS-120 (Part 3 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
37	5	SRMS MANEUVER TO NODE 2 VIEWING	53	Unexpected SRMS shoulder temps.	PDRS
38	6	New process for recording FCMS data	55	Intermittent data from FCMS application	EGIL
39	6	STS-120/10A Consumables Tracking Cue Card	58	Changed REBA Battery serial numbers	EVA
40	6	STS-120/10A Consumables Tracking Cue Card	58	Changed REBA Battery serial numbers	EVA
41	6	STS-120/10A Battery Recharge Plan Cue Card	58	Changed REBA Battery serial numbers	EVA
42	6	STS-120/10A Consumables Tracking Cue Card	58	New LiOH canister to accommodate a longer EVA 3 (due to the tasks that were moved from EVA 2)	EVA
43	6	SRMS MNVR TO PRE-CRADLE POSITION	59	Unexpected SRMS shoulder temps.	PDRS
44	7	On Orbit Installable Handrail Troubleshooting Procedure	63	Unreleased bolt	EVA
45	7	POST EVA 2/PRE EVA 3 TOOL CONFIG	63	Removal/ Reconfiguration of equipment added/reconfigured for EVA 2 SARJ Inspection	EVA
46	7	PRE EVA 3 TOOL CONFIG	63	Removal/ Reconfiguration of equipment added/reconfigured for EVA 2 SARJ Inspection	EVA
47	7	EVA 3 A/L EGRESS AND SETUP	63	Equipment stowage plan change (due to the addition of the SARJ inspection)	EVA
48	7	ATTACH P6 to P5	63	New number of turns on P6 strap (either due to a typo or reanalysis)	EVA
49	7	OUTBOARD RADIATOR CINCH RELEASE	63	Logistical changes (due to reordering of tasks for the SARJ inspection)	EVA

Table 126. Procedure update designations for STS-120 (Part 4 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
50	7	P1 SFU CONFIG FOR CINCH FIRING	63	This procedure was put "On Call" and updated to include steps for a possible EV1 O2 recharge due to the addition of the SARJ inspection	EVA
51	7	MBSU TRANSFER	63	This procedure was updated to include steps for a possible EV2 O2 recharge due to the addition of the SARJ inspection	EVA
52	7	EVA PREP	63	Steps removed to prevent hot mics during EVA Prep/Post	EVA
53	7	EMU PURGE	63	Steps removed to prevent hot mics during EVA Prep/Post	EVA
54	7	PORT SARJ INSPECT	68	Added to due debris found during STBD SARJ inspection	EVA
55	7	PGSC RECONFIG DUE TO STS6 MONITOR PROBLEMS	072A	STS6 monitor problems	FAO
56	8	New process for Shuttle/ISS intercom	074A	Failed primary hardline intercom	INCO
57	8	POST EVA	76	Step delayed due to regeneration of micropurification unit	EVA
58	8	P1 SFU CONFIG POST DEPLOY	77	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	EVA
59	8	HORSESHOE CONNECTOR INSTALL	77	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	EVA
60	8	RPCM S04B-C R&R	77	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	EVA

Table 127. Procedure update designations for STS-120 (Part 5 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
61	9	IMU reset	080B	IMU 1 problems and inability to use star tracker data due to attitude and sun angle	GNC
62	9	POST EVA3/PRE EVA 4 TOOL CONFIG	81	Logistical changes	EVA
63	9	EMU Contingency Resize Matrix (STS-120/10A)	81	Anomalous data on the sublimator of a suit prompted the MCC to look into EMU resizing and they found a few mistakes in the resize matrix	EVA
64	9	INSPECTION MIRROR CONFIGURE FOR EVA	87	Equipment Buildup for SARJ Troubleshooting	EVA
65	9	Wheelock EMU Glove Reconfiguration	88	Small tears in EMU gloves	EVA
66	9	Photo Technique for SARJ EVA 4	92	Added for SARJ Inspection	EVA
67	9	EMU Glove Recommendation for Parazynski	94	Added to alleviate blistering of EV1's hand	EVA
68	10	LiOH Cuecard	096B	The decision to use older LiOH canisters necessitated new steps to prevent dust from being spread throughout the cabin	EECOM
69	10	BATT SWAP	99	EMU battery change to accommodate a longer EVA	EVA
70	10	STS 120 EVA 4 INHIBIT PAD	102	Changes due to addition of SAW repair activity to EVA	EVA
71	10	EVA 4 NOTES, CAUTIONS, AND WARNINGS	102	Changes due to addition of SAW repair activity to EVA	EVA
72	10	PRE EVA 4 TOOL CONFIG	102	Changes due to addition of SAW repair activity to EVA	EVA
73	10	EVA 4 A/L EGRESS AND SETUP	102	Changes due to addition of SAW repair activity to EVA	EVA

Table 128. Procedure update designations for STS-120 (Part 6 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
74	10	SSRMS/OBSS SETUP	102	Procedure added in order to use OBSS for SAW repair activity	EVA/ ROBO/ PDRS
75	10	SSRMS/OBSS MNVR TO 4B SAW	102	SSRMS/OBSS MNVR due to addition of SAW repair activity to EVA	EVA/ ROBO/ PDRS
76	10	4B SAW TROUBLESHOOTING	102	Changes due to addition of SAW repair activity to EVA	EVA
77	10	SSRMS/OBSS MNVR TO APFR EGRESS	102	SSRMS/OBSS MNVR due to addition of SAW repair activity to EVA	EVA/ ROBO/ PDRS
78	10	APFR EGRESS AND OBSS CLEANUP	102	Procedure added in order to use OBSS for SAW repair activity	EVA/ ROBO/ PDRS
79	10	EVA 4 CLEANUP AND A/L INGRESS	102	Changes due to addition of SAW repair activity to EVA	EVA
80	10	EMU Wrist Disconnect Taping for EVA 4	103	Added to prevent contact of metal glove components with the solar arrays (electrocution hazard)	EVA
81	10	SOLAR ARRAY HINGE STABILIZER CONSTRUCTION	106	Added to construct stabilizers for the damaged SAW	EVA
82	10	BERTHED OBSS GRAPPLE FROM WS3	108	Procedure added in order to use OBSS for SAW repair activity	ROBO/ PDRS
83	10	SSRMS OBSS UNBERTH	109	Procedure added in order to use OBSS for SAW repair activity	ROBO/ PDRS
84	10	SSRMS MNVR TO OBSS PRE-GRAPPLE	110	Procedure added in order to use OBSS for SAW repair activity	ROBO/ PDRS
85	11	STS-120/10A Consumables Tracking Cue Card	115	Logistical changes due to SAW repair EVA	EVA

Table 129. Procedure update designations for STS-120 (Part 7 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
86	11	DATE/TIME SET FOR DCS 760 S/N 1016	122	Camera resetting issues	MMACS
87	11	FD11 WS3 OBSS HANDOFF TO SRMS	123A	Procedure added in order to use OBSS for SAW repair activity	ROBO/ PDRS
88	11	EVA Tool Taping Procedures	126	Added to reduce electrocution hazard for SAW repair EVA	EVA
89	11	OBSS UNBERTH, HANDOFF, AND MANEUVER TO PRE- GRAPPLE AT WORKSITE 8	127	Procedure added in order to use OBSS for SAW repair activity	EVA/ ROBO/ PDRS
90	12	SSRMS OBSS GRAPPLE AT WS8	128A	Procedure added in order to use OBSS for SAW repair activity	EVA/ ROBO/ PDRS
91	12	SSRMS SUPPORT OF P6 4B BLANKET REPAIR	129A	Procedure added in order to use OBSS for SAW repair activity	EVA/ROBO
92	11	DOUG Setup Notes	130	This procedure allowed the crew to view a DOUG movie of the trajectory to the SAW repair site	EVA/ ROBO/ PDRS
93	11	RUSSIAN EVA DINO CUTTERS (NIPPERS) TAPING PROCEDURE	132	Added to reduce electrocution hazard for SAW repair EVA	EVA
94	11	Safety tethering to OBSS	134	Changes to the EVA 4 procedure due to need to safety tether to OBSS	EVA
95	11	STS 120 EVA 4 INHIBIT PAD	141	Refinement of this SAW repair procedure	EVA
96	11	EVA 4 NOTES, CAUTIONS, AND WARNINGS	141	Refinement of this SAW repair procedure	EVA
97	11	PRE EVA 4 TOOL CONFIG	141	Refinement of this SAW repair procedure	EVA
98	11	EVA 4 A/L EGRESS AND SETUP	141	Refinement of this SAW repair procedure	EVA
99	11	SSRMS/OBSS SETUP	141	Refinement of this SAW repair procedure	EVA/ ROBO/ PDRS

Table 130. Procedure update designations for STS-120 (Part 8 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
100	11	SSRMS/OBSS MNVR TO 4B SAW	141	Refinement of this SAW repair procedure	EVA/ ROBO/ PDRS
101	11	4B SAW TROUBLESHOOTING	141	Refinement of this SAW repair procedure	EVA
102	11	SSRMS/OBSS MNVR TO APFR EGRESS	141	Refinement of this SAW repair procedure	EVA/ ROBO/ PDRS
103	11	APFR EGRESS AND OBSS CLEANUP	141	Refinement of this SAW repair procedure	EVA/ ROBO/ PDRS
104	11	EVA 4 CLEANUP AND A/L INGRESS	141	Refinement of this SAW repair procedure	EVA
105	12	PRE EVA 4 TOOL CONFIG	139	Equipment omissions in the previously transmitted version of this SAW repair procedure	EVA
106	12	4B SAW TROUBLESHOOTING	139	Typos in the previously transmitted version of this SAW repair procedure	EVA
107	12	EVA 4 CLEANUP AND A/L INGRESS	139	Missing EVA overglove doffing steps in the previously transmitted version of this SAW repair procedure	EVA
108	12	Post EVA4 EMU Resize	140	To return the EMU used for EVA 4 back to its original size for use on a stage EVA (as per message 62, this EMU was resized due so that EV1 could use it as a replacement for his EMU, which had sublimator problems)	EVA
109	12	FD 12 OBSS MNVR FROM UNDOCK TO HANDOFF	143	OBSS movements added for SAW repair EVA	ROBO/ PDRS
110	12	FD 12 PORT OBSS HANDOFF TO SSRMS	144A	OBSS movements added for SAW repair EVA	ROBO/ PDRS

Table 131. Procedure update designations for STS-120 (Part 9 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
111	12	FD 12 POST-EVA OBSS HANDOFF TO SRMS	145A	OBSS movements added for SAW repair EVA	ROBO/PDRS
112	12	LiOH Cuecard	149	Logistical changes	EECOM
113	13	AVIU Reconfig	152B	Broken AVIU switch	INCO
114	13	3.11X HANDOVER ATTITUDE CONTROL CMG TA TO ORBITER VIA SPEC 205	155B	This procedure is in response to the ISS attitude control problems encountered on STS-117. It probably did not make its way into the procedure books before the print deadline	ADCO/GNC
115	13	EVA TRANSFER TO SHUTTLE	156	Different EVA batteries	EVA/ACO
116	13	EVA PREP FOR TRANSFER TO SHUTTLE	157	Different EVA batteries	EVA/ACO
117	13	STS-120/10A Battery Recharge Plan Cue Card	158	Battery information updated to reflect EVA 4	EVA
118	13	FD13 SENSOR CHECKOUT	163	Added to ensure that OBSS still worked after EVA 4	PDRS
119	13	Undocking PAD and Event Summary	164	Additional photos requested due to a degradation of TCS Reflector #1 noticed on FD 3	RNDZ
120	13	SEP BURN	164	Optimization of post-separation trajectory due to extra days at station	RNDZ
121	14	HEATER RECONFIG-CONFIG B	166B	Possibly due to warmer attitudes than expected	EECOM
122	14	OBSS MANEUVER TO HOVER	168	Added due to FD13 Sensor Checkout	PDRS
123	14	OBSS LDRI/IDC RCC SURVEY - STBD	169	Comments added to reflect delays in the procedure	PDRS
124	15	INCREASED MIDDECK AIR CIRCULATION	176A	Added to give crew the optional capability to increase air circulation	EECOM
125	15	NOMINAL DEORBIT PREP CHECKLIST	176A	Modified to give crew the optional capability to increase air circulation	EECOM

Table 132. Procedure update designations for STS-120 (Part 10 of 11).

Procedure Update	FD	Procedure Name	Msg #	Rationale	Console Position
126	15	PAYLOAD ENTRY SWITCH LIST/VERIFICATION	179D	Typo	ACO
127	15	NOMINAL DEORBIT PREP CHECKLIST	179D	Mid Port Payload Bay Floodlight Failure on FD12	EGIL
128	15	DEORBIT PREP BACKOUT	179D	Mid Port Payload Bay Floodlight Failure on FD12	EGIL
129	15	DEORBIT PREP BACKOUT	179D	PCS 1 configuration changes	EECOM
130	15	FINAL ENTRY SWITCH LIST VERIFICATION	179D	Flash Evaporator Configuration	EECOM
131	15	NH3 ACT	180A	Ammonia Boiler Configuration	EECOM
132	15	NH3 RECONFIG	180A	Ammonia Boiler Configuration	EECOM
133	15	OMS He PRESS/ Δ V/BURN TIME	180A	Updated due to extra days in orbit and change from ascending to descending landing opportunities	PROP
134	15	PREBANK TABLES	180A	Updated due to extra days in orbit and change from ascending to descending landing opportunities	GNC
135	15	EOM+3 FLIGHT PLAN REVISION	184A	Revised flight plan due to landing waveoffs	FAO

Table 133. Procedure update designations for STS-120 (Part 11 of 11).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
1	1	0	1	0	1
2	2	0*	2	0	2
3	2	1	2	0	1
4	2	1	2	0	1
5	2	0*	4	2	2
6	2	0	2	0	2
7	2	0	2	0	2
8	2	0	2	0	2
9	3	0*	3	0	3
10	3	1	3	0	2
11	3	2	3	0	1
12	3	0	3	0	3
13	3	1	3	0	2
14	3	0*	4	1	3
15	4	0	4	0	4
16	4	0	4	0	4
17	4	1	4	0	3
18	4	4	4	0	0
19	5	0	5	0	5
20	5	4	6	1	1
21	5	4	7	2	1
22	5	0	6	1	5
23	5	4	6	1	1
24	5	4	6	1	1
25	5	0*	5	0	5
26	5	0*	6	1	5
27	5	1	5	0	4
28	5	5	5	0	0
29	5	1	5	0	4
30	5	4	6	1	1
31	5	4	6	1	1
32	5	4	6	1	1
33	5	5	6	1	0
34	5	5	6	1	0
35	5	5	6	1	0
36	5	4	6	1	1
37	5	5	5	0	0
38	6	5	6	0	1
39	6	5	6	0	1
40	6	5	11	5	1
41	6	5	6	0	1
42	6	4	8	2	2
43	6	5	6	0	1
44	7	6	8	1	1

Table 134. Key flight days for each STS-120 procedure update (Part 1 of 4).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
45	7	4	7	0	3
46	7	4	7	0	3
47	7	4	8	1	3
48	7	0	8	1	7
49	7	4	8	1	3
50	7	4	8	1	3
51	7	4	8	1	3
52	7	6	8	1	1
53	7	6	8	1	1
54	7	4	8	1	3
55	7	7	7	0	0
56	8	7	8	0	1
57	8	7	8	0	1
58	8	4	8	0	4
59	8	4	8	0	4
60	8	4	8	0	4
61	9	0	9	0	9
62	9	4	9	0	5
63	9	8	9	0	1
64	9	4	9	0	5
65	9	8	10	1	1
66	9	4	10	1	5
67	9	8	10	1	1
68	10	9	10	0	1
69	10	8	10	0	2
70	10	8	12	2	2
71	10	8	12	2	2
72	10	8	11	1	2
73	10	8	12	2	2
74	10	8	12	2	2
75	10	8	12	2	2
76	10	8	12	2	2
77	10	8	12	2	2
78	10	8	12	2	2
79	10	8	12	2	2
80	10	8	10	0	2
81	10	8	10	0	2
82	10	8	11	1	2
83	10	8	10	0	2
84	10	8	11	1	2
85	11	8	12	1	3
86	11	0	11	0	11
87	11	8	11	0	3
88	11	8	11	0	3
89	11	8	11	0	3

Table 135. Key flight days for each STS-120 procedure update (Part 2 of 4).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
90	12	8	12	0	4
91	12	8	12	0	4
92	11	8	11	0	3
93	11	8	11	0	3
94	11	8	12	1	3
95	11	10	12	1	1
96	11	10	12	1	1
97	11	10	11	0	1
98	11	10	12	1	1
99	11	10	12	1	1
100	11	10	12	1	1
101	11	10	12	1	1
102	11	10	12	1	1
103	11	10	12	1	1
104	11	10	12	1	1
105	12	10	12	0	2
106	12	11	12	0	1
107	12	10	12	0	2
108	12	8	12	0	4
109	12	8	12	0	4
110	12	8	12	0	4
111	12	8	12	0	4
112	12	8	12	0	4
113	13	11	13	0	2
114	13	0	13	0	13
115	13	8	13	0	5
116	13	8	13	0	5
117	13	8	13	0	5
118	13	8	13	0	5
119	13	3	14	1	10
120	13	8	14	1	5
121	14	0	14	0	14
122	14	8	14	0	6
123	14	0	14	0	14
124	15	14	15	0	1
125	15	14	16	1	1
126	15	0	16	1	15
127	15	12	16	1	3
128	15	12	16	1	3
129	15	0	16	1	15
130	15	0	16	1	15
131	15	0	16	1	15
132	15	0	16	1	15

Table 136. Key flight days for each STS-120 procedure update (Part 3 of 4).

Procedure Update	FD	FD When Issue Identifiable	FD When Update was to be Executed	Number of FD between issue of update and anticipated execution	Number of FD between When issue Was Identifiable and When it was updated
133	15	8	16	1	7
134	15	8	16	1	7
135	15	15	15	0	0

*Likely being reworked or already finished at launch

Table 137. Key flight days for each STS-120 procedure update (Part 4 of 4).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
1	Mistakenly Omitted from timeline for MS5 (Typo)	N/A	Typos and Omissions
2	Failed Flowmeter (Failure occurred on STS-116)	N/A	Sensor "Failure" or Bias
3	Improving IDC coverage of panels 9R, 13R, 9L, and 12L	N/A	Launch Damage (actual or suspected)
4	Improving IDC coverage of panels 9R, 13R, 9L, and 12L	N/A	Launch Damage (actual or suspected)
5	New procedure developed in response to glove damage on STS-118. This procedure was not completed in time to make it into the ISS EVA Systems C/L before the print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
6	Logistical Changes	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
7	Logistical Changes	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)

Table 138. STS-120 update rationales (Part 1 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
8	Logistical Changes	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
9	Details of this procedure were not finalized until after print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
10	PGSC Power cable failure	N/A	Actuator "Failure" or Degradation
11	Tasks simplified by ISS crew item prepositioning	N/A	Procedure Efficiency Optimization
12	Serial numbers called down by crew and recorded on the cue card. Also, there was a typo	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
13	Bad TCS data cable or improper assignment of the COM Port within the Windows operating system.	N/A	Unexpected Software Behavior
14	Details of this procedure were not finalized until after print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
15	The lab window shutter being closed throughout the mission eliminated the need for several steps	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
16	Messages Omitted	N/A	Typos and Omissions
17	PGSC Network problems	N/A	Unexpected Software Behavior
18	Overexposed images from DCS760 cameras (Note: this may not be a procedure update as much as a compliance verification)	N/A	Sensor "Failure" or Bias
19	Confusion over whether to leave a tool on ISS or bring it back	N/A	Equipment List Revision

Table 139. STS-120 update rationales (Part 2 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
20	Added tools for SARJ inspection	SARJ Grinding Problems	Equipment List Revision
21	Added tools for SARJ inspection	SARJ Grinding Problems	Equipment List Revision
22	Added steps to inspect the APFR (it was thought that the glove damage on STS-118 and EVA 1 may be due to poor performance by the APFR)	N/A	Proactive Contingency Preparation and/or Hazard Investigation
23	Changed due to addition of SARJ Inspection	SARJ Grinding Problems	Task Deferral or Reprioritization
24	Removed inhibits and step 1 due to task reordering to accommodate the addition of SARJ Inspection	SARJ Grinding Problems	Task Deferral or Reprioritization
25	Details of this procedure were not finalized until after print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
26	This new procedure is in response to the ISS attitude control problems encountered on STS-117. It probably did not make its way into the procedure books before the print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
27	PGSC Network Problems	N/A	Unexpected Software Behavior
28	IMS update	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
29	PGSC Network Problems	N/A	Unexpected Software Behavior
30	Step reprioritized and reordered due to addition of SARJ Inspection	SARJ Grinding Problems	Task Deferral or Reprioritization
31	CETA Rail damage from MMOD believed to be related to EMU glove damage on STS-118 and EVA 1	N/A	Proactive Contingency Preparation and/or Hazard Investigation
32	SARJ vibrations	SARJ Grinding Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
33	Removal of hardware added in MSG 40 from the EVA	SARJ Grinding Problems	Equipment List Revision
34	Removal of hardware added in MSG 40 from the EVA	SARJ Grinding Problems	Equipment List Revision

Table 140. STS-120 update rationales (Part 3 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
35	Typo	N/A	Typos and Omissions
36	New translation path necessitated a new inhibit.	SARJ Grinding Problems	Unaccounted for Inhibits
37	Unexpected SRMS shoulder temps.	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
38	Intermittent data from FCMS application	N/A	Unexpected Software Behavior
39	Changed REBA Battery serial numbers	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
40	Changed REBA Battery serial numbers	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
41	Changed REBA Battery serial numbers	N/A	Inconsistency between Item's Expected Post-Launch Configuration and Actual Post-Launch Configuration (e.g., packaging error, manufacturing error, etc.)
42	New LiOH canister to accommodate a longer EVA 3 (due to the tasks that were moved from EVA 2)	SARJ Grinding Problems	Consumable Management Replanning
43	Unexpected SRMS shoulder temps.	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
44	Unreleased bolt	N/A	Actuator "Failure" or Degradation
45	Removal/Reconfiguration of equipment added/reconfigured for EVA 2 SARJ Inspection	SARJ Grinding Problems	Equipment List Revision
46	Removal/Reconfiguration of equipment added/reconfigured for EVA 2 SARJ Inspection	SARJ Grinding Problems	Equipment List Revision

Table 141. STS-120 update rationales (Part 4 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
47	Equipment stowage plan change (due to the addition of the SARJ inspection)	SARJ Grinding Problems	Equipment List Revision
48	New number of turns on P6 strap (either due to a typo or reanalysis)	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch
49	Logistical changes (due to reordering of tasks for the SARJ inspection)	SARJ Grinding Problems	Task Deferral or Reprioritization
50	This procedure was put "On Call" and updated to include steps for a possible EV1 O2 recharge due to the addition of the SARJ inspection	SARJ Grinding Problems	Consumable Management Replanning
51	This procedure was updated to include steps for a possible EV2 O2 recharge due to the addition of the SARJ inspection	SARJ Grinding Problems	Consumable Management Replanning
52	Steps removed to prevent hot mics during EVA Prep/Post	N/A	Crew Comfort Optimizations
53	Steps removed to prevent hot mics during EVA Prep/Post	N/A	Crew Comfort Optimizations
54	Added to due debris found during STBD SARJ inspection	SARJ Grinding Problems	Proactive Contingency Preparation and/or Hazard Investigation
55	STS6 monitor problems	N/A	Actuator "Failure" or Degradation
56	Failed primary hardline intercom	N/A	Actuator "Failure" or Degradation
57	Step delayed due to regeneration of micropurification unit	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
58	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	SARJ Grinding Problems	Proactive Contingency Preparation and/or Hazard Investigation
59	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	SARJ Grinding Problems	Proactive Contingency Preparation and/or Hazard Investigation
60	Contingency version of the procedure added in the event that the MBSU Transfer task is deferred from EVA 3	SARJ Grinding Problems	Proactive Contingency Preparation and/or Hazard Investigation

Table 142. STS-120 update rationales (Part 5 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
61	IMU 1 problems and inability to use star tracker data due to attitude and sun angle	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
62	Logistical changes	SARJ Grinding Problems	Equipment List Revision
63	Anomalous data on the sublimator of a suit prompted the MCC to look into EMU resizing and they found a few mistakes in the resize matrix	N/A	Actuator "Failure" or Degradation
64	Equipment Buildup for SARJ Troubleshooting	SARJ Grinding Problems	Equipment List Revision
65	Small tears in EMU gloves	N/A	Actuator "Failure" or Degradation
66	Added for SARJ Inspection	SARJ Grinding Problems	Proactive Contingency Preparation and/or Hazard Investigation
67	Added to alleviate blistering of EVI's hand	N/A	Crew Comfort Optimizations
68	The decision to use older LiOH canisters necessitated new steps to prevent dust from being spread throughout the cabin	N/A	Crew Comfort Optimizations
69	EMU battery change to accommodate a longer EVA	P6 SAW Redeploy Problems	Consumable Management Replanning
70	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Unaccounted for Inhibits
71	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Unaccounted for Inhibits
72	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Equipment List Revision
73	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Equipment List Revision
74	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
75	SSRMS/OBSS MNVR due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Equipment List Revision
76	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
77	SSRMS/OBSS MNVR due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Equipment List Revision

Table 143. STS-120 update rationales (Part 6 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
78	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
79	Changes due to addition of SAW repair activity to EVA	P6 SAW Redeploy Problems	Equipment List Revision
80	Added to prevent contact of metal glove components with the solar arrays (electrocution hazard)	P6 SAW Redeploy Problems	Unaccounted for Inhibits
81	Added to construct stabilizers for the damaged SAW	P6 SAW Redeploy Problems	Equipment List Revision
82	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
83	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
84	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
85	Logistical changes due to SAW repair EVA	P6 SAW Redeploy Problems	Consumable Management Replanning
86	Camera resetting issues	N/A	Unexpected Software Behavior
87	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
88	Added to reduce electrocution hazard for SAW repair EVA	P6 SAW Redeploy Problems	Unaccounted for Inhibits
89	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
90	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
91	Procedure added in order to use OBSS for SAW repair activity	P6 SAW Redeploy Problems	Equipment List Revision
92	This procedure allowed the crew to view a DOUG movie of the trajectory to the SAW repair site	P6 SAW Redeploy Problems	Equipment List Revision
93	Added to reduce electrocution hazard for SAW repair EVA	P6 SAW Redeploy Problems	Unaccounted for Inhibits
94	Changes to the EVA 4 procedure due to need to safety tether to OBSS	P6 SAW Redeploy Problems	Unaccounted for Inhibits
95	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Unaccounted for Inhibits
96	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Unaccounted for Inhibits
97	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
98	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision

Table 144. STS-120 update rationales (Part 7 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
99	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
100	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
101	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
102	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
103	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
104	Refinement of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
105	Equipment omissions in the previously transmitted version of this SAW repair procedure	P6 SAW Redeploy Problems	Equipment List Revision
106	Typos in the previously transmitted version of this SAW repair procedure	P6 SAW Redeploy Problems	Typos and Omissions
107	Missing EVA overglove doffing steps in the previously transmitted version of this SAW repair procedure	P6 SAW Redeploy Problems	Typos and Omissions
108	To return the EMU used for EVA 4 back to its original size for use on a stage EVA (as per message 62, this EMU was resized due so that EV1 could use it as a replacement for his EMU, which had sublimator problems)	N/A	Actuator "Failure" or Degradation
109	OBSS movements added for SAW repair EVA	P6 SAW Redeploy Problems	Equipment List Revision
110	OBSS movements added for SAW repair EVA	P6 SAW Redeploy Problems	Equipment List Revision
111	OBSS movements added for SAW repair EVA	P6 SAW Redeploy Problems	Equipment List Revision
112	Logistical changes	P6 SAW Redeploy Problems	Consumable Management Replanning
113	Broken AVIU switch	N/A	Actuator "Failure" or Degradation
114	This procedure is in response to the ISS attitude control problems encountered on STS-117. It probably did not make its way into the procedure books before the print deadline	N/A	Procedure Updated or Re-evaluated after the Print Deadline for the Procedure Books and before Launch

Table 145. STS-120 update rationales (Part 8 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
115	Different EVA batteries	P6 SAW Redeploy Problems	Consumable Management Replanning
116	Different EVA batteries	P6 SAW Redeploy Problems	Consumable Management Replanning
117	Battery information updated to reflect EVA 4	P6 SAW Redeploy Problems	Consumable Management Replanning
118	Added to ensure that OBSS still worked after EVA 4	P6 SAW Redeploy Problems	Proactive Contingency Preparation and/or Hazard Investigation
119	Additional photos requested due to a degradation of TCS Reflector #1 noticed on FD 3	N/A	Sensor "Failure" or Bias
120	Optimization of post-separation trajectory due to extra days at station	P6 SAW Redeploy Problems	Procedure Efficiency Optimization
121	Possibly due to warmer attitudes than expected	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)
122	Added due to FD13 Sensor Checkout	P6 SAW Redeploy Problems	Proactive Contingency Preparation and/or Hazard Investigation
123	Comments added to reflect delays in the procedure	N/A	Typos and Omissions
124	Added to give crew the optional capability to increase air circulation	N/A	Crew Comfort Optimizations
125	Modified to give crew the optional capability to increase air circulation	N/A	Crew Comfort Optimizations
126	Typo	N/A	Typos and Omissions
127	Mid Port Payload Bay Floodlight Failure on FD12	N/A	Actuator "Failure" or Degradation
128	Mid Port Payload Bay Floodlight Failure on FD12	N/A	Actuator "Failure" or Degradation
129	PCS 1 configuration changes	N/A	Procedure Nominally Updated in Real-time
130	Flash Evaporator Configuration	N/A	Procedure Nominally Updated in Real-time
131	Ammonia Boiler Configuration	N/A	Procedure Nominally Updated in Real-time
132	Ammonia Boiler Configuration	N/A	Procedure Nominally Updated in Real-time

Table 146. STS-120 update rationales (Part 9 of 10).

Procedure Update	Rationale	Discrete Event Rationale Categorization	Rationale Categorization
133	Updated due to extra days in orbit and change from ascending to descending landing opportunities	P6 SAW Redeploy Problems	Consumable Management Replanning
134	Updated due to extra days in orbit and change from ascending to descending landing opportunities	P6 SAW Redeploy Problems	Consumable Management Replanning
135	Revised flight plan due to landing waveoffs	N/A	Unanticipated Environmental/ISS Conditions (e.g., temperatures)

Table 147. STS-120 update rationales (Part 10 of 10).

DATA POINT	MISSION ELAPSED TIME (MINUTES)	NUMBER OF PROCEDURES NEEDING AND BEING REWORKED
Launch	0	26
End of FD 1	360	32
End of FD 2	1800	26
End of FD 3	3240	21
Instant before SARJ Grinding Anomaly	4320	19
Instant after SARJ Grinding Anomaly	4321	40
End of FD 4	4680	40
End of FD 5	6090	31
End of FD 6	7500	28
End of FD 7	8940	19
Instant before SAW Redeploy Anomaly	10095	18
Instant after SAW Redeploy Anomaly	10096	55
End of FD 8	10380	55
End of FD 9	11790	49
End of FD 10	13290	44
End of FD 11	14760	28
End of FD 12	16230	20
End of FD 13	17730	12
End of FD 14	19200	11
End of FD 15	20640	0

Table 148. The STS-120 data time history for the variable *Number of Procedures Needing and Being Reworked*.

TYPES OF PROCEDURE UPDATES	PROCEDURE UPDATE NUMBERS
Due to SARJ Grinding Anomaly and in Time Horizon	20, 21, 23, 24, 30, 32, and 36
Due to SARJ Grinding Anomaly and Beyond Time Horizon (i.e., propagated reworks due to the SARJ Grinding Anomaly)	42, 45, 46, 47, 49, 50, 51, 54, 58, 59, 60, 62, 64, and 66
Due to refinements of previously submitted SARJ Grinding Anomaly related updates	33 and 34
Due to SAW Redeploy Anomaly and in Time Horizon	None
Due to SAW Redeploy Anomaly and Beyond Time Horizon (i.e., propagated reworks due to the SAW Redeploy Anomaly)	69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 87, 88, 89, 90, 91, 92, 93, 94, 109, 110, 111, 112, 115, 116, 117, 118, 120, 122, 133, and 134
Due to refinements of previously submitted SAW Redeploy Anomaly related updates	95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, and 107
Outside Time Horizon and Not Latent at Launch (i.e., propagated reworks not due to a discrete event)	10, 13, 17, 27, 29, 108, 113, 119, 127, and 128
Procedures developed as a result of the rework process	13, 17, 25, 27, 28, 29, 31, 32, 37, 43, 44, 54, 55, 56, 61, 64, 65, 66, 67, 69, 74, 75, 76, 77, 78, 80, 81, 82, 83, 84, 86, 87, 88, 89, 90, 91, 92, 93, 94, 108, 109, 110, 111, 113, 118, 119, 122, and 124

Table 149. List of specially designated STS-120 procedure updates.

FLIGHT DAY	MISSION ELAPSED TIME AT END OF FLIGHT DAY (MINUTES)	NORMALIZED TIME TO LANDING PREPARATION AT THE END OF FD 15	UPDATES SINCE PREVIOUS FLIGHT DAY
0	0	0	0
1	360	0.0174	1
2	1800	0.08721	7
3	3240	0.1570	6
4	4680	0.2267	4
5	6090	0.2951	19
6	7500	0.3634	6
7	8940	0.4331	12
8	10380	0.5029	5
9	11790	0.5712	7
10	13290	0.6439	17
11	14760	0.7151	18
12	16230	0.7863	10
13	17730	0.8590	8
14	19200	0.9302	3
15	20640	1	12

Table 150. STS-120 update times normalized to the landing preparation time.

Tables of Data from All Flights Studied

REFERENCE MISSION ELAPSED TIME IN DAYS	NORMALIZED UPDATE TIME	NORMALIZED UPDATE TIMES (UPDATES SINCE LAST UPDATE TIME)					TOTAL UPDATES SINCE LAST UPDATE TIME (AVERAGE)
		STS-97	STS-115	STS-116	STS-117	STS-120	
0	0	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
0.361*	0.031	0.021 (1)	0.025 (0)	0.021 (0)	0.021 (0)	0.017 (1)	2 (0.4)
2	0.170	0.112 (17)	0.120 (3)	0.102 (6)	0.102 (3)	0.087 (7)	42 (8.4)
						0.157 (6)	
3	0.255	0.210 (13)	0.219 (13)	0.186 (14)	0.185 (5)	0.227 (4)	49 (9.8)
4	0.340	0.309 (7)	0.318 (5)	0.267 (3)	0.267 (2)	0.295 (19)	36 (7.2)
5	0.426	0.407 (7)	0.417 (0)	0.349 (2)	0.35 (4)	0.363 (6)	19 (3.8)
6	0.511	0.504 (5)	N/A	0.430 (4)	0.431 (3)	0.433 (12)	29 (5.8)
						0.503 (5)	
7	0.596	N/A	0.516 (4)	0.513 (2)	0.514 (12)	0.571 (7)	33 (6.6)
				0.594 (3)	0.595 (5)		
8	0.681	0.602 (13)	0.614 (10)	0.676 (19)	0.676 (14)	0.644 (17)	73 (14.6)
9	0.766	0.701 (6)	0.713 (4)	0.7573 (3)	0.757 (1)	0.715 (18)	32 (6.4)
10	0.851	0.801 (7)	0.808 (4)	0.837 (5)	0.838 (2)	0.786 (10)	28 (5.6)
11	0.936	0.900 (4)	0.903 (7)	0.917 (1)	0.919 (3)	0.859 (8)	26 (5.2)
						0.930 (3)	
11.75	1	1 (13)	1 (9)	1 (24)	1 (12)	1 (12)	70 (14)
13	1.106	1.08 (0)	1.10 (4)	N/A	N/A	N/A	4 (0.8)

*End of Startup Delay

Table 151. Update times and rates for all flights normalized to a set of reference update times.

Appendix 3: System Dynamics Model Documentation

This appendix contains the necessary documentation for replication of the simulation results in this dissertation. All of the simulation models used to construct original graphs in this dissertation that were not explicitly described in the dissertation chapters are documented below—with the exception of the Kampmann and Shantzis/Behrens models, which are documented in Kampmann (1991). The syntax in which the documentation is provided is the syntax for model construction in the Vensim[®] software package.

Basic Procedure Rework Model

The Basic Procedure Rework Model is used in this dissertation to investigate the core dynamics of the Procedure Rework Process. The primary numerical integration technique used for analysis of the model and graph development was Euler integration with a fixed time step size. The simulation start time was 0 minutes (coinciding with SRB ignition) and the end time was 18600 minutes.

Conversion Factors & Time Step:

Day to Minute Conversion Factor = 60×24
Units: Minutes/Day

Time Step = 0.25
Units: Minutes

Main Procedure Flow Structure:

Activation Rate for PNR = IF THEN ELSE(Total Inactive Procedures > 0.1, "Inactive Procedures Needing Rework (IPNR)"/Total Inactive Procedures * Total Initial Inactive Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Procedures Needing Rework (IPNR)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

Activation Rate for VP = IF THEN ELSE(Total Inactive Procedures > 0.1, ("Inactive Valid Procedures (IVP)"/Total Inactive Procedures) * Total Initial Inactive Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Valid Procedures (IVP)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

Active Procedure Invalidation Rate During Discrete Event = 0
Units: Procedures/Minute [0, 500, 1]

"Active Procedures Needing Rework (APNR)" = INTEG(Activation Rate for PNR + Procedure Invalidation Rate - Procedure Rework Discovery Rate, Initial Number of Procedures Needing Rework)

Units: Procedures

"Active Valid Procedures (AVP)" = INTEG(Activation Rate for VP + Procedure Rework Completion Rate - Procedure Completion Rate - Procedure Invalidation Rate, Initial Number of Valid Procedures)

Units: Procedures

Baseline Flight Controller Rework Recognition Delay = 30

Units: Minute [1, 500, 5]

Baseline Procedure Invalidation Rate = 0.00069

Units: Procedures/Minute [0, 0.01]

Based on analysis of STS-97, STS-115, STS-116, STS-117, and STS-120

Baseline Time to Complete Procedure Rework = 200

Units: Minute [0, 1000, 5]

"Completed Procedures (CP)" = INTEG (Procedure Completion Rate, Initial Completed Procedures)

Units: Procedures

Daily Procedure Rework Completion Rate = Procedure Rework Completion Rate * Day to Minute Conversion Factor

Units: Procedures/Day

Discrete Procedure Invalidation Rate = Active Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)

Units: Procedures/Minute

Inactive Procedure Invalidation Rate = IF THEN ELSE(Rework Propagation Factor >= 0, MIN("Inactive Valid Procedures (IVP)"/Time to Complete Procedure Rework, ("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)), MAX(("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1), -"Inactive Procedures Needing Rework (IPNR)"/Time to Complete Procedure Rework))

Units: Procedures/Minute

Inactive Procedure Invalidation Rate During Discrete Event = 0

Units: Procedures/Minute [0, 500, 1]

"Inactive Procedures Needing Rework (IPNR)" = INTEG(Inactive Procedure Invalidation Rate - Activation Rate for PNR, Initial Inactive Procedures Needing Rework)

Units: Procedures

"Inactive Valid Procedures (IVP)" = INTEG(-Activation Rate for VP - Inactive Procedure Invalidation Rate, Initial Inactive Valid Procedures)

Units: Procedures

Initial Completed Procedures = 0

Units: Procedures

Initial Inactive Procedures Needing Rework = 0

Units: Procedures [0, 2000]

This initial value is 24.6 for the latent issues scenario

Initial Inactive Valid Procedures = 2500

Units: Procedures

Initial Number of Procedures Being Reworked = 0

Units: Procedures [0, 100]

This initial value is 6.6 for the latent issues scenario

Initial Number of Procedures Needing Rework = 0

Units: Procedures [0, 8]

Initial Number of Valid Procedures = 100

Units: Procedures

Mission Duration = "Mission Duration (in days)" * Day to Minute Conversion Factor

Units: Minute

"Mission Duration (in days)" = 12.9

Units: Day [0, 500]

Procedure Completion Fraction for Mission = 0

Units: Dmnl [0, 1]

Procedure Completion Rate = MIN((Total Number of Procedures*Procedure Completion Fraction for Mission)/Mission Duration, "Active Valid Procedures (AVP)"/Procedure Completion Time)

Units: Procedures/Minute

The Fuzzy Min (Sterman 2000) structure prevents the number of Active Valid Procedures from going negative.

Procedure Completion Time = 10

Units: Minute

Procedure Invalidation Rate = MIN(Baseline Procedure Invalidation Rate + Discrete Procedure Invalidation Rate, "Active Valid Procedures (AVP)"/Procedure Completion Time)

Units: Procedures/Minute

The Fuzzy Min (Sterman 2000) structure prevents the number of Active Valid Procedures from going negative.

Procedure Rework Accumulation = Procedure Rework Completion Rate

Units: Procedures/Minute

Procedure Rework Completion Rate = IF THEN ELSE(Time > Startup Delay, "Procedures Being Reworked (PBR)"/Time to Complete Procedure Rework, 0)

Units: Procedures/Minute

Procedure Rework Discovery Rate = "Active Procedures Needing Rework (APNR)"/Time to Discover Procedure Rework

Units: Procedures/Minute

Procedure Rework Time Horizon = 2000

Units: Minute [0, 5000]

"Procedures Being Reworked (PBR)"= INTEG(Procedure Rework Discovery Rate-Procedure Rework Completion Rate, Initial Number of Procedures Being Reworked)

Units: Procedures

Procedures Needing and Being Reworked = "Procedures Being Reworked (PBR)" + "Procedures Needing Rework (PNR)"

Units: Procedures

"Procedures Needing Rework (PNR)" = "Active Procedures Needing Rework (APNR)" + "Inactive Procedures Needing Rework (IPNR)"

Units: Procedures

Rework Propagation Factor = 0.605

Units: Dmnl [0, 5]

The fraction of inactive procedures that are invalidated when procedures are reworked worked out to be roughly 51% of the total reworked procedures (not including discrete events or latent updates at launch). The baseline number used here leads to an end state in which roughly 51% of the total reworked procedures were due to rework propagation. This factor is changes to 0.185 in the latent updates at launch scenario.

Startup Delay = 520

Units: Minute [0, 1000, 5]

Time in Days = Time/Day to Minute Conversion Factor
Units: Days

Time of Discrete Event = 100
Units: Minute [0, 10000, 5]
This value must be a multiple of the time step or else the discrete event will not occur.

Time to Complete Procedure Rework = Baseline Time to Complete Procedure Rework + Baseline Time to Complete Procedure Rework * Rework Completion Time Attention Shifting Factor * (1 - "Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)")
Units: Minute

Time to Discover Procedure Rework = Baseline Flight Controller Rework Recognition Delay + Rework Recognition Delay Attention Shifting Factor * Baseline Flight Controller Rework Recognition Delay * (1 - "Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)")
Units: Minute

Total Inactive Procedures = "Inactive Valid Procedures (IVP)" + "Inactive Procedures Needing Rework (IPNR)"
Units: Procedures

Total Initial Inactive Procedures = Initial Inactive Procedures Needing Rework + Initial Inactive Valid Procedures
Units: Procedures

Total Number of Procedures = Initial Number of Valid Procedures + Initial Number of Procedures Needing Rework + Initial Number of Procedures Being Reworked + Total Initial Inactive Procedures
Units: Procedures

Total Procedures Reworked = INTEG (Procedure Rework Accumulation, 0)
Units: Procedures

"Valid Procedures (VP)" = "Inactive Valid Procedures (IVP)" + "Active Valid Procedures (AVP)" + "Completed Procedures (CP)"
Units: Procedures

Flight Controller Attention Shifting Structure:

"Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)" = INTEG(Shift in Focus to Rework, Initial Fraction of Flight Controller Resources Devoted to Procedure Rework)
Units: Dmnl

"Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)" =
INTEG(-Shift in Focus to Rework, Initial Fraction of Flight Controller Resources
Devoted to Rework Discovery)

Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Procedure Rework = 1 - Initial
Fraction of Flight Controller Resources Devoted to Rework Discovery

Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Rework Discovery = 1

Units: Dmnl [0, 1]

Resource Fraction per Procedure Reworked = 0.2

Units: Dmnl/Procedure [0, 1]

Rework Completion Time Attention Shifting Factor = 1

Units: Dmnl [0.1, 5, 5]

Rework Recognition Delay Attention Shifting Factor = 1

Units: Dmnl [0.1, 5, 5]

Shift in Focus to Rework = (Target Flight Controller Resources Applied towards
Procedure Rework - "Fraction of Flight Controller Resources Devoted to Procedure
Rework (FRDPR)"/Time to Shift Focus

Units: Dmnl/Minute

Target Flight Controller Resources Applied towards Procedure Rework = MIN(1,
"Procedures Being Reworked (PBR)" * Resource Fraction per Procedure Reworked)

Units: Dmnl

Time to Shift Focus = 1

Units: Minute [1, 5]

Light Delay Model

The light delay model is used in this dissertation to simulate the light delay over time on a mission to Mars. In this model, a minimum energy transfer or *Hohmann Transfer* (Bate et al. 1971, pp. 163-166) is assumed from a circular Earth Solar Orbit to Mars Perihelion. Once the spacecraft arrives at Mars Perihelion, a maneuver is performed to insert the spacecraft into Mars' elliptical orbit about the Sun. The primary numerical integration technique used for analysis of the model and graph development was second order Runge-Kutta integration with an automatically adjusted step size. The simulation start time is 0 days (coinciding with the insertion maneuver into the Hohmann Transfer orbit).

Conversion Factors & Time Step:

Seconds to Days Conversion Factor = $1/(60 * 60 * 24)$
Units: Days/second

Time Step = 0.007812
Units: Days

Earth Solar Orbit Dynamics:

Change of X earth = \dot{X} earth
Units: Kilometer/Day

Change of Y earth = \dot{Y} earth
Units: Kilometer/Day

Change of \dot{X} earth = "Gravitational Parameter of Sun (adjusted for time step units)" *
X distance between Earth and Sun/Distance between Earth and Sun³
Units: Kilometer/(Day * Day)
Assumes negligible affect of gravity between Earth and Mars. Formula derived in
Howell (2002) and Bate et al. (1971, pp. 3-14).

Change of \dot{Y} earth = "Gravitational Parameter of Sun (adjusted for time step units)" *
Y distance between Earth and Sun/Distance between Earth and Sun³
Units: Kilometer/(Day * Day)
Assumes negligible effect of gravity between Earth and Mars. Formula derived in
Howell (2002) and Bate et al. (1971, pp. 3-14).

Distance between Earth and Sun = $\text{SQRT}(X \text{ earth}^2 + Y \text{ earth}^2)$
Units: kilometers
Assumes no movement of Sun and that the XY plane coincides with the orbital
plane

"Earths Orbital Velocity (if circular orbit)" = $\text{SQRT}(\text{"Gravitational Parameter of Sun (adjusted for time step units)"} / \text{"Earths Semi-Major Orbital Axis"})$
Units: Kilometer/Day

"Earths Semi-Major Orbital Axis" = 1.49598e+008
Units: kilometers

Gravitational Parameter of Sun = 1.32712e+011
Units: Kilometer * Kilometer * Kilometer/(seconds * seconds)
From Bate et al. (1971, pp. 429).

"Gravitational Parameter of Sun (adjusted for time step units)" = Gravitational Parameter of Sun * (1/Seconds to Days Conversion Factor)^2
Units: Kilometer * Kilometer * Kilometer/(Day * Day)

Initial X earth = 0
Units: kilometers

Initial Xdot earth = "Earths Orbital Velocity (if circular orbit)"
Units: kilometers/Day

Initial Y earth = -"Earths Semi-Major Orbital Axis"
Units: kilometers

Initial Ydot earth = 0
Units: kilometers/Day

X distance between Earth and Sun = -X earth
Units: kilometers
Assumes no movement of the Sun

X earth = INTEG (Change of X earth, Initial X earth)
Units: kilometers

Xdot earth = INTEG (Change of Xdot earth, Initial Xdot earth)
Units: kilometers/Day

Y distance between Earth and Sun = -Y earth
Units: kilometers
Assumes no movement of the Sun

Y earth = INTEG (Change of Y earth, Initial Y earth)
Units: kilometers

Ydot earth = INTEG (Change of Ydot earth, Initial Ydot earth)
Units: kilometers/Day
Assumes negligible effect of gravity between Earth and Mars

Spacecraft Solar Orbit Dynamics:

Acceleration from Insertion Maneuver = IF THEN ELSE(Distance between Spacecraft and Sun >= Maneuver Initiation Distance, Delta V Available for Mars Solar Orbit Insertion/Time for Maneuver, 0)
Units: Kilometer/(Day * Day)

Aphelion Velocity of Transfer Orbit = $\text{SQRT}(2 * \text{"Gravitational Parameter of Sun (adjusted for time step units)" * (1/\text{Mars Perihelion} - 1/(2 * \text{"Semi-Major Axis of Transfer Orbit"})$))

Units: Kilometer/Day

Change of X spacecraft = Xdot spacecraft

Units: Kilometer/Day

Change of Xdot spacecraft = "Gravitational Parameter of Sun (adjusted for time step units)" * X distance between Spacecraft and Sun/Distance between Spacecraft and Sun³

Units: Kilometer/(Day * Day)

Assumes negligible effect of gravity between Earth and Mars. Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Change of Y spacecraft = Ydot spacecraft

Units: Kilometer/Day

Change of Ydot spacecraft = "Gravitational Parameter of Sun (adjusted for time step units)" * Y distance between Spacecraft and Sun/Distance between Spacecraft and Sun³

Units: Kilometer/(Day * Day)

Assumes negligible effect of gravity between Earth and Mars. Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Delta V Available for Mars Solar Orbit Insertion = INTEG (-Acceleration from Insertion Maneuver, Initial Delta V Available for Mars Solar Orbit Insertion)

Units: Kilometer/Day

Delta V for Mars Solar Orbit Insertion = Perihelion Velocity of Mars-Aphelion Velocity of Transfer Orbit

Units: Kilometer/Day

Distance between Earth and Spacecraft = $\text{SQRT}((X \text{ earth} - X \text{ spacecraft})^2 + (Y \text{ earth} - Y \text{ spacecraft})^2)$

Units: kilometers

Distance between Spacecraft and Sun = $\text{SQRT}(X \text{ spacecraft}^2 + Y \text{ spacecraft}^2)$

Units: kilometers

Initial Delta V Available for Mars Solar Orbit Insertion = -Delta V for Mars Solar Orbit Insertion

Units: Kilometer/Day

This value is negative because the maneuver will occur when the spacecraft is moving in the negative X direction.

Initial X spacecraft = Initial X earth

Units: kilometers

Initial Xdot spacecraft = Perihelion Velocity of Transfer Orbit
Units: kilometers/Day

Initial Y spacecraft = Initial Y earth
Units: kilometers

Initial Ydot spacecraft = 0
Units: kilometers/Day

Maneuver Distance Margin = 0
Units: Kilometer
When using integration techniques other than second order Runge-Kutta integration with automatically adjusted step size, it may be necessary to set this parameter to a value greater than zero to ensure that the insertion maneuver at Mars Perihelion occurs.

Maneuver Initiation Distance = Mars Perihelion - Maneuver Distance Margin
Units: Kilometer

Mars Perihelion = 2.06645e+008
Units: Kilometer
Source: <http://www.marspedia.org/>

"Mars Semi-Major Orbital Axis" = 2.27941e+008
Units: kilometers
From Howell (2002).

Perihelion Velocity of Mars = $\text{SQRT}(2 * \text{"Gravitational Parameter of Sun (adjusted for time step units)" * (1/Mars Perihelion}-1/(2 * \text{"Mars Semi-Major Orbital Axis"}))$
Units: Kilometer/Day

Perihelion Velocity of Transfer Orbit = $\text{SQRT}(2 * \text{"Gravitational Parameter of Sun (adjusted for time step units)" * (1/"Earths Semi-Major Orbital Axis"}-1/(2 * \text{"Semi-Major Axis of Transfer Orbit"}))$
Units: kilometers/Day
Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-16).

"Semi-Major Axis of Transfer Orbit" = ($\text{"Earths Semi-Major Orbital Axis" + Mars Perihelion}$)/2
Units: kilometers

Spacecraft Velocity = $\text{SQRT}(\text{Xdot spacecraft}^2 + \text{Ydot spacecraft}^2)$
Units: Kilometer/Day

Time for Maneuver = 0.008

Units: Day

This number is roughly on the order of an eleven minute burn

Time of Flight = $3.14159 * \text{SQRT}(\text{"Semi-Major Axis of Transfer Orbit"}^3 / \text{"Gravitational Parameter of Sun (adjusted for time step units)"})$

Units: Days

Formula from Bate et al. (1971, pp. 165).

X distance between Spacecraft and Sun = -X spacecraft

Units: kilometers

X spacecraft = INTEG (Change of X spacecraft, Initial X spacecraft)

Units: kilometers

Xdot spacecraft = INTEG (Acceleration from Insertion Maneuver + Change of Xdot spacecraft, Initial Xdot spacecraft)

Units: kilometers/Day

Y distance between Spacecraft and Sun = -Y spacecraft

Units: kilometers

Y spacecraft = INTEG (Change of Y spacecraft, Initial Y spacecraft)

Units: kilometers

Ydot spacecraft = INTEG (Change of Ydot spacecraft, Initial Ydot spacecraft)

Units: kilometers/Day

Light Delay Calculation:

Speed of Light = $299792 * 60$

Units: Kilometer/Minute

Source <http://www.speed-light.info/>

Light Delay = Distance between Earth and Spacecraft/Speed of Light

Units: Minute

Flight Specific Procedure Rework Models

The flight specific procedure rework models are used in this dissertation to calibrate the general procedure rework model with flight specific data. The primary numerical integration technique used for analysis of the model and graph development was Euler integration with a fixed time step size. The simulation start time was 0 minutes (coinciding with SRB ignition) and the end time depended on the duration of the mission (16000 minutes, 17000 minutes, 18600 minutes, 20000 minutes, and 22000 minutes for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively).

Conversion Factors & Time Step:

Day to Minute Conversion Factor = 60×24
Units: Minutes/Day

Time Step = 0.25
Units: Minutes

Main Procedure Flow Structure:

Activation Rate for PNR = IF THEN ELSE(Total Inactive Procedures > 0.1, "Inactive Procedures Needing Rework (IPNR)"/Total Inactive Procedures * Total Initial Inactive Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Procedures Needing Rework (IPNR)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

Activation Rate for VP = IF THEN ELSE(Total Inactive Procedures > 0.1, "Inactive Valid Procedures (IVP)"/Total Inactive Procedures * Total Initial Inactive Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Valid Procedures (IVP)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

"Active Procedures Needing Rework (APNR)" = INTEG (Activation Rate for PNR + Procedure Invalidation Rate-Procedure Rework Discovery Rate, Initial Number of Procedures Needing Rework)
Units: Procedures

"Active Valid Procedures (AVP)" = INTEG(Activation Rate for VP + Procedure Rework Completion Rate - Procedure Completion Rate - Procedure Invalidation Rate, Initial Number of Valid Procedures)
Units: Procedures

Baseline Flight Controller Rework Recognition Delay = 30
Units: Minute

The final value of this parameter was derived from the iterative calibration analyses performed with this model.

Baseline Procedure Invalidation Rate = 0.0004014
Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 0.0006411, 0.0007065, 0.0008097, 0.0004014, and 0.001875 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Baseline Time to Complete Procedure Rework = 200

Units: Minute

The final value of this parameter was derived from the iterative calibration analyses performed with this model.

"Completed Procedures (CP)"= INTEG (Procedure Completion Rate, Initial Completed Procedures)

Units: Procedures

This state variable exists primarily for diagramming purposes.

Discrete Procedure Invalidation Rate = IF THEN ELSE(Rework Propagation Factor >= 0, MIN("Inactive Valid Procedures (IVP)"/Time to Complete Procedure Rework, ("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Procedure Invalidation Rate During Discrete Event One * PULSE(Time of Discrete Event One, 1) + Procedure Invalidation Rate During Discrete Event Two * PULSE(Time of Discrete Event Two, 1) + Procedure Invalidation Rate During Discrete Event Three * PULSE(Time of Discrete Event Three, 1), MAX(("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Procedure Invalidation Rate During Discrete Event One * PULSE(Time of Discrete Event One, 1) + Procedure Invalidation Rate During Discrete Event Two * PULSE(Time of Discrete Event Two, 1) + Procedure Invalidation Rate During Discrete Event Three * PULSE(Time of Discrete Event Three, 1), -"Inactive Procedures Needing Rework (IPNR)"/Time to Complete Procedure Rework))

Units: Procedures/Minute

Flight Controller Rework Recognition Delay = Baseline Flight Controller Rework Recognition Delay + Baseline Flight Controller Rework Recognition Delay * Rework Recognition Delay Attention Shifting Factor * (1 - "Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)")

Units: Minute

Inactive Procedure Invalidation Rate = MIN("Inactive Valid Procedures (IVP)"/Minimum Invalidation Time, ("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event One * PULSE(Time of Discrete Event One, 1) + Inactive Procedure Invalidation Rate During Discrete Event Two * PULSE(Time of Discrete Event Two, 1) + Inactive Procedure Invalidation Rate During Discrete Event Three * PULSE(Time of Discrete Event Three, 1))

Units: Procedures/Minute

Inactive Procedure Invalidation Rate During Discrete Event One = 9

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 12, 7, 20, 9, and 14 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Inactive Procedure Invalidation Rate During Discrete Event Two = 17

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 0, 0, 0, 17, and 37 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Inactive Procedure Invalidation Rate During Discrete Event Three = 5

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 0, 0, 0, 5, and 0 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

"Inactive Procedures Needing Rework (IPNR)" = INTEG (Inactive Procedure Invalidation Rate - Activation Rate for PNR, Initial Inactive Procedures Needing Rework)

Units: Procedures

"Inactive Valid Procedures (IVP)" = INTEG (-Activation Rate for VP - Inactive Procedure Invalidation Rate, Initial Inactive Valid Procedures)

Units: Procedures

Initial Completed Procedures = 0

Units: Procedures

Initial Inactive Procedures Needing Rework = 15

Units: Procedures

This initial value was based on flight data and thus differed for each mission. Values of 34, 21, 31, 15, and 20 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Initial Inactive Valid Procedures = 2500

Units: Procedures

Initial Number of Procedures Being Reworked = 1

Units: Procedures

This initial value was based on flight data and thus differed for each mission. Values of 15, 9, 4, 1, and 6 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Initial Number of Procedures Needing Rework = 0

Units: Procedures

Initial Number of Valid Procedures = 100

Units: Procedures

Minimum Invalidation Time = 5

Units: Minute

Mission Duration = "Mission Duration (in days)" * Day to Minute Conversion Factor

Units: Minute

"Mission Duration (in days)" = 13.841

Units: Day

This parameter was based on flight data and thus differed for each mission. Values of 10.8319, 11.7958, 12.8646, 13.841, and 15.0993 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Procedure Completion Fraction for Mission = 0.7

Units: Dmnl [0, 1]

Procedure Completion Rate = MIN((Total Number of Procedures*Procedure Completion Fraction for Mission)/Mission Duration, "Active Valid Procedures (AVP)"/Procedure Completion Time)

Units: Procedures/Minute

The "fuzzy min" structure here (Serman 2000) prevents the state variable "Active Valid Procedures (AVP)" from going negative

Procedure Completion Time = 10

Units: Minute

Procedure Invalidation Rate = MIN(Baseline Procedure Invalidation Rate + Discrete Procedure Invalidation Rate, "Active Valid Procedures (AVP)"/Procedure Completion Time)

Units: Procedures/Minute

The "fuzzy min" structure here (Serman 2000) prevents the state variable "Active Valid Procedures (AVP)" from going negative

Procedure Invalidation Rate During Discrete Event One = 1

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 3, 1, 0, 1, and 7 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Procedure Invalidation Rate During Discrete Event Two = 0

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 0, 0, 0, 0, and 0 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Procedure Invalidation Rate During Discrete Event Three = 2

Units: Procedures/Minute

This parameter was based on flight data and thus differed for each mission. Values of 0, 0, 0, 2, and 0 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Procedure Rework Completion Rate = IF THEN ELSE(Time > Startup Delay, "Procedures Being Reworked (PBR)"/Time to Complete Procedure Rework, 0)

Units: Procedures/Minute

Procedure Rework Discovery Rate = "Active Procedures Needing Rework (APNR)"/Time to Discover Procedure Rework

Units: Procedures/Minute

Procedure Rework Time Horizon = 2000

Units: Minute

The final value of this parameter was derived from the iterative calibration analyses performed with this model.

"Procedures Being Reworked (PBR)" = INTEG(Procedure Rework Discovery Rate-Procedure Rework Completion Rate, Initial Number of Procedures Being Reworked)

Units: Procedures

Procedures Needing and Being Reworked = "Procedures Being Reworked (PBR)" + "Procedures Needing Rework (PNR)"

Units: Procedures

"Procedures Needing Rework (PNR)" = "Active Procedures Needing Rework (APNR)" + "Inactive Procedures Needing Rework (IPNR)"

Units: Procedures

Rework Propagation Factor = 0.125

Units: Dmnl

This parameter was based on flight data (it was selected to reproduce the number of propagated updates not due to discrete events that occurred on these flights) and thus differed for each mission. Values of 0.145, 0.16, 0.177, 0.125, and 0.0735 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Startup Delay = 520

Units: Minute

The final value of this parameter was derived from the iterative calibration analyses performed with this model.

Time of Discrete Event One = 8

Units: Minute

This parameter was based on flight data and thus differed for each mission. Values of 4200, 5640, 5325, 8, and 4320 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Time of Discrete Event Two = 4650

Units: Minute

This parameter was based on flight data and thus differed for each mission. Values of 0 (N/A), 0 (N/A), 0 (N/A), 4650, and 10095 were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Time of Discrete Event Three = 7320

Units: Minute

This parameter was based on flight data and thus differed for each mission. Values of 0 (N/A), 0 (N/A), 0 (N/A), 7320, and 0 (N/A) were used for STS-97, STS-115, STS-116, STS-117, and STS-120, respectively.

Time to Complete Procedure Rework = Baseline Time to Complete Procedure Rework + Baseline Time to Complete Procedure Rework * Rework Completion Time Attention Shifting Factor * (1 - "Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)")

Units: Minute

Time to Discover Procedure Rework = Flight Controller Rework Recognition Delay

Units: Minute

Total Inactive Procedures = "Inactive Valid Procedures (IVP)" + "Inactive Procedures Needing Rework (IPNR)"

Units: Procedures

Total Initial Inactive Procedures = Initial Inactive Procedures Needing Rework + Initial Inactive Valid Procedures

Units: Procedures

Total Number of Procedures = Initial Number of Valid Procedures + Initial Number of Procedures Needing Rework + Initial Number of Procedures Being Reworked + Total Initial Inactive Procedures

Units: Procedures

Total Procedures Reworked = INTEG(Rework Accumulation, 0)

Units: Procedures

"Valid Procedures (VP)" = "Inactive Valid Procedures (IVP)" + "Active Valid Procedures (AVP)" + "Completed Procedures (CP)"

Units: Procedures

Flight Controller Attention Shifting Structure:

"Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)" =
INTEG(Shift in Focus to Rework, Initial Fraction of Flight Controller Resources Devoted
to Procedure Rework)

Units: Dmnl

"Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)" =
INTEG(-Shift in Focus to Rework, Initial Fraction of Flight Controller Resources
Devoted to Rework Discovery)

Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Procedure Rework = 1 - Initial
Fraction of Flight Controller Resources Devoted to Rework Discovery

Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Rework Discovery = 1

Units: Dmnl

Resource Fraction per Procedure Reworked = 0.2

Units: Dmnl/Procedure

The final value of this parameter was derived from the iterative calibration
analyses performed with this model.

Rework Accumulation = Procedure Rework Completion Rate

Units: Procedures/Minute

Rework Completion Time Attention Shifting Factor = 1

Units: Dmnl

The final value of this parameter was derived from the iterative calibration
analyses performed with this model.

Rework Recognition Delay Attention Shifting Factor = 1

Units: Dmnl

The final value of this parameter was derived from the iterative calibration
analyses performed with this model.

Shift in Focus to Rework = (Target Flight Controller Resources Applied towards
Procedure Rework - "Fraction of Flight Controller Resources Devoted to Procedure
Rework (FRDPR)"/Time to Shift Focus

Units: Dmnl/Minute

Target Flight Controller Resources Applied towards Procedure Rework = MIN(1,
"Procedures Being Reworked (PBR)" * Resource Fraction per Procedure Reworked)

Units: Dmnl

Time to Shift Focus = 1
Units: Minute [1,5]

The Flow Controlled Procedure Rework Model

The Flow Controlled Procedure Rework Model is essentially the Basic Procedure Rework Model with several structural modifications for implementing flow control. The primary numerical integration technique used for analysis of the model and graph development was Euler integration with a fixed time step size. The simulation start time was 0 minutes (coinciding with SRB ignition) and the end time was 18600 minutes.

Rather than repeating the common elements of this model and the Basic Procedure Rework Model, only the elements that represent additions or modifications to Basic Procedure Rework Model are provided below.

Additions to the Basic Procedure Rework Model to implement flow control:

Accumulation of Resource Minutes = "Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)"
Units: Dmnl

Baseline Time to Complete Inactive Procedure Rework = 30000
Units: Minute [0, 1000, 5]

"Fraction of Resources Available for Inactive Procedure Rework Discovery (FRAIRD)" = INTEG (-Resource Activation Rate, Initial Fraction of Resources Available for Inactive Procedure Rework)
Units: Dmnl

"Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)" = INTEG (Resource Activation Rate, Initial Fraction of Resources Utilized for Procedure Rework)
Units: Dmnl

Inactive Procedure Rework Completion Rate = IF THEN ELSE(Resource Fraction per Inactive Procedure Needing Rework > 0, "Inactive Procedures Needing Rework (IPNR)"/ Time to Complete Inactive Procedure Rework, 0)
Units: Procedures/Minute

Initial Procedure Rework Horizon = 2000
Units: Minute

Minimum Time to Complete Inactive Procedure Rework = Baseline Time to Complete Inactive Procedure Rework * Rework Time Improvement Factor
Units: Minute [0, 1000, 5]

Procedure Rework Horizon Change Factor = 0
Units: Dmnl [0, 2.5]

Procedure Rework Horizon Change Time = 14000

Units: Minute

Resource Activation Rate = (Target Resources Applied towards Inactive Procedure Rework - "Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)"/ Time to Activate Resources for Rework of Inactive Procedures Needing Rework

Units: Dmnl/Minute

Resource Fraction per Inactive Procedure Needing Rework = 0.5

Units: Dmnl/Procedure [0, 1]

Rework Time Improvement Factor = 0.02

Units: Dmnl [0, 1]

Target Resources Applied towards Inactive Procedure Rework = MIN(1, "Inactive Procedures Needing Rework (IPNR)" * Resource Fraction per Inactive Procedure Needing Rework)

Units: Dmnl

Time to Activate Resources for Rework of Inactive Procedures Needing Rework = 30

Units: Minute [1, 30]

Time to Complete Inactive Procedure Rework = Baseline Time to Complete Inactive Procedure Rework - (Baseline Time to Complete Inactive Procedure Rework - Minimum Time to Complete Inactive Procedure Rework) * "Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)"

Units: Minute

Total Resource Minutes for Inactive Procedure Rework = INTEG(Accumulation of Resource Minutes, 0)

Units: Minute

Modifications to the Basic Procedure Rework Model to implement flow control:

Inactive Procedure Invalidation Rate = IF THEN ELSE(Rework Propagation Factor >= 0, MIN("Inactive Valid Procedures (IVP)"/Time to Complete Procedure Rework, ("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)) + Inactive Procedure Rework Completion Rate * Rework Propagation Factor, MAX(("Procedures Being Reworked (PBR)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1) + Inactive Procedure Rework Completion Rate * Rework Propagation Factor, -"Inactive Procedures Needing Rework (IPNR)"/Time to Complete Procedure Rework))

Units: Procedures/Minute

"Inactive Procedures Needing Rework (IPNR)" = INTEG (Inactive Procedure Invalidation Rate - Activation Rate for PNR - Inactive Procedure Rework Completion Rate, Initial Inactive Procedures Needing Rework)

Units: Procedures

"Inactive Valid Procedures (IVP)" = INTEG (Inactive Procedure Rework Completion Rate-Activation Rate for VP-Inactive Procedure Invalidation Rate, Initial Inactive Valid Procedures)

Units: Procedures

Procedure Rework Time Horizon = Initial Procedure Rework Horizon + STEP(Procedure Rework Horizon Change Factor * Initial Procedure Rework Horizon, Procedure Rework Horizon Change Time)

Units: Minute [0, 5000]

Light Delayed Procedure Rework Model

The Light Delayed Procedure Rework Model is used in this dissertation to investigate the dynamics of the Procedure Rework Process during long duration missions to land on distant celestial bodies. It assumes a Hohmann Transfer to Mars Perihelion and includes a maneuver for insertion into Mars' solar orbit. The primary numerical integration technique used for analysis of the model and graph development was Euler integration with a fixed time step size. The simulation start time was 0 minutes (coinciding with launch) and the end time was 347000 minutes (roughly coinciding with the insertion into Mars' solar orbit).

Conversion Factors & Time Step:

Day to Minute Conversion Factor = 60*24

Units: Minutes/Day

Time Step = 0.25

Units: Minutes

Seconds to Minutes Conversion Factor = 1/60

Units: Minutes/second

Time in Days = Time/Day to Minute Conversion Factor

Units: Days

Main Procedure Flow Structure:

Accumulation of Reworked Procedures = Procedure Rework Completion Rate

Units: Procedures/Minute

Activation Rate for PNR = IF THEN ELSE(Total Inactive Procedures > 0.1, "Inactive Procedures Needing Rework (IPNR)"/Total Inactive Procedures * Total Initial Inactive

Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Procedures Needing Rework (IPNR)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

Activation Rate for VP = IF THEN ELSE(Total Inactive Procedures > 0.1, "Inactive Valid Procedures (IVP)"/Total Inactive Procedures * Total Initial Inactive Procedures/(Mission Duration - Procedure Rework Time Horizon), "Inactive Valid Procedures (IVP)"/Procedure Rework Time Horizon)
Units: Procedures/Minute

"Active Procedures Needing Rework (APNR)" = "Observable Procedures Needing Rework (OPNR)"+"Unobservable Procedures Needing Rework (UPNR)"
Units: Procedures

"Active Valid Procedures (AVP)" = INTEG(Activation Rate for VP + Update Observability Rate - Procedure Completion Rate - Procedure Invalidation Rate, Initial Number of Valid Procedures)
Units: Procedures

Baseline Procedure Invalidation Rate = 0.00069
Units: Procedures/Minute

Baseline Time for Flight Controllers to Recognize Rework = 30
Units: Minute [1, 500, 5]

Baseline Time to Complete Procedure Rework = 200
Units: Minute [1, 1000, 5]

"Completed Procedures (CP)"= INTEG (Procedure Completion Rate, Initial Completed Procedures)
Units: Procedures

Daily Procedure Rework Completion Rate = Procedure Rework Completion Rate * Day to Minute Conversion Factor
Units: Procedures/Day

Discrete Procedure Invalidation Rate = Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)
Units: Procedures/Minute

Flight Controller Rework Recognition Delay = Baseline Time for Flight Controllers to Recognize Rework + Rework Recognition Delay Attention Shifting Factor * Baseline Time for Flight Controllers to Recognize Rework * (1 - "Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)")
Units: Minute

Inactive Procedure Invalidation Rate = IF THEN ELSE(Rework Propagation Factor >= 0, MIN("Inactive Valid Procedures (IVP)"/Minimum Invalidation Time, ("Procedures Being Reworked by Ground (PBRG)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)), MAX(("Procedures Being Reworked by Ground (PBRG)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1), -"Inactive Procedures Needing Rework (IPNR)"/Time to Complete Procedure Rework))
Units: Procedure/Minute

Inactive Procedure Invalidation Rate During Discrete Event = 0
Units: Procedures/Minute [0, 500, 1]

"Inactive Procedures Needing Rework (IPNR)" = INTEG (Inactive Procedure Invalidation Rate-Activation Rate for PNR, Initial Inactive Procedures Needing Rework)
Units: Procedures

"Inactive Valid Procedures (IVP)" = INTEG (-Activation Rate for VP - Inactive Procedure Invalidation Rate, Initial Inactive Valid Procedures)
Units: Procedures

Initial Completed Procedures = 0
Units: Procedures

Initial Inactive Procedures Needing Rework = 0
Units: Procedures [0, 2000]

Initial Inactive Valid Procedures = 25000
Units: Procedures

Initial Number of Observable Procedures Needing Rework = 0
Units: Procedures [0, 0, 1]

Initial Number of Procedures Being Reworked = 0
Units: Procedures [0, 100]
Based on the assumption that no procedures are being reworked at the beginning of the mission

Initial Number of Unobservable Procedures Needing Rework = 0
Units: Procedures

Initial Number of Valid Procedures = 100
Units: Procedures

Minimum Invalidation Time = 5
Units: Minute [0, 1000, 5]

Mission Duration = "Mission Duration (in days)" * Day to Minute Conversion Factor
Units: Minute

"Mission Duration (in days)" = 240
Units: Day [0, 500]

Observability Rate = DELAY FIXED (Procedure Invalidation Rate, Light Delay, 0)
Units: Procedures/Minute

"Observable Procedures Needing Rework (OPNR)" = INTEG(Activation Rate for PNR +
Observability Rate - Procedure Rework Discovery Rate, Initial Number of Observable
Procedures Needing Rework)
Units: Procedures

Procedure Completion Fraction for Mission = 0
Units: Dmnl [0, 1]

Procedure Completion Rate = MIN((Total Number of Procedures * Procedure
Completion Fraction for Mission)/Mission Duration, "Active Valid Procedures
(AVP)"/Procedure Completion Time)
Units: Procedures/Minute
The Fuzzy Min structure (Sterman 2000) prevents the Active Valid Procedure
stock from going negative.

Procedure Completion Time = 10
Units: Minute

Procedure Invalidation Rate = MIN(Baseline Procedure Invalidation Rate + Discrete
Procedure Invalidation Rate, "Active Valid Procedures (AVP)"/Procedure Completion
Time)
Units: Procedures/Minute
The Fuzzy Min structure (Sterman 2000) prevents the Active Valid Procedure
stock from going negative.

Procedure Invalidation Rate During Discrete Event = 0
Units: Procedures/Minute [0, 500, 1]

Procedure Rework Completion Rate = IF THEN ELSE(Time > Startup Delay,
"Procedures Being Reworked by Ground (PBRG)"/Time to Complete Procedure Rework,
0)
Units: Procedures/Minute

Procedure Rework Discovery Rate = "Observable Procedures Needing Rework
(OPNR)"/Time to Discover Procedure Rework
Units: Procedures/Minute

Procedure Rework Time Horizon = 2000

Units: Minute

"Procedures Being Reworked (PBR)" = "Procedures Being Reworked by Ground (PBRG)" + "Procedures With Updates Unobservable on Spacecraft (PWUOS)"

Units: Procedures

"Procedures Being Reworked by Ground (PBRG)" = INTEG(Procedure Rework Discovery Rate - Procedure Rework Completion Rate, Initial Number of Procedures Being Reworked)

Units: Procedures

Procedures Needing and Being Reworked = "Active Procedures Needing Rework (APNR)" + "Inactive Procedures Needing Rework (IPNR)" + "Procedures Being Reworked (PBR)"

Units: Procedures

"Procedures With Updates Unobservable on Spacecraft (PWUOS)" = INTEG(Procedure Rework Completion Rate-Update Observability Rate, 0)

Units: Procedures

Rework Propagation Factor = 0.605

Units: Dmnl [0, 5]

The fraction of inactive procedures that are invalidated when procedures are reworked worked out to be roughly 51% of the total reworked procedures (not including discrete events or latent updates at launch). The baseline number used here is the same that was used in the Basic Procedure Rework Model.

Shift in Focus to Rework = (Target Flight Controller Resources Applied towards Procedure Rework - "Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)"/Time to Shift Focus

Units: Dmnl/Minute

Startup Delay = 520

Units: Minute [0, 1000, 5]

Time of Discrete Event = 100

Units: Minute [0, 1000, 5]

This parameter value must be a multiple of the time step.

Time to Complete Procedure Rework = Baseline Time to Complete Procedure Rework + Baseline Time to Complete Procedure Rework * Rework Completion Time Attention Shifting Factor * (1 - "Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)")

Units: Minute

Time to Discover Procedure Rework = Flight Controller Rework Recognition Delay
Units: Minute

Total Inactive Procedures = "Inactive Valid Procedures (IVP)" + "Inactive Procedures
Needing Rework (IPNR)"
Units: Procedures

Total Initial Inactive Procedures = Initial Inactive Procedures Needing Rework + Initial
Inactive Valid Procedures
Units: Procedures

Total Number of Procedures = Initial Number of Valid Procedures + Initial Number of
Unobservable Procedures Needing Rework + Initial Number of Procedures Being
Reworked
Units: Procedures

Total Procedures Reworked = INTEG (Accumulation of Reworked Procedures, 0)
Units: Procedures

"Unobservable Procedures Needing Rework (UPNR)"= INTEG (Procedure Invalidation
Rate - Observability Rate, Initial Number of Unobservable Procedures Needing Rework)
Units: Procedures

Update Observability Rate = DELAY FIXED(Procedure Rework Completion Rate, Light
Delay, 0)
Units: Procedure/Minute

"Valid Procedures (VP)" = "Active Valid Procedures (AVP)" + "Inactive Valid
Procedures (IVP)" + "Completed Procedures (CP)"
Units: Procedures

Flight Controller Attention Shifting Structure:

"Fraction of Flight Controller Resources Devoted to Procedure Rework (FRDPR)" =
INTEG (Shift in Focus to Rework, Initial Fraction of Flight Controller Resources
Devoted to Procedure Rework)
Units: Dmnl

"Fraction of Flight Controller Resources Devoted to Rework Discovery (FRDRD)" =
INTEG (-Shift in Focus to Rework, Initial Fraction of Flight Controller Resources
Devoted to Rework Discovery)
Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Procedure Rework = 1 - Initial
Fraction of Flight Controller Resources Devoted to Rework Discovery
Units: Dmnl

Initial Fraction of Flight Controller Resources Devoted to Rework Discovery = 1
Units: Dmnl

Resource Fraction per Procedure Reworked = 0.1
Units: Dmnl/Procedure [0, 0.1]

Rework Completion Time Attention Shifting Factor = 1
Units: Dmnl [0.1, 5, 5]

Rework Recognition Delay Attention Shifting Factor = 1
Units: Dmnl [0.1,5,5]

Target Flight Controller Resources Applied towards Procedure Rework = MIN(1,
Resource Fraction per Procedure Reworked * "Procedures Being Reworked by Ground
(PBRG)")
Units: Dmnl

Time to Shift Focus = 1
Units: Minute [1, 5]

Earth Solar Orbit Dynamics:

Change of X earth = Xdot earth
Units: Kilometer/Minutes

Change of Xdot earth = "Gravitational Parameter of Sun (adjusted for time step units)" *
X distance between Earth and Sun/Distance between Earth and Sun³
Units: Kilometer/(Minutes * Minutes)
Assumes Negligible affect of gravity between Earth and Mars.
Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Change of Y earth = Ydot earth
Units: Kilometer/Minutes

Change of Ydot earth = "Gravitational Parameter of Sun (adjusted for time step units)" *
Y distance between Earth and Sun/Distance between Earth and Sun³
Units: Kilometer/(Minutes * Minutes)
Assumes negligible effect of gravity between Earth and Mars.
Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Distance between Earth and Sun = SQRT(X earth² + Y earth²)
Units: kilometers
Assumes no movement of Sun and that the XY plane coincides with the orbital
plane.

"Earths Orbital Velocity (if circular orbit)" = $\text{SQRT}(\text{"Gravitational Parameter of Sun (adjusted for time step units)"} / \text{"Earths Semi-Major Orbital Axis"})$
Units: Kilometer/Minutes

"Earths Semi-Major Orbital Axis" = 1.49598e+008
Units: kilometers

Gravitational Parameter of Earth = 398601
Units: Kilometer * Kilometer * Kilometer / (seconds * seconds)
From Howell (2002) and Bate et al. (1971, pp. 429).

"Gravitational Parameter of Earth (adjusted for time step units)" = Gravitational Parameter of Earth * (1/Seconds to Minutes Conversion Factor)²
Units: Kilometer * Kilometer * Kilometer / (Minutes * Minutes)

Gravitational Parameter of Sun = 1.32712e+011
Units: Kilometer * Kilometer * Kilometer / (seconds * seconds)
From Bate et al. (1971, pp. 429).

"Gravitational Parameter of Sun (adjusted for time step units)" = Gravitational Parameter of Sun * (1/Seconds to Minutes Conversion Factor)²
Units: Kilometer * Kilometer * Kilometer / (Minutes * Minutes)

Initial X earth = 0
Units: kilometers

Initial Xdot earth = "Earths Orbital Velocity (if circular orbit)"
Units: Kilometer/Minutes

Initial Y earth = -"Earths Semi-Major Orbital Axis"
Units: kilometers

Initial Ydot earth = 0
Units: Kilometer/Minutes

Universal Gravitation Constant = 6.67e-020
Units: (Kilometer * Kilometer * Kilometer) / (kilogram * seconds * seconds)
From Howell (2002) and Bate et al. (1971, pp. 4).

X distance between Earth and Sun = -X earth
Units: kilometers
Assumes no movement of the Sun.

Xdot earth = INTEG (Change of Xdot earth, Initial Xdot earth)
Units: Kilometer/Minutes

X earth = INTEG(Change of X earth, Initial X earth)
Units: kilometers

Y distance between Earth and Sun = -Y earth
Units: kilometers
Assumes no movement of the Sun.

Y earth = INTEG (Change of Y earth, Initial Y earth)
Units: kilometers

Ydot earth = INTEG (Change of Ydot earth, Initial Ydot earth)
Units: Kilometer/Minutes
Assumes negligible effect of gravity between Earth and Mars.

Spacecraft Solar Orbit Dynamics:

Acceleration from Insertion Maneuver = IF THEN ELSE(Distance between Spacecraft and Sun > Maneuver Initiation Distance, Delta V Available for Mars Solar Orbit Insertion/Time for Maneuver, 0)
Units: Kilometer/(Minutes*Minutes)

Aphelion Velocity of Transfer Orbit = SQRT(2 * "Gravitational Parameter of Sun (adjusted for time step units)" * (1/Mars Perihelion - 1/(2 * "Semi-Major Axis of Transfer Orbit")))
Units: Kilometer/Minute

Change of X spacecraft = Xdot spacecraft
Units: Kilometer/Minutes

Change of Xdot spacecraft = "Gravitational Parameter of Sun (adjusted for time step units)" * X distance between Spacecraft and Sun/Distance between Spacecraft and Sun³
Units: Kilometer/(Minutes * Minutes)
Assumes negligible effect of gravity between Earth and Mars.
Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Change of Y spacecraft = Ydot spacecraft
Units: Kilometer/Minute

Change of Ydot spacecraft = "Gravitational Parameter of Sun (adjusted for time step units)" * Y distance between Spacecraft and Sun/Distance between Spacecraft and Sun³
Units: Kilometer/(Minutes*Minutes)
Assumes negligible effect of gravity between Earth and Mars.
Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-14).

Delta V Available for Mars Solar Orbit Insertion = INTEG (-Acceleration from Insertion Maneuver, Initial Delta V Available for Mars Solar Orbit Insertion)

Units: Kilometer/Minutes

Delta V for Mars Solar Orbit Insertion = Perihelion Velocity of Mars - Aphelion Velocity of Transfer Orbit

Units: Kilometer/Minute

Distance between Earth and Spacecraft = SQRT((X earth - X spacecraft)^2 + (Y earth - Y spacecraft)^2)

Units: kilometers

Distance between Spacecraft and Sun = SQRT(X spacecraft^2 + Y spacecraft^2)

Units: kilometers

Initial Delta V Available for Mars Solar Orbit Insertion = -Delta V for Mars Solar Orbit Insertion

Units: Kilometer/Minutes

Initial X spacecraft = Initial X earth

Units: kilometers

Initial Xdot spacecraft = Perihelion Velocity of Transfer Orbit

Units: Kilometer/Minutes

Initial Y spacecraft = Initial Y earth

Units: kilometers

Initial Ydot spacecraft = 0

Units: Kilometer/Minutes

Maneuver Distance Margin = 0

Units: Kilometer

Maneuver Initiation Distance = Mars Perihelion - Maneuver Distance Margin

Units: Kilometer

"Mars Orbital Velocity (if circular orbit)" = SQRT("Gravitational Parameter of Sun (adjusted for time step units)"/"Mars Semi-Major Orbital Axis")

Units: Kilometer/Minutes

Mars Perihelion = 2.06645e+008

Units: Kilometer

Source: <http://www.marspedia.org/>

"Mars Semi-Major Orbital Axis" = 2.27941e+008

Units: kilometers

From Howell (2002)

Perihelion Velocity of Mars = $\text{SQRT}(2 * \text{"Gravitational Parameter of Sun (adjusted for time step units)" * (1/\text{Mars Perihelion} - 1/(2 * \text{"Mars Semi-Major Orbital Axis"})}))$

Units: Kilometer/Minute

Perihelion Velocity of Transfer Orbit = $\text{SQRT}(2 * \text{"Gravitational Parameter of Sun (adjusted for time step units)" * (1/\text{"Earths Semi-Major Orbital Axis"} - 1/(2 * \text{"Semi-Major Axis of Transfer Orbit"})}))$

Units: Kilometer/Minutes

Formula derived in Howell (2002) and Bate et al. (1971, pp. 3-16).

"Semi-Major Axis of Transfer Orbit" = ($\text{"Earths Semi-Major Orbital Axis"} + \text{Mars Perihelion}$)/2

Units: kilometers

Spacecraft Distance from Earth = 0

Units: Kilometer [0, 3.75e+008, 1e+006]

Spacecraft Velocity = $\text{SQRT}(\text{Xdot spacecraft}^2 + \text{Ydot spacecraft}^2)$

Units: Kilometer/Minute

Time for Maneuver = 1

Units: Minute

Time of Flight = $3.14159 * \text{SQRT}(\text{"Semi-Major Axis of Transfer Orbit"}^3 / \text{Gravitational Parameter of Sun (adjusted for time step units)})$

Units: Minute

Formula from Bate et al. (1971, pp. 165).

X distance between Spacecraft and Sun = -X spacecraft

Units: kilometers

X spacecraft = $\text{INTEG}(\text{Change of X spacecraft, Initial X spacecraft})$

Units: kilometers

Xdot spacecraft = $\text{INTEG}(\text{Acceleration from Insertion Maneuver} + \text{Change of Xdot spacecraft, Initial Xdot spacecraft})$

Units: Kilometer/Minutes

Y distance between Spacecraft and Sun = -Y spacecraft

Units: kilometers

Y spacecraft = INTEG(Change of Y spacecraft, Initial Y spacecraft)

Units: kilometers

Ydot spacecraft = INTEG (Change of Ydot spacecraft, Initial Ydot spacecraft)

Units: Kilometer/Minutes

Light Delay Calculation:

Light Delay = IF THEN ELSE(Switch for Constant Distance from Earth = 1, Spacecraft Distance from Earth/Speed of Light, Distance between Earth and Spacecraft/Speed of Light)

Units: Minute

Speed of Light = 299792 * 60

Units: Kilometer/Minute

Source <http://www.speed-light.info/>

Switch for Constant Distance from Earth = 0

Units: Dmnl [0, 1, 1]

The Light Delayed, Flow Controlled Procedure Rework Model

The Light Delayed, Flow Controlled Procedure Rework Model is essentially the Light Delayed Procedure Rework Model with several structural modifications for implementing flow control. The primary numerical integration technique used for analysis of the model and graph development was Euler integration with a fixed time step size. The simulation start time was 0 minutes (coinciding with launch) and the end time was 347000 minutes (roughly coinciding with the insertion into Mars' solar orbit).

Rather than repeating the common elements of this model and the Light Delayed Procedure Rework Model, only the elements that represent additions or modifications to Light Delayed Procedure Rework Model are provided below.

Additions to the Light Delayed Procedure Rework Model to implement flow control:

Baseline Time to Complete Inactive Procedure Rework = 30000

Units: Minute [0, 1000, 5]

"Fraction of Resources Available for Inactive Procedure Rework Discovery (FRAIRD)" = INTEG(-Resource Activation Rate, Initial Fraction of Resources Available for Inactive Procedure Rework)

Units: Dmnl

"Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)" =
INTEG(Resource Activation Rate, Initial Fraction of Resources Utilized for Procedure
Rework)

Units: Dmnl

Inactive Procedure Rework Completion Rate = IF THEN ELSE(Resource Fraction per
Inactive Procedure Needing Rework > 0, "Inactive Procedures Needing Rework
(IPNR)"/Time to Complete Inactive Procedure Rework, 0)

Units: Procedures/Minute

Initial Procedure Rework Horizon = 2000

Units: Minute

Minimum Time to Complete Inactive Procedure Rework = Baseline Time to Complete
Inactive Procedure Rework * Rework Time Improvement Factor

Units: Minute [0, 1000, 5]

Procedure Rework Horizon Change Factor = 0

Units: Dmnl [0, 2.5]

Procedure Rework Horizon Change Time = 340000

Units: Minute

Resource Activation Rate = (Target Resources Applied towards Inactive Procedure
Rework - "Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)"/
Time to Activate Resources for Rework of Inactive Procedures Needing Rework

Units: Dmnl/Minute

Resource Fraction per Inactive Procedure Needing Rework = 0.5

Units: Dmnl/Procedure [0, 1]

Rework Time Improvement Factor = 0.02

Units: Dmnl [0, 1]

Target Resources Applied towards Inactive Procedure Rework = MIN(1, "Inactive
Procedures Needing Rework (IPNR)" * Resource Fraction per Inactive Procedure
Needing Rework)

Units: Dmnl

Time to Activate Resources for Rework of Inactive Procedures Needing Rework = 30

Units: Minute [1, 30]

Time to Complete Inactive Procedure Rework = Baseline Time to Complete Inactive Procedure Rework - (Baseline Time to Complete Inactive Procedure Rework - Minimum Time to Complete Inactive Procedure Rework) * "Fraction of Resources Utilized for Inactive Procedure Rework (FRUIPR)"

Units: Minute

Modifications to the Light Delayed Procedure Rework Model to implement flow control:

Inactive Procedure Invalidation Rate = IF THEN ELSE(Rework Propagation Factor >= 0, MIN("Inactive Valid Procedures (IVP)/Minimum Invalidation Time, ("Procedures Being Reworked by Ground (PBRG)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1)), MAX(("Procedures Being Reworked by Ground (PBRG)" * Rework Propagation Factor)/Time to Complete Procedure Rework + Inactive Procedure Invalidation Rate During Discrete Event * PULSE(Time of Discrete Event, 1), - "Inactive Procedures Needing Rework (IPNR)"/Time to Complete Procedure Rework))

Units: Procedure/Minute

"Inactive Procedures Needing Rework (IPNR)" = INTEG(Inactive Procedure Invalidation Rate - Activation Rate for PNR - Inactive Procedure Rework Completion Rate, Initial Inactive Procedures Needing Rework)

Units: Procedures

"Inactive Valid Procedures (IVP)" = INTEG(Inactive Procedure Rework Completion Rate - Activation Rate for VP - Inactive Procedure Invalidation Rate, Initial Inactive Valid Procedures)

Units: Procedures

Procedure Rework Time Horizon = Initial Procedure Rework Horizon + STEP(Procedure Rework Horizon Change Factor * Initial Procedure Rework Horizon, Procedure Rework Horizon Change Time)

Units: Minute [0, 5000]

Bibliography

- Albers, D. J.; Julien C. Sprott; and J. P. Crutchfield (2006), "Persistent chaos in high dimensions," *Physical Review E*, Vol. 74, No. 057201.
- Ancona, Deborah G.; Gerardo A. Okhuysen; and Leslie A. Perrow (2001), "Taking Time to Integrate Temporal Research," *Academy of Management Review*, Vol. 26, No. 4, pp. 512-529.
- Ancona, Deborah G.; Paul S. Goodman; Barbara S. Lawrence; and Michael L. Tushman (2001), "Time: A New Research Lens," *Academy of Management Review*, Vol. 26, No. 4, pp. 645-663.
- Ancona, Deborah and Mary J. Waller (2007), "The Dance of Entrainment: Temporally Navigating across Multiple Pacers." In R. Hodson and Beth Rubin (eds.), *Research in the Sociology of Work*, Vol. 17, *Workplace Temporalities*, Elsevier.
- Apostolakis, George E. (1990), "The Concept of Probability in Safety Assessments of Technological Systems," *Science*, Vol. 250, No. 4986, pp. 1359-1364.
- Apostolakis, George E. (2004), "How Useful is Quantitative Risk Assessment?" *Risk Analysis*, Vol. 24, No. 3, pp. 515-520.
- Bate, Roger R.; Donald D. Mueller; and Jerry E. White (1971), *Fundamentals of Astrodynamics*, Dover Publications, New York, NY.
- Bennett, Stuart (1996), "A Brief History of Automatic Control," *IEEE Control Systems Magazine*, Vol. 16, No. 3, pp. 17-25.
- Boccaletti, S.; C. Grebogi; Y.-C. Lai; H. Mancini; and D. Maza (2000), "The control of chaos: theory and applications," *Physics Reports*, Vol. 329, No. 3, pp. 103-197.
- Bourrier, Mathilde (2005), "The Contribution of Organizational Design to Safety," *European Management Journal*, Vol. 23, No. 1, pp. 98-104.
- Boyce, William E. and Richard C. DiPrima (1997), *Elementary Differential Equations and Boundary Value Problems*, 6th Edition, John Wiley and Sons, Inc., New York, NY.
- Brooks, Fredrick P., Jr. (1995), *The Mythical Man-Month: Essays on Software Engineering*, The 20th Anniversary Edition, Addison-Wesley, Reading, MA.
- Brown, R.; E. Braunstein; R. Brunet; R. Grace; T. Vu; J. Busa; and W. Dwyer (2002), "Timeliner: Automating Procedures on the ISS," *Proceedings of the AIAA SpaceOps 2002 Conference*, Oct. 9-12, Houston, TX.

- Bryson, Arthur E., Jr. (1996), "Optimal Control—1950 to 1985," *IEEE Control Systems Magazine*, Vol. 16, No. 3, pp. 26-33.
- Caldwell, Barrett S. (2003), "Distributed Supervisory Coordination with Multiple Operators and Remote Systems," *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, 5-8 October, Washington D.C. pp. 442-447.
- Caldwell, Barrett S. (2005), "Analysis and modeling of information flow and distributed expertise in space-related operations". *Acta Astronautica*, Vol. 56 No. 9-12, pg. 996-1004.
- Caldwell, Barrett S. and Sudip K. Ghosh (2003), "Supportion Operations-Reference Knowledge Development Cycles for Collaborative, Distributed Research," *Proceedings of the HCI International 2003: 10th International Conference on Human Computer Interaction*, 22-27 June, Heraklion, Greece.
- Caldwell, Barrett S. and Enlie Wang (2003), "Event Cycle and Knowledge Development in NASA Mission Control Center," *Proceedings of the HCI International 2003: 10th International Conference on Human Computer Interaction*, 22-27 June, Heraklion, Greece.
- Caldwell, Barrett S.; Keena S. Byrd; and Jeffrey C. Onken (2007a), "Flight Controller Information Technology use for Task Coordination in Mission Operations," *Proceedings of the 2nd IAASS Conference*, 14-16 May, Chicago, IL.
- Caldwell, Barrett S.; Ralph C. Palmer III; Christina Kokini; Keena S. Byrd; Lalaine Ignacio; and Jeffrey C. Onken (2007b), "Information Alignment and Distributed Human Coordination of Safety Critical Systems," *Proceedings of the 2nd IAASS Conference*, 14-16 May, Chicago, IL.
- Canadian Space Agency (2006), *Flight History of the Canadarm*. Available from: <<http://www.space.gc.ca/asc/eng/exploration/canadarm/flight.asp>> [29 May 2008].
- Carroll, John S. (1993), "Out of the Lab and Into the Field: Decision Making in Organizations," in Keith Murnighan (ed.) *Social Psychology in Organizations: Advances in Theory and Research*, Prentice Hall, Englewood Cliffs, NJ, pp. 38-62.
- Carroll, John S. (1998), "Organizational Learning Activities in High-Hazard Industries: The Logics Underlying Self-Analysis," *Journal of Management Studies*, Vol. 35, No. 6, pp. 699-717.
- Carroll, John S.; Jenny W. Rudolph; and Sachi Hatakenaka (2002), "Learning from Experience in High-Hazard Organizations," in B. Straw and R Kramer (eds.), *Research in Organizational Behavior*, JAI Press.
- Cartwright, T. J. (1991), "Planning and Chaos Theory," *Journal of the American Planning Association*, Vol. 57, No. 1, pp. 44-56.

- Challis, Simon; Kai-Uwe Peters; and Andrew Herd (2007), "Operations Procedure Validation as a Risk Mitigation Approach and its Relevance to Safety," *Proceedings of the 2nd IAASS Conference*, May 14-16, Chicago, IL
- Chen, Guanrong; Jorge L. Moiola; and Hua O. Wang (2000), "Bifurcation Control: Theories, Methods, and Applications," *International Journal of Bifurcation and Chaos*, Vol. 10, No. 3, pp. 511-548.
- Chevreau, F. R.; J. L. Wybo; and D. Cauchois (2006), "Organizing learning processes on risks by using the bow-tie representation," *Journal of Hazardous Materials*, Vol. 130, No. 3, pp. 276-283.
- Chow, Renee; Klaus Christoffersen, and David D. Woods (2000), "A Model of Communication in Support of Distributed Anomaly Response and Replanning," *Proceedings of the 19th Triennial Congress of the International Ergonomics Association and 44th Annual Meeting of the Human Factors and Ergonomics Society*, July 30-August 4, San Diego, CA, pp. I-34-I-37.
- Clark, Stuart and Valerie Jamieson (2007), "Millions spent, but was gravity result worth it?" *New Scientist Magazine*, Vol. 194, No. 2600, pp. 9.
- Cook, Richard I. and David D. Woods (2006), "Distancing Through Differencing: An Obstacle to Organizational Learning Following Accidents," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 329-338.
- Crocker, Alan R. (2005), "Operational Considerations in the Development of Autonomy for Human Spaceflight," *Proceedings of the 1st Space Exploration Conference*, January 30-February 1, Orlando, FL.
- Davidson, Keay (2003), "NASA's nuclear-fueled oddsmaking: Assurances can't calm fears of a 'Chernobyl in the sky,'" *San Francisco Chronicle*, April 28, pp. A-8.
- De Neufville, Richard (2003), "Real Options: Dealing With Uncertainty in Systems Planning and Design," *Integrated Assessment*, Vol. 4, No. 1, pp. 26-34.
- De Weck, Olivier L.; Richard De Neufville; and Mathieu Chaize (2004), "Staged Deployment of Communications Satellite Constellations in Low Earth Orbit," *AIAA Journal of Aerospace Computing, Information, and Communication*, Vol. 1, No. 3, pp. 119-136.
- Dechert, W. Davis; Julien C. Sprott; and David J. Albers (1999), "On the probability of chaos in large dynamical systems: A Monte Carlo study," *Journal of Economic Dynamics and Control*, Vol. 23, No. 8, pp. 1197-1206.

- Dekker, Sidney W. A. (2005), *Ten Questions About Human Error: A New View of Human Factors and System Safety*, Lawrence Erlbaum Associate Inc., Mahwah, NJ.
- Dekker, Sidney W. A. (2006), "Resilience Engineering: Chronicling the Emergence of Confused Consensus," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 77-92.
- Delapp, Linda P. (2008), NASA JSC FAO, Emails to the author, 11 March to 2 July, Personal Communication.
- Dijkstra, Arthur (2006), "Safety Management in Airlines," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 183-203.
- Dillon, Robin L.; M. Elisabeth Paté-Cornell; and Seth D. Guikema (2003), "Programmatic Risk Analysis for Critical Engineering Systems under Tight Resource Constraints," *Operations Research*, Vol. 51, No. 3, pp. 354-370.
- Draper, Charles Stark; Eldon C. Hall; G. W. Mayo; J. E. Miller; and E. G. Schwarm (1963), "Engineering and Reliability Techniques for Apollo Guidance, Navigation, and Control at MIT Instrumentation Laboratory," *Unpublished Manuscript*, MIT Museum. Cambridge, MA.
- Dulac, Nicolas (2007), *A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems*, Ph.D. Dissertation, Aeronautics and Astronautics, Massachusetts Institute of Technology.
- Dulac, Nicolas and Nancy Leveson (2004), "An Approach to Design for Safety in Complex Systems," *Proceedings of the 14th International Symposium of the International Council on Systems Engineering*, June 20-24, Toulouse, France.
- Dulac, Nicolas; Nancy G. Leveson; David Zipkin; Stephen Friedenthal; Joel Cutcher-Gershenfeld; John S. Carroll; and Betty Barrett (2005), "Using System Dynamics for Safety and Risk Management in Complex Engineering Systems," *Proceedings of the 2005 Winter Simulation Conference*, Dec. 5-8, Orlando, FL, pp. 1311-1320.
- Dulac, Nicolas; Brandon D. Owens; Nancy G. Leveson; and John S. Carroll (2007a), "A Hybrid Approach to the Creation of Dynamic Risk Management Models," *Proceedings of the 25th International System Dynamics Conference*, Jul. 29-Aug. 2, Boston, MA.
- Dulac, Nicolas; Brandon D. Owens; Nancy G. Leveson; and John S. Carroll (2007b), "A Formal Modeling Approach to Risk Management in the Development of Space Exploration Systems," *Proceedings of the 2nd IAASS Conference*, May 14-16, Chicago, IL.

- Dulac, Nicolas; Brandon D. Owens; Nancy G. Leveson; Betty Barrett; John S. Carroll; Joel Cutcher-Gershenfeld; Stephen Friedenthal; Joseph R. Laracy; and Joseph Sussman (2007c), "Demonstration of a New Dynamic Approach to Risk Analysis for NASA's Constellation Program," *MIT CSRL Final Report to the NASA ESMD Associate Administrator*, Cambridge, MA.
- Dunbar, Roger L. M. and William H. Starbuck (2006), "Learning to Design Organizations and Learning from Designing Them," *Organization Science*, Vol. 17, No. 2, pp. 171-178.
- Efimov, Denis V. and Alexander L. Fradkov (2006), "Adaptive tuning to bifurcation for time-varying nonlinear systems," *Automatica*, Vol. 42, No. 3, pp. 417-425.
- Engel, Avner and Tyson R. Browning (2008), "Designing Systems for Adaptability by Means of Architecture Options," *Systems Engineering*, Vol. 11, No. 2, pp. 125-146.
- Eppinger, Steven D.; Daniel E. Whitney; Robert P. Smith; and David A. Gebala (1994), "A Model-Based Method for Organizing Tasks in Product Development," *Research in Engineering Design*, Vol. 6, No. 1, pp. 1-13.
- ESD Uncertainty Management Committee (2004), "Uncertainty Management For Engineering Systems Planning and Design," *Engineering Systems Monograph*, Engineering Systems Symposium, Cambridge, MA.
- Esper, Jennifer E. and Carrie D. Olsen (2007), "A Study of International Space Station Ground/Crew Communication Methods with Applications to Human Moon and Mars Missions," *Proceedings of the AIAA Space 2007 Conference and Exposition*, Sept. 18-20, Long Beach, CA.
- Everitt, C. W. Francis (2007), "First Results from Gravity Probe B," *Proceedings of the 2007 April Meeting of the American Physical Society*, Apr. 14-17, Jacksonville, FL.
- Everitt, C. W. Francis (2008), "Physics Plea," *New Scientist Magazine*, Vol. 198, No. 2659, pp. 23.
- Franklin, Gene F.; J. David Powell; and Abbas Emami-Naeini (2002), *Feedback Control of Dynamic Systems*, Prentice-Hall, Upper Saddle River, NJ.
- Frey, Daniel D.; Fredrik Engelhardt; and Edward M. Greitzer (2003), "A role for 'one-factor-at-a-time' experimentation in parameter design," *Research in Engineering Design*, Vol. 14, No. 2, pp. 65-74.
- Fricke, Ernst and Armin P. Schulz. (2005), "Design for Changeability (DfC): Principles To Enable Changes in Systems Throughout Their Entire Lifecycle," *Systems Engineering*. Vol. 8, No. 4, pp. 342-359.

- Forrester, Jay W. (1961), *Industrial Dynamics*, Pegasus Communications, Waltham, MA.
- Forrester, Jay W. (1968), *Principles of Systems*, Productivity Press, Cambridge, MA.
- Forrester, Jay W. (1969), *Urban Dynamics*, Pegasus Communications, Waltham, MA.
- Forrester, Jay W. (1971), "Counterintuitive Behavior of Social Systems," *Technology Review*, Vol. 73, No. 3, pp. 52-68.
- Forrester, Jay W. (1973), *World Dynamics*, 2nd Edition, Pegasus Communications, Waltham, MA.
- Forrester, Jay W. (1985), "'The' model versus a modeling 'process'." *System Dynamics Review*, Vol. 1, No. 1, pp. 133-134.
- Forrester, Jay W. (2007a), "System dynamics—a personal view of the first fifty years," *System Dynamics Review*, Vol. 23, No. 2/3, pp. 345-358.
- Forrester, Jay W. (2007b), "System dynamics—the next fifty years," *System Dynamics Review*, Vol. 23, No. 2/3, pp. 359-370.
- Forsberg, Kevin and Harold Mooz (1992), "The Relationship of Systems Engineering to the Project Cycle," *Engineering Management Journal*, Vol. 4, No. 3, pp. 36-42.
- Freudenberg, William R. (1988), "Perceived Risk, Real Risk: Social Science and the Art of Probabilistic Risk Assessment," *Science*, Vol. 242, No. 4875, pp. 44-49.
- Fuller, David A. (2003), "Managing Risk in Space Operations: Creating and Maintaining a High Reliability Organization," *Proceedings of the AIAA Space 2003 Conference and Exhibition*, September 23-25, Long Beach, CA.
- Garrett, Sandra K. and Barrett S. Caldwell (2002), "Mission Control Knowledge Synchronization: Operations to Reference Performance Cycles," *Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society*, September 30-October 4, Baltimore, MD, pp. 1345-1349.
- Gehman, Harold W., Jr. (Chairman) (2003), *The Columbia Accident Investigation Board Report*, U.S. Government Accounting Office, Washington, D.C.
- Graham, John D. and James W. Vaupel (1981), "Value of a Life: What Difference Does It Make?" *Risk Analysis*, Vol. 1, No. 1, pp. 89-95.
- Griffin, Michael D. (2007), "Systems Engineering and the 'Two Cultures' of Engineering," *Remarks from the 2007 William E. Boeing Distinguished Lecture*, Purdue University, March 28, West Lafayette, IN.

- Hall, Rex D. and David J. Shayler (2003), *Soyuz: A Universal Spacecraft*, Springer-Praxis.
- Hassan, Rania; Richard De Neufville; Olivier De Weck; Daniel Hastings; and Daniel McKinnon (2005), "Value-at-Risk Analysis for Real Options in Complex Engineered Systems," *2005 IEEE International Conference on Systems, Man and Cybernetics*, Vol. 4 pp.3697-3704, 10-12 Oct., Hawaii.
- Hecht, Jeff (2004), "Spacecraft to measure Earth's drag on space-time," *New Scientist Magazine*, Online Edition (<http://www.newscientist.com/>), April 13.
- Hecht, Jeff (2008), "Gravity Probe B scores 'F' in NASA review," *New Scientist Magazine*, Online Edition (<http://www.newscientist.com/>), May 20.
- Hills, Graham and David Tedford (2003), "The Education of Engineers: the Uneasy Relationship between Engineering, Science and Technology," *Global Journal of Engineering Education*, Vol. 7, No. 1, pp. 17-28.
- Hollnagel, Erik (2006), "Resilience Engineering – Challenge of the Unstable," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 9-17.
- Hollnagel, Erik; David D. Woods, and Nancy G. Leveson (eds.) (2006), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT.
- Hollnagel, Erik and David D. Woods (2006), "Epilogue: Resilience Engineering Precepts," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 347-358.
- Hollnagel, Erik and Gunilla Sundstrom (2006), "States of Resilience," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 339-346.
- Howell, Kathleen C. (2002), *Fall 2002 Course Notes and Assignments for AAE 532: Orbit Mechanics*, Purdue University, West Lafayette, IN.
- Howell, Kathleen C.; Brian T. Barden; and Martin W. Lo (1997), "Application of Dynamical Systems Theory to Trajectory Design for a Libration Point Mission," *Journal of the Astronautical Sciences*, Vol. 45, No. 2, pp. 161-178.
- Huber, George P. (1991), "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science*, Vol. 2, No. 1, pp. 88-115.
- Jaap, John; Patrick Meyer; Elizabeth Davis; and Lea Richardson (2006), "In-Space Crew-Collaborative Task Scheduling," *Proceedings of the AIAA SpaceOps 2006 Conference*, June 19-23, Rome, Italy.

- Jamieson, Valerie (2007), "Gravity probe measures Earth's dent in space-time," *New Scientist Magazine*, Online Edition (<http://www.newscientist.com/>), April 16.
- Kampmann, Christian (1991), "Replication and Revision of a Classic System Dynamics Model: Critique of 'Population Control Mechanisms in a Primitive Agricultural Society,'" *System Dynamics Review*, Vol. 7, No. 2, pp. 159-198.
- Kearney, Michael W., III (1987), "The Evolution of the Mission Control Center," *Proceedings of the IEEE*, Vol. 75, No. 3, pp. 399-416.
- Kerwin, Joseph P. (1986), *Untitled July 28, 1986 Memorandum to the NASA Associated Administrator for Spaceflight Regarding the Cause of Death of the Challenger Astronauts*, National Aeronautics and Space Administration. Available from: <<http://history.nasa.gov/kerwin.html>> [May 9, 2008].
- Koga, R.; S. D. Pinkerton; T. J. Lie; and K. B. Crawford (1993), "Single-word multiple bit upsets in static random access devices," *IEEE Transactions on Nuclear Science*, Vol. 40, No. 6, pp. 1941-1946.
- Koon, Wang Sang; Martin W. Lo; Jerrold E. Marsden; and Shane D. Ross (2008), *Dynamical Systems, the Three-Body Problem and Space Mission Design*, Marsden Books.
- Korsmeyer, David J. and Ernest Smith (2008), "Applications of Intelligent Systems for Advanced Mission Operations," *Proceedings of the AIAA SpaceOps 2008 Conference*, May 12-16, Heidelberg, Germany.
- Korsmeyer, David J.; Daniel J. Clancy; James M. Crawford; and Mark E. Drummond (2005), "Crew-Centered Operations: What HAL 9000 Should Have Been," *Proceedings of the 1st Space Exploration Conference*, January 30-February 1, Orlando, FL.
- Kraft, Christopher C. (2001), *Flight: My Life in Mission Control*. Penguin Putnum Inc., New York, NY.
- Kranz, Eugene F. (2000), *Failure is not an Option: Mission Control from Mercury to Apollo 13 and Beyond*, Berkeley Books, New York, NY.
- Kuhn, Thomas S. (1970), *The Structure of Scientific Revolutions*, 2nd Edition, University of Chicago Press, Chicago, IL.
- La Porte, Todd R. (1996), "High Reliability Organizations: Unlikely, Demanding, and At Risk," *Journal of Contingencies and Crisis Management*, Vol. 4, No. 2, pp. 60-71.

- La Porte, Todd R. and Paula Consolini (1991), "Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations," *Journal of Public Administration Research and Theory*, Vol. 1, No. 1, pp. 19-48.
- Landis, Robert R.; David J. Korsmeyer; Paul A. Abell; Daniel R. Adamo; and Thomas D. Jones (2008), "A Piloted Orion Flight to a Near-Earth Object: A Feasibility Study," *Proceedings of the AIAA SpaceOps 2008 Conference*, May 12-16, Heidelberg, Germany.
- Leplat, Jacques (1987), "Occupational Accident Research and Systems Approach," in Jens Rasmussen, Keith Duncan, and Jacques Leplat (eds.), *New Technology and Human Error*, pp. 181-191, John Wiley & Sons, New York.
- Leslie, Christopher E. (2006), "Crew-Centric Mission Objective and Detail Flight Planning," *Proceedings of the AIAA SpaceOps 2006 Conference*, June 19-23, Rome, Italy.
- Leveson, Nancy G. (1995), *Safeware: System Safety and Computers*, Addison-Wesley Publishing Company, Reading, MA.
- Leveson, Nancy G. (2002), "A Systems Model of Accidents," *Proceedings of the 20th International Conference of the System Safety Society*, Aug. 5-9, Denver, CO.
- Leveson, Nancy G. (2003), "A New Approach to Hazard Analysis for Complex Systems," *Proceedings of the 21st International Conference of the System Safety Society*, Aug. 4-8, Ottawa, Canada.
- Leveson, Nancy G. (2004), "A New Accident Model for Engineering Safer Systems," *Safety Science*, Vol. 42, No. 4, 237-270.
- Leveson, Nancy G. (2009), *System Safety Engineering: Back To The Future*. Cambridge, MA, Forthcoming.
- Leveson, Nancy G. and Janice L. Stolzy (1987), "Safety Analysis Using Petri Nets," *IEEE Transactions on Software Engineering*, Vol. 13, No. 3, pp. 386-397.
- Leveson, Nancy G.; Mirna Daouk; Nicolas Dulac; and Karen Marais (2004), "A Systems Theoretic Approach to Safety Engineering," *Engineering Systems Monograph*, Engineering Systems Symposium, Cambridge, MA.
- Leveson, Nancy G.; Nicolas Dulac; Betty Barrett; John S. Carroll; Joel Cutcher-Gershenfeld; and Stephen Friedenthal (2005), "Risk Analysis of NASA Independent Technical Authority," *MIT CSRL Report to the NASA Office of the Chief Engineer*, Cambridge, MA.

- Leveson, Nancy G.; Nicolas Dulac; David Zipkin; Joel Cutcher-Gershenfeld; John S. Carroll; and Betty Barrett (2006), "Engineering Resilience into Safety-Critical Systems," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 95-123.
- Leveson, Nancy G.; Nicolas Dulac; Karen Marais; and John S. Carroll (2009), "Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems," *Organization Studies*, Vol. 30, Forthcoming.
- Lewis, Frank L. (1992), *Applied Optimal Control and Estimation: Digital Design and Implementation*, Prentice-Hall, Upper Saddle River, NJ.
- Liebergot, Sy and David M. Harland (2006), *Apollo EECOM: Journey of a Lifetime*, 2nd Edition, Apogee Books, Burlington, Ontario, Canada.
- Lo, Martin W.; Bobby Williams; Williard E. Bollman; Dongsuk Han; Yungsun Hahn; Julia L. Bell; Edward A. Hirst; Robert A. Corwin; Philip E. Hong; Kathleen C. Howell; Brian Barden; and Roby Wilson (1998), "Genesis Mission Design," *Proceedings of the 1998 AIAA/AAS Astrodynamics Specialist Conference*, Aug. 10-12, Boston, MA.
- Lorenz, Edward N. (1963), "Deterministic Nonperiodic Flow," *Journal of the Atmospheric Sciences*, Vol. 20, No. 2, pp. 130-141.
- Lorenz, Edward N. (1993), *The Essence of Chaos*, University of Washington Press, Seattle, WA.
- Lovell, Jim and Jeffrey Kluger (1994), *Apollo 13: Lost Moon*, Pocket Books, New York, NY.
- Lyneis, James M.; Kenneth G. Cooper; and Sharon A. Els (2001), "Strategic management of complex projects: a case study using system dynamics," *System Dynamics Review*, Vol. 17, No. 3, pp. 237-260.
- Lyneis, James M. and David N. Ford (2007), "System dynamics applied to project management: a survey, assessment, and directions for future research," *System Dynamics Review*, Vol. 23, No. 2/3, pp. 157-189.
- Maier, Mark W. and Eberhardt Rechtin (2000), *The Art of Systems Architecting*, 2nd Edition, CRC Press, Boca Raton, FL.
- Marais, Karen, Joseph H. Saleh, and Nancy G. Leveson (2006), "Archetypes for Organizational Safety," *Safety Science*, Vol. 44, No. 7, pp. 565-582.

- McCallum, Bill (2000), "On-orbit inventory management: Knowing what's on the International Space Station," *Logistics Spectrum*, Vol. 34, No. 2, pp. 29-30.
- McDonald, Nick (2006), "Organisational Resilience and Industrial Risk," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 155-180.
- McManus, Hugh and Daniel Hastings (2006), "A Framework for Understanding Uncertainty and its Mitigation and Exploitation in Complex Systems," *IEEE Engineering Management Review*, Vol. 34, No. 3, pp. 81-94.
- Meadows, Dennis L. and Donella H. Meadows (eds.) (1973), *Towards Global Equilibrium: Collected Papers*, Pegasus Communications, Waltham, MA.
- Meadows, Dennis L.; William W. Behrens III; Donella H. Meadows; R. F. Naill; Jorgen Randers; and E. K. Zahn (1974), *The Dynamics of Growth in a Finite World*, Pegasus Communication, Waltham, MA.
- Meadows, Dennis L. (2007), "A brief and incomplete history of operational gaming in system dynamics," *System Dynamics Review*, Vol. 23, No. 2/3, pp. 199-203.
- Meadows, Donella H.; Dennis L. Meadows; Jorgen Randers, and William W. Behrens III (1972), *The Limits to Growth*, Universe Books, New York, NY.
- Meadows, Donella; John Richardson; and Gerhart Bruckmann (1982), *Groping in the Dark: The first decade of global modelling*, John Wiley and Sons, New York, NY.
- Meadows, Donella; Jorgen Randers; and Dennis Meadows (1992), *Beyond the Limits: Confronting Global Collapse, Envisioning a Sustainable Future*, Chelsea Green Publishing, Post Mills, VT.
- Meadows, Donella; Jorgen Randers; and Dennis Meadows (2004), *Limits to Growth: The 30-Year Update*, Chelsea Green Publishing, White River Junction, VT.
- Mindell, David A. (2008), *Digital Apollo: Human and Machine in Spaceflight*, MIT Press, Cambridge, MA.
- Mishkin, Andrew; Young Lee; David Korth; and Troy LeBlanc (2007), "Human-Robotic Missions to the Moon and Mars: Operations Design Implications," *Proceedings of the 2007 IEEE Aerospace Conference*, Mar. 3-10, Big Sky, MT.
- MIT ESD Symposium Committee (2002), *ESD Terms and Definitions*, Version 14, Cambridge, MA.

- MIT ESD Uncertainty Management Committee (2004), "Uncertainty Management For Engineering Systems Planning and Design," *Engineering Systems Monograph*, Engineering Systems Symposium, Cambridge, MA.
- Morecroft, John D. W. (1983), "System Dynamics: Portraying Bounded Rationality," *Omega-The International Journal of Management Science*, Vol. 11, no. 2, pp. 131-142.
- Morgan, Gareth (1997), *Images of Organization*, 2nd Edition, Sage Publications, Thousand Oaks, CA.
- Mullane, Richard Michael (2006), *Riding Rockets: The Outrageous Tales of a Space Shuttle Astronaut*, Scribner, New York, NY.
- Mullins, Justin (2004), "Neutron stars steal space probe's glory," *New Scientist Magazine*, Vol. 183, No. 2464, pp. 10.
- Murphy, Dean M. and M. Elisabeth Pate-Cornell. (1996), "The SAM Framework: Modeling the Effects of Management Factors on Human Behavior in Risk Analysis," *Risk Analysis*, Vol. 16, No. 4, pp. 501-515.
- National Aeronautics and Space Administration (NASA 1987), *Implementation of the Recommendations of the Presidential Commission on the Space Shuttle Challenger Accident*, Report to the President of the United States of America, Washington, D.C.
- National Aeronautics and Space Administration (NASA 2005), *NASA's Implementation Plan for Space Shuttle Return to Flight and Beyond*, Volume 1, 10th Edition, June 3, Washington, D.C.
- National Aeronautics and Space Administration Kennedy Space Center (NASA KSC 2002), "NASA TV Viewers can hitch a Space Shuttle Ride," *Press Release No. 02-179*, September 19, Kennedy Space Center, FL.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2000), *STS-97 Mission Control Center Status Reports*, Houston, TX, Status Report No. 8-15.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2005a), "Mission Control Center," *NP-2005-04-004-JSC*, Houston, TX.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2005b), "Statement on Foam Shedding from External Tank," *Press Release No. 05-207*, July 28, Houston, TX.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2006a), *STS-115 Flight Plan: JSC-48000-115*, Final Version, July 5, Houston, TX.

- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2006b), *STS-115 Mission Control Center Status Reports*, Houston, TX, Status Report No. 7-13.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2006c), *STS-116 Flight Plan: JSC-48000-116*, Final Version, November 7, Houston, TX.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2006d), *STS-116 Mission Control Center Status Reports*, Houston, TX, Status Report No. 8-19.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2007a), *STS-117 Flight Plan: JSC-48000-117*, Final Version, February 16, Houston, TX.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2007b), *STS-117 Mission Control Center Status Reports*, Houston, TX, Status Report No. 6-17.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2007c), *STS-120 Flight Plan: JSC-48000-120*, Final Version, October 4, Houston, TX.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2007d), *STS-120 Mission Control Center Status Reports*, Houston, TX, Status Report No. 10-24.
- National Aeronautics and Space Administration Johnson Space Center (NASA JSC 2008), *Columbia Crew Survival Investigation Report: NASA/SP-2008-565*, Houston, TX.
- National Aeronautics and Space Administration Marshall Space Flight Center (NASA MSFC 2004), *Gravity Probe B Status Report No. 04-118*, April 23, Huntsville, AL.
- Neogi, Natasha A. (2002), *Hazard elimination using backwards reachability techniques in discrete and hybrid models*, Ph.D. Dissertation, Aeronautics and Astronautics, Massachusetts Institute of Technology.
- Newberry, Byron (2005), "Engineering Globalization: Oxymoron or Opportunity?" *IEEE Technology and Society Magazine*, Vol. 24, No. 3, pp. 8-15.
- Norman, Donald A. (1983), "Design Rules Based on Analyses of Human Error," *Communications of the ACM*, Vol. 26, No. 4, pp. 254-258.

- Norman, Donald A.; Andrew Ortony; and Daniel M. Russell (2003), "Affect and machine design: Lessons for the development of autonomous machines," *IBM Systems Journal*, Vol. 42, No. 1, pp. 38-44.
- Ogata, Katsuhiko (1997), *Modern Control Engineering*, 3rd Edition, Prentice-Hall, Upper Saddle River, NJ.
- Overbye, Dennis (2004), "A Wrinkle in Space-Time," *New York Times*, April 13.
- Owens, Brandon D.; Michael E. Adams; William J. Bencze; Gaylord Green; and Paul Shestople (2006), "The Effects of Radiation Events on Gravity Probe B," *Proceedings of the 9th Annual Military and Aerospace Programmable Logic Devices (MAPLD) International Conference*, Sept. 26-28, Washington, D.C.
- Owens, Brandon D. and Nancy G. Leveson (2006), "A Comparative Look at MBU Hazard Analysis Techniques," *Proceedings of the 9th Annual Military and Aerospace Programmable Logic Devices (MAPLD) International Conference*, Sept. 26-28, Washington, D.C.
- Owens, Brandon D.; Margaret Stringfellow Herring; Nicolas Dulac; Nancy G. Leveson; Michel D. Ingham; and Kathryn Anne Weiss (2008), "Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission," *Proceedings of the 2008 IEEE Aerospace Conference*, Mar. 1-8, Big Sky, MT, paper 1279.
- Paté-Cornell, M. Elisabeth (1984), "Fault Trees vs. Event Trees in Reliability Analysis," *Risk Analysis*, Vol. 4, No. 3, pp. 177-186.
- Paté-Cornell, M. Elisabeth (1990), "Organizational Aspects of Engineering System Safety: The Case of Offshore Platforms," *Science*, Vol. 250, No. 4985, pp. 1210-1217.
- Paté-Cornell, M. Elisabeth (1996), "Uncertainties in risk analysis: Six levels of treatment," *Reliability Engineering and System Safety*, Vol. 54, No. 2, pp. 95-111.
- Paté-Cornell, M. Elisabeth and Dean M. Murphy (1996), "Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications," *Reliability Engineering and System Safety*, Vol. 53, No. 2, pp. 115-126.
- Paté-Cornell, M. Elisabeth; Dean M. Murphy; Linda M. Lakats; and David M. Gaba (1996), "Patient risk in anesthesia: Probabilistic risk analysis and management improvements," *Annals of Operations Research*, Vol. 67, No. 1, pp. 211-233.
- Paté-Cornell, M. E. and Robin Dillon (2001), "Probabilistic risk analysis for the NASA space shuttle: a brief history and current work," *Reliability Engineering and System Safety*, Vol. 74, No. 3, pp. 345-352.

- Patterson, Emily S.; Jennifer Watts-Perotti; and David D. Woods (1999), "Voice Loops as Coordination Aids in Space Shuttle Mission Control," *Computer Supported Cooperative Work*, Vol. 8, pp. 353-371.
- Patterson, Emily S. and David D. Woods (2001), "Shift Changes, Updates, and the On-Call Architecture in Space Shuttle Mission Control," *Computer Supported Cooperative Work*, Vol. 10, pp. 317-346.
- Perrow, Charles (1999), *Normal Accidents: Living with High-Risk Technologies*, 1999 Edition, Princeton University Press, Princeton, NJ.
- Pitt, Joseph C. (2001), "What Engineers Know," *Techné: Journal of the Society for Philosophy and Technology*, Vol. 5, No. 3, pp. 17-30.
- Popper, Karl R. (1934), *Logik der Forshung*, Springer Press, Vienna, Austria.
- Rappaport, Roy A. (1968), *Pigs for the Ancestors: Ritual in the Ecology of a New Guinea People*, Yale University Press, New Haven, CT.
- Rasmussen, Jens (1987), "Cognitive control and human error mechanisms," in J. Rasmussen, Keith Duncan, and Jacques Leplat (Eds.), *New Technology and Human Error*, John Wiley & Sons, New York, NY, pp. 53-61.
- Rasmussen, Jens (1990), "The role of error in organizing behaviour," *Ergonomics*, Vol. 33, No. 10/11, pp. 1185-1199.
- Rasmussen, Jens (1997), "Risk Management in a Dynamic Society: A Modelling Problem," *Safety Science*, Vol. 27, No. 2/3, pp. 183-213.
- Reason, James (1990), "The Contribution of Latent Human Failures to the Breakdown of Complex Systems," *Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences*, Vol. 327, No. 1241, *Human Factors in Hazardous Situations*, pp. 475-484.
- Reason, James (1995), "A Systems Approach to Organizational Error," *Ergonomics*, Vol. 38, No. 8, pp. 1708-1721.
- Repenning, Nelson P. (2001), "Understanding fire fighting in new product development," *The Journal of Product Innovation Management*, Vol. 18, No. 5, pp. 285-300.
- Richards, Matthew G.; Adam M. Ross; Daniel E. Hastings; and Donna H. Rhodes (2008), "Two Empirical Tests of Design Principles for Survivable System Architecture," *Proceedings of the 18th International Symposium of the International Council on Systems Engineering*, Jun. 15-19, Utrecht, Netherlands.

- Rickards, James G. (2008), "A Mountain, Overlooked: How Risk Models Failed Wall St. and Washington," *The Washington Post*, October 2, pp. A23.
- Roberts, Karlene H. (1990a), "Managing high reliability organizations," *California Management Review*, Vol. 32, No. 4, pp. 101-114.
- Roberts, Karlene H. (1990b), "Some characteristics of one type of high reliability organization," *Organization Science*, Vol. 1, No. 2, pp. 160-176.
- Rochlin, Gene I., Todd R. La Porte; and Karlene H. Roberts (1987), "The Self-Designing High Reliability Organization: Aircraft carrier flight operations at sea," *Naval War College Review*, Vol. 40, No. 4, pp. 76-90.
- Rogers, William P. (Chairman) (1986), *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, U.S. Government Accounting Office, Washington, D.C.
- Roosevelt, Theodore (1910), "Citizenship in a Republic," *Remarks from an April 23, 1910 Speech at the Sorbonne*, Paris, France.
- Rose, David A. and Walter H. Miller, Jr. (2006), "Training System Considerations for Exploration Program Space Operations," *Proceedings of the AIAA SpaceOps 2006 Conference*, June 19-23, Rome, Italy.
- Ross, Adam M.; Donna H. Rhodes; and Daniel E. Hastings (2008), "Defining Changeability: Reconciling Flexibility, Adaptability, Scalability, Modifiability, and Robustness for Maintain System Lifecycle Value," *Systems Engineering*, Vol. 11, No. 3, pp. 246-262.
- Rowe, William D. (1994), "Understanding Uncertainty," *Risk Analysis*, Vol. 14, No. 5, pp. 743-750.
- Rudolph, Jenny W. and Nelson P. Repenning (2002), "Disaster Dynamics: Understanding the Role of Quantity in Organizational Collapse," *Administrative Science Quarterly*, Vol. 47, No. 1, pp. 1-30.
- Rusnak, Kevin M. (2000), "Interview with John W. Aaron," *NASA Johnson Space Center Oral History Project Transcript*, Houston, TX.
- Rusnak, Kevin M. (2002), "Interview with Charles L. Dumis," *NASA Johnson Space Center Oral History Project Transcript*, Houston, TX.
- Sagan, Scott D. (1993), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton, NJ.

- Sagan, Scott D. (2004a), "Learning from *Normal Accidents*," *Organization & Environment*, Vol. 17, No. 1, pp. 15-19.
- Sagan, Scott D. (2004b), "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security," *Risk Analysis*, Vol. 24, No. 4, pp. 935-946.
- Seabrook, John (2006), "The Game Master," *The New Yorker*, Vol. 82, No. 36, pp. 88-99.
- Seife, Charles (2003), "Columbia Disaster Underscores the Risky Nature of Risk Analysis," *Science*, Vol. 299, No. 5609, pp. 1001-1002.
- Senge, Peter M. (2006), *The Fifth Discipline: The Art and Practice of the Learning Organization*, Revised Edition, Currency Doubleday, New York, NY.
- Shalin, Valerie L. (2005), "The roles of humans and computers in distributed planning for dynamic domains," *Cognition, Technology & Work*, Vol. 7, No. 3, pp. 198-211.
- Shantzis, Steven B. and William W. Behrens III (1973), "Population Control Mechanisms in a Primitive Agricultural Society," in Meadows, D. L. and D. H. Meadows (eds.), *Towards Global Equilibrium: Collected Papers*, MIT Press, Cambridge, MA, pp. 258-288.
- Sierhuis, Maarten; Thomas E. Diegelman; Chin Seah; Valerie Shalin; William J. Clancey; and Albert M. Selvin (2007), "Agent-Based Simulation of Shuttle Mission Operations," *Proceedings of the Spring Simulation Multiconference*, Mar. 25-29, Norfolk, VA.
- Siddiqi, Afreen (2006), *Reconfigurability in Space Systems: Architecting Framework and Case Studies*, Ph.D. Dissertation, Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA.
- Sprott, Julien C. (1993), "How common is chaos?" *Physics Letters A*, Vol. 173, No. 1, pp. 21-24.
- Stanford University (2008a), *May 2008 Gravity Probe B Mission Status Update*. Available from: <<http://einstein.stanford.edu/highlights/hlindexmain.html>> [4 June 2008].
- Stanford University (2008b), *Fall 2008 Gravity Probe B Mission Status Update*. Available from: <<http://einstein.stanford.edu/highlights/hlindexmain.html>> [30 Sept. 2008].
- Stanley, Douglas O. et al. (2005), *NASA's Exploration Systems Architecture Study Final Report*, NASA TM-2005-214062.

- Stanley, Douglas O.; Stephen A. Cook; John Connolly; and Jeffrey M. Hanley (2006), "Exploration Systems Architecture Study: Overview of Architecture and Mission Operations Approach," *Proceedings of the AIAA SpaceOps 2006 Conference*, June 19-23, Rome, Italy.
- Stark, Jaroslav and Kate Hardy (2003), "Chaos: Useful at Last?" *Science*, Vol. 301, No. 5637, pp. 1192-1193.
- Sterman, John D. (1984), "Appropriate Summary Statistics for Evaluating the Historical Fit of System Dynamics Models," *Dynamica*, Vol. 10, No. 2, pp. 51-66.
- Sterman, John D. (1991), "A Skeptic's Guide to Computer Models," in Barney, G. O. et al (Eds.), *Managing A Nation: The Microcomputer Software Catalog*, Westview Press, Boulder, CO, pp. 209-229.
- Sterman, John D. (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin/McGraw-Hill, New York, NY.
- Sterman, John (2002), "All models are wrong: reflections on becoming a systems scientist," *System Dynamics Review*, Vol. 18, No. 4, pp. 501-531.
- Stringfellow, Margaret V. (2008), *Safety-Driven System Engineering Process*, S.M. Thesis, Aeronautics and Astronautics, Massachusetts Institute of Technology.
- Stringfellow, Margaret V.; Brandon D. Owens; Nicolas Dulac; and Nancy G. Leveson (2008), "A Safety-Driven Systems Engineering Process," *Proceedings of the 18th International Symposium of the International Council on Systems Engineering*, Jun. 15-19, Utrecht, Netherlands.
- Strogatz, Steven H. (1994), *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, Westview Press, Cambridge, MA.
- Sundstrom, Gunilla and Erik Hollnagel (2006), "Learning How to Create Resilience in Business Systems," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 235-252.
- Turneure, J. P.; C. W. F. Everitt; B. W. Parkinson; D. Bardas; S. Buchman; D. B. DeBra; H. Dougherty; D. Gill; J. Grammer; G. B. Green; G. M. Gutt; D.-H. Gwo; M. Heifetz; N. J. Kasdin; G. M. Keiser; J. A. Lipa; J. M. Lockhart; J. C. Mester; B. Muhlfelder; R. Parmley; A. S. Silbergleit; M. T. Sullivan; M. A. Taber; R. A. Van Patten; R. Vasser; S. Wang; Y. M. Xiao; and P. Zhou (2003), "Development of the Gravity Probe B Flight Mission," *Advances in Space Research*, Vol. 32, No. 7, pp. 1387-1396.

- Tversky, Amos and Daniel Kahneman. (1974), "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185, No. 4157, pp. 1124-1131.
- Urbina, Ian (2008), "Growing Pains for a Deep-Sea Home Built of Subway Cars," *New York Times*, April 8.
- Uri, John J. (2005), "Five Years of NASA Research on ISS—A Continuing Saga," *Proceedings of the 56th International Astronautical Congress*, Oct. 17-21, Fukuoda, Japan.
- Vincenti, Walter G. (1990), *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History*, The Johns Hopkins University Press, Baltimore, MD.
- Watts, Jennifer C.; David D. Woods; and Emily S. Patterson (1996), "Functionally Distributed Coordination during Anomaly Response in Space Shuttle Mission Control," *Proceedings of the IEEE 3rd Annual Symposium on Human Interaction with Complex Systems*, 25-28 August, Dayton, OH.
- Watson, Stephen R. (1994), "The meaning of probability in probabilistic safety analysis," *Reliability Engineering and System Safety*, Vol. 45, No. 3, pp. 261-269.
- Webb, Dennis J. and Ernest E. Smith (2008), "Mission Operations Support for the Constellation Program," *Proceedings of the AIAA SpaceOps 2008 Conference*, May 12-16, Heidelberg, Germany.
- Weick, Karl E. (1987), "Organizational Culture as a Source of High Reliability," *California Management Review*, Vol. 29, No. 2, pp. 112-127.
- Weick, Karl E. and Karlene H. Roberts (1993), "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly*, Vol. 38, No. 3, pp. 357-381.
- Weick, Karl E.; K. M. Sutcliffe; and D. Obstfeld (1999), "Organizing for High Reliability: Processes of collective mindfulness," in B. Straw and R. Sutton (Eds.), *Research in Organizational Behavior*, Vol. 23, JAI Press, Greenwich, CT, pp. 81-123.
- Weinberg, Alvin M. (1972), "Science and trans-science," *Minerva*, Vol. 10, No. 2, pp. 209-222.
- Weiss, Kathryn A.; Nicolas Dulac; Stephanie Chiesi; Mirna Daouk; David Zipkin; and Nancy Leveson (2006), "Engineering Spacecraft Mission Software using a Model-Based and Safety-Driven Design Methodology," *AIAA Journal of Aerospace Computing, Information, and Communication*, Vol. 3, No. 11, pp. 562-586.

- Wesson, Paul S. and Mark Anderson (2008), "The Gravity Probe B Bailout," *IEEE Spectrum*, Online Edition (<http://www.spectrum.ieee.org>), October 1.
- Wiegmann, Douglas A. and Scott A. Shappell (2003), *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*, Ashgate Publishing, Burlington, VT.
- Woods, David D. (2006), "How to Design a Safety Organization: Test Case for Resilience Engineering," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 315-325.
- Woods, David D. and Richard I. Cook (2002), "Nine Steps to Move Forward from Error," *Cognition, Technology, and Work*, Vol. 4, No. 2, pp. 137-144.
- Woods, David D. and Richard I. Cook (2006), "Incidents – Markers of Resilience or Brittleness?" in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 69-76.
- Woods, David D. and Erik Hollnagel (2006), "Prologue: Resilience Engineering Concepts," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 1-6.
- World Health Organization (WHO 2000), *Papua New Guinea: Introduction*, Available from: < <http://www.wpro.who.int/countries/04png/> > [12 August 2008].
- Wreathall, John (2006), "Properties of Resilient Organizations: An Initial View," in E. Hollnagel, D. D. Woods, and N. G. Leveson (eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing Co., Burlington, VT, pp. 275-285.
- Zemba, Yuriko; Maia J. Young; and Michael W. Morris (2006), "Blaming leaders for organizational accidents: Proxy logic in collective- versus individual-agency cultures," *Organizational Behavior and Human Decision Processes*, Vol. 101, No. 1, pp. 36-51.

