

**A LEAN SAFETY REVIEW PROCESS FOR
PAYLOADS ON THE INTERNATIONAL
SPACE STATION**

by

Javier de Luis

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2003

©2003 Javier de Luis. All rights reserved. The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part

Signature of
Author

_____ ⁷
Javier de Luis
~~System Design and Management Program~~
June 2003

Certified By

M

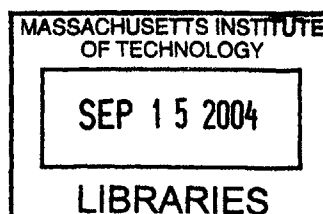
Prof. Jeffrey A. Hoffman
Thesis Supervisor
Professor of the Practice of Aerospace Engineering

Accepted By

Prof. Steven D. Eppinger
Co-Director, LFM/SDM
GM LFM Professor of Management Science and Engineering Systems

Accepted By

Prof. Paul A. Lagace
Co-Director, LFM/SDM
Professor of Aeronautics & Astronautics and Engineering Systems



BARKER

THIS PAGE INTENTIONALLY LEFT BLANK

A LEAN SAFETY REVIEW PROCESS FOR PAYLOADS ON THE INTERNATIONAL SPACE STATION

by

Javier de Luis

Submitted to the System Design and Management Program in
partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

ABSTRACT

The International Space Station has the potential to serve as a unique test platform to enable technologies for a wide array of manned and unmanned NASA missions. In order to live up to its promise, the resources required to develop and fly an experiment on the Station must be commensurate with the scientific return that will be obtained. This thesis applies the set of tools and principles known collectively as Lean Engineering to the Payload Safety Review process, one of the activities that must be satisfied by payloads prior to flying. The goal of this study is to attempt to reduce the required resources needed to fly a payload on the Station.

Using the MIT Lean Aerospace Initiative Transformation to Lean roadmap, three separate payload examples of increasing degree of complexity are analyzed. Value streams are derived, and estimates for duration and labor requirements are presented based on past experience and data obtained from various stakeholders. Opportunities for waste (*muda*) reduction are identified. In addition, a comparative analysis is presented where the Safety Review Process is contrasted to similar issues faced by industry over the last several decades as manufacturing processes were transformed in order to increase quality while simultaneously reducing cost.

Insights from these analyses, supported by stakeholder data from payload developers and the NASA Payload Safety Review Panel, are used to suggest a redesign to improve the Safety Review process. Three specific recommendations are proposed: 1) Establishment of a group outside NASA that can provide experienced, design assistance to payload developers as an integral part of their design teams; 2) Empowerment of these integrated teams through elimination of the monuments created by intermediary safety reviews conducted by organizations outside the control of the Payload Safety Review Panel; and 3) Preparation of a Safety Verification and Review Plan at the start of each development effort which would contain the schedule and content for all safety-related review activities and data submittals, and would *pull* these activities throughout the process only when necessary.

The revised process reduces the number of discrete steps from a maximum of 27 to 10. Duration of the process and the amount of labor required to complete it are reduced by up to 60% and 20%, respectively. Cost savings on the order of \$10 million/year, depending on the number and complexity of the payloads, are obtained.

Thesis supervisor: Jeffrey A. Hoffman

Title: Professor of the Practice of Aerospace Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

<i>C H A P T E R 1 : I N T R O D U C T I O N.....</i>	<i>11</i>
1.1 What is Lean?.....	13
1.2 The International Space Station.....	16
1.3 The Payload Safety Review Process	18
1.4 Summary.....	23
<i>C H A P T E R 2 : T R A N S I T I O N T O L E A N.....</i>	<i>25</i>
2.1 Strategic Planning and Adopting a Lean Paradigm.....	26
2.2 Focus on the Value Stream.....	29
2.2.1 Value Streams	29
2.2.2 Stakeholders.....	38
2.2.3 Focus on the Value Stream: Summary	39
2.3 Develop Lean Structure and Behavior.....	40
2.4 Create and Refine Transformation Plan.....	40
2.5 Implement Lean Initiatives.....	41
2.6 Focus on Continuous Improvement.....	44
2.7 Summary.....	45
<i>C H A P T E R 3 : C O M P A R I S O N B E T W E E N T H E P U R S U I T O F Q U A L I T Y I N A M E R I C A N M A N U F A C T U R I N G AND SAFETY IN SPACE.....</i>	<i>47</i>
3.1 Why Compare?.....	47
3.2 Parallels	48
3.2.1 Emergent Properties	48
3.2.2 Difficult to Quantify.....	50
3.2.3 The Role of Perception.....	51
3.3 Differences.....	52
3.3.1 Statistical Techniques	52
3.3.2 Production Line and Learning Curves.....	53
3.3.3 Experience Base.....	53
3.4 Quality.....	54
3.4.1 Building the Product to Specifications.....	55
3.4.2 Building the Product to Meet Customer Needs.....	55
3.4.3 Building a Good Product Affordably	57
3.5 Safety.....	58
3.5.1 Building the Payload to Specifications.....	59
3.5.2 Building Safety into the Payload.....	59
3.5.3 Building a Safe, Cost-Effective Payload.....	61
<i>C H A P T E R 4 : S T A K E H O L D E R S ' P E R S P E C T I V E</i>	<i>65</i>
4.1 Cell Culture Unit	65
4.2 Synchronized Position, Hold, Engage, Reorient Experimental Satellites (SPHERES).....	70
4.3 Enhanced Dynamic Load Sensing Experiment/Mir Structural Dynamics Experiment.....	74
4.4 Payload Safety Review Panel.....	77
4.5 Summary.....	82
<i>C H A P T E R 5 : D E S I R E D S T A T E.....</i>	<i>85</i>
5.1 Define Value	85
5.2 Identify Value Stream.....	87
5.3 Flow the Product.....	91
5.4 Pull the Product Through the Process.....	94
5.5 Strive for Perfection.....	96
5.6 New Value Stream	97
5.7 Metrics	102
<i>C H A P T E R 6 : S U M M A R Y A N D R E C O M M E N D A T I O N S F O R F U T U R E W O R K.....</i>	<i>109</i>

6.1	Summary.....	109
6.2	Future Work.....	112
<i>A P P E N D I X A : N A S A R E F E R E N C E D O C U M E N T S.....</i>		<i>115</i>
<i>A P P E N D I X B : D E T A I L E D P A Y L O A D S A F E T Y P R O C E S S F L O W.....</i>		<i>119</i>
<i>A P P E N D I X C : P R E S E N T A T I O N F O R T H E P A Y L O A D S A F E T Y R E V I E W P A N E L.....</i>		<i>127</i>

LIST OF FIGURES

Figure 1-1: The International Space Station at Completion (artist rendering courtesy NASA)	18
Figure 1-2: Example of a Payload Hazard Report	24
Figure 2-1: The Transition to Lean Roadmap (courtesy, MIT Lean Aerospace Initiative).....	26
Figure 2-2: Tiered Suppliers simplify the Product Flow	28
Figure 2-3: Payload Developers Cannot be Easily Organized Hierarchically.....	28
Figure 2-4: Type 1 Payload Safety Review Value Stream.....	33
Figure 2-5: Type 2 Payload Safety Review Value Stream.....	34
Figure 2-6: Type 3 Payload Safety Review Value Stream.....	35
Figure 2-7: Total Time Required to Complete the Payload Safety Review Process	37
Figure 2-8: Total Labor Required to Complete the Payload Safety Review Process.....	38
Figure 3-1: Components from the SPHERES Experiment.....	49
Figure 3-2: Components Arranged in a Potentially Unsafe Manner.....	49
Figure 3-3: Normal Distribution of a Key Parameter in a Process.	56
Figure 3-4: Narrowing the Distribution Reduces Rejected Components	57
Figure 4-1: The Cell Culture Unit in its Flight Configuration.....	66
Figure 4-2: The Various Types of Cells that Will Be Grown in the Cell Culture Unit Facility.....	67
Figure 4-3: SPHERES Testing on Previous KC-135 Flights	71
Figure 4-4: SPHERES satellite, actual (left) and rendered with callouts (right).....	71
Figure 4-5: Enhanced Dynamic Load Sensor Units	75
Figure 5-1: The Proposed Lean Value Stream.....	98
Figure 5-2: Total Time Required to Complete the Payload Safety Review Process	101
Figure 5-3: Total Labor Required to Complete the Payload Safety Review Process.....	101
Figure 5-4: Average Labor Required (in boxes) for Each Process	103

LIST OF TABLES

Table 1-1: The Multiple Phases of the Payload Safety Review Process.....	20
Table 2-1: Summary of Payload Examples Used for Value Stream Mapping	30
Table 2-2: Summary Table for Process Durations and Required Labor	36
Table 2-3: Stakeholder Summary Table.....	39
Table 4-1: Main Points and Observations from Interview with the CCU Integration Engineer (K. Slater).....	70
Table 4-2: Main Points and Observations from Interview with the SPHERES Project Manager (S. Sell).....	74
Table 4-3: Main Points and Observations from Interview with the EDLS Hardware Development Manager (E. Bokhour).....	77
Table 4-4: Main Points and Observations from Interview with the Payload Safety Review Panel.....	82
Table 5-1: Value Terminology Defined for the NASA Payload Safety Review Process.....	86
Table 5-2: Comparison of Desired State with Previous Processes.....	99
Table 5-3: Average Expected Savings per Type of Payload.....	103
Table 5-4: Savings Due to Implementation of Lean Process Changes.....	104
Table 5-5: Cross Reference of Proposed Recommendations to Issues Raised.....	106

ACKNOWLEDGMENTS

It was not without more than a little trepidation that I re-entered the academic learning environment after an absence of over a decade. However, I felt that it is important to periodically expand upon the knowledge that one has acquired over the years out in the real world by exposure to the latest theories, practices, and tools. The Systems Design and Management program offered me this opportunity, and I would like to acknowledge all the faculty, staff, and students that made this past year memorable. In particular, I would like to thank my colleagues Ignacio Grossi and Tom Seitz not only for all their help and unique insights, but most importantly for always setting the bar just a little higher in everything they did.

I would like to thank the employees of Payload Systems for picking up the slack while I've been away and allowing me the chance to take this sabbatical year. I especially would like to thank Joe Parrish and Pam Moriarty for really making it possible for me to focus on my academic concerns while they took care of the company.

I pestered many people to obtain information and data from the stakeholders of the existing process. I thank them all, but especially those that I annoyed the most, including Kim Slater, Steve Sell, Ed Bokhour, and Skip Larsen.

I would also like to acknowledge Professor Debbie Nightingale, who introduced me to the concepts of *lean* and thereby got me started on the path that ultimately led to this thesis. And of course, my thesis advisor, Professor Jeffrey Hoffman, for opening doors at NASA which allowed me to gather data that I could not have hoped to obtain otherwise, and for providing his unique perspective as an astronaut to the analysis of the process.

Finally, I would like to thank my family: my wife, Jean, for putting up with me, and my new twin daughters, Isabel and Maya, who arrived two months early. I thought that everything was set for them not to be born until after this thesis was done. They had other plans. I guess I just got a head start in getting used to my kids not doing what I want them to do.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1:

Introduction

The International Space Station stands at a crossroads. Since the launch of its first element in 1998, activity on-board the ISS has focused on completing the assembly of its major components. Resources devoted to experiments designed to exploit the unique long-term microgravity environment that the station provides have been understandably limited, as crew time, power, and up-mass brought by the Shuttle from Earth have been dedicated to the assembly task.

This is about to change. By 2006, the ISS will be essentially complete¹. The European and Japanese modules will join the US laboratory in providing an unprecedented amount of resources for conducting experiments with pressurized payloads, while at the same time the ISS truss structure will provide similar facilities for experiments requiring exposure to the vacuum of space. While the Shuttle Columbia disaster will likely delay the schedule, it is unavoidable that the transition from the assembly phase to the fully-functional utilization phase will occur.

Once the ISS is fully operational, experiments will need to be developed that can exploit this unique facility. At the same time, NASA is being faced with additional tasks and missions that will require the expenditure of resources. The Orbital Space Plane,² the Next Generation Launch System³, the Mars program⁴, and the Next Generation Space Telescope⁵ are all programs that will be pursued in the coming years, and all will require significant fractions of the NASA budget in order to be successfully completed. Therefore, it is unrealistic to assume that significant new resources will become available to fund development of experiments for the ISS. It is also unrealistic to assume that a significant number of experiments will be funded by agencies outside NASA, or by private corporations, at levels higher than during the Shuttle era, where such non-NASA payloads represented a small fraction of the total.

In addition to funding difficulties, NASA also faces the problem of attracting high-caliber researchers to the ISS. Over the years, manned spaceflight's reputation in the research communities for many of the disciplines that the ISS seeks to attract has suffered. In order to live up to its promise, the resources required to develop and fly an experiment on the Station must be commensurate with the scientific return that will be obtained. If performing experiments on ISS

is perceived as impractical and too costly, then the benefits of the Station will never be fully realized, and top researchers at academic and other scientific institutions will never be brought into the program to design and operate experiments.

As construction of the International Space Station (ISS) nears completion, this unique facility has the potential to provide an invaluable platform for the conduct of a multitude of experiments, ranging from fundamental science investigations to technology demonstrations. In order to live up to its promise, the resources required to develop and fly an experiment on the Station must be commensurate with the scientific return that will be obtained. If performing experiments on ISS is perceived as impractical and too costly, then the benefits of the Station will never be fully realized. This thesis applies the set of tools and principles known collectively as Lean Engineering to the Payload Safety Review process, one of the activities that must be satisfied by payloads prior to flying. The goal of this study is to attempt to reduce the required resources needed to fly a payload on the Station.

NASA must therefore find a way, in the face of limited resources, to develop experiments that can exploit the unique capabilities of the ISS in order to allow the station to live up to its potential as a microgravity laboratory. It must also do this while making the experiment development and operations process simpler for the user, reducing the amount of time and complications required to conduct experiments in space.

This work proposes that the tools and methodologies developed over the last 30 years in the field of industrial manufacturing, known collectively as *Lean Thinking*, can be used by NASA to reduce costs, increase output, and increase user satisfaction. While the concepts of *lean* were originally used exclusively on factory floors, they have over the last decade expanded to include all aspects of an enterprise, from relationships with suppliers and subcontractors to customer satisfaction and end-of-life issues. At first glance, these may seem far removed from the problems facing NASA today. However, many of the issues, from reliance on quality assurance to the use of old or obsolete plants and equipment, are in fact quite similar. This document will show that lessons already learned by industry in applying *lean* to their commercial activities can provide valuable insight to NASA.

In order to test this thesis, we will perform a *lean* transformation exercise on the NASA Payload Safety Review process. This process has been developed over the years as a means of ensuring

the safety of the payloads that are to be flown on the Space Shuttle, and now on ISS. It is just one of the many processes that a payload must go through before it can fly. It is well documented, and therefore provides a good starting point for our analysis. It is expected that future efforts will focus on other processes, *e.g.*, crew training, procedures development, payload integration, *etc.*

This chapter provides an overview of *lean*, from both an historical and a present-day perspective. It should be noted that it is not our intent to provide an in-depth presentation of all the concepts and techniques that form part of the theory and practice of *lean*. Instead, we will focus on those concepts that are particularly applicable to the NASA Payload Safety Review process, while providing a brief background of the other topics. Similarly, this chapter will also provide an overview of the ISS, as well as the Payload Safety Review process.

1.1 What is Lean?

In 1990 James Womack, Daniel Jones, and Daniel Roos published *The Machine that Changed the World*⁶. This seminal book established the basis for the methods and techniques that are now collectively known as *lean*. Using the automotive industry as a case study, they showed how some Japanese companies (most notably, Toyota) had evolved from the mass-production concept developed by Henry Ford and widely used by North American and European companies. This evolution had been made necessary because of the severe material and labor shortages present in Japan after World War II. They simply could not afford to set-up large-scale, mass-production facilities like those used by their American competitors. The authors called the new system *Lean Production*. The term ‘lean’ was used in this context because this production method utilized *less* of everything when compared to mass-production: less material inventories, less time to develop a new product, less time to produce a car, less space in the plant, and so on.

The focus of *The Machine that Changed the World* was mainly on production. The authors focused on the activities that took place on the factory floor, although they did consider external influences, such as supply-chain coordination and customer relationship management. In their second book, *Lean Thinking*⁷, Womack and Jones expanded the concepts of lean production to cover other aspects of the *lean* enterprise model. In other words, they moved off the factory floor and into the front-office. In this book, *lean* is presented as a way of thinking about an organization and its processes and is the driving force behind the integration of the individual *lean*

efforts carried out in each one of the activities or processes of the enterprise. Most importantly, they introduced the five basic principles of *lean* thinking:

- Specify the *value* of specific products. A product has value when it satisfies the customer's needs at an acceptable price at the right time. Creating this value is the ultimate reason that an enterprise exists.
- Identify the *value stream* for each product. The value stream is the process that brings a product from its conception to the customer. Analyzing the value stream of a product is a first step in implementing *lean* practices into an enterprise.
- Make value *flow* without interruptions. This implies that interfaces between any two activities in the value stream, whether they are internal or external to the firm, must be minimized and streamlined in such a way that the product does not encounter any resistance (non-value added activities) in moving to the next step in the process.
- Let the customer *pull* value from the producer. This principle simply says that a product does not proceed through an upstream activity unless a downstream step requires it. At the end of the process, it is the customer that ultimately should pull the product from the process. Following this principle eliminates unwanted inventories at the factory or on the sales lot.
- Pursue *perfection*. This process is never static. An enterprise should be constantly looking for ways to improve each step in the process. As one step is improved, it will inevitably produce additional changes in upstream or downstream steps, which in turn can be looked at as opportunities for improvement.

No discussion of the principles of *lean* would be complete without mentioning the search and elimination of *muda*. *Muda* is a Japanese word that means *useless* or *waste*. *Muda* can be found everywhere. In a value stream, each step can be mapped into one of three categories: activities that create value; activities that do not create value for the end user but are necessary (at least for now); and activities that add no value at all. In *lean* thinking, the third type of activities are pure *muda* and must be eliminated. Once this is done, the second type, those that do not add value but are necessary, can be examined for opportunities to improve, or reduce them. Once this is done,

the first type of activities, those that in fact do add value, can be examined for opportunities for improvement.

The most common types of muda as defined by Taiichi Ohno, the creator of the Toyota Production System, are⁸:

- *mistakes* in any step of the production process,
- *overproduction* of parts or final products,
- *excessive inventory* of raw materials,
- *unnecessary processing*,
- *unnecessary motion* of people,
- *unnecessary transportation* of goods,
- and *waiting times*.

A close examination of this list reveals that even though it was originally developed for a large scale manufacturing operation, its application to a much broader, enterprise-level context is readily apparent. For example, excessive inventory is a problem that can plague automobile manufacturers, fast-food chains, or law firms (if one thinks of graduating law-students as inventory).

However, the list is not all-inclusive. In particular, when considering enterprise-level waste, it is important to add two important sources of waste to the ones described above: opportunity costs and structural inefficiencies⁹. Opportunity Cost waste results, for example, from lost opportunities in the marketplace or ill-defined business strategies. Structural Inefficiency waste is produced, for example, by inappropriate organizational structures or bad business model structures.

Recently, the concept of *lean* has continued to evolve and expand in its applications. A recently published book, *Lean Enterprise Value*¹⁰, written by members of MIT's Lean Aerospace Initiative (LAI), attempts to formally apply *lean* in the much-broader enterprise context. One of the key insights the authors have is that an enterprise is an interconnected whole comprised of one or more organizations having related activities, unified operations, and a common business purpose. All these different entities constitute what is known as the *stakeholders*. In order to survive, an

enterprise must create value for each and every one of its stakeholders. The value or benefit one stakeholder is looking for very often conflicts with that of many others as not all the stakeholders necessarily obtain value from the end products delivered by the enterprise. A *lean* enterprise reaches its highest efficiency when all the stakeholders are satisfied by what they obtain from their contributions. In this context, *enterprise* can refer to any complex human activity, including manufacturing, for-profit and not-for-profit organizations, *etc.*

Another important contribution of this work was the identification of specific barriers to *lean* transformation that tend to be present in large enterprises, and in particular within the aerospace industry. These are referred to as *monuments* and *misalignments*. These can be a tangible or intangible. They can be an institution, a factory, or even a cultural or historical mindset. They can be local in their scope (a certain expensive, state-of-the-art, machine that *must* be used regardless of whether it is needed or not in order to justify its purchase), regional (a center or laboratory located in a particular congressional district which must be kept open), or even national or international. For example, throughout the cold war US military strategy called for fighting two full-scale wars. This strategy guided military procurements and deployments. After the fall of the Berlin Wall, US strategy did not adapt right away. This misalignment has only recently been corrected, and the military has begun the process to restructure itself in light of the modern, more complicated multi-threat world.

In summary, *Lean* presents us with a way of thinking that can be applicable to a wide range of human activities, from factory production to large, global enterprises. Its set of five principles can be used to improve the process, reduce the cost, and increase the quality of products and services. By focusing on value to the stakeholders (and its corollary, the elimination of *muda*, monuments and misalignments), *lean* thinking allows improvement efforts to be applied directly where they can do the most good, without sacrificing other value-added features of the end product.

Can *lean* be applied to the NASA Payload Safety Review process? Before we can answer that, it will be useful to briefly describe the ISS program, as well as the station itself.

1.2 The International Space Station

Space stations have featured prominently in many human space mission plans. Although they were seen by many space visionaries as springboards to manned missions to the Moon and other

planets, in the United States, space stations took a back-seat to the Apollo lunar program throughout the 1960's. Apollo did not require a space station to achieve its goal of reaching the moon before the end of the decade. As the moon program wound down, some of the Apollo hardware was modified and used to establish the first long-term US space outpost, Skylab, in the 1970's. Skylab was manned by three separate crews of three astronauts each, who conducted a wide variety of astronomical and microgravity experiments, before the station was abandoned in 1974¹¹.

Originally, the Space Shuttle was conceived as a system to haul personnel and cargo from the Earth's surface to an orbiting space station. However, due to the large budget reductions that NASA absorbed throughout the 1970's, development of a space station was deferred until the Space Shuttle was operational. NASA offered to use the Shuttle to dock with the Soviet Salyut space station, but these discussions collapsed when US-Soviet relations deteriorated after the Soviet invasion of Afghanistan in 1979. As an interim solution, the US teamed with the European Space Agency to develop the Spacelab module for the Space Shuttle. Spacelab greatly increased the capabilities of the Shuttle to conduct microgravity experiments in earth orbit. However, it did not provide for a permanently manned presence.

In 1984 during his State of the Union address, President Reagan called for NASA to build a space station. With this new mandate, NASA began development of what would ultimately come to be known as Space Station *Freedom*. This concept underwent several design modifications in response to changing budget pressures and priorities. In 1993, it underwent a final major redesign effort¹². Significant Russian participation in the program culminated in the present concept, known as the International Space Station, which includes not only the US and Russia, but also Europe, Japan, Canada, and other participants, which provide station hardware, launch services, and astronaut crew members (Figure 1-1)

In the years since this last redesign effort, the ISS has continued to be modified. Most recently, a major issue has developed with regards to the number of permanent crew members that will be stationed at any one time. Originally, the ISS was envisioned to house up to seven astronauts. However, this requires that sufficient life-boats be present, in the form of Russian Soyuz capsules or other craft capable of evacuating the crew to Earth. At this point, only a single, three-seat Soyuz spacecraft is permanently docked to ISS. Nevertheless, the ISS concept has remained remarkably stable over the last decade.



Figure 1-1: The International Space Station at Completion (artist rendering courtesy NASA)

The first element of the ISS was launched in 1998. The European module, Columbus, will arrive in 2005, and the Japanese module, Kibo, in 2006, though this might be delayed in light of the Columbia accident of February, 2003. Once complete, the ISS will provide facilities for both pressurized (located within the astronaut living space) experiments as well as non-pressurized experiments (attached to multiple points on the ISS truss or outer structures).

1.3 The Payload Safety Review Process

Determining whether a payload or component is safe to fly on-board the Space Shuttle or International Space Station is one of the most critical and important functions performed by NASA. All personnel involved in the process are uniquely aware that seemingly benign minor design decisions which might have no impact on a comparable ground-based piece of hardware could have disastrous consequences when operated under the unique constraints posed by manned spaceflight. For example, a sharp edge or a burr left on a metallic component might lead to a small cut to an operator on the ground. The same defect, however, might cause a tear in an astronaut's EVA spacesuit, which could lead to decompression or death.

The primary document which specifies safety requirements for payloads is NSTS 1700.7B, Safety Policy and Requirements for Payloads Using the Space Transportation System, and NSTS

1700.7B, ISS Addendum, Safety Policy and Requirements for Payloads Using the International Space Station. From these governing documents, specific requirements are derived for different hardware systems, depending in part on whether they are crew equipment, payloads or facilities, and on their location on the Shuttle or ISS (external, pressurized, Spacelab, *etc.*) However, the specifications in 1700.7B documents are considered to take precedence in case of any conflicts.

In the case of payloads, the primary derived document is NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements for Payloads using the ISS. This document outlines the essential review process that all payloads must go through in order to be certified to fly safely on the station. In addition, there are numerous other specifications that govern other aspects of payload integration, including environmental interfaces, crew operations, stowage, *etc.* While these do not formally contain safety requirements, they do often govern the design of particular aspects of payloads that may have safety implications. A complete list of all documents that are used in the Payload Safety Review process is attached in Appendix A.

It often comes as a surprise to payload developers that the NASA Payload Safety Review process is not concerned with whether a payload actually achieves its experimental objectives, but only whether it does not pose a risk to the crew or the vehicle. This is not to say that other organizations within and outside of NASA (such as the contracting center that is actually paying for the payload to be designed and developed) are not *very* concerned that the resources and time spent on developing the payload actually produce meaningful scientific results, only that the Payload Safety Review Panel's primary concern is that no hazards are created; whether a payload actually works or not is secondary.

This distinction is important, because while different payloads may have more or less stringent requirements to ensure functionality (such as redundant systems, backups, design margins, *etc.*), they all must meet *exactly* the same safety requirements. In other words, regardless of whether the payload being developed is a multi-billion dollar observatory, or a several hundred thousand dollar crystal-growth experiment, they both must demonstrate that none of their systems or operations can pose any danger to the crew or vehicle, and, if hazards are created, that they are properly controlled.

The Payload Safety Review process is divided into four phases, roughly corresponding to standard milestones in the payload development cycle. In practice, these phases are often combined so

that a payload is only reviewed three times, twice, or even once. At the end of the last phase, any open items are listed in a Tracking Log, which must be closed out before the payload is allowed to fly. These various phases are summarized in Table 1-1 below.

The process begins with identification of the payload system architecture and the major hazards posed by the hardware or operations. These hazards might consist of everything from electrical shock to unexpected release or explosion of pressurized containers. “Long poles”, that is, items that could conceivably require a lot of attention or design effort, are identified. “Non-starters”, items that pose particular problems with regards to safety, are also identified. For example, there are materials that are not safe to fly under any reasonable circumstances due to their toxic or flammability properties. If a payload plans on using these, it is important that the developer be aware of these restrictions early, so that alternatives might be found.

Table 1-1: The Multiple Phases of the Payload Safety Review Process.

<i>Safety Milestone</i>	<i>Payload Development Milestone</i>	<i>Requirements</i>
<i>Phase 0</i>	<i>Conceptual Design Review or Systems Requirement Review</i>	<i>System Architecture identified Major Hazards</i>
<i>Phase 1</i>	<i>Preliminary Design Review</i>	<i>“Long-Poles” identified “Non-starters” identified All hazards identified All causes identified Initial controls identified Initial verification methods identified</i>
<i>Phase 2</i>	<i>Critical Design Review</i>	<i>All controls identified Some verifications performed</i>
<i>Phase 3</i>	<i>Delivery</i>	<i>Final causes and controls identified All verifications performed</i>
<i>Tracking Log</i>	<i>Prior to Launch</i>	<i>Clean up of any control left unimplemented at Phase 3</i>

By the time of the Phase 1 review, all hazards, their causes, controls, and verification methods have been identified. *Controls* refers to the means that will be used to ensure that a particular cause will not occur. For example, a fuse might be used to ensure that current in a circuit is limited, so that the circuit components cannot overheat or fail. *Verification methods* refers to the means that will be used to ensure that the controls are indeed present. In the example of the fuse, a

verification method might be to inspect to ensure that the fuse is indeed present in the final assembled payload.

As the development progresses, the actions described in the verification methods are performed, and the corresponding controls are implemented. This progress is reported in the Phase 2 and Phase 3 reviews. Ideally, all controls are implemented by the time of the final review. In actuality, it is not unusual to have some verification methods that have not been completed at this stage. For example, this would be the case for any verification method that can only be implemented once the payload is installed in the Shuttle. These are listed in a Payload Tracking Log.

For each of these reviews, it is the responsibility of the payload developer to prepare and present a report that describes the payload, its operations, and the associated hazards. Prior to the review, and during the review itself, the Panel will ask questions regarding the material that is presented. The Panel relies on a four-pronged approach for evaluating the risk posed by a payload:

- *Multiple Reviews.* By having up to four reviews, the Panel has an opportunity to revisit the payload several times. Safety is a system property that emerges over time and can change in unexpected manners even if relatively minor changes are made to the overall hardware. This is especially true when software is used to ensure functionality or to control hazards¹³. Multiple reviews decrease the chance that these changes go unnoticed.
- *Drill-down.* Although Panelists cannot possibly be experts in all areas of engineering and science, they can draw upon a very broad experience base at the Johnson Space Center. In addition, in evaluating a payload, the Panel often will “drill-down” into one or two particular areas with which they may be very familiar, in order to get a sense of the capabilities of the payload development team. If they find that the team is lacking, they might in turn bring in additional experts to evaluate other areas. If the team answers the questions competently, then the Panel will be more willing to trust the developer’s engineering judgment in other areas.
- *Relationship with developer.* If the Panel has experience with a particular payload development team or with the engineers on it, then this experience will influence their questions on any new payload that the team brings forward. This can be either

a negative or positive impact, of course. Mutual trust between the Panel and the payload development team is important.

- *Precedent, legacy, and reflowed hardware.* Hardware that is reflowed, and that functioned properly the first time it flew, is viewed differently than new hardware going through the process the first time. In fact, a much shorter, streamlined approach for reflowed hardware has been recently implemented.

The major tool used for conveying payload information from the development team to the Panel is the Payload Hazard Report, an example of which is shown in Figure 1-2. The report is divided into six main sections. The top lists the name of the hazard, the governing paragraphs in the controlling documents, the number, and whether it is a catastrophic (death, loss of vehicle) or critical (injury, damage to vehicle) hazard. It also provides a brief description of the hazard itself.

The next section lists the possible causes of the hazard. One hazard might have multiple causes. In the example shown, the two causes that are listed are improper design or improper material selection. Both of these causes could lead to rupture or leakage of a pressure system. In the following section, each of the causes that have been identified are associated with controls. In identifying proper controls, the question is asked: How is the hazard cause going to be prevented from happening? Depending on the type of hazard, and whether it is critical or catastrophic, there may be requirements for multiple controls. Each control must have a way of verifying that it is actually working. In the example shown, the hazard cause of “improper design” is controlled by using the appropriate factors of safety, as well as selecting pressure vessels in accordance with an agreed-upon standard. These controls in turn are verified by analyzing the design for compliance, proof-testing the hardware, performing an independent inspection, and doing a leak test.

As can be seen, a single hazard branches out into multiple causes, which in turn branch out into multiple controls and finally verification methods. The numbering of the items of the various sections reflects this tree-like structure, allowing each verification method to be traced back to its “parent” control.

The final two sections of the report indicate the status of the verification method (whether it has been completed or not) and provide room for the appropriate signatures for the Panel and the payload developer.

Ideally, once the Hazard Reports are presented in Phase 1, the only changes that are made are to the status of the verification methods. Of course, this rarely happens. It is normal that as a design progresses, new hazards, controls or verification methods might be identified, substituted, or replaced. The Panel expects this. The expectation is, however, that the major items are all identified early in the process, to allow the Panel plenty of opportunity during the multiple reviews to truly determine the safety of the payload.

1.4 Summary

This chapter presented an overview of the three systems that are the focus of our analysis: Lean Engineering, the International Space Station, and the Payload Safety Review process. Obviously, much more could be written and presented on each of these three topics. Significant further information can be found in the referenced publications. Hopefully, the overview will now allow us to move into how these three topics can be synthesized to provide more value to payload developers as they integrate their payloads for flight on-board the ISS, while providing higher levels of safety.

In Chapter 2, we will begin the analysis by determining the state of the present process. The value stream will be mapped out. In addition, limitations present in the existing system with regards to its ability to transform to a *lean* method of operation will be identified. In Chapter 3, a different analysis will be presented. There, a comparison of the existing Payload Safety Review process with other processes that have already undergone *lean* transformation will be presented. Similarities and limitations between the processes will be identified, with the hope of gaining insights that would help in implementing *lean* principles into the NASA Payload Safety Review process. Both of these methods of analysis will be validated by comparing them to responses and data obtained from stakeholders in the existing Payload Safety Review process. This data is presented in Chapter 4.

Finally, in Chapter 5, all the analysis, data, and insights are brought together to design a new “desired state” for the process. Specific detailed recommendations are presented to allow the *lean* transformation of the process. A *lean* value stream is presented, and quantifiable metrics are used to demonstrate benefits of the proposed process over the one that currently exists. Finally, the report concludes with a series of recommendations for implementation of the *lean* process in the area of payload safety, as well as for extending this analysis into other areas of payload integration.

2. PAYLOAD HAZARD REPORT		No.
FUNCTION		CCU-F-12
SUBSYSTEM		PHASE
Cell Culture Unit		I
HAZARD CATEGORY	HAZARD CATEGORY	DATE
Pressure, Structure	Fire, Explosion	13-Feb-99
DESCRIPTION		
Water Leakage or Rupture and/or Explosion of Pressure System		
NSTS 1700.7B ISS ADDENDUM para 200.3, 200.4a, 201.3, 202.2c, 208.3, 208.4, 208.4a, 208.4c, 208.4d, 209.1a		
		HAZARD CATEGORY
		<input checked="" type="checkbox"/> Catastrophic (rupture)
		<input checked="" type="checkbox"/> Critical (leakage)
INCIDENTAL HAZARDS		
Rupture/explosion of gas supply (O ₂ , N ₂ , and CO ₂) and liquid cooling pressure system results in significant damage to/loss of orbiter, ISS, crew or other payloads.		
HAZARD EFFECTS		
1. Inadequate design strength to withstand MDP and other loading environments..		
2. Improper materials selection and processing including usage of stress corrosive sensitive materials.		
(continued)		
HAZARD PREVENTION		
1.1 Design fluid systems to withstand MDP FOS \geq 2.5 (regulators, orifices, filters and valves), FOS \geq 4.0 (lines and fittings) and MDP FOS \geq 2.0 (pressure vessels).		
1.2 Select pressure vessel in compliance with MIL-STD 1522A.		
2. Select materials in accordance with MSFC-SPEC-522B, table 1 and MAPTIS.		
COMPLIANCE REQUIREMENTS		
1.1.1 Analyze design to verify compliance with required FOS.		
1.1.2 Proof test of flight hardware pressurized system.		
1.1.3 QA review of pressure system to ensure functionality, independence and installation of flow control devices.		
1.1.4 Leak check of flight hardware pressurized system.		
1.2.1 QA review of pressure vessel certification documentation		
1.2.2 QA inspection of flight hardware prior to delivery		
2. Submit materials list to JSC/EM2 for materials certification.		
STATUS OF VERIFICATION		
1.1.1 Open		
1.1.2 Open		
1.1.3 Open		
1.1.4 Open		
1.2.1 Open		
1.2.2 Open		
2. Open		
APPROVAL	PAYLOAD ORGANIZATION	STS
PHASE I		
PHASE II		
PHASE III		

ISCT Form 5470

Figure 1-2: Example of a Payload Hazard Report

Chapter 2: Transition to Lean

The MIT Lean Aerospace Initiative has developed several tools to assist enterprises in transitioning their processes to a *lean* footing. For example, they have developed the Lean Enterprise Model (LEM), which helps in understanding the key *lean* principles and practices as they apply to a particular organization. These principles and practices, as they apply to the Payload Safety Review process, were outlined in Chapter 1. Another tool that is available is the Lean Enterprise Self Assessment Tool (LESAT), which allows an enterprise to evaluate where they are and how they are progressing in their transition to *lean*. LESAT is a useful tool to implement both at the start of the transition as well as at various points during the process, as it provides a snapshot of the current state.

In this chapter however, attention will be focused on defining the existing state of the process we are attempting to transform, and obtaining insights to issues and unique characteristics of the process that must be considered. Otherwise, this analysis would run the risk of not being able to appreciate aspects of the Payload Safety Review process that might appear to be “wasteful” (*muda*) to space-naïve observers.

The tool that will be used to assist in defining this existing state of the process is one that has been developed to help guide enterprises in their *lean* transitions. This transition is unique to each enterprise. A large airplane manufacturer with a billion-dollar production line will not face the same issues as a government agency whose major product is paper reports and presentations. However, the MIT Lean Aerospace Initiative has developed a Transition to Lean (TTL) Roadmap, which allows each enterprise to ask itself the right questions to begin this process, as well as providing insight that can help in defining the desired final state for the process in question¹⁴. The TTL will be used in this chapter both to help identify the existing state of the process as well as to gain insights into potential problems and concerns that may pose difficulties in transforming the process to a more *lean* footing.

Figure 2-1 shows this TTL Roadmap. In the remaining sections of this chapter, we will go through the various steps and attempt to apply them to the NASA Payload Safety Review process.

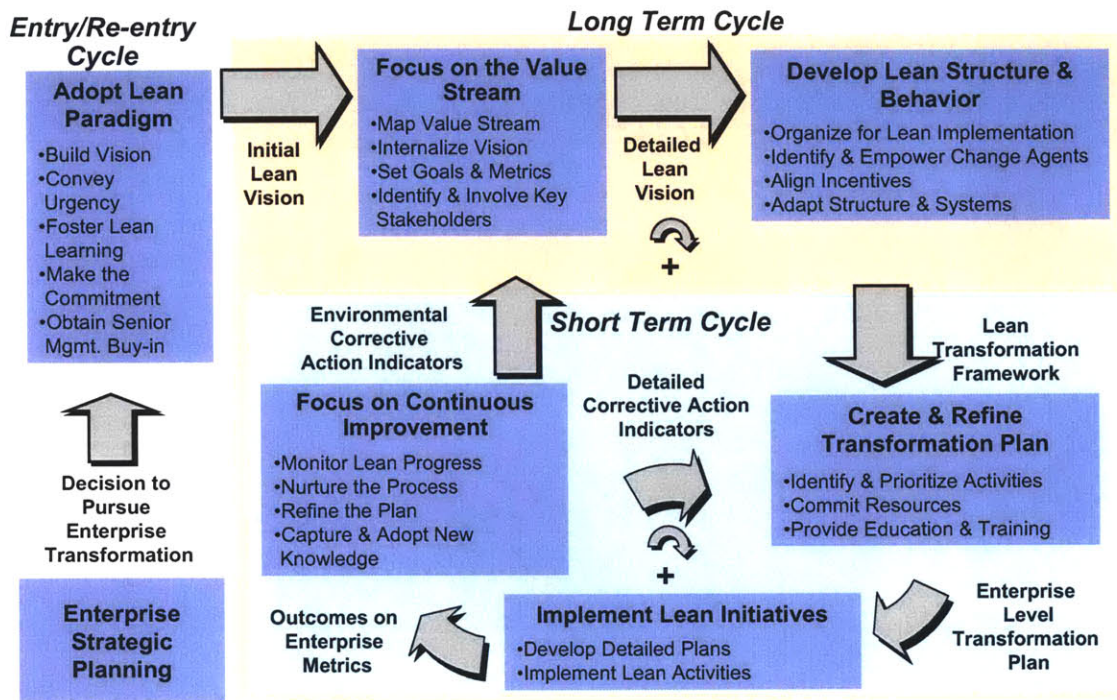


Figure 2-1: The Transition to Lean Roadmap (courtesy, MIT Lean Aerospace Initiative)

2.1 Strategic Planning and Adopting a Lean Paradigm

Any enterprise-level transformation of the scale envisioned by TTL must start at the top. While it is true that ultimately buy-in from all levels in an organization must be obtained, the process cannot start without leadership at the very upper levels of the enterprise. This commitment is expressed in tangible form by providing opportunities for learning about *lean* principles and practices, first to the key personnel in the organization and ultimately, to all stakeholders.

This critical initial step poses a problem for the NASA Payload Safety Review process. It is of course possible to obtain a commitment and buy-in of the senior NASA officials responsible for the Payload Safety Review process. In fact, at a meeting with Mr. Skip Larsen, the NASA PSRP chairman, it was clear that the PSRP has already implemented many *lean* principles, even without formally using that name. He and his staff were very supportive of continuing and expanding the process.

In the case of the individual payload developers, obtaining this commitment may be more problematic. On the one hand, it is the payload developers themselves that have the most to gain by a more efficient Payload Safety Review process. Resources for development of payloads are always in tight supply. Any savings obtained by a *lean* process would be welcome. This is especially true if the payloads are being developed in a large organization, where the benefits of a *lean* transformation can be enjoyed by multiple projects, and, conversely, any start-up costs associated with the transformation activities can be spread out.

In the case of smaller developers (*e.g.*, small businesses or university laboratories), who typically have very limited resources, even a small amount of savings from a *lean* process could have a significant impact. Such a transformed process would yield immediate benefits, and there should be no problem in obtaining commitment from these small developers. However, these small organizations may require additional outside support in order to properly integrate themselves into the *lean* process, since they typically do not have any additional resources to devote to transformation activities. For example, small organizations might require assistance in training their personnel or in offsetting start-up costs associated with obtaining information technology that properly interfaces with the new *lean* process. Many of these issues have been identified in a recent study that focused on the problems faced by large companies that attempt to impose *lean* principles on their small business suppliers¹⁵. In many ways, that is a similar situation to the one being studied here.

A related problem stems from the large number of payloads being developed. Presently, the JSC PSRP has almost 400 payloads either in-flight or in development. While undoubtedly there are some teams developing multiple payloads, it is still likely that the number of payload developers easily number in the hundreds. This number will only increase as the ISS transitions from its assembly to its operational phase. These organizations cannot easily be consolidated into “first tier” and “second tier” suppliers, as is often done when *lean* is applied to a traditional manufacturing process. For example, in the automobile industry, a first-tier supplier might deliver complete brake assemblies to the manufacturing plant. In turn, they receive components for the assemblies from second-tier suppliers. The production process is streamlined as the number of suppliers that the manufacturer has to deal with directly is reduced (Figure 2-2). The manufacturer can work with the first tier suppliers in implementing a *lean* transformation and they in turn will flow down the lessons-learned to the other suppliers at the lower tiers.

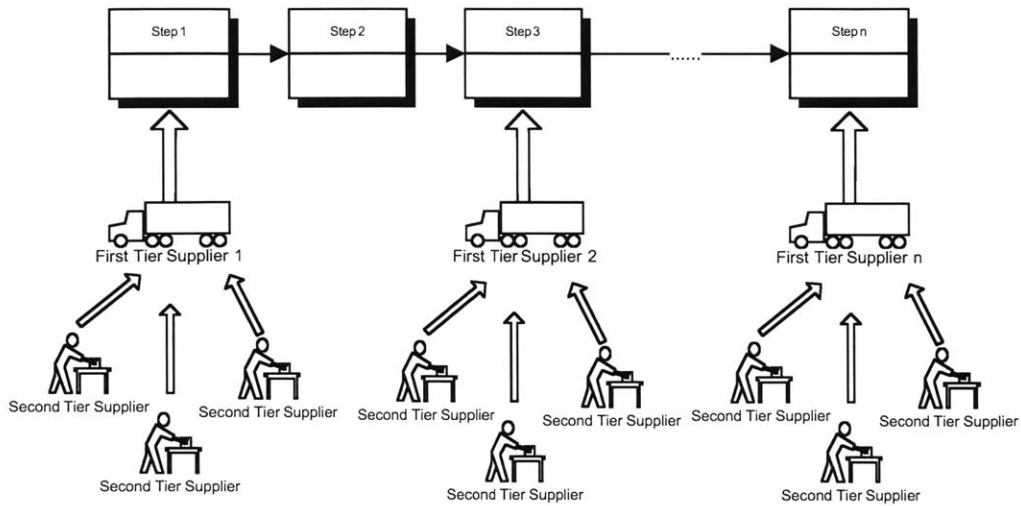


Figure 2-2: Tiered Suppliers simplify the Product Flow

This will not work in the case of the NASA Payload Safety Review process. The primary product of this process is not a payload or a tangible item but is in fact information, and this information must be provided at various steps in the process flow. It is information that is passed from the payload developers to NASA, and it is information that is ultimately processed at the various steps. This makes it very difficult to consolidate payloads in a hierarchical, first-tier-second-tier structure. The payloads themselves will simply be too diverse to allow for this sort of consolidation (Figure 2-3). The PSRP cannot work with only a small number of developers and expect the lessons-learned to flow down to the others. The resources required for this can be significant. This problem will be revisited in Chapter 5 when specific recommendations are made to transform the Payload Safety Review process.

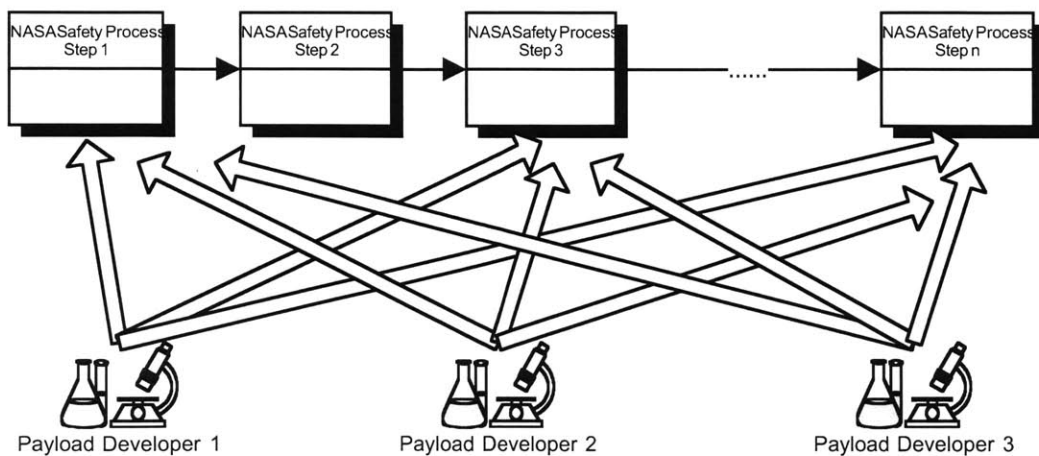


Figure 2-3: Payload Developers Cannot be Easily Organized Hierarchically

2.2 Focus on the Value Stream

The first step in the Transition to Lean is to identify each element of the chain of events that make up the process. By focusing on this Value Stream, it will allow each step to be evaluated with regards to whether it is value-added, wasteful but necessary, or pure waste or *muda*.

2.2.1 Value Streams

The first issue that must be faced is that there really is no single process that can be mapped. Depending on the size and complexity of the payload, as well as how it is being developed (whether it is internal to NASA, a Department of Defense payload, commercial, *etc.*), the safety process can be modified and tailored. This flexibility in the process can be a positive factor, as it allows tailoring which can be used to prevent *muda*. However, it does complicate the analysis.

For this reason, three examples of the Payload Safety Review process will be presented, corresponding to three different levels of complexity in the payload design. This is not meant to be a new overall classification system for all payloads; NASA already has numerous such systems. They tend to differentiate the payloads based on overall complexity in their design, integration, and operations. The three examples presented below are simply illustrations of three different payloads and the different process they have gone through in order to satisfy the safety requirements:

- *Type 1: Small, internal, low complexity.* This is typically payload developed in less than two years that operates within the pressurized volume of the Station or Space Shuttle. There are no major or significant hazards associated with it, but it does have one or two unique characteristics that merit discussion and review by the Safety Panel. The steps and the estimates for the durations of each task are based on the Synchronized Position, Hold, Engage, Reorient Experimental Satellites (SPHERES) program, which is scheduled to fly to ISS in 2004. While cost does not necessarily correspond to safety and complexity, experiments of this category typically range in cost from \$500,000 to \$4,000,000.
- *Type 2: Complex, internal, large amounts of crew interaction.* This is an internal payload which has significant crew operation and interaction. It relies on crew observation and procedures for control of some of its hazard causes. It is integrated directly

with the NASA Johnson Space Center, without an intermediary contracting center or agency. The steps and estimates for this type of payload are based on the Middeck Active Control Experiment (MACE) which flew on STS-67 in 1995. Payloads of this type can range in cost from \$3,000,000 to \$10,000,000.

- *Type 3: Complex, facility-class payloads.* This is a payload designed for multiple flights and for use by many different Principal Investigators. There are several major significant hazards. It is developed under contract with a NASA field center or other agency. There is significant oversight, including intermediary reviews prior to the formal Payload Safety Reviews. Estimates for this type are based on the Cell Culture Unit, which is scheduled to fly to ISS in 2006. Payloads in this class can cost \$8,000,000 or more.

The three examples are summarized in Table 2-1 below: Note that even though all three are internal payloads, external payloads do not necessarily pose additional complications. There can be very simple external payloads that are contained inside pre-fabricated canisters and attach in the Space Shuttle payload bay, and very complex external payloads that are released from the Shuttle and free-fly in orbit. We chose the three payloads in the table as representatives simply because data was available for those three specific programs.

Table 2-1: Summary of Payload Examples Used for Value Stream Mapping

Type of Payload	Characteristics	Typical Cost (Millions)	Example Payload
1. Small, Internal, Low Complexity	Few Hazards, direct integration with NASA JSC	.5 to 4	SPHERES.
2. Complex, internal, large amounts of crew interaction	Crew interaction for control of hazards, direct integration with NASA JSC	3 to 10	MACE
3. Complex, facility-class payloads	Many hazards, significant contracting-center oversight	8 +	CCU

For each type of payload example, the value stream can now be drawn from the perspective of the payload developer. Estimates for the duration and labor required for each step in the value stream will be based on the example payload for each type. These estimates do not include labor provided by the NASA Payload Safety Review panel or other outside organizations. In each example, the values are based on actual events or, for events that have not yet occurred, on estimates using other, similar payloads as a basis. The number of people listed is meant to

indicate total manpower over a given duration. In other words, if a task requires two people for 2 days, it may be that in reality, four people are needed for 2 days, but only at half-time.

Even though for each type of payload real examples were used in determining the value stream, for some steps in the value stream it was felt appropriate to list ranges for time and labor, as opposed to single values. These ranges are intended to indicate variations depending on the complexity of the payload. Within each of the three types discussed, as the payload becomes more complex, the main impact tends to be on the hazard, control, and methods identification steps, as well as on verification. The time needed for preparation of the review materials, as well as for the review themselves, is not assumed to vary, at least to the level of detail in this analysis.

Figure 2-4 shows the value stream for payloads similar to those in the Type 1 category: small, low complexity payloads with relatively few hazards. If the elements in the figure are compared to the generic description of the process from Chapter 1, it is seen that this payload does not have separate Phase 0, 1, and 2 reviews, and instead has a combined review at approximately the timeframe that would correspond to a Phase 2 review. This is done because the payload does not have major, non-standard hazards or controls. It is not using any materials that would pose offgasing or toxicity problems. For the payload that was used as an example for this figure (SPHERES), there was one major hazard relating to the use of compressed gases. However, the gas was stored in such a way, and the quantities were low enough so as not to pose a major risk or concern to the Payload Safety Review Panel. More details on the SPHERES payload are presented in Section 4.2.

Figure 2-5 below shows the value stream for Type 2, a slightly more complex payload. This payload is also internal, but it requires significantly more crew interaction and training. In fact, it relies on the crew members' observations as controls for several of its hazard causes: The MACE payload, on which this figure is based, used a two meter long articulating structure as a testbed to measure the performance of structural control algorithms on flexible non-linear structures whose dynamics change in microgravity. The test article exhibited large amplitude motions, posing a collision hazard with the crew or with other payloads inside the Space Shuttle. This value stream shows a payload for which all four phase safety reviews were supported. Even though the Phase 0 review is often skipped, this review was conducted in this case because of the collision hazard, as well as managerial programmatic requirements,

Figure 2-6 shows the value stream for the most complex payload in our set of examples. This is a complex, facility-class experiment that will be re-flown many times on-board the International Space Station. The example used in developing this value stream is the Cell Culture Unit (described in more detail in Section 4.1). The payload is being developed by a private contractor under contract with a NASA field center. For this reason, prior to the official safety reviews held by the NASA Payload Safety Review Panel at the Johnson Space Center, intermediary reviews must be held with safety representatives from the field center, in order to obtain approval to submit the safety package to the NASA Payload Safety Review panel. This is required because the contracting center wishes to review all submittals in order to ensure that they contain the proper information and meet all their requirements. Steps associated with this activity will be examined closely in Chapter 5.

In addition, the value stream also shows a “Delta Phase 1” Safety review that was conducted because several hazards were not properly addressed at the Phase 1 review. While the expectation is that all hazard reports will be signed at the review, with the increase in complexity of the payload the likelihood that a delta review will be required for at least some of the phases is increased. For this reason, it has been kept in the value stream as a typical event for this type of payloads. Clearly, eliminating these delta reviews would reduce the time and resources required for the process. This will be examined in Chapter 5.

The value streams for the three different types of payloads can be used to help identify those steps that clearly produce value, as well as for those steps which are clearly *muda*. At this stage, it is somewhat difficult to do this without some additional insight that will be obtained as we progress through the Transition to Lean Roadmap, as well as from the comparative analysis that will be presented in Chapter 3 and the stakeholder interviews in Chapter 4. Once this is done, we will revisit the definition of value for the Payload Safety Review Process and draw a *lean, muda*-free value stream in Chapter 5. Nevertheless, some preliminary observations can be made: For example, for all three types of payloads one initial place to look for *muda* is in the periods between submittal of the packages and the conduct of the review themselves. Obviously, part of this time is required in order to review the submitted documents. However, it is quite unlikely that the full 60 days (or 45 in the case of Phase 0) are used reviewing the submittals. The process is set up to give the Panel time within that 60 day span to review the documents and identify any “long-pole” issues that may come up. This would allow the payload developer an opportunity prior to the

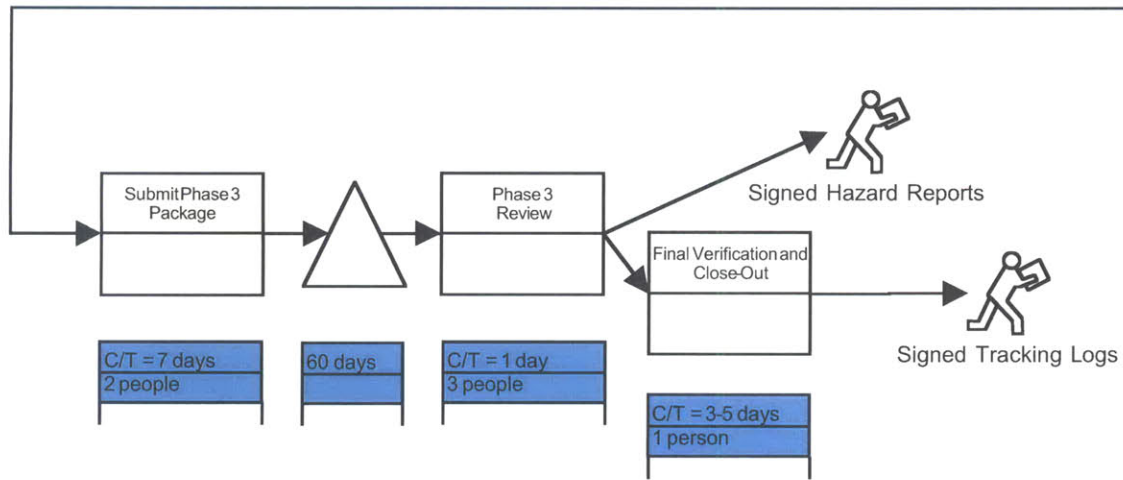
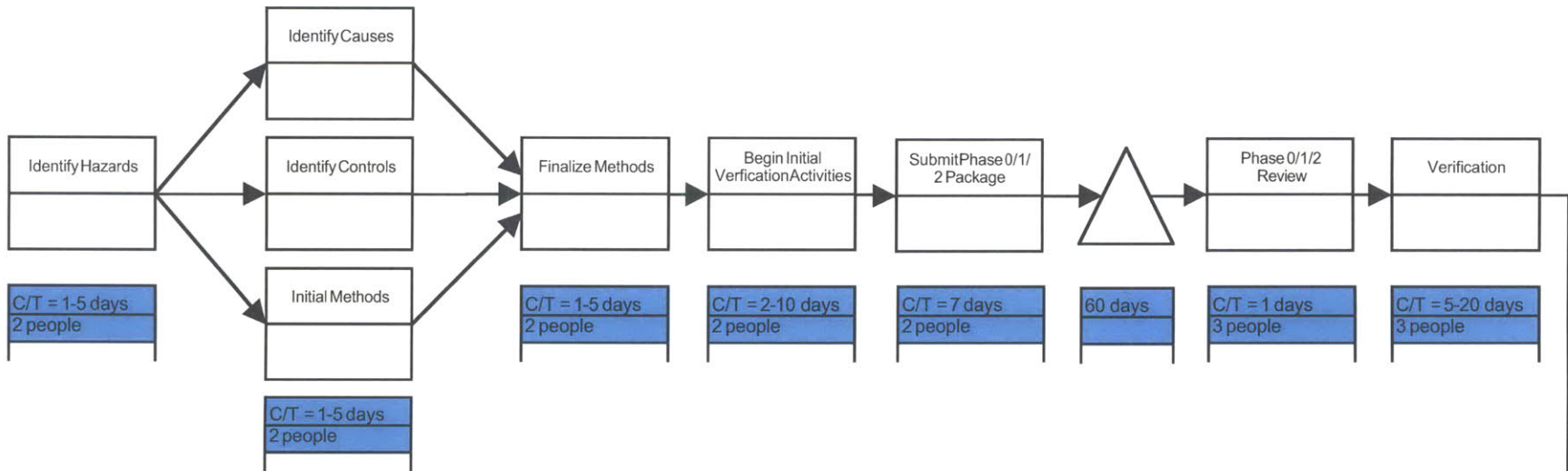


Figure 2-4: Type 1 Payload Safety Review Value Stream

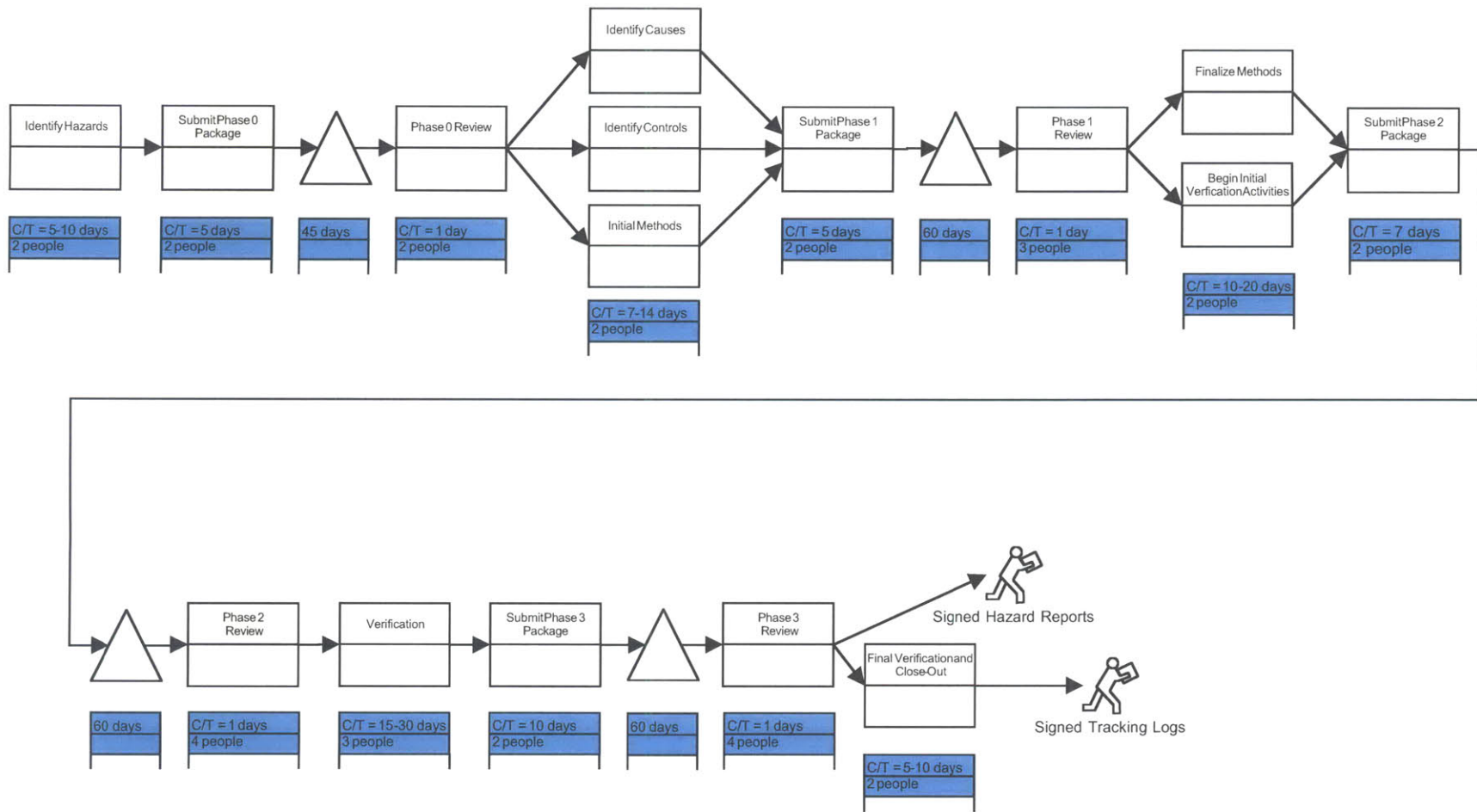


Figure 2-5: Type 2 Payload Safety Review Value Stream

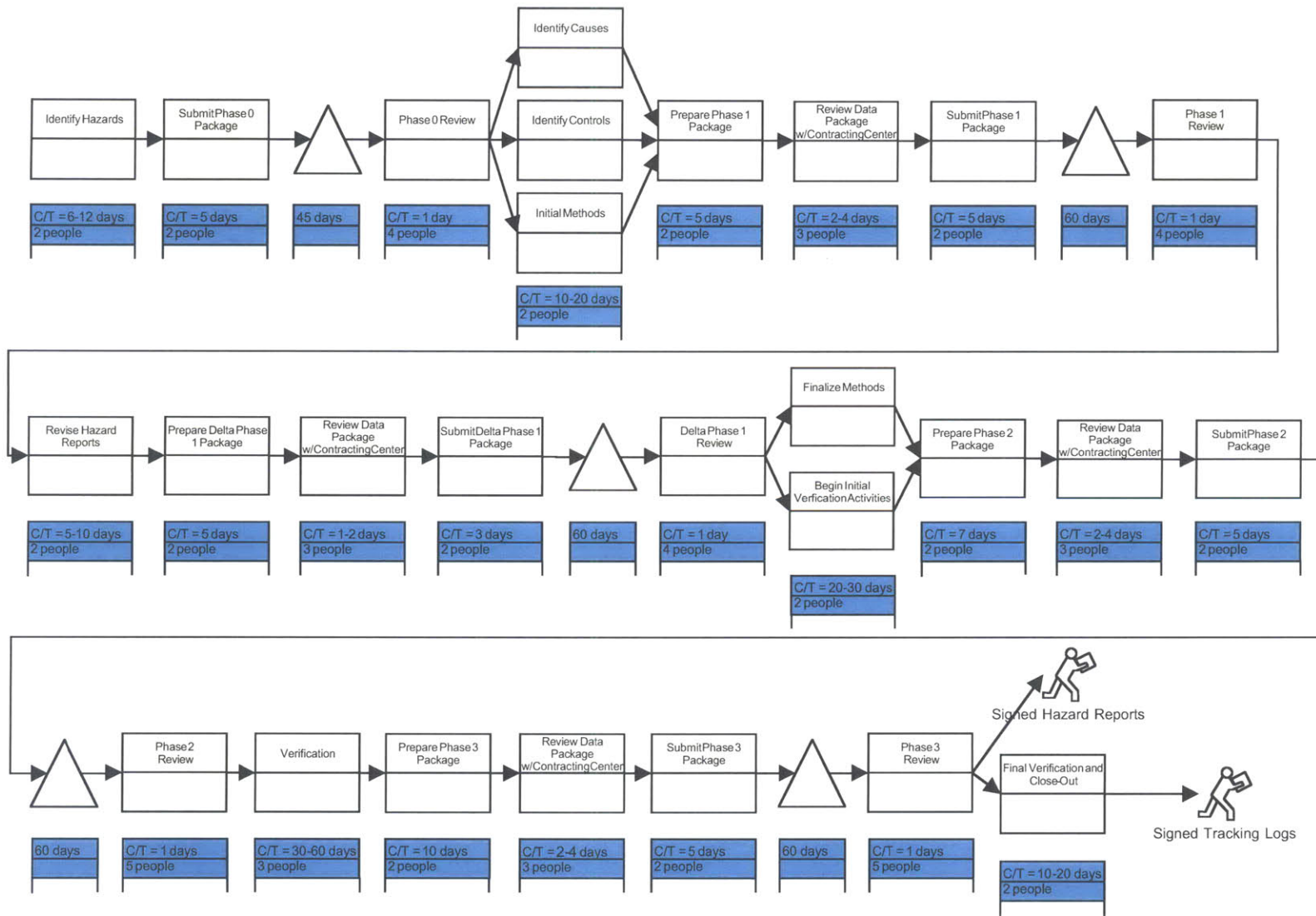


Figure 2-6: Type 3 Payload Safety Review Value Stream

review to address these issues. Shortening this review time by increasing the quality of the submittals or identifying long-pole issues prior to submittals would have a significant impact on the length of the process. Of course, this does not preclude us from looking for *muda* in the other steps as well, such as reducing the overall number of reviews.

It should be noted that the three value streams presented could be drawn in significantly more detail. Within each step, there are numerous activities that must take place. For example, in order to properly identify hazards, the various subsystems, ranging from power, to materials, to operations, must be analyzed thoroughly. Feedback must be given to the appropriate engineering staff in order for safety-required modifications to be properly incorporated. The durations listed in the value streams do not take into account the fact that these other design activities must also occur between the phases. This level of detail was not included here because it varies too much from payload to payload and would actually obscure some of the basic characteristics of the process that we are trying to modify. However, a more detailed list and short description of the types of activities that must normally occur in a typical Payload Safety Review process are given in Appendix B.

Table 2-2 shows the durations and labor needed, as well as waiting time, for each of our three examples. Minimum and maximum values are calculated by taking the minimum and maximum for each step in the value stream for which a range was specified. Two things should be noted in this table. First, even for the simplest payloads, the cost of satisfying the NASA Payload Safety Review process is not insignificant. Even with little complexity, the labor required can easily exceed 100 person-days. Second, the waiting times rise enormously as the complexity of the payload increases. This is directly due to the additional reviews that must be supported.

Table 2-2: Summary Table for Process Durations and Required Labor

<i>Type of Payload</i>	<i>Min Duration (days)</i>	<i>Max Duration (days)</i>	<i>Waiting Time (days)</i>	<i>Min Labor (person-days)</i>	<i>Max Labor (person-days)</i>
Type 1	149	186	120	62	149
Type 2	298	340	225	166	265
Type 3	428	506	285	335	528

It is possible to graph the information from the value streams as a function of payload complexity. To do this, it will be assumed that complexity within each type of payload varies linearly with cost. In other words, the more complex, the more expensive. We realize that this is

not always necessarily true, but it will be used here as an approximation. With this in mind, for each step in the value streams for which a range is specified, a linear extrapolation is used between the cost ranges specified in Table 2-1. Figure 2-7 shows the duration required to complete the process for each payload type, while Figure 2-8 shows the required labor.

It should be noted that for both figures, we can note two things: First, there is overlap between the curves: the most complex Type 1 experiment can cost more than the least complex Type 2 experiment and yet require less time to complete the NASA Payload Safety Review process. This is simply due to the fact that some experiments can be expensive but relatively straightforward from a safety perspective. Others can be completely opposite.

Second, the curves do not match up. In other words, the least complex Type 2 experiment takes longer and requires more manpower than the most complex Type 1 experiment. This is not surprising. The differences in the value streams between the two types are mostly due to the additional reviews (and the associated waiting times). Regardless of complexity, if additional reviews must be supported, then the process will take longer and require more labor. In addition, for Type 3, significant additional labor is needed to support the contracting organization reviews, which is not present in Type 2 and contributes to the gap between the two curves.

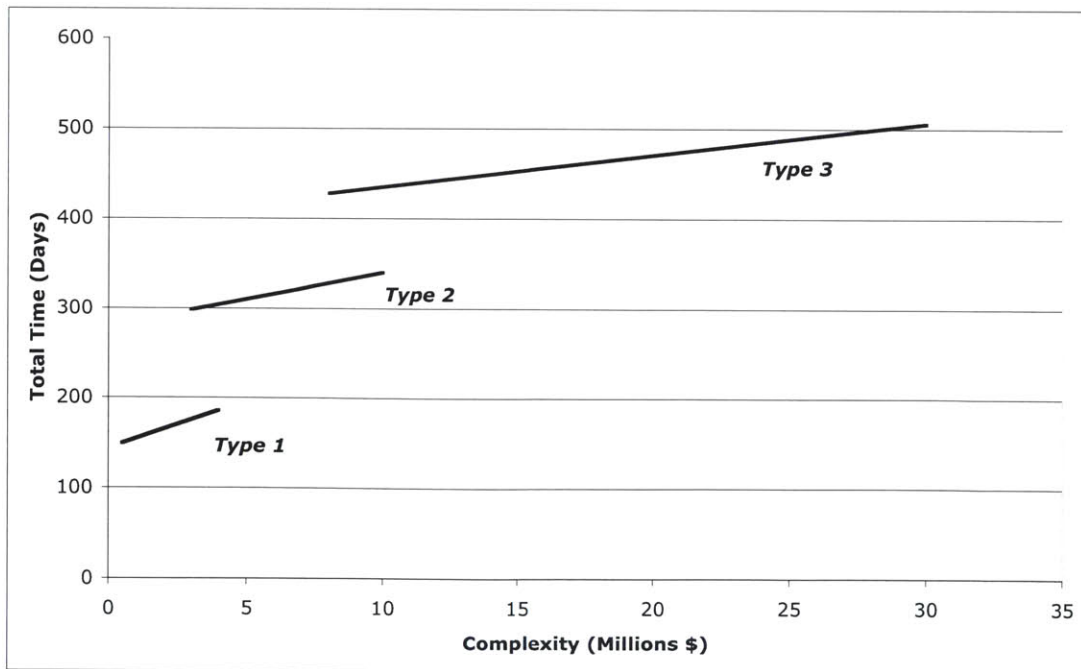


Figure 2-7: Total Time Required to Complete the Payload Safety Review Process

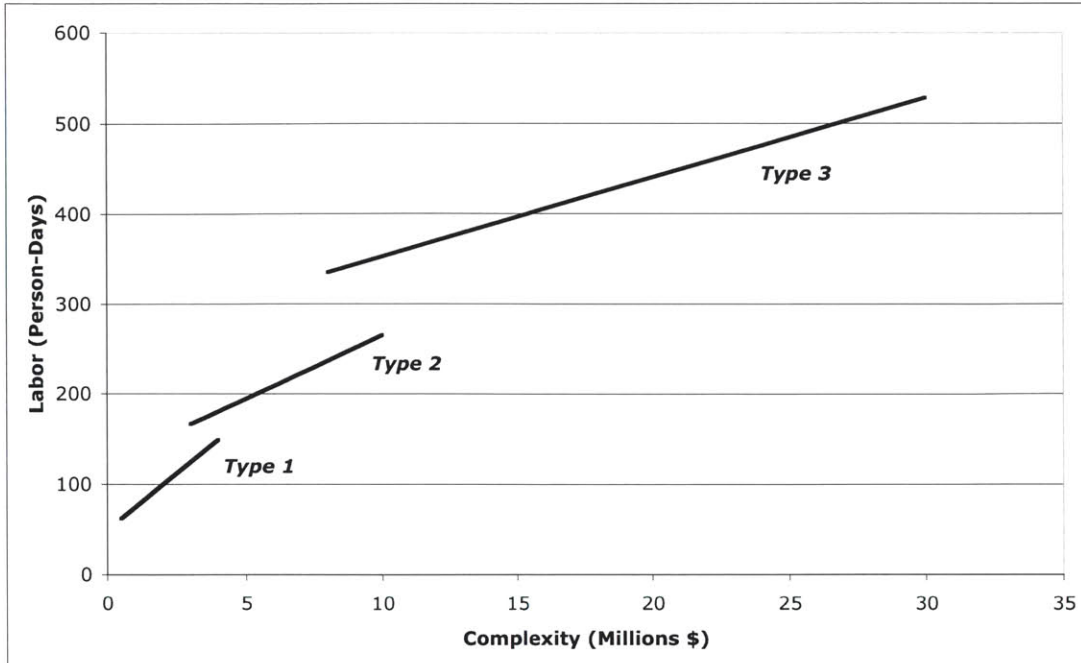


Figure 2-8: Total Labor Required to Complete the Payload Safety Review Process

Please note that the figures *are not* meant to allow the reader to pick a point on the x-axis corresponding to the cost of their payload and immediately know the labor and duration required to satisfy the Payload Safety Review process. These are merely illustrative examples, based on three separate, unique payloads. Each payload is different, and each payload must be evaluated individually in order to properly determine which steps in the Payload Safety Review process it will follow. The examples merely serve to show the trends in the cost and duration of the process as payload complexity increases.

2.2.2 Stakeholders

As was mentioned earlier, the value streams in the previous sections were drawn from the point of view of the payload developer. However, one key component of *lean* thinking at the enterprise level is to ensure that *all* stakeholders are properly identified, and that their needs are addressed. This concept has recently been pursued in much more detail within the MIT Lean Aerospace Initiative¹⁶.

The table below shows the various stakeholders involved in developing a payload for ISS, along with their primary and secondary needs. Note that we have divided the payload development activity into the principal investigator (PI) and the primary contractor, since typically the hardware

fabrication is not performed by the PI. Safety of the payload is arguably a primary or secondary need for all the primary stakeholders. The table should not be interpreted to imply that a stakeholder would sacrifice a secondary need for a primary one. It simply reflects what the primary concern of an individual stakeholder might be. However, for a successful payload, *all* the needs must be adequately addressed.

Table 2-3: Stakeholder Summary Table

<i>Stakeholder</i>	<i>Primary Need</i>	<i>Secondary Need</i>
<i>Principal Investigator</i>	<i>Scientific Return</i>	<i>Safety of Payload</i>
<i>Primary Contractor</i>	<i>Financial and Technical Performance</i>	<i>Safety of Payload</i>
<i>Taxpayer (Society)</i>	<i>Financial and Technical Performance</i>	<i>Safety of Payload</i>
<i>Astronauts</i>	<i>Safety of Payload</i>	<i>Technical Performance</i>
<i>NASA Safety Panel</i>	<i>Safety of Payload</i>	<i>Technical Performance</i>
<i>Tech. Community</i>	<i>Scientific Return</i>	<i>Safety of Payload</i>
<i>Funding Agent</i>	<i>Financial and Technical Performance</i>	<i>Safety of Payload</i>
<i>Shareholders</i>	<i>Return on Investment</i>	<i>Potential for Future Work</i>
<i>Employees</i>	<i>Salary and Job Stability</i>	<i>Potential for Future Work</i>
<i>Suppliers</i>	<i>Payment</i>	<i>Potential for Future Work</i>

2.2.3 Focus on the Value Stream: Summary

Several different issues were raised in this section, and before moving on to the rest of the steps in the Transformation Roadmap, it is useful to summarize them here:

- Opportunities for applying *lean* principles in the NASA ISS Payload Safety Review process appear to exist, in particular with regards to the steps involved in reviewing the submitted documents.
- Decreasing the likelihood of “long-poles” or surprises being found in the submittals might allow reduction in the required review time and reduce the likelihood of “delta” phase safety reviews.
- Intermediary reviews conducted in addition to the reviews required should be examined closely with regard to the value they bring to the process.
- Safety of the payload is a high-level need for all the primary stakeholders involved in the development and use of the hardware.

2.3 *Develop Lean Structure and Behavior*

Once the value stream and the stakeholders are identified, the next step in the *lean* transformation is to begin the organization of the enterprise to assist in the transformation. Some of the steps that might be involved here include identifying key personnel who could act as change agents in the process, aligning the various information and other systems to permit *lean* transformation, and aligning incentives for the people involved to reward successful implementation.

Once again, the unique structure of the NASA Payload Safety Review process poses problems in the implementation of this step. While it is certainly possible to align the resources under direct NASA control to permit *lean* operations, it is much more difficult to implement the same transformation with the myriad of payload developers that are the organizations directly responsible for the design and operation of the payloads. The same issues identified earlier in Section 2.1, which described how the size, diversity, number, and capabilities of the payload developers limited their ability to adopt a *lean* paradigm come into play here as well. While developers could in principle significantly benefit from *lean* transformation, they may simply not have sufficient resources, whether they be financial, manpower, or time, to adequately support it.

Another limitation regards the alignment of incentives to reward the adoption of *lean* practices. NASA, as a mostly civil-service organization, is limited with regards to its incentives and human resource practices. It is simply more difficult to transfer or realign personnel within a government organization than it is at a private company. Similarly, more constraints exist with regards to monetary or other rewards.

Both of these limitations can be overcome. What is needed is a way to streamline the interfaces between the payload developers and the NASA Payload Safety Review process, and to provide the payload developers with the resources needed to properly support the new *lean* systems. In addition, this must be done in such a way that properly rewards steps taken towards the adoption of *lean* behavior, and allows the removal of roadblocks to the transformation.

2.4 *Create and Refine Transformation Plan*

Once change agents have been identified and incentives aligned, the process is now ready to enter a short term cycle where the actual *lean* transformation takes place. The first step in this process is

to develop a transformation plan and to provide the resources, including education and training for all personnel, needed to accomplish it.

As mentioned in Section 2.1, the NASA Payload Safety Review Panel has already begun a wide array of activities aimed at streamlining and simplifying the process for payload developers. These activities have included the consolidation of Hazard Report forms, the extensive use of video, teleconferencing, and web-based facilities to reduce travel costs, and the elimination of some reviews for less complex payloads. Presently, they are performing a review of NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements document, with the goal of reducing or eliminating requirements that do not truly contribute to payload safety.

The efforts of the panel are laudable. They engaged in this streamlining activity before any of the other integration processes at NASA and have produced tangible results that have simplified the Payload Safety Review process while maintaining high levels of payload safety. As part of the *lean* transformation of the process, these activities that have produced positive, tangible results should be embraced and enhanced. The Panel can build upon this by appointing a person responsible for all process change activities, who could interface with the payload developers (or a subset of them) to permit prioritization of those activities whose transformation could yield tangible results. As a first step, the focus of the transformation should be on those steps in the value chain where the most non-value-added time is spent, as identified in Section 2.2. These would include the reduction of the delays leading up to the various design reviews, as well as the further reduction in the number of the reviews through consolidation or elimination.

With regard to providing education and training, the PSRP already provides short courses and web-based information on the Payload Safety Review process for the benefit of payload developers. It would be useful to incorporate into this already-established system courses that could be used to inform how the process being transformed will benefit the ultimate goal of producing a safe payload, as well as how payload developers could better interface with it.

2.5 *Implement Lean Initiatives*

At this step in the Roadmap, the actual *lean* transformation activities begin to be implemented. Within the PSRP, the person appointed to lead the transformation in the previous step would

begin implementing the plan, building upon the various changes that have already been implemented. Unfortunately, this person would face two major stumbling blocks:

First, while the PSRP can set up the process that must be followed to determine whether a payload is safe or not, it does not have the authority to direct the payload developers technically. Ultimately, it is the payload developers themselves that are responsible for submitting a safe design. The PSRP can advise and suggest design or process alternatives, but it has no power to actually require specific changes. If a payload developer can determine an alternative design that meets the safety requirements, the PSRP must accept that. As long as the milestones in the process are met, the PSRP cannot direct a developer to adopt a specific design, even though doing so might reduce the resources required to develop the payload. However, in general we have found that payload developers are very receptive towards any design advice given by the Panel and in fact would welcome more of it (see the stakeholder interviews in Chapter 4). Therefore if the Panel or some other organization well-versed in safety requirements and procedures were to provide design guidance, the developers would welcome it and this stumbling block could be removed.

Second, as has been shown, many of the payloads presented to the PSRP are actually being developed through other NASA centers or other government organizations. Typically, a private company or university, under contract with a NASA center, designs and builds a payload. The developer is usually responsible for the integration of that payload, including the preparation and presentation of the safety documentation. As was discussed earlier in this chapter, payload developers often must also satisfy integration and safety engineers at the contracting center through which the payload is managed. So, for example, if a university develops a payload for flight on-board ISS through a contract with the NASA Ames Research Center, the payload developer at the university usually must get approval of all safety documentation from safety engineers at NASA Ames, prior to submitting or presenting the information to the NASA Payload Safety Review Panel at the Johnson Space Center.

The problem in this arrangement is obvious: even if the Panel implements a change that could improve the Payload Safety Review process, it does not have any authority to require that a similar change be made at other NASA centers. What is worse, the contracting centers often impose requirements on the payload developers which are actually more stringent than those imposed by the Panel. Often this is done because past experience has shown that there will be growth in the

use of resources (mass, power, *etc.*) as the project progresses, and the safety engineers at the NASA center wish to be sufficiently below maximum levels of these requirements so as allow for this growth. Other times, it is done because the center has other constraints, external to the requirements of the Payload Safety Review Panel. Regardless of the reason, the end-result is a “bullwhip effect” for safety requirements, similar to that seen in retail or accounting systems¹⁷: one organization imposes safety requirements, plus a buffer. The next organization downstream also has safety requirements, and also imposes a buffer. Everyone in the process ends up holding a safety “stock”. By the time it arrives at the payload developer, safety requirements are amplified, which drives up the cost of the total payload.

There is often an assumption that while these “extra” reviews might be wasteful, they are not detrimental to the achievement of a safe payload. After all, what is the harm in having “another pair of eyes” look over the design? However, supporting these extra reviews requires the payload developer to expend resources, which are not infinite. Extra reviews, reports, and travel which ultimately only duplicate activities that are more properly conducted by the NASA Payload Safety Review Panel take away resources from other payload development activities, activities which if pursued might in fact improve the safety or the performance of the payload being developed.

In order for the benefits of *lean* transformation to be realized, changes in the process implemented by the PSRP must be reflected throughout the entire agency. Otherwise, the resulting process might appear *lean* from the point of view of the PSRP but in fact be just as cumbersome as before from the point of view of the payload developers. It should be noted that Sean O’Keefe, the current NASA administrator, has recognized the problems caused by different centers sometimes working at cross-purposes, not only with regard to payload integration but also for the entire Agency across all its programs and systems. In 2002, he implemented the *One NASA* program¹⁸. The program emphasizes a unified strategic plan, a strong commitment to teamwork, tools and capabilities for greater collaboration across the Agency, and more efficient systems within the Agency. Once implemented, the initiative will enable NASA to perform its missions by 1) fostering more collaboration across the Agency, and 2) promoting more efficient systems and processes throughout the Agency. It can only be hoped that this change will be reflected in the payload integration and Payload Safety Review process as well, and that conflicting and contradictory requirements will be eliminated.

2.6 Focus on Continuous Improvement

The last step in the Transition to Lean Roadmap can be summed up very simply: you cannot rest on your laurels. Even after the plan has been implemented and initial results have started to appear, it is important to continuously monitor the process and be prepared to refine the process in response to new or unforeseen events. Equally important, all the changes, systems, and processes that have been implemented must be captured, in order to provide a depository of this new knowledge that will be available even after personnel have transitioned out of the program. In this way, new innovations and processes can be built upon the successes of those that have already been implemented, without perhaps repeating the same mistakes. Finally, metrics must be identified that allow the team, and the outside world, to measure the improvements that have been achieved through the *lean* implementation.

Identification of exactly what these metrics are is an important task. In a private company, metrics such as profit, return on investment, *etc.* can be calculated and compared. Ultimately, the question that must be answered is, did *lean* make money? For the NASA Payload Safety Review process, there is no obvious metric as clear-cut as a corporation's bottom line. Instead, a mix of metrics will consist of:

- Reduction in the baseline time required to move through the process, as well as to complete the tasks required by the process. In other words, the value streams presented in this chapter must be compared with the actual value stream once *lean* has been implemented.
- Customer satisfaction, as measured by customer surveys and complaints
- Efficiency, as measured by the *total* number of personnel required to support a typical payload. This number would include both payload developers and NASA personnel.

Taken together, these three metrics would provide a tangible measure of the success or failure of any proposed changes undertaken as a result of *lean* transformation.

2.7 Summary

The Transition to Lean Roadmap has provided a good framework for the analysis of the existing process and the identification of potential pitfalls that may arise as *lean* transformation is undertaken. However, given that the TTL Roadmap was developed primarily using a commercial enterprise as a model, it is not surprising that several issues are raised which are unique to this process. Some of these issues appear in several steps of the Roadmap, which indicates that they may pose significant problems when it comes time to actually implement the transformation.

The main issues raised in this chapter can be summarized as follows:

- Opportunities for applying *lean* principles in the NASA ISS Payload Safety Review process appear to exist, in particular with regard to the steps involved in reviewing the submitted documents. Safety of the payload has been found to be a high-level need for all the primary stakeholders in the process, which is indicative that any changes which focus on improving safety will be treated with a high priority.
- The diversity and number of payloads poses various challenges for successfully integrating them into a *lean* process. Among these are the lack of resources available at the payload developer organizations for supporting the Payload Safety Review process, and the inability to combine and coordinate safety issues across various payloads with similar requirements.
- The limitations due to the contract and organizational structure of NASA restricts the authority of the PSRP in implementation of changes to the process. It also limits the technical direction that the PSRP can provide to the payload developers.
- Metrics do exist to allow measurement of any improvements arising from the *lean* transformation. These must be used to validate any proposed changes to the process.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3:

Comparison Between the Pursuit of Quality in American Manufacturing and Safety in Space

In the previous chapter, the NASA Payload Safety Review process was examined using the Transition to Lean Roadmap as a tool. The existing value streams were mapped, and insights were obtained with regard to potential difficulties that may lie ahead as *lean* practices are implemented into this enterprise. In this chapter, the same fundamental problem, the *lean* transformation of the Payload Safety Review process, will be examined from a very different direction. Instead of directly analyzing the existing state of the process, we will investigate another class of enterprises that have successfully transformed themselves. In doing so, we will draw comparisons and identify similarities and differences with the NASA Payload Safety Review process.

3.1 Why Compare?

In the 1970's, American industry was faced with a seemingly insurmountable dilemma. Foreign imports, most notably from Japan, were taking market share away from well-established industries such as automobiles, televisions, and electronics. These imported products were consistently both cheaper and of higher quality than their domestic counterparts. At the same time, wage pressures and inflation made it very difficult to reduce costs, and the conventional wisdom was that higher quality could only be achieved by increasing costs. Industry was caught in a Catch-22: the customer demanded *lower* price, and simultaneously an *increase* in the level of quality.

In the 2000's, the US space program is in a somewhat similar dilemma. NASA is constantly being asked to do more with less. The International Space Station will greatly increase the opportunities for research and discovery, however funds for development of payloads and facilities are in short supply as federal budget dollars are divided among other priorities, both within and outside NASA. At the same time, safety cannot be compromised. NASA's version of the Catch-22 is: it must lower costs (because less funds are available), and must maintain or increase the levels of

safety of its hardware and experiments. Their “customer” (the taxpayers) is demanding both a *lower* price and an *increase* in the level of safety.

American manufacturing solved its dilemma by embracing a set of tools that allowed them to lower cost while simultaneously improve quality. These tools, or sets of tools, form part of many systems and can be referred to by many names: The Toyota Manufacturing System, Total Quality Management, Lean Manufacturing, *etc.* At their core, they all focus on the reduction of waste, the improvement of manufacturing processes at each step, and the empowerment of labor and management to allow these steps to happen.

The question we now ask is, are there lessons that can be learned from the experience of American industry over the last 30 years that can help NASA out of its present dilemma? As was shown above, there are some similarities of the two situations. But there are also important differences. This chapter will discuss both.

3.2 *Parallels*

3.2.1 Emergent Properties

One of the key similarities between safety and quality lies in the fact that both are emergent properties of systems. Figure 3-1 shows several components used in a recent spaceflight experiment (SPHERES, described in more detail in Chapter 4). The components make up part of the propulsion subsystem for this payload. They are a small carbon dioxide canister, electrical wire and a battery pack. The first question posed is: is the propulsion subsystem of high quality? Does knowledge of these components allow us to make a determination of the quality of the subsystem as a whole? Clearly, the answer is no. Whether or not the subsystem is of sufficient quality depends on many other factors: how it is assembled, how it is intended to be operated, what testing will be done, *etc.* Without this information, we cannot make an accurate determination of overall quality.

Similarly, we can ask: is the subsystem safe? While each of the components by themselves could be judged to be “safe” (we may have to assume that the canister and battery are manufactured according to well established standards), it is not possible to say that the subsystem as a whole is “safe”. If there are any doubts on this, in Figure 3-2 we have simply rearranged the components so that the wire now winds around the gas canister, and is connected to the battery pack. In

theory, the battery could now conceivably heat up the canister until it explodes. In order to now determine whether the subsystem is safe, we would need to know how much energy there is in the battery pack, what the pressure of the tank is, whether there is a burst disk, *etc.* Even after we know these additional details, it might still not be possible to determine safety without knowing the environment this subsystem would operate in, how long it would operate, the likelihood of a battery rapidly discharging, *etc.*

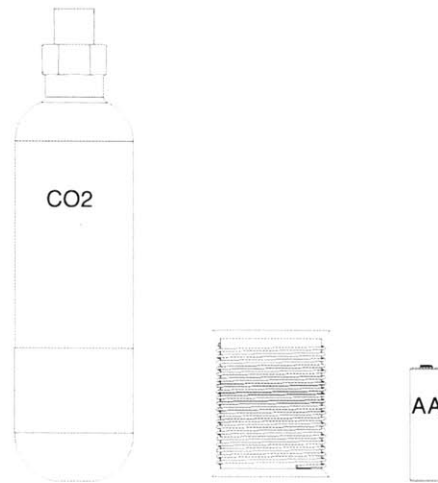


Figure 3-1: Components from the SPHERES Experiment

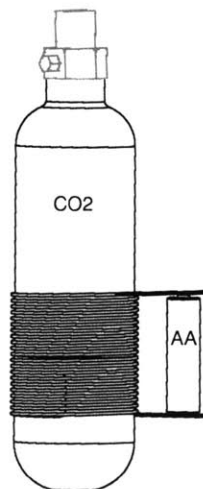


Figure 3-2: Components Arranged in a Potentially Unsafe Manner

In other words, safety and quality can both only be determined at a system level. It is very difficult, if not impossible, to make accurate determinations by simply looking at a parts list or an operations manual. This is not to say that certain quantifiable measures might not be critical in determining whether a system is safe or not. For example, the satisfying “thump” heard when closing a car door is perceived by the users as a sign that a car is “well-built”. Therefore, knowing the tolerances and gaps between the door and the car body would be a good indicator of whether this particular car model will be perceived as being of high quality. But this determination is only made thanks to the fact that there is an extensive database and history of automobile and customer satisfaction data to draw upon. This data was collected by studying production lines and customer buying patterns, as well as by conducting interviews and surveys of customers, mechanics, *etc.* It is only thanks to this information that this particular quality feature has been able to be reduced to a quantifiable manufacturing measurement.

The same issue arises when trying to determine safety. In the example of Figure 3-2, it may be determined, after analysis of the operation, components, manufacturing techniques, *etc.*, that the key feature that allows the system to be safe is a precisely tuned burst disk attached to the canister that allows venting in case of overpressure. If this is the case, then simply knowing that this burst disk is part of the design, and that it has been tested and certified according to some established standard, might allow us to make a determination that the system is safe. But, as was the case with the car door, we can only arrive at this conclusion *after* having gone through an extensive and detailed analysis of the system as a whole.

In summary, both safety and quality, as emergent properties, can only be determined by taking a holistic view of the entire system. Where large amounts of data and experience are available, as in the case of a mass-produced component, it may be possible to reduce the evaluation of quality or safety to simple, quantifiable measures. However, in the case of NASA payloads, this data is more often than not unavailable. As will be shown later in this chapter, this introduces additional complications when trying to apply the lessons learned from the pursuit of quality in manufacturing to the safety arena.

3.2.2 Difficult to Quantify

Another characteristic shared by both properties, quality and safety, is the difficulty faced when trying to assign a quantifiable value to them. There is no generally accepted, quantifiable measure

of an object's quality. A Yugo is generally seen as being of lower quality than a Mercedes, but it is not possible to say that a Yugo has quality X and a Mercedes has quality Y . This is not to say that there are not many prizes, measures, and competitions that are meant to quantify and rank quality products and processes. However, they are not universally applicable across all systems.

The same is true for safety, though attempts to quantify safety have been made and some techniques do exist. Probabilistic Risk Assessment¹⁹ (PRA) is one well-known method that attempts to quantify the risk of a system. However, in order to have value, PRA requires statistically significant data for all the components that make up the system, as well as extensive failure analyses to attempt to identify all the failure modes. This information and analyses are rarely available, are very expensive to produce, and are therefore rarely used by payload developers with limited resources. In addition, the underlying data used in these assessments can often be subjective, thus limiting the use of any results obtained from it.

Similarly, various types of Failure Modes and Effects Analyses²⁰ (FMEA) attempt to quantify the likely failure scenarios for different systems. However they also rely on expert opinion and advice in assigning probabilities of failure and of detection, as well as the importance of the failure consequences. As was the case with PRA, this information is often out of reach for a typical payload developer.

In the absence of an easily obtainable measure for either property, evaluation of a payload's or product's safety and quality again falls on a holistic examination of the entire system. Experience, common sense, and generally accepted industrial standards all play a role in this evaluation. Unfortunately, they cannot be reduced to a single, quantifiable measure.

3.2.3 The Role of Perception

Finally, there exists one other important factor in the way that both properties, quality and safety, are similar. Perception on the part of the user or other stakeholder plays a significant role in the determination of whether a product or payload is of high quality, or if it is safe. Note that this is not to say that the evaluation of these two properties can depend exclusively on the user's perception. It simply says that the user's perception of whether a system is safe or of high quality can impact how the system is treated and used once it is deployed.

This can be illustrated with an example. Automobile manufacturers have for years used the same basic designs and components for a wide range of products spanning their entire product lines. The same engines, shocks, transmissions, *etc.*, could be found both in their low-end economy vehicles and on their high-end “luxury” cars. And yet, the marketplace was prepared to pay a premium for the latter, because these cars were perceived to be of higher quality, even though they were not. Perception impacted how these products were treated.

In the case of safety, perception can also play a role in the evaluation of a system. In 1996, the maiden flight of the Ariane V ended in disaster when the rocket was destroyed shortly after liftoff. An investigation found that the failure was due to an error in the guidance platform, which was also used on the earlier Ariane IV^{21,22}. In re-using the platform design, the differences between the two rockets’ data systems were not properly taken into account in the software, leading to incorrect commands being issued by the on-board computer to the nozzles of the booster rockets and the main engines. This in turn led to disintegration of the rocket due to high aerodynamic stress, as the entire rocket stack deflected in response to the changes in thrust angles.

Major components of the guidance system were identical to those used in the earlier Ariane IV. They had not failed in dozens of prior launches. In hindsight, it is of course clear that they should have been reviewed more carefully. However, at the time, the system was *perceived* as being safe.

3.3 Differences

It would be naïve to say that just because of the similarities listed above we can draw broad conclusions regarding the applicability of lessons and techniques learned in improving quality over to the problems faced by NASA safety. There also exist some key differences that must be taken into account. These are briefly outlined in this section.

3.3.1 Statistical Techniques

Many of the lessons and techniques that have been used to improve quality over the last few decades rely on the fact that thousands, if not millions, of identical products are being manufactured on a production line. With such a large sample base, it is possible to use techniques such as Shewart Control Charts²³ or Six-Sigma^{24 25} to improve quality at each step of the production process. It is also possible to quantify quality levels based on the behavior of a single parameter (as was the case in the previously mentioned example of the car door seals).

In the payload development world, production lines are significantly shorter. Rarely are more than a handful of copies built of any single payload or hardware element. In addition, they are usually assembled in a “craftsman” mode rather than on a mass production assembly line. Sufficient samples for proper application of statistical techniques are simply not available.

3.3.2 Production Line and Learning Curves

For similar reasons, the design and fabrication of payloads, from the developer’s perspective, cannot count on learning curves either to improve the quality and safety of payloads or to reduce the labor and resources needed to produce a finished system. There are simply not enough copies of any single item made, nor are they made at a sufficiently high rate for the labor used in their fabrication to improve significantly between the first and the last item that is produced. It is only in very few cases, such as companies that manufacture unmanned launch vehicles, that the number of units produced approach levels where learning curves begin to have significant impact.

3.3.3 Experience Base

Finally, the most significant difference that might prevent us from blindly applying the lessons and techniques learned in the quality world to the NASA Payload Safety Review process is probably the fact that the experience base from which to draw data, expertise, and lessons learned simply does not exist for NASA payloads. Simply put, compared to the number of consumer and military products that are mass-produced, the total number of payloads produced for spaceflight, even in the ISS era, is miniscule. This makes evaluation of their safety more difficult because there is often no *a priori* general understanding of the payload or its function. For example, in the commercial world dominant designs for individual products establish themselves rather quickly. User interfaces for computers, to take one example, are now so well entrenched that a product that significantly deviates from them, for example by using non-standard functions for the mouse buttons, or by placing window controls in different locations, would have difficulty being accepted in the marketplace²⁶. A consumer thinking of purchasing such a product would immediately notice these differences, since he can draw upon his general understanding and past history with other, similar products, and would focus on these differences in evaluating the quality, or the safety, of such a product.

If we extend this example into the payload development world, we find that user interface standards are not well established. Each experiment is different. There are numerous manuals and requirements (see Appendix A for a partial list) that attempt to provide verifiable specifications for payload developers. However, experience shows that these tend to be too rigid, since they cannot possibly anticipate all the different configurations of future experiments, and they are often too complicated for the average payload developer to read, understand, and implement. It may be that it is inevitable, given the wide range of payloads and experiments, that a large amount of variation must be accepted by the system. However, it is also true that this variation has direct, and often negative, implications on the Payload Safety Review process.

Having briefly examined some of the similarities and differences between safety and quality, it is now possible to look in more detail into how quality was improved in commercial industries and see if it is possible to apply some of the lessons to the NASA Payload Safety Review process. This is done with the full knowledge of the limitations and differences discussed above. Nevertheless, as will be shown, we believe that there are lessons that in fact can be learned and transferred, thereby increasing value, reducing cost, and maintaining the needed levels of safety for NASA payloads.

3.4 Quality

This section will provide an overview of how industry, both in the US and around the world, managed to transform itself from mass to *lean* production, and thereby reduce costs and increase quality simultaneously. This process can be broken down into several distinct stages, which correspond to different levels of quality or stages of customer satisfaction (A much more detailed discussion of this topic can be found in S. Shiba's seminal work on the subject²⁷):

- Stage 1: Building the product to specifications.
- Stage 2: Building the product to meet customer needs.
- Stage 3: Building a good product affordably.

A fourth stage, which attempts to build products in anticipation of customer needs, can also be defined but is not covered here because it is not directly applicable to spaceflight payload

development. The following sections will briefly describe these stages, with a focus on the key characteristics that may be applicable to the NASA Payload Safety Review process.

3.4.1 Building the Product to Specifications

When mass production manufacturing was first introduced, quality was not a primary concern. There was such a pent-up demand for consumer goods that customers were eager to buy, regardless of the level of quality. Essentially, if a product met its specifications, and these were often quite lax, it was sent out of the factory and into the marketplace. Inspections, usually at the end of the production line, ensured that these minimal standards were met. Customers or dealers were expected to fix whatever problems would arise.

Even as products grew in complexity, the system did not change much. As consumers were provided with more choices, and they began to demand quality in their products, industry responded by introducing more quality inspections in the process. In the 1950's, W.E. Deming introduced Statistical Quality Controls in Japan to aid in this process. This could be seen as the first step in the evolution of manufacturing out of the mass-production model. However, these controls were really used more often than not as means to assist the quality inspectors. The basic premise, that you could inspect your way to a quality product, remained unchanged.

This system produced an environment in which the quality inspectors were, by default, in an antagonistic relationship with the producers of the product. Often, the inspectors worked for entirely different divisions or even entirely different companies. All the inspectors could do was to reject a product for being out of spec. This reflected badly on the production team and also meant that they had to produce a replacement product. Having a product rejected meant that the material and labor that went into it was now considered to have been wasted, thereby driving up overall costs.

3.4.2 Building the Product to Meet Customer Needs

Beginning in the 1950's, and continuing to the present, the development of the consumer economy along with the post-war reconstruction of industrial nations forced major changes in the way that manufacturers designed and produced their products. Consumers were no longer satisfied to accept any product, regardless of its quality or usefulness. There was now an oversupply of most consumer goods. Manufacturers began to really compete with each other on

price, features, and finally quality. In addition, as trade barriers disappeared or were greatly reduced, national industries could no longer rely on a “captured” domestic market.

As the expectation of higher quality developed, industry responded by expanding the use of inspection as a means to ensure the quality of the final product. Use of statistical methods was increased. However, this approach suffers from a fundamental problem. Figure 3-3 shows a standard bell-shaped curve, representative of any single given parameter in a production process. In an automobile manufacturing production line, for example, it could represent the variation in the length of a wheel axle. Inspectors measure this parameter, and their measurements will fall all along this curve. At some point, the measurement falls too far from the center, and the product is deemed out of spec and is rejected.

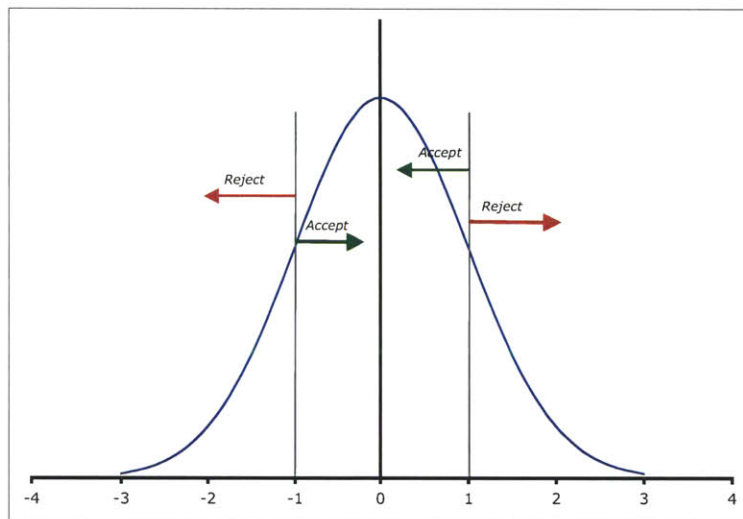


Figure 3-3: Normal Distribution of a Key Parameter in a Process.

As quality is increased, the threshold above which a product is not accepted is moved closer and closer to the center of the curve. While this results in an increase in the quality of the product that leaves the factory, it also produces a proportional increase in rejected products, which of course produces higher waste and therefore higher costs. Clearly, this solution would not be sufficient for achieving the combined goals of both higher quality and higher costs. Reliance on inspection as a means to achieving quality was not sufficient.

3.4.3 Building a Good Product Affordably

The answer to the dilemma of producing higher quality products while maintaining or even lowering cost is relatively straightforward: instead of ever-tightening standards, producing more and more waste, it is better never to produce any products that fall outside the given standards in the first place. In other words, instead of moving the points at which a product is rejected closer to the center, a manufacturer instead attempts to narrow the overall curve, thereby producing virtually no waste in the manufacturing process. This is illustrated in Figure 3-4, where the threshold lines have remained at the same point, but the area under the curve in the acceptable range is significantly higher than in Figure 3-3. As the curve is tightened more and more, the need for after-the-fact inspections is reduced.

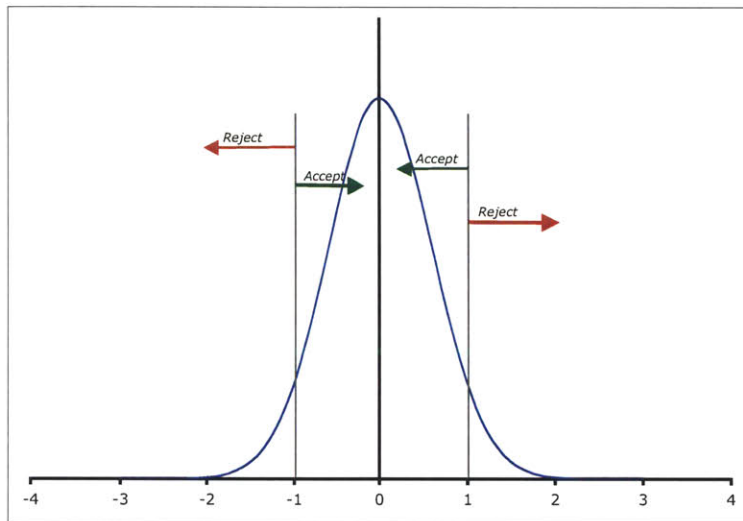


Figure 3-4: Narrowing the Distribution Reduces Rejected Components

While the answer is simple and straightforward, achieving a production line where every product is of high quality and inspections can be virtually eliminated is quite the opposite. There is no one single, straightforward answer. Instead, a wide array of techniques have over the years been instituted in modern production facilities. These techniques are known by many names, including Total Quality Management²⁸ (TQM), Bottleneck Theory²⁹, and of course, Lean Manufacturing.

Regardless of what they are called and which specific tools are used, several common methods are usually if not always present. It is not important, for our purposes, to be too specific regarding which tool belongs to which method. These include the previously mentioned statistically-based

production monitoring tools, which, as we discussed earlier in the chapter, may not be applicable to the NASA Payload Safety Review process. Several others tools, however, may be more useful:

- First and foremost, achieving high quality and low cost always requires an *analysis and monitoring of the entire manufacturing process*. It is not sufficient to simply inspect a product at the end, or even at one or two “quality” checkpoints.
- Second, since the entire process is being monitored, *feedback is provided at each step of the process*. A product does not proceed to the subsequent step in the manufacturing if it has *any* defects, no matter how small.
- Third, the production workers are given the responsibility and the power for both detecting quality problems, as well as for developing improvements to prevent them in the future. This often involves creating *cells*, or *integrated product teams*, composed of workers, engineers, designers, and even management, that bring together all the knowledge and authority needed to address problems as they arise in the production process.
- Finally, the entire production system needs to be changed over from a “*push*” system to a “*pull*” system. As was shown in Chapter 2, this means that product is only produced when there is a *pull* from the customers. In other words, a new product only leaves the factory when there is a customer waiting to purchase it. In practical implementations, this translates to a focus on reducing work-in-progress (WIP) and parts and supply inventories, thereby reducing the resources required to store inventory and components that have not been sold.

Using these techniques (and many others that are much more specific to particular industries), industry around the world has managed to achieve what was once thought impossible: increasing quality and customer satisfaction, while simultaneously lowering cost and increasing profits. Can these be used by the NASA Payload Safety Review process? This will be examined in the next section.

3.5 Safety

Having examined how the approach to producing quality products has evolved over the last several decades, we will now examine how a parallel evolution can be seen in the production of

safe payloads for NASA. This section will go through the same three phases described above, except this time, instead of examining how quality was improved in commercial products, we will examine how safety can be improved in NASA payloads, and we will draw insights that may be useful in achieving the goal of producing safe payloads while lowering costs.

3.5.1 Building the Payload to Specifications

Payloads, like commercial products, have specifications that they must meet. Typically, these specifications are verified through a combination of analysis, inspection, and testing. However, unlike a commercial product, when specifications for payloads are written there often exists very little prior experience with similar systems. This can lead to the all-too-common situation of a payload meeting all its specifications but not actually performing its intended scientific purpose.

In addition, as was shown earlier in this chapter, safety is an emergent property, just like quality. A payload can meet all its specifications and still be unsafe, just as a product could meet all its specifications, and still be of unacceptable quality. And of course, since payloads are unique systems and are usually produced in small quantities, there is little if any opportunity to associate overall levels of system safety to quantifiable specifications, since a large database of prior-built systems does not exist.

In these cases, safety is assured in the same manner as quality was assured during the early days of mass-production: a team of independent inspectors review, inspect, and analyze the final product to determine whether it poses a threat to the spacecraft or the crew. And, as was the case in mass-production, it is inevitable that antagonistic relationships develop between those responsible for the production of the payload and those responsible for the inspections.

It is interesting to note that during the early days of the space program, a process of this type did not pose a major problem. Apollo was a national priority. Resources were plentiful. If inspections revealed a problem late in the fabrication process, the system was repaired or replaced with a backup.

3.5.2 Building Safety into the Payload

As the Apollo era ended, and NASA began to focus on low-Earth orbit operations using the Space Shuttle, two forces combined to change the way the hardware was being developed for space. First, the financial commitment on the part of the government for space activities waned,

leading to greatly decreased resources allocated to NASA. Second, the Shuttle represented a major shift in the operations of NASA. Shuttle activities were going to focus on conducting experiments. The value of the program, at least in part, would be measured by the quality and quantity of the scientific results obtained during Shuttle missions.

As the types and numbers of experiments increased, and as budget resources decreased, NASA began to rely on a sequential series of reviews to verify that the payloads being built would not pose a threat to either vehicle or crew. This eventually developed into the four phase Payload Safety Review process that is in use today.

As we have seen, this process relies on the payload developer considering the safety implications of his or her payload at all stages of the payload development. Periodically, the payload developer prepares and presents a safety data package to NASA. NASA personnel review the information contained in the package, and based on their understanding and the questions asked at the safety reviews where the payload developer presents the design, the payload is approved for flight.

This approach addresses the fundamental problem brought on due to safety being an emergent property by allowing NASA experts to periodically review the design, and to do this early enough so that safety considerations can be “built-into” the payload early in the design process. The multiple reviews allow NASA to revisit the design at different stages of maturity, allowing a holistic picture of the entire payload to emerge. As we have seen, this is the only way that safety can be properly evaluated.

However, much like the manufacturing industry discovered, this approach has similar fundamental limitations. Chief among them is the maintenance of the antagonistic relationship between the “inspectors” (in this case, the NASA Payload Safety Review Panel and their staff of safety experts), and the payload developer organization. The process is laid out sequentially, with clear responsibilities. The payload developer prepares and presents the information. NASA personnel review and sign-off on it. This is exactly the same relationship that was present in the earlier discussion on quality. If NASA does not sign off at each review, this leads to re-work, re-design, and additional expenses on the part of the payload developer.

In this system, NASA assigns a Payload Safety Engineer (PSE) to each payload to help the payload developers get through the safety certification process. Nominally, the PSE can offer advice and suggestions. However, his ability to provide design guidance is limited: contractually,

he does not have that authority, and in practical terms, he often has too many payloads to monitor to be able to delve deeply into the designs of each of them. Responsibility for the payload ultimately rests solely with the payload developer. The PSE therefore does not form part of an integrated team with the payload developer, and more often than not finds himself in the same antagonistic relationship with the developer as the rest of the Panel.

In summary, this system, while it does accomplish its goal of certifying payloads as being safe, does so by potentially increasing the costs to the payload developer. It also does not utilize the knowledge resident in the PSEs in the most effective manner. In the next section, we will examine how the process can be improved, using many of the lessons presented in the earlier discussion on quality.

3.5.3 Building a Safe, Cost-Effective Payload

As was shown previously, mass production industries transitioned from manufacturing quality but expensive products, to manufacturing quality and affordable products, by implementing a series of tools and techniques in their production line. Recall from Figure 3-4 that the process of tightening the distribution curves of products required reducing the fraction of product that fell outside the acceptable limits. Can a similar approach be undertaken in the payload development process? The next several paragraphs compare each of the tools from Section 3.4.3 and attempts to apply them to the existing payload development process:

- *Monitoring of the Entire Process.* It was shown in Section 3.4.3 that monitoring at a handful of checkpoints, usually by a team separate from those producing the product, was not sufficient for ensuring high quality. The same is true with regards to safety. Presently, safety is checked up to four separate times during the development of a payload, at each of the Phase Safety Reviews. However, the design decisions which affect the safety of the payloads are being made continuously throughout its development cycle.
- *Feedback.* The present system only provides feedback to the design as part of the four discreet Phase Safety Reviews. However, since these safety reviews occur separately from the design reviews themselves (*e.g.*, Preliminary Design Review, Critical Design Review, Acceptance Review, *etc.*), the feedback can often lead to significant design modifications. Often, a payload developer is faced with a choice

of either doing a Phase Safety Review prior to a design review, and therefore presenting an immature design to the Safety Panel, or doing the safety review afterwards, and risk major design modifications to the payload just presented at the design review.

- *Integrated Teams.* Presently, the responsibility for developing a safe payload rests with the payload organization. However, the knowledge and experience needed to design a safe payload often reside just as much with NASA personnel as with the payload developer. This is especially true if the developer is new to the spaceflight world and is unfamiliar with the systems of the International Space Station. As NASA tries to increase the number of experimenters and improve the quality of the science done on the ISS, this problem will only get worse. NASA personnel, in the form of the Payload Safety Engineers (PSE), can help fill this need. However, as was shown earlier, the PSEs, while they can provide information, are not authorized to make design decisions. They also are responsible on average for 15 to 20 payloads at any one time, which also reduces their ability to provide significant design guidance.
- *Creation of a Pull System.* Presently, the Payload Safety Review process is essentially a “one-size-fits-all” system. The number of reviews, and the information presented at each of them, is laid out well in advance in several NASA documents. In actuality, some tailoring of the process occurs, influenced by the input of the PSEs. However, as was discussed in the previous paragraph, the PSEs are limited in the amount of involvement they can have with each payload. This can lead to an overproduction of information on the part of the payload developers, since they often err on the side of providing an over-abundance of information in order to ensure they have a successful safety review.

The present system relies on reviews of the data and design, submitted by the payload developer, by external personnel who may not be very familiar with the developed hardware. If the four tools listed above were applied to the existing Payload Safety Review process, they would allow the transition to a process where the reviewers and the payload developer form an empowered, integrated team. This team would be capable of preparing and submitting “perfect” data packages at each step of the process, reducing waste and expended resources.

The issue that is still before us is how to implement these tools into the existing process. However, it is clear that the solution will lie in properly bridging the gap that presently exists between the developers, who are most familiar with the payload, and the Panel, who are most familiar with the safety requirements. If this gap can be narrowed, all four of the above tools could be properly implemented. What would be needed is for a person or organization, experienced with the safety requirements, to be able to support the payload developers as part of an integrated team. This person would attend design meetings and reviews, thereby monitoring the process throughout the design cycle. In addition, he could provide feedback and design input to the team and be able to draw upon additional NASA resources as needed. He would bring to the developer team the missing knowledge and experience that is needed in order to properly take into account the safety aspects of flying on the International Space Station. Whether this organizational structure can be achieved within the constraints and limitations posed by the Payload Safety Review process will be examined in Chapter 5, when the desired state of the process is presented.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4:

Stakeholders' Perspective

In order to obtain data on the existing state of the NASA Payload Safety Review process, interviews with a number of stakeholders were carried out. These stakeholders included hardware developers, integration engineers, and representatives from the NASA Johnson Space Center Payload Safety Review Panel. These interviews are summarized in this chapter. Their input was used in determining the existing value streams, as discussed in Chapter 2. More importantly, their issues and concerns must be explicitly addressed in designing the ideal state value stream that will be presented in the next chapter.

4.1 Cell Culture Unit

The Cell Culture Unit (CCU) is part of the NASA Ames Biological Research Project. The unit is designed to provide a state-of-the-art laboratory for the growth and sampling of monolayer and suspended cells in microgravity. A drawing of the flight unit is shown in Figure 4-1. The nominal CCU mission consists of two identical units flown into orbit inside the Shuttle Middeck. The units are continuously powered during launch and ascent. Once docked with ISS, the astronauts will transfer the units and place the first one in a rack and the second one in the ISS centrifuge. In this way, the cells in microgravity and the 1-g controls (in the centrifuge) are collocated, allowing direct comparison of the results obtained. The CCU is a facility-class payload. It is designed to be reflown dozens of times on the ISS and to support culturing of a wide assortment of cells, as shown in Figure 4-2, from different principal investigators.

The CCU is considered a medium-complexity payload, due primarily to the wide array of potential hazardous fluids which must be used to properly culture the cells, and to the need for significant crew interaction in the transfer and sampling of the biological specimens. For this reason, interaction with the Safety Panel began very early in the project, and a Phase 0 Safety Review was held in July, 1997, prior to the Conceptual Design Review. A Phase 1 Safety Review was held in February, 1999, which resulted in several issues being left unresolved. A Delta Phase 1 Review was then held in August, 1999, during which all Hazard Reports were signed.

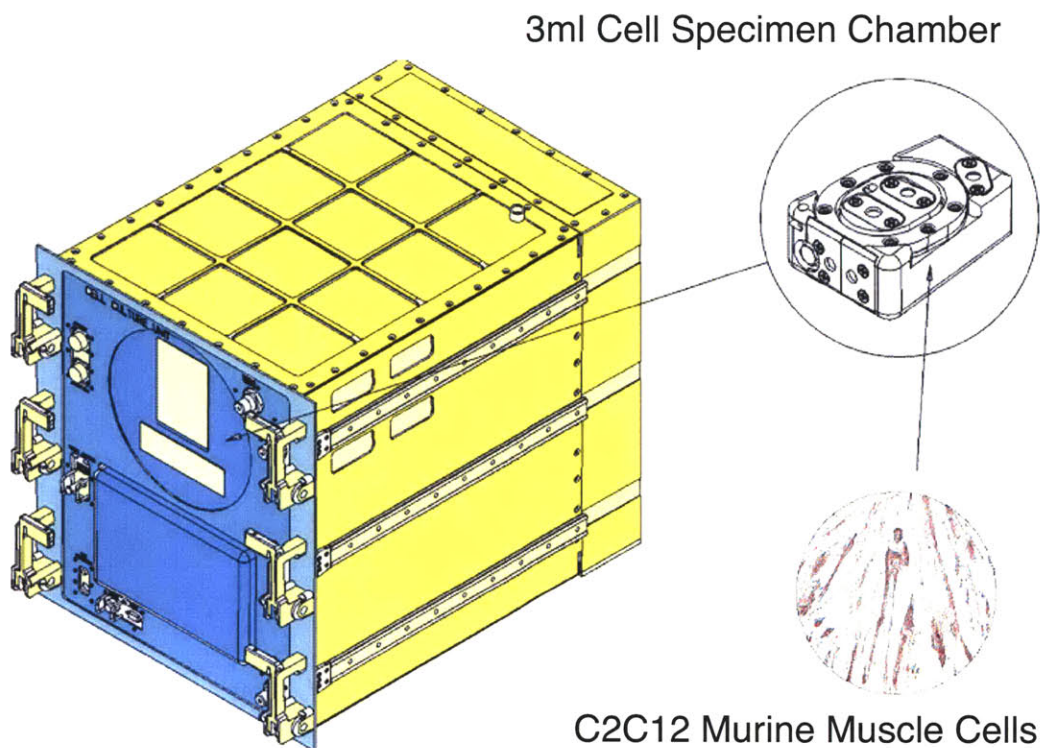


Figure 4-1: The Cell Culture Unit in its Flight Configuration

Ms. Kim Slater is the Integration Engineer for the Cell Culture Unit. She has been with the project since its inception and was the lead engineer responsible for both the Phase 0 and the Phase 1 data packages. She has also worked as an integration engineer on over a half dozen other payloads that have flown on Shuttle, *Mir*, and ISS. Ms. Slater was interviewed over the course of several weeks in the fall of 2002. Her comments are presented here, and observations based on her information will be presented at the end of the section.

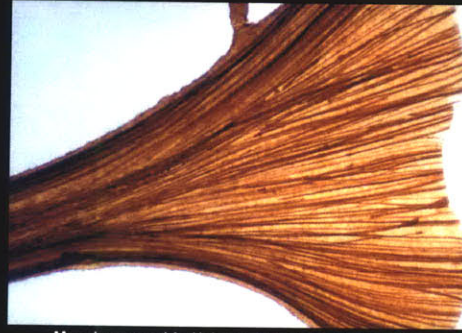
Ms. Slater divided up her main areas of concern into the following four categories:

Access to Information

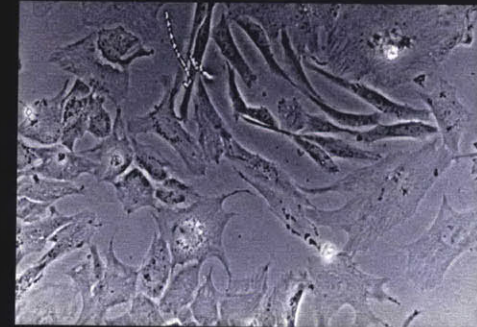
“If Payload developers were given better access to safety analysis data, they would be better prepared and rely less on JSC Payload Safety Engineers. General guidelines are easy to find. Specifics are often not.” To illustrate this point, Ms. Slater used the example of her experience trying to obtain information regarding levels of containment for hazardous fluids within the CCU. In general, guidelines state that hazardous fluids must be enclosed by a certain number of levels of containment. The number of levels depends on the toxicity level of the contained fluid. In order to determine the toxicity levels of a particular fluid, the developer must submit the fluid and



Muscle cell fibers (10-20 diam) from Dr. Herman Vandenburg of the Miriam Hospital, Brown University



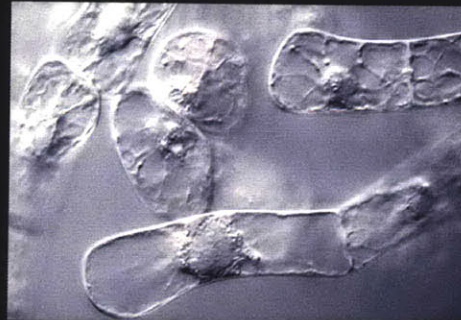
Muscle organoids (1-2mm diam) from Dr. Herman Vandenburg of the Miriam Hospital, Brown University



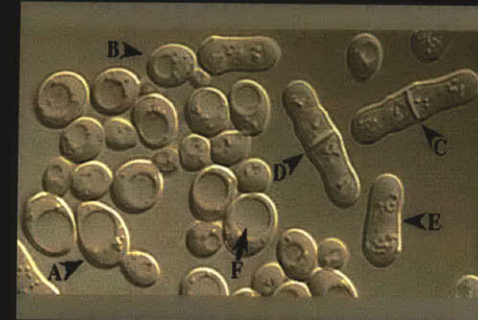
Osteoblasts (10-15 long) of 17 day old embryonic chick bone (calvaria) cells from Dr. Louis Gerstenfeld via Dr. William Landis, Children's Hospital, Harvard Medical School



Euglena gracilis (40-50 long) from Dr. John Kiss of Miami University



BY2 tobacco cells (60 diam) from Dr. Richard Cyr of Pennsylvania State University



Saccharomyces cerevisiae (see A and B) and fission yeast *Schizosaccharomyces pombe* (7-14 long, see C, D, and E) from NIH yeast web site <http://www.ncbi.nlm.nih.gov/Yeast>, image generated by Frans Hochstenbach and Noah Sciaky

Reference specimens selected for development testing of the Cell Culture Unit in support of research on-board the International Space Station

Figure 4-2: The Various Types of Cells that Will Be Grown in the Cell Culture Unit Facility (units in micrometers, unless otherwise specified)

concentration level to the Payload Safety Review Panel staff and wait for a determination of what toxicity level the fluids fall under. The developer then can use this information to design into the system the appropriate levels of containment. The problem that she found was that obtaining this toxicity assessment took a long period of time, on the order of many months. And, as designs and requirements evolved and new fluids were added, the process had to be repeated. She points out that if the toxicity data were accessible on-line, or in a document, she could have performed the analysis and design independently and then submitted the complete design for review. What happens now is that often, because of the long delays in obtaining a definitive answer from the NASA toxicologists, the design engineers assume the worst case and move on. While this results in a safe design, it also often results in an overly designed system, and one that is more expensive and more complex for the crew to operate than it needs to be.

Ms. Slater finishes by pointing out that a similar problem exists in the area of general materials data. In her opinion, “the on-line materials database is extremely user-unfriendly, and the only available printed version of materials data is dated 1987. All materials tested *since* 1987 are almost impossible for a developer to investigate without help from someone at JSC.”

Experience of Engineering Support

As has been discussed previously, a payload is typically assigned a NASA Payload Safety Engineer (PSE) to be an interface between the payload developer and the Panel. This person is supposed to become a contact point for all safety matters and to refer the payload developer to specialists when necessary. In Ms. Slater’s experience, “the PSE can be a good source of general advice, but not much more. What is most valuable to the developer is direct contact with specialists to address specific safety concerns. The PSE relationship sets up an additional level through which one must communicate to ultimately get at the answer to a concern.”

Her concern in this area is also due to the fact that in the past, she has found that the PSEs tended to be newer, younger safety engineers, and thus their experience was naturally limited. It is the more experienced Panel members who have the ultimate judgment over the safety of a particular payload design. Since these evaluations and judgment calls are usually made at the Safety Reviews, and not sooner, the impact to the design (and redesign) is greater. If a senior safety engineer were involved at an earlier stage, the payload design team would be more capable of intelligently engineering safety features into the design.

Inconsistent Interpretation of Safety Guidelines

Payload Safety guidelines intentionally allow the developer flexibility in interpreting and addressing safety hazards. However, at different phases in the Payload Safety Review process, different Payload Safety Engineers may review the same hazard and require widely different controls. This forces the payload developer to respond and often modify the system design to accommodate different interpretations. Ms. Slater has had direct experience with this when, in the area of fluid containment, the container walls were sometimes considered as non-credible leak sources, while at other times those same walls were only counted as a single layer of containment. She states “interpretations at a review should not be changed, unless new data make the earlier interpretation incorrect.”

Fear of Standardization

Some hazards may be addressed with controls that are easily accommodated and implemented. For example, the safety of battery circuit protection is fairly complex, but the safety controls are quite simple. The Payload Safety Review Panel assists payload developers by publishing guidelines, but rarely gives direct design advice. According to Ms. Slater, “If designers of small payloads were given a typical battery design as an example of an acceptable one, it is likely that both the developer and safety panel would spend less effort arriving at a better, safer conclusion.”

Multi-Phase System

The Payload Safety Review process is iterative by design. This feature forces the payload design team to revisit safety controls through the design, fabrication and testing process. Although generally a positive feature of the Payload Safety Review process, this iterative process can in some cases instill some unnecessary re-work. In Ms. Slater’s experience, sometimes design features that have been reviewed and approved at one phase are unnecessarily re-opened at a subsequent review. While in some cases there may be reasons for this, in others it just leads to a waste of resources as the same issues and questions are re-visited and re-explained. Eliminating this redundancy may speed up the process and allow more time to review new or changed hazard sources. It should be possible for the PSE or some other Panel member to be able to make these decisions.

Ms. Slater has provided an excellent summary of her main points and concerns. As will be seen, many of these are repeated by other stakeholders that provided input to this work. Any proposed

lean-based modification to the existing system must at a minimum address these concerns that have been raised. The table below summarizes her main points, and lists observations that can be made from her comments.

Table 4-1: Main Points and Observations from Interview with the CCU Integration Engineer (K. Slater)

Main Points	Observations
<i>Access to Information</i>	<ul style="list-style-type: none"> If additional information on Payload Safety Review processes were made available, developers would use it, thereby simplifying the process Time lags between information requests and obtaining the information must be reduced, in order to have a timely impact on payload design.
Experience of Engineering Support	<ul style="list-style-type: none"> In order to be efficient, the role of the PSE should be filled by more senior engineers. Alternatively, the PSE should not interpose him or herself between the developer and the source of technical information on the Panel
Inconsistent Interpretation of Safety Guidelines	<ul style="list-style-type: none"> Safety-related findings at reviews should not be easily modified
Fear of Standardization	<ul style="list-style-type: none"> Developers should be made aware of previously-flown or state-of-the-practice designs. Design guidance from personnel knowledgeable of the safety requirements should be available to the payload developers.
Multi-Phase System	<ul style="list-style-type: none"> The process should allow tailoring to reduce or eliminate phases as required by the complexity of the payload.

4.2 Synchronized Position, Hold, Engage, Reorient Experimental Satellites (SPHERES)

SPHERES (Synchronized Position Hold Engage and Reorient Experimental Satellites) is a formation flying spacecraft testbed. The testbed provides a cost-effective, long duration, replenishable, and easily reconfigurable platform with representative dynamics for the development and validation of metrology, formation flying, and autonomy algorithms. These control algorithms are applicable to systems involving the coordinated motion of multiple satellites in a micro-gravity environment. The SPHERES system has prior flight experience on the NASA KC-135 Reduced Gravity aircraft (Figure 4-3) and has also been in constant use in air table testing for almost three years. Aboard the International Space Station (ISS), SPHERES will be used to conduct risk-reduction investigations in preparation for missions of interest to the Air Force and NASA.

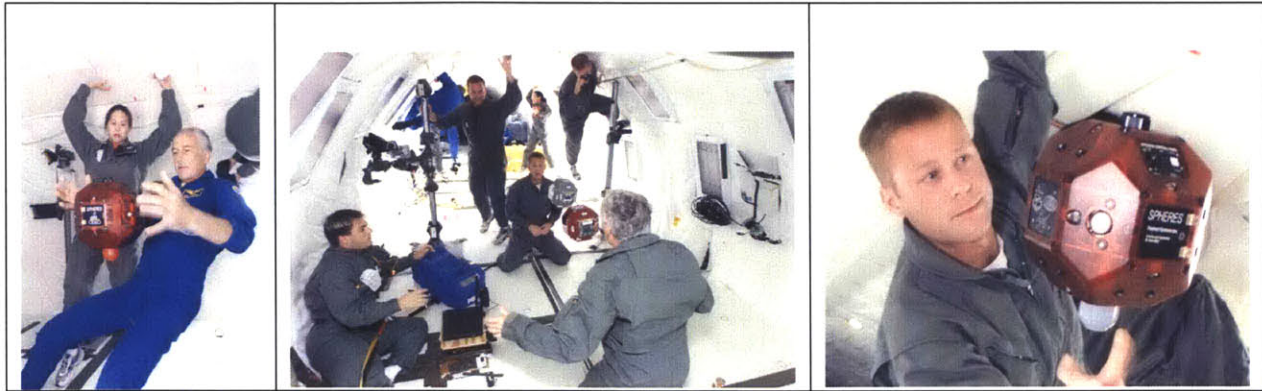


Figure 4-3: SPHERES Testing on Previous KC-135 Flights
(Photos courtesy of NASA)

The SPHERES experiment is designed to operate in the internal volume of the ISS. The experiment consists of three 8-inch diameter free-flying “satellites,” five ultrasound beacons, and an ISS laptop workstation. Each satellite is self-contained with on-board battery power, cold-gas propulsion (CO₂), and processing systems. The satellites communicate with each other and with a controlling laptop via a wireless RF link. One of the satellites is shown in Figure 4-4.

SPHERES is scheduled to be flown up to the ISS on-board STS-115. It has completed all the NASA Safety Reviews, and all Hazards have been signed and closed. Mr. Steve Sell is the project manager for SPHERES. He has been with the program since the beginning and was responsible for the development of all the safety review packages and presentations.

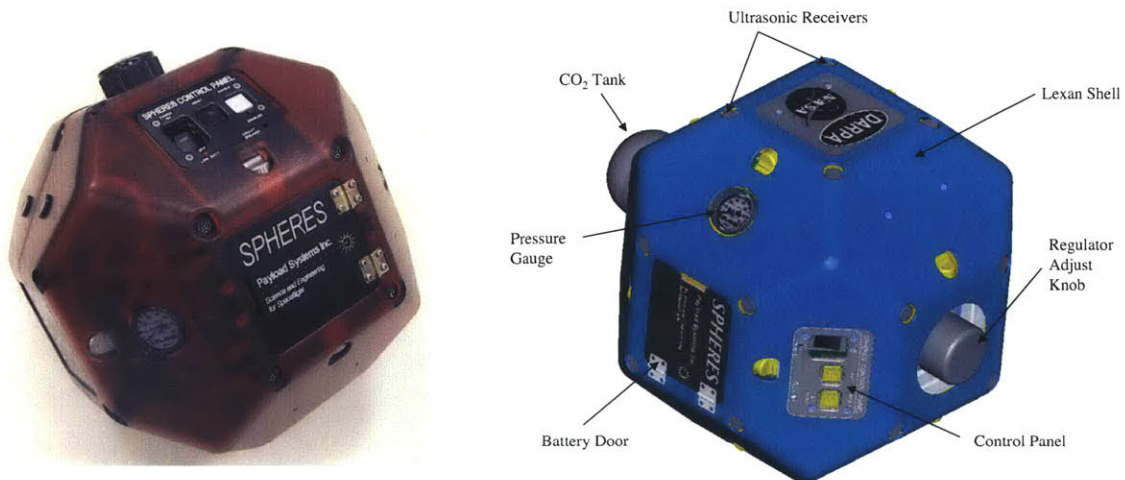


Figure 4-4: SPHERES satellite, actual (left) and rendered with callouts (right)

In discussions, Mr. Sell indicated that the single biggest problem he faced in dealing with the safety aspects of SPHERES was the difficulty in obtaining a correct, definitive answer to safety-related questions. He pointed out that official Phase Safety Reviews, the Panel members themselves were always very clear and direct as to what was required. In fact, Mr. Sell had nothing but praise for the Panel members themselves. However, outside of the reviews, it was impossible to have anybody at NASA provide a final, definitive answer. He speculated that this was due to the fact that the Panel has the final word with regards to the interpretation of the primary requirements document, NSTS/ISS 13830³⁰. Therefore, most of the people that support the panel ultimately end up falling back on that document and just telling the payload developers to “follow what is in 13830”. This is not very helpful when the question is in fact asking for an interpretation of what is in that document.

Mr. Sell gave as an example the fact that prior to the Phase 2 review, he was told by his Payload Safety Engineer that he needed a fracture control plan. He was surprised by this, since SPHERES is a small payload, not attached to any structure, and is stowed in lockers during launch. Nevertheless, the PSE pointed out that NSTS/ISS 13830 says that payloads need to develop a fracture control plan, so SPHERES needed one. Just prior to the Phase 2 review, after the fracture control plan had been written and submitted, he was contacted by a Panel member asking him why he had submitted a plan in the first place. It turned out that, as Mr. Sell had suspected, SPHERES did not require a plan and only needed to show that during normal operations it would not shatter due to firing of the CO2 thrusters, a calculation that was already included in the Phase 2 data submittal. Of course, at this point, the time and resources required to develop the plan had already been expended. If the PSE had been more familiar with the requirements, or if he had been more familiar with the data package that was submitted, this extra effort could have been avoided.

SPHERES is being funded by the Defense Advanced Research Programs Agency (DARPA). As a Department of Defense payload, it is being integrated through the Space Test Program(STP) office at the Johnson Space Center. In principle, STP representatives are supposed to act as the advocates for the payload at all NASA JSC integration activities, including the safety reviews. However, Mr. Sell indicated that he saw the STP as an extra layer of bureaucracy separating him even further from the people with the answers, *e.g.*, the Panel members themselves. He attributed part of his problems to the presence of this extra layer, although his experience with other non-

DOD payloads where STP was not involved was not, in fact, much different from what he experienced with SPHERES.

One particular problem he faced, however, was the insistence of the STP representatives to be the single point of contact between the SPHERES team and the rest of NASA. In principle, all questions from the team had to go through STP. This resulted in what Mr. Sell called a giant game of “telephone”. When Mr. Sell or one of his team would ask a question, by the time it reached the person who could actually answer it, through emails or telephone calls, it had been misinterpreted so much that it was no longer relevant. He attributed some of this to normal human dynamics. However, he also stated that a great deal of the problem was the fact that neither the STP personnel nor the PSE could spend sufficient time to learn about the payload. He often had the impression that at every conversation, phone call, or meeting, he had to remind and re-brief everybody as to exactly what the payload was. This results in the same questions being asked over and over and incorrect information being circulated within NASA.

Mr. Sell also expressed frustration at the fact that it was very difficult to be given actual solutions to the design problems he faced. Instead, he was merely given general guidelines. He was not sure why this was the case, but he speculated that it was because the Panel cannot really provide design direction to him, since they are not the organization paying for the development of the payload. Coincidentally, he used as an example a similar one that had been previously discussed by Ms. Slater: the battery circuit used inside each SPHERES test article. The units used a set of AA alkaline batteries. Many payloads have flown before with these commercial batteries. This is acceptable as long as some basic protection measures are taken, such as the placement of diodes to prevent overcharging. However, he was unable to obtain a specific circuit that had been approved before by the Panel. So instead, an electrical engineer on his team designed one from scratch, interpreting the requirements in NSTS/ISS 13830. Mr. Sell made the point that it probably took ten times longer to design the circuit than it would have taken to simply copy one that had flown in the past.

Table 4-2 summarizes the main points of the interview with Mr. Sell, as well as observations and concerns that arise from the discussion. These questions need to be addressed in designing a Payload Safety Review process based on *lean* principles.

Table 4-2: Main Points and Observations from Interview with the SPHERES Project Manager (S. Sell)

Main Points	Observations
"Can't get a straight answer"	<ul style="list-style-type: none"> • Payload developers must have access to NASA personnel that are able to make decisions and commit the Panel.
Lack of design guidance	<ul style="list-style-type: none"> • Personnel knowledgeable about previously flown and approved systems must form part of the payload development team.
Incorrect information provided outside of safety reviews	<ul style="list-style-type: none"> • PSEs and others charged with assisting developers should be experienced.
Bureaucracy levels	<ul style="list-style-type: none"> • Turnover of personnel should be avoided.
Insistence on being single point of contact	<ul style="list-style-type: none"> • Access to knowledgeable panel members should be provided to payload developers • Information should be transferred directly between interested parties. Others should be kept informed, but not put in the critical path. • PSEs and other personnel should support limited number of payloads, in order to allow them to become more familiar with the technical requirements of each project.

4.3 Enhanced Dynamic Load Sensing Experiment/Mir Structural Dynamics Experiment

The Enhanced Dynamic Load Sensor was designed to measure crew disturbances inside the Mir Space Station. It consisted of a set of sensors: a touch pad, a handhold, and a foot restraint, connected to a central data collection unit. Examples of the sensors are shown in Figure 4-5. The sensors would record data throughout the day as the crew went about their normal routine. The intent was to record the forces and moments that the crew imparts to the surrounding structure, and to use this data in the design of vibration isolation systems for payloads on-board ISS. The Mir Structural Dynamics Experiment (MiSDE) was a complimentary experiment that consisted of multiple accelerometer heads placed throughout the Mir Space Station that would record the acceleration of the Station whenever a docking, thruster firing, or other event occurred. The goal was to obtain dynamic data that could be used to model the ISS, as well as to help design vibration isolation systems.

Mr. Ed Bokhour was the Hardware Development Manager for both of these programs. His experience was unique in that these two projects were some of the first NASA programs to fly on Mir. They were therefore some of the earliest payloads that had to satisfy both NASA and Russian integration requirements.



Figure 4-5: Enhanced Dynamic Load Sensor Units

Mr. Bokhour recalls that his impression was always that the NASA Payload Safety Review process was actually one of the more well-defined integration processes that his payloads had to go through. The other payload integration processes were very unclear, and remained so until a knowledgeable person was found that was able to provide some guidance. However safety was better. The safety process was described in various documents, which were very useful. In the end, though, Mr. Bokhour indicates that it always came down to the personal contact and relationships that had been built. “If you had someone good to explain what the next two or three steps were, it was much easier to deal with.” Mr. Bokhour recalls one instance where he was having difficulties determining the proper derating criteria to use in a flexible electrical umbilical. The Panel’s electrical expert helped him get started and reviewed the results well before the Phase 2 review. That would have been very difficult to accomplish without his help. Mr. Bokhour does not believe, though, that this level of assistance is generally available. It is very easy to get overwhelmed by the complexity of the process, but if you found someone to call and ask questions of, then the process became simpler. Finding this person was the challenge.

Mr. Bokhour indicates that most of his effort was initially spent simply trying to understand what the process was. Having a good process description document helped, but another human was still needed to help explain how things really worked. He estimates that it took a year and several safety reviews before he realized that if you were able to talk to the relevant Safety Panel support person and dealt with the issues beforehand, things went very well at the actual review.

Mr. Bokhour recalls how in several experiments, including MiSDE, personnel were sometimes placed between his team and the safety contacts they were used to speaking with directly. Usually,

the intermediaries were part of a safety office attached to whatever organization was actually managing the development contract (in the case of MiSDE, it was McDonnell Douglas Aerospace). Often, their view differed on how the safety documentation and presentations should be prepared. These differing views generated a lot of conflict, multiple revisions of documents, and many testy phone calls. This experience serves to reinforce Mr. Bokhour's previous point that the more layers of interpretation between the Panel and payload developer, the harder the process becomes. Nobody should be defining what the process is or what is expected in the data packages except the Panel. His view is that "one-degree of separation" between the payload developers and the safety panel is the maximum, and that one layer should be Safety Panel support staff and no one else.

Mr. Bokhour also recalls several instances where requirements seemed to change from one safety review to the next. He attributed this in part to the fact that the process was still evolving at the time. However, he also felt that sometimes you got a different answer to a question depending on whom you asked. Also, he realizes that as technology changes, safety requirements will also evolve. He did express concern that a less experienced payload developer, someone who had not been through the process several times, would have a very difficult time navigating the various reviews and data submittals without significant assistance.

Ultimately, it is Mr. Bokhour's observation that the process is actually designed not so much to "prove" to the Panel that the payload is safe, but to prove it to ourselves, the payload developers. In the end, to make a payload safe you need the efforts of the engineers designing and building it. This final observation contains a lot of insight: the Panel cannot hope to inspect, review, and completely evaluate every payload to a sufficient level to be able to say, without a doubt, that it is safe. The only way that the system can function is for the payload developers to design a safe payload from the onset. Table 4-3 summarizes the main points from this interview.

Table 4-3: Main Points and Observations from Interview with the EDLS Hardware Development Manager (E. Bokhour)

Main Points	Observations
"Importance of personal contacts"	<ul style="list-style-type: none"> The experience of moving a payload through the existing process depends strongly on the access to the Panel members and their support staff
"One degree of separation" between developers and panel	<ul style="list-style-type: none"> NASA should speak with one voice regarding safety. Requirements from the Panel should flow through to the payload developers without modification or interpretation.
Evolving requirements	<ul style="list-style-type: none"> Payload Developers should be kept informed of evolving requirements, and not only find out about them at the Reviews..
"Prove safety to ourselves"	<ul style="list-style-type: none"> The existing process recognizes the difficulty and cost in depending solely on external verifications to demonstrate safety. The process already relies on having the personnel with the most knowledge of the payload be the ones that ultimately are responsible for safety. This is a first step towards a lean approach.

4.4 Payload Safety Review Panel

The Payload Safety Review Panel (PSRP) is the organization within NASA that is charged with determining that the numerous payloads that fly on-board ISS or Shuttle do not pose a danger to either the crew or the vehicle. The Panel consists of one full-time and one substitute member from each of the Johnson Space Center directorates and technical areas, which forms a core of approximately 10 to 12 panel members. In addition, the Panel has approximately 15 discipline engineers, most of them contractor employees. The Panel can also draw from toxicologists, secretaries, support people, *etc.*, as needed, from NASA and the numerous on-site contractors. The entire organization consists of approximately 50 people full time, plus others as needed.

On January 31, 2003, just prior to the Columbia accident, a meeting was held with various members of the panel in order to solicit their perspective on the Payload Safety Review process. It was the intent for the meeting to be free-ranging, so that the Panel could express their views on the issues and concerns of greatest importance to them. However, they were asked prior to the meeting, to comment about three specific areas that had arisen during discussions with other stakeholders, so as to provide them with the opportunity to gather in advance any information they may require:

- *The “standard” payload developer process:* This was meant to cover any generic issues the Panel saw with regards to problems they faced with the majority of payload developers.
- *The roles and responsibilities of the international partners:* Issues relating to the certification of international payloads.
- *The safety approach for in-house and crew equipment:* Is the process for handling internal NASA payloads and government furnished equipment (GFE) different from that for payloads supplied by the external user community?

The attendees at the meeting were Skip Larsen, head of the PSRP, and several of his staff: Mike Ciancone, John Steils, and Leanne E. Brasington. The slide presentation that was shown during the discussion is contained in Appendix C.

The discussion started by reviewing the number of payloads that the panel expects to process in the coming years. It was noted that the reduction in crew size from seven to three full-time astronauts on the ISS at any one time has decreased the planned number of payloads. However, they expect that to change once the crew size goes up. Eventually, they expect the number of payloads to reach a plateau. In other words, it will not keep growing indefinitely, as the rate of retiring of older payloads will eventually match the rate at which new payloads are introduced. Today, the panel has approximately 400 active payloads in various stages of the Payload Safety Review process.

Mr. Larsen mentioned that the recently-established European Space Agency “franchise” operation is expected to off-load about 8% of the payloads. The franchise system was set up to allow the ISS international partners a way of certifying their own payloads as being safe to fly. The Payload Safety Review Panel is in the final stages of establishing a similar franchise in Japan. The Canadians were also offered the opportunity to conduct safety reviews, but they have declined due to the large overhead required, the proportionally smaller number of payloads the Canadians expect to fly, and the proximity of Canada to the United States.

The intent of setting up the franchises is for international payload developers to be able to obtain safety certification of their hardware locally, without having the expense of supporting the process in Houston. It is also expected that the franchises would be responsible for certification of all payloads that fly to ISS on vehicles other than Shuttle. At present, the only other vehicles of this

type are the Russian Soyuz and Progress capsules (as a matter of international treaty, the Russian safety certification process is independent of the regular PSRP process and was not studied as part of this project). However, long-term ISS plans call for European and Japanese unmanned transfer vehicles. The PSRP felt that it was better to set up this process earlier, so as to work out any problems before these new vehicles go into service.

The Panel discussed how, in setting up the franchise concept, they were quite concerned about not establishing another layer of bureaucracy between payload developers and the Panel. They were quite frustrated with the existing situation with some other NASA centers that impose additional requirements on their contractors, over and above those imposed by the PSRP.

There is a four to six year phase-in period, during which the PSRP will monitor, conduct audits, and observe the franchise meetings. The intent is to start with simpler payloads, and move on to more complex ones. Memorandums of Understanding have been signed for various technical areas, including materials, fracture control, inspection standards, *etc.* From the start, the franchise Panels will have the authority to sign Hazard Reports. Overall, the NASA Payload Safety Review Panel was very positive about the franchise concept and expressed a willingness to set up additional franchises as needed, even within the United States.

A great deal of time was spent discussing the processing and generation of information, which is ultimately the major product of the Payload Safety Review process. The Panel mentioned several initiatives that have recently been implemented:

- DMS (Data Management System): This allows the panel to receive and process all payload safety information electronically. They are also in the process of digitizing their archived payload information. There are still issues, however, regarding how accessible this data will be to payload developers. For example, there may be proprietary concerns if one payload developer is allowed to look up data on another payload.
- Web-X (a virtual meeting system): This is a pilot program, but the PSRP is the main user right now. This is being done in an attempt to reduce the travel and support cost for attending the actual reviews themselves.

With regards to training needed to familiarize oneself with the Payload Safety Review process, the Panel strongly recommends that anyone doing safety send their integration engineers to NASA

for on-site safety training courses, which are held regularly at the Johnson Space Center. They are also attempting to place some of the training material on their website, where it would be more widely accessible.

The main document governing safety on board ISS, NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements for Payloads using the ISS, is undergoing another review this year. The last time it was reviewed was in 1998. As they review it, the Panel indicated that they are trying to ask themselves whether each particular requirement is necessary, and whether it adds to the ultimate goal of increasing safety. If this is not true, they will remove it.

The discussion then shifted toward the interaction of payload developers with the Panel. There was an acknowledgement that there is a tendency on the part of the developers to load up the data packages with information that is not relevant to the safety analysis. In particular, there has been a recent tendency to spend a lot of time discussing data flows and controls, even when the payload is using no software hazard controls. The Payload Safety Engineers (PSE) are supposed to be the primary point of contact and information for the payload developers. There are approximately 20 PSEs, and most of them are contractor, not NASA, employees. As there are almost 400 active payloads, PSEs cannot, as a rule, attend design reviews (*e.g.*, Preliminary Design Reviews, Critical Design Reviews, *etc.*), nor do they offer specific design solutions and alternatives.

In discussing the process that Government Furnished Equipment (GFE, or the payloads that are developed in-house at NASA) goes through, it was pointed out that there is another panel, not the PSRP, which is responsible for certifying that class of hardware. It is called the Safety Mission Assurance Team (SMART), which is a subpanel of the ISS Safety Review Panel (SRP). In theory, all payloads must satisfy NSTS/1700.7B, Safety Policy and Requirements for Payloads Using the Space Transportation System, though the various panels often tailor the document as applicable. SMART uses SSP 50021, Safety Requirements Document for the International Space Station.

At several points in the discussion regarding GFE it was mentioned how there was more of an integrated team responsible for the GFE data packages and reviews. Often, the same group of people developing the hardware were also responsible at various points for its safety assessment. John Steils, who had previously worked developing GFE, expressed the opinion that it would

take GFE a lot longer to get through the system if they needed to go through the PSRP requirements. Nobody believed, however, that unsafe GFE was being flown.

During the final wrap-up, there was concern expressed that any modification of the system needs to ensure that it prevents “erosion” of the requirements. It is often difficult to fight against the mentality that “It’s flown *n* times, so it must be safe”. Focus has to be on the fundamental processes that determine whether a payload is safe or not. Mr. Larsen also mentioned a bad experience in the 1990’s when many payload developers started sub-contracting safety to inexperienced consultants. These consultants offered to “take care” of safety for a payload, often at an attractive price. However, they rarely had the experience or knowledge to deliver on their commitments, nor did they have the time to become sufficiently familiar with the design of the payloads they were supposed to be integrating. The situation in one case deteriorated so badly that the PSRP was forced to tell another NASA organization that they had to fire their safety consultants. Mr. Larsen wanted to make sure that we did not fall into this trap.

Overall, the impression that was presented was that the PSRP has accomplished a significant amount of process improvement over the last decade. They have taken an active role in simplifying the requirements and reducing the meetings and reviews that must be supported by the payload developer. Their focus is, in fact, on the developer and how they can make his or her job easier. At the same time, they remain very conscious of their responsibility to the astronauts and the space program in general of not allowing anything unsafe to fly. Table 4-4 summarizes the main points from the discussion.

Table 4-4: Main Points and Observations from Interview with the Payload Safety Review Panel

Main Points	Observations
Establishment of franchises	<ul style="list-style-type: none"> This is a very positive development. It moves the decision making power in the Payload Safety Review process closer to the payload developers. Illustrates a willingness on the part of PSRP to change the existing system.
Use of Data Management System, Web-X, etc..	<ul style="list-style-type: none"> Shifting away from paper submittals is a positive sign. However, deadlines and the number of reviews have not changed.
Overproduction of data by developers, role of the PSE	<ul style="list-style-type: none"> The PSEs have too many payloads to monitor. PSEs would need to increase their interaction with developers to better tailor the packages. Even if PSE load was reduced, it is unclear whether contractually, PSEs could give more direction to developers.
Frustration with requirements from other Centers GFE Process	<ul style="list-style-type: none"> Requirements should be standardized across NASA centers There is acknowledgement that the GFE process is different and more efficient, even though both processes meet the same requirements. One reason lies in the tighter integration between the developers and the GFE Safety Panel.
Concern over additional bureaucracy	<ul style="list-style-type: none"> Whatever changes result from the application of <i>lean</i> principles, they must ultimately produce measurable benefits to existing stakeholders

4.5 Summary

There was a great deal of overlap in the comments expressed by numerous stakeholders. In general, the view throughout was that interactions with the Panel itself, or with its supporting staff, tended to be productive and useful, though sometimes the turn-around time to obtain information was too long. Interposition of layers between the developer and the PSRP was viewed as a negative factor by all the stakeholders, including the Panel itself. This was irrespective of whether the layers were another organization within JSC, another NASA center, or even a separate, external company. This inefficiency was made even worse when the personnel in an intermediary layer insisted on having information channeled exclusively through them, while simultaneously not having the resources to truly become part of the integrated payload team.

Most of the payload developers expressed the view that personal contacts had a significant impact on the quality of their experience with the Payload Safety Review process. Being able to find the correct person with the information that was needed quickly was extremely important. Incorrect

or inconsistent information, as well as evolving requirements, was cited several times as an important concern.

The reforms to the process that have been undertaken by the Payload Safety Review Panel over the last decade have significantly helped in reducing the cost and resources needed to properly integrate a payload. The Panel is understandably very concerned that any reforms not compromise safety just for the sake of lowering cost. However, by their actions, it is clear that they are committed to continuously improve the process.

In the next chapter, these observations from the stakeholders, along with the analyses presented previously, will be brought together to design a proposed, ideal state for the Payload Safety Review process.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5: Desired State

Up to this point, we have approached the analysis of the NASA Payload Safety review process from three different directions:

- Using the LAI Transformation Roadmap, we have mapped the existing value streams and identified concerns and issues that may arise as *lean* practices are introduced into the process
- We have made comparisons between the problem of ensuring safety in payloads with limited resources and that of creating high quality products at low cost, and have been able to draw out similarities and differences between the two process characteristics.
- We have documented real experiences from users of the existing process and made observations regarding possible areas of improvements, as well as areas where the process has been already changed with measurable results.

With this information, it is now possible to recast the NASA Payload Safety Review process as a *lean* process, using the principles that were outlined in Chapter 1. In this chapter, we will march through each of the five *lean* principles and describe how the process should be changed in order to properly align itself with them. As we do this, however, we must bear in mind the various issues and concerns that were raised throughout this document as the process was analyzed in the three ways mentioned above. At the end of this chapter, we will explicitly list all of the concerns that have been previously raised and compare our desired *lean* state against them, to ensure that they have been properly addressed.

5.1 Define Value

The fundamental principle of *lean* is that all activities must be focused on delivering value. Anything that does not deliver value must be eliminated or, at worse, significantly reduced. The only question that can arise lies in defining exactly what is meant by value.

System architects define value as that which “... is delivered when the primary external process(es) acts on the operand in such a way that the needs of the beneficiary are satisfied at a desirable cost.” This definition is worth examining further. The various terms can be translated from “architecture-speak” to our own terminology, as shown in Table 5-1.

Table 5-1: Value Terminology Defined for the NASA Payload Safety Review Process

Architecture Definition	Translation
• External process	• Payload Safety Review process
• Operand	• The payload (including operations, testing, crew procedures, support systems, etc.)
• Beneficiary	• The stakeholders (as described in Chapter 2)
• Desirable Cost	• Within the available resources

So, if the definition is rewritten for our particular process, it becomes:

Value is delivered when the Payload Safety Review process produces a safe payload for the astronauts, developers, etc., within the available resources.

Note that the definition does not talk about safety reviews, the data packages, meetings, *etc.* The focus is on changing the state of the payload from a potentially *unsafe* state to one that is *safe* to operate. This is an extremely important distinction. In designing our desired *lean* process, it is not sufficient to simply streamline the information delivery tools. The focus has to be on how the various steps in the process contribute to the delivery of value, in other words, how they contribute to delivering a safe payload. As will be shown shortly, many of the reforms undertaken so far deal primarily with simplifying the tools and do not address some of the fundamental structural limitations of the existing process.

In their appropriately named volume, *Lean Enterprise Value*, Murman *et al.* define value as “how various stakeholders find particular worth, utility, benefit, or reward in exchange for their respective contributions to the enterprise”. In Chapter 2, it was shown how it is possible to identify the various stakeholders and their respective needs. All of the stakeholders have either a primary or secondary need for the payload to be safe. This is a very fortunate situation. A *lean* enterprise reaches its highest efficiency when all the stakeholders are satisfied by what they obtain

from their contributions. Often, stakeholder needs can be contradictory. In this case, they are not.

However, this is not to say that there may not be conflicts with regard to the second part of the definition, “in exchange for their respective contributions.” In a world of infinite resources, there is no optimization that can be done. It would always be possible to spend more and more money on additional testing, more redundancy, *etc.*, with no adverse consequences. In our design of a *lean* process, we must assume, as was said in Chapter 1, that there are a fixed amount of resources, even if we do not know, *a priori*, what these resources are. In other words, our *lean* process must ultimately require the same or less resources to deliver a safe payload than the process it is replacing. However, in evaluating this, cost for the entire process must be taken into account. So, for example, it is possible that costs on the payload developer side might increase, but costs on the NASA side will go down. That would be fine, as long as the sum yields a net savings.

With this understanding, we will utilize the value definition above and move onto the second principle for *lean*, identifying the value stream.

5.2 Identify Value Stream

The existing value streams were presented in Chapter 2. As was shown, depending on the complexity of the payloads, the value stream may not appear to be too un-*lean*. The main issues appeared to be the long wait times between submittal of the data package and the scheduling of the actual review itself for the various phases. This could easily be addressed, perhaps using a more user-friendly and interactive data-submittal system.

As the payload complexity increased, and we delved deeper into the value stream, additional problems became apparent. Some also arose in discussions with the various stakeholders as described in Chapter 4. One issue that stood out was the apparent difficulty in obtaining accurate information from the Panel outside of the reviews themselves, which leads to over-production of the submitted data or to the need to conduct Delta Phase Safety reviews. This problem could manifest itself in the form of simply not being able to reach the person with the right information, of getting incorrect information, or of not being provided with existing, already-flown designs for hardware components.

In light of our definition of value from the previous section, how might these concerns be addressed?

In principle, the Payload Safety Engineer (PSE) is responsible for providing the link between the payload developer and the Payload Safety Review Panel. In theory, this is a unique and invaluable role in the Payload Safety Review process. The PSE should be able to bridge the gap between the payload developer, who has all the knowledge of the payload design, operations, procedures, *etc.*, and the PSRP and its support staff, where the knowledge of the safety requirements resides, as well as the final authority for the determination of the safety status of the payloads. However, it is clear from the comments of the stakeholders that the present implementation of the PSE function is not satisfactory.

In order for the PSE to fulfill this liaison function, three changes would have to be made:

- The role of the PSE should only be filled by mid-level to senior experienced engineers. They should have the demonstrated ability either to provide answers to safety-related questions from the payload developers or to put the developers into contact with the members of the Panel who possess the required information.
- Each PSE should be assigned fewer payloads, so as to allow time to properly engage the payload development team. This must include, at a minimum, attending key design reviews and meetings.
- And finally, the PSE should have the authority to provide to the payload developers design guidance and direction, based on the PSE's previous experience and on rulings and information provided by the PSRP.

The first two of these points could be easily accommodated within the existing process. It would simply be necessary to change the experience-mix and increase the number of the PSE staff. Recall, however, that at present, there are only about 20 PSEs for approximately 400 payloads. Also, several stakeholders indicated that from their perspective the PSE roles tend to be filled by junior, less experienced engineers. This may in part be due to the fact that these roles are usually filled with contractor (not Civil Service) personnel. There is, therefore, an incentive to hire the least costly, and presumably least experienced, engineers. However, these issues are not insurmountable and are within the existing system's capability to address.

The third point is more problematic. Presently, the Payload Safety Review Panel (PSRP) is *not* the contracting organization for the any payload, regardless of whether they are being developed by NASA, the Department of Defense, other government agencies, or a commercial enterprise. In the case of NASA, payloads are normally managed through the numerous NASA field centers. Therefore, the PSRP does not have the authority to provide design direction to the payload developers, only to determine whether a given design meets the NASA safety requirements outlined in NSTS/ISS 13830. It may be possible within the existing government-contract structure and regulations to provide some design guidance, for example by providing previously flown and approved designs. However, it would be difficult within the present structure for the PSRP, through the PSEs, to provide true design direction to the payload developers.

Instead of trying to redefine the role of the PSE, it would be more productive to focus on the three points above as job requirements for a new position, one of a Payload Safety Facilitator (PSF), and decide in which stakeholder organization it would make the most sense for this role to be filled. Four options exist:

- As part of the NASA PSRP
- As part of the payload developer organization
- As part of the contracting organization (NASA field center, DoD, *etc.*)
- Somewhere else.

We have already discussed fulfilling this role within the PSRP structure and have shown that there are likely to be contractual limitations that prevent this from happening. With regards to the second option, in an ideal world with infinite resources, each payload developer organization would have on-staff an experienced safety expert, capable of answering all safety-related questions or making contact with PSRP members who can. However, given that there are presently over 400 payloads within the PSRP system, and many of those being developed by very small companies or university laboratories, this is unlikely.

Can the contracting organization fulfill this role? After all, they already have the contractual authority to provide technical direction. If they have personnel with the safety-related experience, and with the knowledge of the PSRP, then they could easily provide their payload developers with this service for those payloads which they manage. However, as we will see in the next section,

there are limitations to this approach, chief among them being the need to integrate the PSF into the development team, and not let the position become one that only provides supervision, inspection, or oversight.

In addition, if each contracting organization provided this role, it would also not address another concern which arose in the discussion of Chapter 2: if one looks at the Payload Safety Review process from the perspective of the PSRP, they see 400 individual payload developers trying to interface with their systems. There is little to no possibility of consolidation of the payloads into “First Tier”, “Second Tier”, *etc.*, classifications, as is done with suppliers in a traditional *lean* manufacturing process. Since the individual contracting organizations are each only responsible for a few payloads, it is not likely that they can perform any sort of consolidation among their own payloads, in order to streamline the Payload Safety Review process.

For these reasons, the fourth option provides a better alternative: an external organization set up to assist developers in designing safe payloads and in documenting this design as part of a *lean* Payload Safety Review process. Such an organization would consist of experienced Payload Safety Facilitators that would have knowledge of NASA’s safety requirements, and, more importantly, experience in their interpretation. They would work in partnership with the PSRP, and would be able to direct developers quickly to the resources available at the PSRP and their supporting staff, in order to obtain answers to questions at any point in the payload development process, not just as part of the safety reviews. Finally, they would also be able to provide developers with previously flown and approved designs and systems that can be used to reduce development and safety risk.

By not being part of the contracting organization, and by providing real, value-added capabilities, the PSFs should be perceived by the payload developers as being “part of the team”. At the same time, by not being part of the PSRP, they have the freedom to be much more direct in their recommendations and directions with regards to payload design. Clearly, there is no guarantee that their recommendations would be ultimately accepted by the PSRP. However, by drawing only on experienced personnel to staff the PSF positions, as well as by providing previously flown and approved designs for use by the developers, the likelihood that the hardware design arising from the efforts of the integrated design team would meet the NASA safety requirements is greatly increased.

Finally, in addition to providing this needed expertise to the payload developers, the PSFs would also be able to perform the consolidation function discussed previously. Similar payloads, or payloads on the same mission or flight increment, could be presented together to the PSRP, thereby reducing the amount of time required for review. Also, this external organization could provide a centralized repository for data, documents, previously flown data packages, training material, *etc.* As was shown in Chapter 4, some of this is already done by the PSRP. This organization could extend and simplify the process for access to this information.

In summary, significant improvement to the process would result from the implementation of this external PSF function. It would eliminate one of the major shortcomings in the present system, which is that safety-related information is difficult to obtain and is often not timely. Of course, this would come at a non-insignificant cost, a cost that will have to be taken into account when the total process cost for the new *lean* Payload Safety Review process is calculated later in this chapter. Remember, it is the intent for the PSFs to become part of the payload development team. They should attend design reviews, integration meetings, *etc.* Even though much of this could be accomplished through video or teleconferencing, it would still be necessary to limit the number of payloads assigned to each PSF. This will drive up the cost of implementing this change in the process. For now, we will list it as our first proposed change for the transformation of the Payload Safety Review process, and continue to the third *lean* principle, flowing the product.

Proposed Change #1:

Establish an external organization, staffed by personnel (Payload Safety Facilitators) that would work in partnership with the PSRP, and who can provide experienced, timely design guidance and direction to the payload developers as an integral part of their design teams.

5.3 Flow the Product

One of the principles of *lean* is that the product (in our case, the payload and the information needed to ensure that it is safe) should flow without any interruption. Anything that interrupts this flow is *muda* and should be eliminated.

When the various value streams were mapped in Chapter 2, it was shown that payload developers must sometimes obtain approval of submittals to the PSRP from their contracting organization, whether it is another NASA center, the Department of Defense, or other government agency. This results in a series of intermediary reviews where information is sent to the contracting center, reviewed, and returned to the payload developer for changes. The process is repeated until the contracting center is satisfied, at which point the data packages are sent on to the PSRP.

Is this *muda*? Does this interrupt the flow of the product down the process and increase the time and cost needed to arrive at a safe payload? To answer this, it is necessary to focus on where the authority resides for certifying a payload as being safe to fly? Clearly, it resides exclusively with the Payload Safety Review Panel. Inputs from other organizations to the design of the payload, from the point of view of safety, cannot be assumed to have any definitive validity. They do not bind the PSRP. In fact, several of the stakeholders related instances where they had been given design guidance that proved to be incorrect once it was reviewed by the PSRP.

Therefore, the personnel at the contracting centers that are responsible for reviewing the data generated by the payload developers are in an untenable situation: they have the authority to approve or disapprove the data submittals, and, since they are part of the contracting organization, can in fact require changes to be carried out before the information is sent to the PSRP. However, they have no real power to make the final decisions with regard to the safety certification of the payload. Their function, as it is performed in the present process, does not contribute towards creating value, as we have defined it, *i.e.*, creating a safe payload.

This does not in any way mean that their technical contributions are worthless. Quite the contrary. If we assume that the people performing these reviews at the various NASA centers are quite experienced with the Payload Safety Review process, they could have invaluable contributions to make. In particular, they could in fact provide data, previously-flown designs, *etc.*, to the payload developers which would be used to produce a safer payload. The problem is that in the present system, this interaction is conducted essentially in a manner reminiscent of the way that quality was “assured” in old-style mass production factories (Chapter 3). The reviewers typically do not engage in the process until the developer is already far along both with the payload design and with the creation of the safety data packages. The reviewers tend to be responsible for a large number of payloads, which prevents them from having sufficient time to spend on any single one. This means that the payload developer often must spend a significant

amount of time and resources “spooling-up” the reviewers, so that they can understand the information presented to them. Ultimately, it is unavoidable that an antagonistic relationship is created between the reviewers and the payload developer, a relationship that is made even worse by the fact that their function does not provide value, since they do not ultimately control the determination of what is or is not safe.

The answer lies in changing the way the personnel that presently review the data submittals are utilized in the process. Instead of requiring payload developers to provide data packages for review to the NASA centers prior to submittal, the personnel that nominally do these reviews should engage with the design team well prior to the data package submittal. They should offer their design experience and advice as members of an integrated design team. The output should be an integrated data package that is submitted directly to the NASA PSRP, without any intermediary reviews. This of course, is exactly the role that was previously discussed as being filled by the Payload Safety Facilitators in the previous section. Therefore, implementation of the PSF function would also provide this capability to the payload developer.

Once these intermediary review steps are eliminated, the payload safety data will flow unimpeded from the developer (with the active and continuous input from the PSF), to the Payload Safety Review Panel. We cannot underestimate the importance of eliminating these *muda* steps. Ultimately, the responsibility for developing a safe payload must reside with the team that is also responsible for the design. They are the ones who know the design and the tradeoffs that have been done in order to meet all the various requirements. The present process gives a veto on what is submitted to the PSRP to personnel that do not have this knowledge in an attempt, ultimately, to assure a safe payload through an after-the-fact inspection. It is an excellent example of a *monument*, a way of doing things that may have had a justification in the past, but now only results in higher costs, longer delays, and no increase in value, i.e., safety.

To summarize, the discussion above leads us to our next recommendation:

Proposed Change #2:

Payload development contracts should clearly state that the payload developer has the ultimate responsibility for producing a safe payload. The developer should therefore have final say in any submittals of information to the NASA PSRP. Intermediate reviews conducted outside of the PSRP are “monuments,” and should be eliminated.

5.4 Pull the Product Through the Process

In a pull system, nothing is produced at any step unless it is specifically needed by the step immediately downstream. Buildup of inventory in front of each step, or safety stocks, is not permitted. The reasoning behind this is that it makes no sense to produce anything for which there has not been a demonstrated need. This overproduction is simply *muda*.

The first way that overproduction can manifest itself in the Payload Safety Review process is by safety data packages containing information that is not needed to adequately assess the safety of the payload. The Panel indicated (Chapter 4) that many packages exhibit this problem, in particular with regards to including detailed descriptions of their data systems when no software hazard control is present. Assuming that the developers do not wish to produce documents with information that is not needed, a possible cause of this is that the developers are not sufficiently familiar with the requirements, or they lacked information that would have helped them to better tailor their data submittals. The incorporation of an experienced Payload Safety Facilitator, actively engaged as part of an integrated team, should greatly decrease this type of overproduction.

A second, more important source of overproduction of information lies in the fixed structure of the existing process. As described in Chapter 3, sequential review of the design is a valid way of quantifying the level of an emerging property such as *safety*. Only by going over the entire design at various points in the development timeline can the PSRP ensure itself that the ultimate product is indeed safe. However, the recognition that the method is fundamentally valid does not mean that a set number of discreet safety reviews is the only way to accomplish this goal.

It is quite common in the present process for payloads not to be required to support all four reviews called out for in the baseline process. Occasionally, however, additional reviews may be required. In Chapter 2, value streams for three different payloads were created. In each case, the number of reviews had been reduced or increased depending on the complexity and special features of the payload.

This flexibility to tailor the standard process to the unique requirements and features of each payload is an excellent innovation that already reduces the costs required to support the payload safety integration. The only issue is that since this is done on a case-by-case basis, it is difficult to properly plan for this flexibility at the start of a project. What would be needed is an explicit and

detailed list of criteria available to payload developers so that they would know, *a priori*, whether their hardware would be required to satisfy four, three, or even fewer safety reviews.

It is possible, however, to go further and think about a system where discreet reviews are no longer required. Recall that the PSFs, if they perform their function properly, are meant to serve as the link between the developer and the PSRP. There is no reason that the PSF could not also be responsible for recommending the frequency, timing, and content of submittals to the PSRP. This could be done beginning with smaller, less complex payloads and, as confidence in the process is increased be extended to more complex hardware.

This process would function by having the PSF assigned to each payload perform an initial safety analysis early in the development process. This analysis would consist of determining the initial hazards, controls, *etc.*, much in the same way that it is presently done. In addition, the PSF would also prepare a Safety Verification and Review Plan, which would propose a schedule for the PSRP review activities, and whether there is specific support they might require from the PSRP staff personnel. Such a plan might propose, for example, that all hazards be reviewed off-line, because there are no major systems that would require a real-time meeting. It might propose that a review would need to be held to discuss one particular subsystem that is more problematic or has more hazardous potential. It might also inform the PSRP that the payload anticipates requiring input from certain PSRP staff with unique skills (*e.g.*, toxicologists, EVA operations, *etc.*). This would allow the PSRP to be able to anticipate the use of the resources that they control and to plan accordingly.

The PSRP would not necessarily have to agree to the Plan that is delivered to them. They would be able to make modifications, perhaps requiring additional reviews or data submittals. However, once the plan is agreed to, it would provide both the PSRP and the payload developer with a common plan for all the safety-related activities. Only information required by the Plan (and by extension, the PSRP) would be generated. Overproduction would be reduced, as only information called out for by the tailored Plan would be *pulled* from the payload development team.

The concern might be raised that such a modification to the process reduces independent oversight and therefore might lead to abuse, and more importantly, less safe payloads. It would be necessary to guard against that by doing periodic audits of payloads, to ensure that they are

indeed complying with all the safety requirements that they indicate in their Plans. In addition, initially only smaller, less complex payloads would follow this new process. More complex payloads would still undergo the traditional multi-phase reviews. There is also evidence from other industries and processes that have done similar changes that would indicate that abuse does not increase when stakeholders are allowed to self-police. The insurance industry, for example, now routinely pays claims below a certain amount without any claim adjusters having to perform inspections³¹. They have found through periodic audits that no significant increase in fraud or abuse has occurred.

In summary, transformation of the Payload Safety Review process to a *pull* system should have the effect of focusing the reviews and the resources of the PSRP on the payloads and hazards that have the most potential for causing safety concerns on ISS. This should serve to reduce the safety risk while allowing payload developer resources to be focused exclusively on those areas of concern.

Proposed Change #3:

The Payload Safety Facilitators will prepare a Safety Verification and Review plan for each payload and submit the plan for approval to the PSRP at the start of each development effort. The plan would contain the schedule and content for all safety-related review activities and data submittals and would pull these activities throughout the process..

5.5 *Strive for Perfection*

The final principle of *lean* engineering is the continuous striving for improvement. Even after all the *muda* has been eliminated, and even after significant gains have been made in productivity and reduction of costs, the transformation cannot be allowed to stop. Each change in one step of the process will likely have an effect on the other steps, especially those immediately preceding and following it. These should be looked at as additional opportunities for improvement.

The Payload Safety Review process is no exception. A series of proposed changes has been suggested here. It would be presumptuous to believe that this is a comprehensive list. Undoubtedly, additional opportunities for improvement will become apparent once these modifications have been put in place. We should bear in mind, however, that the time span for

developing payloads, even if *lean* changes are implemented throughout all the integration and development processes, not just safety, is not likely to span less than one year for less complex payloads, and multiple years for others. Therefore, it is important to be very careful to not be continuously changing the system once a payload has begun its development.

Does this pose a fundamental conflict with *lean*? Not necessarily. Change and improvement can still occur. However, these improvements must be evaluated not only with regard to their impact on the overall process, but also with regard to their impact on the payload developers. For example, certain changes might only be implemented in a “grandfathered” mode, where existing payloads follow the established process and only new projects are affected.

5.6 *New Value Stream*

It is now possible to take the three recommendations made in this chapter and redraw the value stream for the Payload Safety Review process. This has been done in Figure 5-1. Since the steps in this new value stream are *pulled*, only a single process is needed to represent all three payload types from Chapter 2. The durations for the steps are consistent with those from the existing process. For each step, the ranges specified are the minimum and maximum values for that step across all three of the payload types. In order to be conservative, the labor requirements were simply taken to be the maximum value needed by the most complex payload, Type 3. When new steps were added, duration and labor was estimated based on past experience with similar tasks.

A few obvious differences between this value stream and the existing ones stand out:

- The multiple reviews have been replaced by the payload SVR plan, with a single review at the end of the process. As stated previously, in many cases even this review might not be needed, but it is included here, along with the standard 60 day submittal period, in order to be conservative.
- The Payload Safety Facilitator plays a lead role in most of the tasks. This is consistent with the PSF being part of an integrated payload development team, and not simply an outsider that periodically has input into the process.

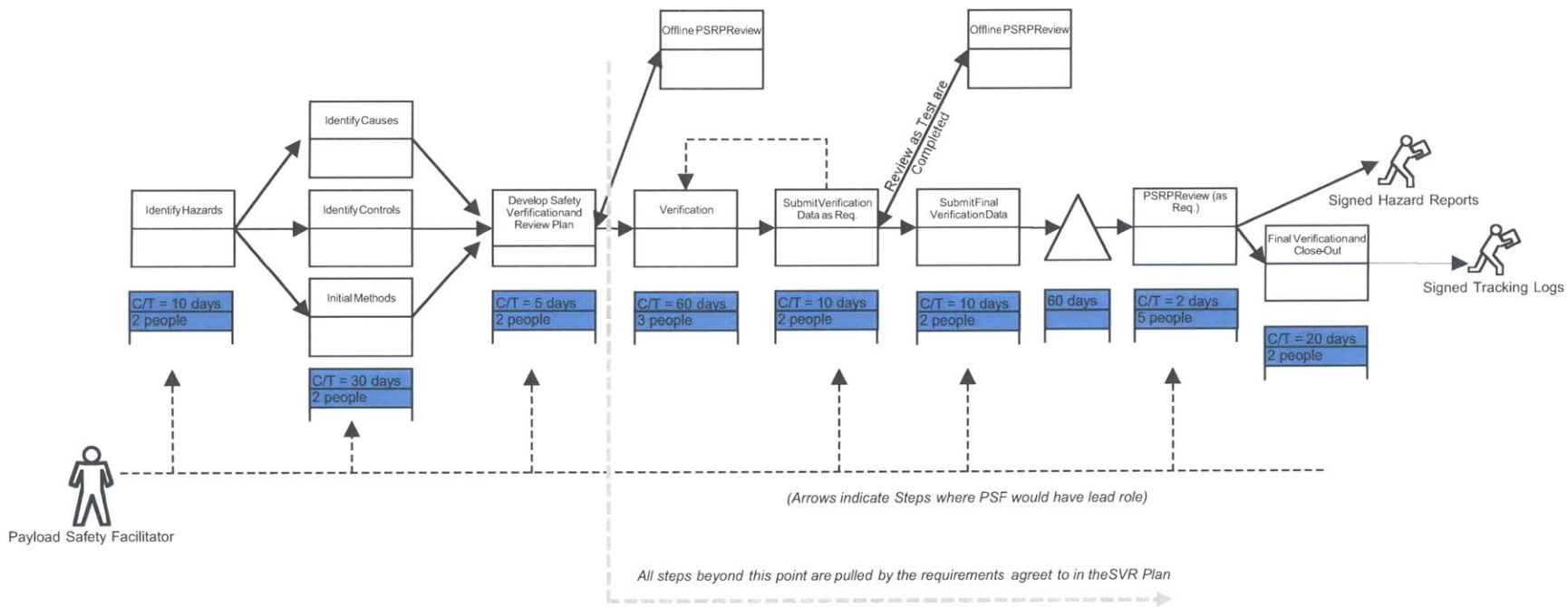


Figure 5-1: The Proposed Lean Value Stream

- The dashed line closing the loop between the Verification and the Data Submittal steps is meant to indicate that this occurs as the verification steps are completed. In other words, the PSF does not wait for all the hazards to be closed out before submitting them. On the contrary, they are submitted as soon as possible on a continuing basis. The days listed in the diagram, however, are cumulative for all activities.
- The number of person-days to complete the tasks have not been changed from the assumptions used for the present processes. This therefore assumes that the PSF replaces an equivalent person in the present payload development team. In many cases, this would be a conservative assumption, since the PSF brings significant safety and spaceflight experience to the team.

The time needed to complete the process, as well as the person-days and wait time, have been significantly reduced. Table 5-2 lists the duration and labor required for each of the processes from Chapter 2, along with the equivalent information for the new *lean* value stream.

Table 5-2: Comparison of Desired State with Previous Processes

Type of Payload	Min Duration (days)	Max Duration (days)	Waiting Time (days)	Min Labor (person-days)	Max Labor (person-days)
Type 1	149	186	120	62	149
Type 2	298	340	225	166	265
Type 3	428	506	285	335	528
Desired	90	203	60	73	409

The table shows that the shortest amount of time that the Payload Safety Review process can now take is 90 days, compared with 149 days from before. The longest it can take is 203 days, as compared with 506 from the existing state. These are reductions of 39% and 59%, respectively, in large part due to the reduction in the number of reviews and their associated waiting times. Note that these times *do not* include the time required to properly design and fabricate the payload. The durations simply refer exclusively to the amount of time needed to satisfy the Payload Safety Review process.

The table also shows that the minimum labor required with the new process is 73 person-days. However, the existing process could, theoretically, require only 62 person-days to complete. At the level of the assumptions used for these calculations, these numbers are more or less the same.

Even if they are not, what this says is that the existing process, as it is applied to the simplest of payloads, is already very *lean*. The proposed modifications may actually not benefit these cases, since the existing process is already able to tailor itself to the very limited requirements of these payloads. The main benefit that is achieved is that this tailoring can now be extended to other, more complex payloads. The data in the table shows this in that the maximum amount of labor required has been reduced from 528 to 409 days, a 22% reduction.

This data is better seen in Figure 5-2, which reproduces the results from Chapter 2 and adds the total time required by the new, *lean* process, and Figure 5-3, which does the same thing for the required labor. Again, in plotting these two figures, complexity is assumed to scale linearly with cost of the payload.

Clearly, the proposed changes have a positive effect on the overall process from the point of view of reducing the time and manpower required to complete it. The changes also have the benefit that, from the perspective of the PSRP, the only change they would need to make is to review the Safety Verification Plan and sign-off on the data and presentations that would be required. In some respects, it is no different than what is done now on an ad-hoc basis, where some payloads are able to reduce the number of reviews. The proposed process allows this to occur in a more uniform manner, and, due to the presence of the PSF, to accomplish this in a way which does not increase risk or decrease the oversight of the PSRP.

In conclusion, it has been mentioned earlier that all the time durations presented here refer exclusively to the amount of time required to satisfy the Payload Safety Review process, and not to the overall amount of time required to design and build a payload. This can depend on many other factors. However, reduction in the time required by the safety process means that the overall time it takes to go from experiment concept to flight on ISS will not be governed by how long it takes to meet all the steps in the existing process. Application of *lean* principles, if applied across the board for all payload integration activities, means that the time required to move from ground-based experiments to the ISS will be determined by the complexity of the experiment, and not according to an *a priori* schedule. Shortening this time will be seen as a very positive development by the best and brightest researchers that the ISS hopes to attract in order to fulfill its promise as a real working microgravity laboratory.

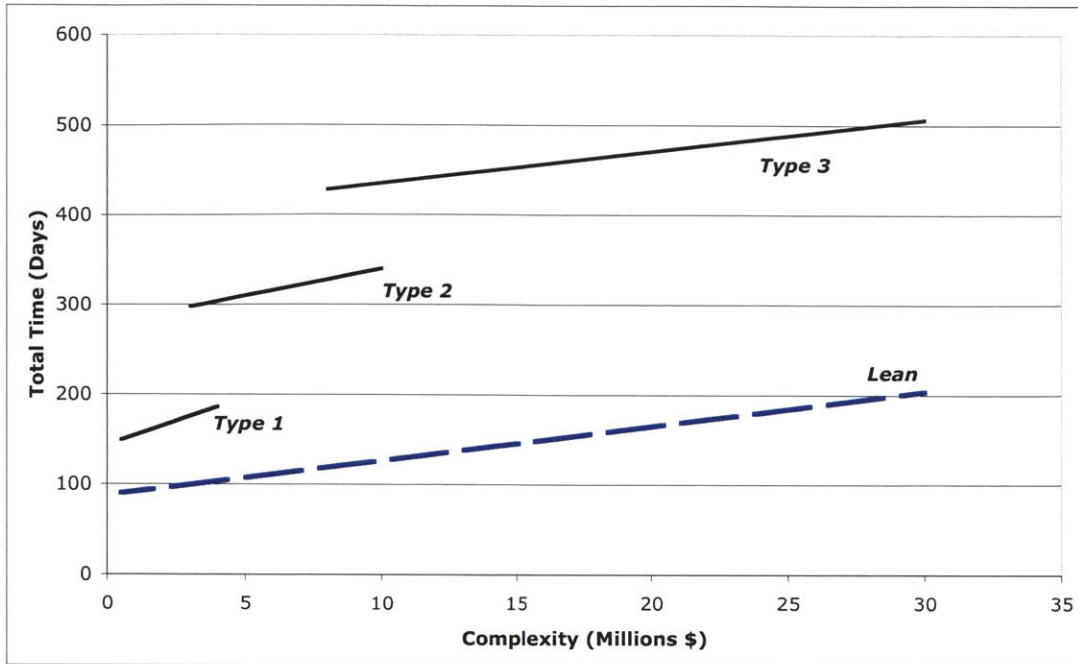


Figure 5-2: Total Time Required to Complete the Payload Safety Review Process

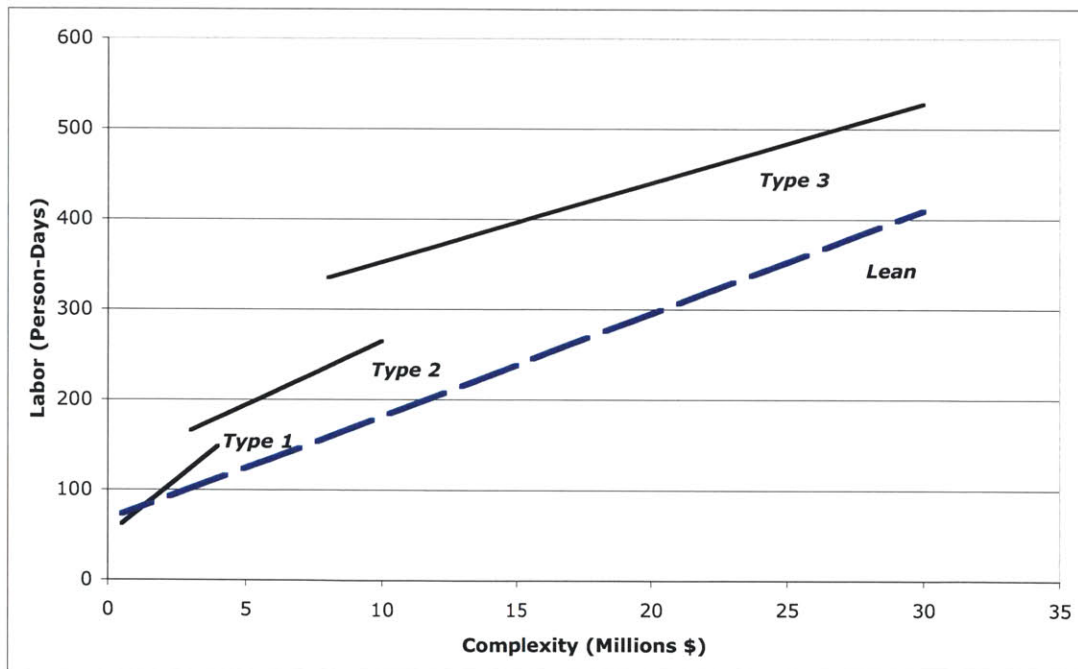


Figure 5-3: Total Labor Required to Complete the Payload Safety Review Process

5.7 Metrics

In Chapter 2, three metrics were proposed to evaluate any proposed change to the process.

These were:

- Reduction in baseline time required to move through the process
- Customer satisfaction, as measured by customer surveys and complaints
- Efficiency, as measured by the *total* number of personnel required to support a typical payload.

It has already been shown that the first of these, reduction in time required, has been achieved. The second metric cannot be adequately evaluated until the system is in place, and stakeholder feedback is obtained.

The third metric, efficiency, has also been demonstrated, since the total labor required has been reduced. It is possible to estimate the cost savings of the proposed *lean* process. Savings arise primarily due to the reduction in time to complete the Payload Safety Review process. For the purposes of this calculation, we will not consider any savings within the PSRP itself or within the contracting agency. In other words, it is assumed that the same number of PSEs continue to work for the PSRP and to function in their existing role. It is also assumed that the contracting agency personnel that under the old process reviewed that payload developer data are still present in an advisory function, no longer reviewing the data packages prior to submittal to the PSRP. These are both very conservative assumptions. Obviously, if the new process is effective, over time fewer PSEs and contracting agency personnel will be needed to directly support the payload developers, and they can be reassigned to other duties.

For each of the three payload types, an average complexity can be calculated, and the corresponding labor determined from Figure 5-3. At the same complexity level, the corresponding labor for the new *lean* process can be calculated as well. This is illustrated in Figure 5-4.

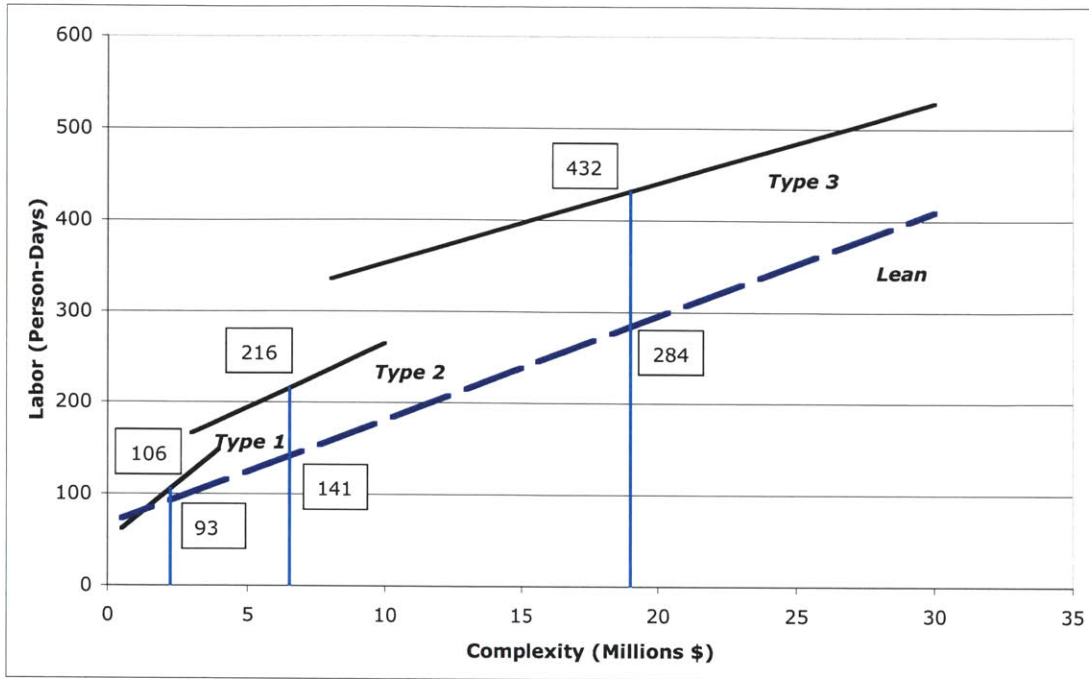


Figure 5-4: Average Labor Required (in boxes) for Each Process

Assuming a total burdened cost of \$180,000/year (and 230 work days per year) for labor costs, the average savings per payload can be calculated and is shown in Table 5-3:

Table 5-3: Average Expected Savings per Type of Payload

Type of Payload	Avg. Labor (person-days)	Lean Labor (person-days)	Avg. Cost	Lean Cost	Savings
Type 1	106	93	\$82,957	\$72,783	\$10,174
Type 2	216	141	\$169,043	\$110,348	\$58,696
Type 3	432	284	\$338,087	\$222,261	\$115,826

In order to estimate total savings, it will be assumed that the 400 experiments presently in the PSRP system are divided equally between experiments of Type 1, Type 2, and Type 3. It will also be assumed that the development time (time from contract start to delivery of the hardware) for the three types of experiments are 1.5, 2, and 3 years, respectively, reflecting the fact that development time also often scales with complexity. Under these assumptions, the total savings can be calculated to be as shown in Table 5-4.

Table 5-4: Savings Due to Implementation of Lean Process Changes

Type of Payload	Savings	Dev. Time (years)	Savings/Payload/Year	No. of Payloads	Total Savings/year
Type 1	\$10,174	1.5	\$6,783	133	\$902,087
Type 2	\$58,696	2	\$29,348	133	\$3,903,261
Type 3	\$115,826	3	\$38,609	133	\$5,134,957
Total			\$74,739	399	\$9,940,304

Therefore, the proposed transformation can produce savings on the order of ten million dollars per year. Recall that no savings were assumed either for the PSRP or for the contracting agencies. If these conservative assumptions were to be relaxed, the cost savings would be even more striking. Of course, it must be repeated that the values used for task durations are only estimates based on a payload of medium complexity. The numbers can vary widely, and a more detailed study should attempt to better define both the existing and the expected future payload distribution. However, it is clear that *lean* transformation can in fact result in significant savings.

What about the cost of the Payload Safety Facilitators? Recall that their labor was assumed to reduce the labor required by the payload developer by a proportional amount. In other words, for each PSF, there will be one less person employed by the payload developers. Therefore, the costs should remain the same. However, this may not be realistic. It is often difficult for existing organizations to be reduced in size. It may be more appropriate to assume that at least initially, the PSF would supplement the existing payload developer labor force.

If this is the case, then it is possible to calculate how many PSFs could be hired using the savings from the new process. Assuming as before a labor cost of \$180,000, \$10 million in savings per year could support 56 new hires. For the purposes of comparison, this is more than double the existing number of Payload Safety Engineers. With 400 payloads in development, each PSF would have assigned between seven and eight payloads, which is a workload approximately half that of the PSEs under the existing system. Therefore, the PSFs could devote more than double the resources, on average, to the payloads than what is presently accomplished. This workload may still be too high to allow the PSF to adequately focus on each experiment. However, if additional savings are obtained through the reduction in the levels of PSEs or of contracting agency personnel, then the ratio of experiments to PSF could be reduced even further.

Finally, it is prudent to return to the concerns that have been raised throughout the course of this document, either by the stakeholders that were interviewed or by the analyses presented in Chapters 2 and 3, and ensure that our proposed changes properly address them. The concerns are summarized in Table 5-5, along with a cross-reference to each of the proposed recommendations and a short explanation regarding how the concern is in fact resolved. This cross-reference matrix serves as a check on our analysis to ensure that none of the concerns expressed earlier have been ignored.

In summary, implementation of the three recommendations listed in this chapter results in a *lean* process that satisfies the criteria that were laid out in Chapter 2. It produces a shorter value stream and requires less time and labor in order to complete the steps. Even if new personnel are hired to fill the role of Payload Safety Facilitators, the new process requires, in the worst case, no more resources than the existing one, while significantly reducing the process durations and interfaces. At the same time, it addresses all the major issues and concerns raised throughout the course of this analysis.

Table 5-5: Cross Reference of Proposed Recommendations to Issues Raised

Issues/Concerns	Recommendation			Comments
	1	2	3	
From the Transformation to Lean Roadmap (Section 2.7):				
Opportunity for applying <i>lean</i> principles in the NASA ISS Payload Safety Review process appear to exist,	✓	✓	✓	<ul style="list-style-type: none"> The proposed transformation builds upon the existing changes instituted by the PSRP over the last decade. Proposed changes require participation of all major stakeholders An external organization would have flexibility to combine safety efforts for similar payloads Flown designs will be made available to similar payloads. An external organization would not have the same restrictions that the PSRP presently has. Design guidance and direction could be given. Proposed changes yield a shorter process, with less required labor.
The diversity and number of payloads	✓			
Limitations due to the contract and organizational structure of NASA	✓	✓		
Metrics must be used to validate any proposed changes to the process.	✓	✓	✓	
From the Quality-Lean Comparative Analysis (Section 3.5.3):				
Monitoring of the Entire Process	✓		✓	<ul style="list-style-type: none"> The Safety Verification and Review Plan provides for tailoring the safety review process, depending on complexity and hazards Monitoring will be provided by the PSRP and the PSFs The PSFs will provide continuous input and feedback to the developer team The PSFs will form part of the integrated development team. Since they are not part of the PSRP, an antagonistic relationship with the team will be avoided. The Safety Verification and Review Plan will specify the reporting and verification requirements for each payload. No data will be created that is not called out in the SVRP
Feedback	✓			
Integrated Teams	✓			
Creation of a Pull System			✓	
From the Observations of K. Slater (Section 4.1):				
Access to Information	✓	✓		<ul style="list-style-type: none"> The PSF is an easily accessible source of information The PSF will be able to contact additional resources on the PSRP in a timely manner Elimination of intermediary reviews and personnel will reduce errors and delays.

Experience of Engineering Support	✓		<ul style="list-style-type: none"> The role of the PSE will be filled by more senior engineers. The PSF will draw upon experienced PSRP staff when needed.
Inconsistent Interpretation of Safety Guidelines	✓	✓	<ul style="list-style-type: none"> Intermediary reviews will be eliminated, which reduces sources for inconsistent information The PSF will provide continuity across reviews, reducing inconsistencies.
Fear of Standardization	✓		<ul style="list-style-type: none"> The PSF will provide design guidance and direction to the payload developer team.
Multi-Phase System		✓	<ul style="list-style-type: none"> The SVRP will tailor the reviews for each payload
<hr/>			
From the Observations of S. Sell (Section 4.2)			
"Can't get a straight answer"	✓		<ul style="list-style-type: none"> The PSF is an easily accessible source of information
Lack of design guidance	✓		<ul style="list-style-type: none"> The PSF will provide design guidance and direction to the payload developer team.
Incorrect information provided outside of safety reviews	✓	✓	<ul style="list-style-type: none"> Intermediary reviews are eliminated, which reduces sources for inconsistent information The PSF will provide continuity across reviews, reducing inconsistencies.
Bureaucracy levels	✓	✓	<ul style="list-style-type: none"> Intermediary reviews from contracting organizations will be eliminated The PSF will allow better access to PSRP staff
Insistence on being single point of contact	✓		<ul style="list-style-type: none"> The PSF will not be the single point of contact. As an integrated member of the team, he will facilitate contact among the required personnel. The PSF will support a limited number of payloads, in order to allow more familiarity with the technical requirements of each project and enhance the ability to respond to questions from the PSRP.
<hr/>			
From the Observations of E. Bokhour (Section 4.3):			
"Importance of personal contacts"	✓		<ul style="list-style-type: none"> The PSF is an easily accessible source of information. The PSF will allow better access to PSRP staff.
"One degree of separation" between developers and panel	✓	✓	<ul style="list-style-type: none"> Intermediary reviews from contracting organizations will be eliminated.
Evolving requirements	✓	✓	<ul style="list-style-type: none"> Intermediary reviews will be eliminated, which will reduce sources of inconsistent information The PSF will provide continuity across reviews, reducing inconsistencies. The PSF can help to quickly disseminate any necessary changes to the Payload Safety Review process.
"Prove safety to ourselves"	✓		<ul style="list-style-type: none"> As an integrated member of the design team, the PSF will bring the

knowledge of the Payload Safety Review process to the center of the design team.

From the Observations of the PSRP (Section 4.4):				
Establishment of franchises	✓	✓	✓	<ul style="list-style-type: none"> The proposed changes will build upon this already-expressed willingness to modify and improve the safety review system.
Use of Data Management System, Web-X, etc.	✓			<ul style="list-style-type: none"> The proposed process will rely on telepresence and other technologies to allow the PSFs to properly integrate with the design teams.
Overproduction of data by developers, role of the PSE	✓		✓	<ul style="list-style-type: none"> The Safety Verification and Review Plan will specify the reporting and verification requirements for each payload. No data will be created that is not called out in the SVRP. Intermediary reviews are eliminated.
Frustration with requirements from other Centers			✓	
GFE Process	✓			<ul style="list-style-type: none"> The proposed process aligns more closely with the existing GFE process, by having PSF integrated into the design teams.
Concern over additional bureaucracy	✓	✓		<ul style="list-style-type: none"> Whatever changes result from the application of <i>lean</i> principles, they must ultimately produce measurable benefits to existing stakeholders

Chapter 6:

Summary and Recommendations for Future Work

6.1 Summary

The International Space Station is one of the most complex engineering projects ever attempted by humankind. It is a project on the scale of the Apollo moon landings, being performed at a fraction of the cost and with the added complications and interfaces brought along by the participation of a half-dozen international partners. As in all manned spaceflight activities, safety, whether it be the safety of the crew or of the vehicle itself, is of critical importance. A catastrophic accident or astronaut death could derail or even end the program, putting an end to a permanent human presence in space for the foreseeable future.

With the stakes so high, and especially after the Columbia tragedy, it would seem that attempting to transform a system designed to ensure the safety of payloads flown on the Station would be imprudent, or at the very least, untimely. After all, the Payload Safety Review process has functioned well in the Shuttle era. Payloads have never caused a major hazard aboard a US spaceflight that has led to death, injury, or damage. In addition, the NASA Payload Safety Review Panel has itself already instituted many process changes, designed to streamline and reduce the cost associated with this integration activity.

However, it is precisely because of the central role that safety plays in all spaceflight activities that a *lean* transformation of the processes used to ensure it must be undertaken. Operations on-board the International Space Station will be very different than those that have gone before. These are less structured activities than traditional “missions” and require more flexibility and efficiency. There will be more payloads, more on-orbit time, less training, and more opportunities for discovery. The existing system can support these activities, but it will be time-consuming and expensive. These resources may simply not be available.

The work described in this document has shown that application of *lean* principles, when it is accomplished with a full understanding of the unique technical restrictions and opportunities of the human spaceflight world, can yield significant savings in both time and resources. It was shown that while many of the steps in the MIT Lean Aerospace Initiative Transformation to Lean

roadmap are directly applicable to the Payload Safety Review process, more are not. This is due in part to the limitations of the payload development contract structure, which prevents design direction from being given to the payload developers by the people that are most familiar with the safety requirements. The decentralized nature of the existing process, with its large number of payload developers ranging in size from large corporations to small university laboratories, can also be a barrier to a successful implementation of *lean* transformation.

The Roadmap was applied to three separate examples of payloads of increasing degrees of complexity. Three separate value streams were derived, and estimates for duration and labor requirements were presented based on past experience and data obtained from various stakeholders. These value streams identified several opportunities for *muda* reduction, especially with regards to the reduction in the amount of delay between submittal of the data and the actual review, and the elimination of intermediary review steps imposed by organizations outside the control of the Payload Safety Review Panel.

Another perspective on the problem of designing safe payloads using limited resources was obtained by comparing the similar issues faced by industry over the last several decades in increasing the quality while reducing the cost of their products. Both of these processes have several similarities as well as several important differences. Among the former was the fact that both quality and safety are emergent properties of systems that cannot be adequately evaluated without a holistic perspective, which includes not only the hardware and software, but also the operations, manufacturing standards, *etc.* Among the latter was the fact that the sheer number of mass-produced items allows the application of statistical quality control techniques that are simply not available in the craftsman-like environment in which most payloads are created.

Nevertheless, the analytical comparison yielded several important insights. First, the present system relies almost exclusively on discreet evaluation phases and not on a continuous monitoring of the process. Second, opportunities for feedback from personnel knowledgeable about the safety requirements are limited. Third, there are no integrated teams, and instead the payload developers and the safety personnel exist in two separate, sometimes antagonistic, organizations. And finally, the existing system does not *pull* its requirements from the developers as they are needed, which leads to overproduction and waste.

These analyses were supported by data obtained from numerous stakeholders in the process. Integration engineers, project managers, and the Safety Panel itself were interviewed and their experiences and impressions of the present system were summarized and compared. Their comments were subsequently tabulated in a cross-reference matrix where all proposed changes to the process were evaluated to ensure that all issues and concerns had been properly addressed.

These insights from the analyses and the stakeholder data were used to design potential improvements to the Payload Safety Review process. Three specific recommendations were proposed:

- Establishment of a group of Payload Safety Facilitators outside the Safety Review Panel or other NASA contracting center, staffed by personnel who can provide experienced, timely design guidance and direction regarding safety issues to payload developers as an integral part of their design teams.
- Empowerment of these integrated payload development teams through elimination of *monuments* created by intermediary safety reviews conducted by organizations outside the control of the Safety Review Panel.
- The preparation of a Safety Verification and Review plan for each payload at the *start* of each development effort, which would contain the schedule and content for all safety-related review activities and data submittals and would *pull* these activities throughout the process.

Note that all the recommendations retain the role of the Payload Safety Review Panel as the final authority regarding safety of all payloads that fly to ISS. The Payload Safety Facilitators can provide guidance and direction to the payload developers, based on their own experience, and can provide easier access to the Panel resources. The Panel, however, must ultimately be satisfied that the payload is safe to fly.

The number of discrete steps in the Payload Safety Review process, which had been 27, 16, or 12 depending on the complexity of the payload, was reduced to 10 in the proposed redesign. Duration of the process was reduced between 40% and 60%, again depending on complexity. Required labor, as measured by labor-hours, was reduced by 20% for the most complex payloads, though it remained essentially unchanged for the simplest payloads, due to the fact that in these cases the Payload Safety Review Panel has already implemented several notable *lean* process

improvements. Nevertheless, the proposed changes were shown to yield savings on the order of \$10 million/year, depending on the number and complexity of the payloads.

In summary, a *lean* transformation of the Payload Safety Review process can yield important benefits, both in the reduction of the amount of dollars spent as well as in the amount of time required for a payload to satisfy all the safety requirements. These savings can be achieved with very few modifications to the existing organizations responsible for the Payload Safety Review process and without jeopardizing the safe operations of the ISS.

6.2 Future Work

The work that was described in this document proposed a series of changes to improve the existing NASA Payload Safety Review process. Now that this *desired state* has been derived, the next step would be to engage the various stakeholders directly to bring about implementation of these changes. The difficulty of this task, given the large number of interested parties and the general slow pace of change inherent in any bureaucracy, cannot be overestimated. However, as noted in Chapter 2, successful implementation of *lean* transformation must begin with a buy-in from the top. Recent events at NASA, such as the already-mentioned *One NASA* initiative (see Chapter 2), as well as the demonstrated willingness of the Panel to implement changes to the process over the last decade, makes us hopeful that this transformation can in fact succeed.

The analysis presented here could also be applied to the other safety processes within NASA, such as those used in the development of operational hardware, crew hardware, or government furnished equipment, which are reviewed by other NASA safety Panels. When this was discussed with the PSRP, it appeared that these processes incorporate several features that might be attractive to the Payload Safety process, including a much tighter integration between the developers and the other Panel members. Some of those features are reflected in the proposed *lean* process in Chapter 5. A more explicit comparison with those other safety processes could yield even further opportunities for improvement.

Another area of future work lies in the extension of this analysis to other NASA processes. So far, the effort focused exclusively on the Payload Safety Review process. This is only one of a number of integration processes that payloads must satisfy before they can fly on-board the ISS. Physical integration of the hardware, crew training, flight operations planning, *etc.*, are examples of

other NASA processes that could benefit from an application of the *lean* principles described here. As was the case for safety, however, it is important that these analyses be conducted by personnel familiar not just with *lean* engineering, but also with the technical and operational details of the process. Otherwise, it is very easy, from a purely *lean* perspective, to identify a process step as *muda* where in fact the step is critical due to the unique requirements of spaceflight. The Payload Safety Review process tends to be considered as one that is extremely well defined and one that has demonstrated a willingness to change and improve. Other processes may be quite different. While that might make implementation of any *lean* changes more difficult, it could also significantly increase the opportunities for improvement and savings.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A: NASA Reference Documents

The documents below define the requirements, processes, and products for the entire Payload Integration process.

SSP 50200: Station Program Implementation Plans

SSP 50200 Volume 1: Station Program Management Plan

SSP 50200 Volume 2: Program Planning and Manifesting

SSP 50200 Volume 3: Cargo Analytical Integration

SSP 50200 Volume 4: Payload Engineering Integration

SSP 50200 Volume 5: Logistics and Maintenance

SSP 50200 Volume 6: Cargo Physical Processing

SSP 50200 Volume 7: Training

SSP 50200 Volume 8: Increment Execution Preparation

SSP 50200 Volume 9: Real-Time Operations

SSP 50200 Volume 10: Sustaining Engineering

Program Documents

SSP 57011: Payload Verification Program Plan

SSP 57057: ISS Payload Integration Template

SSP 52054: ISS Program Payloads Certification of Flight Readiness Implementation Plan, Generic

SSP 54504: IDRDR Annex 5, Payload Tactical Plan Blank Book

Payload Safety

SSP 50062: NASA/CSA Bilateral Safety and Mission Assurance Requirements

SSP 50145: NASA/NASDA Bilateral Safety and Product Assurance Requirements

SSP 50146: NASA/RSA Bilateral Safety and Mission Assurance Process Requirements

SSP 50182: NASA/ASI Bilateral Safety and Product Assurance Requirements

SSP 50191: NASA/ESA Bilateral Safety and Product Assurance Requirements

NSTS 1700.7B: Safety Policy and Requirements for Payloads Using the Space Transportation System

NSTS 1700.7B, ISS Addendum: Safety Policy and Requirements for Payloads Using the International Space Station

NSTS/ISS 13830: Payload Safety Review and Data Submittal Requirements for Payloads Using the ISS

IP Transportation Vehicle Safety Documents

NSTS/ISS 18798: Interpretations of NSTS/ISS Payload Safety Requirements

KHB 1700.7: Space Shuttle Ground Safety Handbook

SSP 52005: Payload Flight Equipment Requirements and Guidelines for Safety-Critical Structures

SSP 57025: ISS Payload Interface System Fault Tolerance Document

Payload Integration Agreements

SSP 57059: Standard Payload Integration Agreement (PIA) for Pressurized Payloads

SSP 57060: Payload Integration Agreement Increment Addendum Blank Book for Pressurized Payloads

SSP 57061: Standard Integration Agreement PIA Blank Book for Unpressurized Payloads

SSP 57062: Payload Integration Agreement Increment Addendum Blank Book for Unpressurized Payloads

SSP 57063: Standard Payload Integration Agreement Blank Book for Small Payloads (Pressurized)

SSP 52000-EIA-ERP: EXPRESS Integration Agreement (EIA) Blank Book for EXPRESS Rack Payloads

SSP 52000-EIA-EPP: EXPRESS Integration Agreement (EIA) Blank Book for EXPRESS Pallet Payloads

JFX-TBD: PIA Blank Book for JEM Exposed Facility Payloads

SSP 52000-PDS: Payload Data Sets Blank Book

Payload Interface Requirements and Verifications Documents

SSP 57000: Pressurized Payloads Interface Requirements Document

SSP 57003: Attached Payload Interface Requirements Document

SSP 57001: Pressurized Payload Hardware Interface Control Document (ICD) Template

SSP 57004: Attached Payloads Hardware ICD Template

JCX-99041: JEM Pressurized Payloads Standard ICD

JCX-95055: JEM Exposed Facility Payloads Standard ICD

TBD: APM ICD Template

SSP 57002: Payload Software ICD Template
SSP 57010: Generic Payload Verification Plan for Pressurized Payloads
SSP 57013: Generic Payload Verification Plan for Attached Payloads
JFX-TBD: JEM EF Standard Payload Verification Plan
JFX-TBD: JEM PM Standard Payload Verification Plan
TBD: APM Generic Payload Verification Plan
TBD: RSA Interface Documents

ISS Payload Accommodations Handbooks

SSP 57020: Pressurized Payload Accommodations Handbook (PAH)
SSP 57021: Attached Payload Accommodations Handbook
SSP 52000-PAH-KSC: KSC Payload Launch Site Processing PAH
SSP 57800: Payload Software Integration and Verification PAH
MLM-HB-AI-001: Multi-Purpose Logistics Module Cargo Accommodations Handbook
SSP 50467: ISS Cargo Stowage Technical Manual: Pressurized Volume
TBD: RSA Payloads Accommodations Handbook
JCX-TBD: JEM Payload Accommodations Handbook
COL-RIBRE-MA-0007-00: Columbus Payload Accommodations Handbook Attached Pressurized Module
SSP 52000-UG-ERP: User's Guide for EXPRESS Rack
SSP 52000-UG-EPP: User's Guide for EXPRESS Pallet

Payload Operations Reference Documents

SSP 50305: POIC to Generic User Interface Definition Document
SSP 50323: Payload User Development Guide (PUDG) for the Space Station Training Facility (SSTF) Payload Training Capability (PTC)
SSP 50323 Appendix I: Payload Users Development Guide - Appendix I
SSP 50254: Operations Nomenclature
SSP 50313: Display and Graphic Commonality Standard
SSP 50503: International Space Station Onboard Training Media Requirements
SSP 58200: Multilateral Payload Regulations
SSP 58026-01: Generic Payload Simulator Requirements Document Volume 1
SSP 58304-01: Ground Support Personnel Training and Certification Plan

SSP 58309: Payload Training Implementation Plan

SSP 58313: NASA Payload Regulations

SSP 58700: U.S. Payload Operations Data File Management Plan

Transportation Vehicle Requirements

NSTS 21000-IDD-ISS: Space Shuttle Program-to-Space Station Program IDD

NSTS 21000-IDD-SML: Shuttle/Payload IDD for Small Payload Accommodations

NSTS 21000-IDD-MDK: Shuttle/Payload IDD for Middeck Accommodations

RPO1193: Progress M Cargo Transport Vehicle Technical Description

TBD: IP Transportation Vehicle Documents

Appendix B:

Detailed Payload Safety Process Flow

Preliminary Design Phase

Safety Engineer reviews payload preliminary design for susceptibility to suite of potential safety hazards as follows:

Materials:

Assess materials used in custom and commercially purchased components for flammability, toxic outgassing, and ability to withstand thermal extremes and vacuum; Select and recommend preferable materials to design team.

Structures:

Analyze structural design to withstand launch, re-entry and landing loads; Assess materials for stress corrosion potential, fatigue or improper fastener use. Assign applicable Factors Of Safety to design. Assemble preliminary fracture control plan.

EMI:

Assess potential electromagnetic emissions from payload.

Hazardous Fluids:

Quantify hazardous fluids and analyze for toxicity levels. Recommend containment scenarios based on fluids requirements and general system design.

Crew Contact Hazards:

Define requirements for sharp edges; Assess system for rotating parts and potential pinch hazards.

Battery:

Analyze battery for energy potential and potential hazards including short circuit, overcharging, temperature extremes and electrolyte leakage. Provide preliminary circuit design commensurate with battery energy potential.

Thermal:

Provide preliminary system level thermal analysis to show that design is single failure tolerant and will not provide a hazard to crew, payload or Orbiter/Station systems.

Electrical Shock:

Identify all potential connectors which will be crew accessible and set requirements to ensure crew cannot contact powered components.

Electrical Power Distribution:

Analyze preliminary power distribution requirements. Define wire size, and appropriate circuit protection

Pressurized Systems:

Assess preliminary design of pressurized components for appropriate

containment of pressurized gas. Assign appropriate Factors Of Safety, proper materials selection, and safe release of gases in the event of a single-point failure.

Rotating Equipment:

Assess system for rotating parts (fans, etc.) Include rotating parts in Fracture Control Plan. Assign appropriate rotation rates and containment should breakage occur.

Lasers:

Should Lasers be used, assess for FDA specified LASER classification, and assign appropriate containment of LASER to preclude hazard to crew.

Pyrotechnics:

Design pyrotechnic devices to incorporate fault tolerance for inadvertent firing.

Jettison/Payload release:

Define electrical/mechanical measures to preclude inadvertent or premature payload release.

Radio frequency radiation interfering with STS circuitry:

Assess RF emissions and define inhibits should levels exceed allowable limits.

Engineering team modifies design accordingly.

Materials:

Incorporate favorable materials into design where possible; Where favorably rated materials cannot be incorporated, begin work-around design to mitigate or isolate unfavorable material.

Structures:

Begin ruggedizing structural design, or implement vibration isolation measures as necessary.

EMI:

Provide preliminary design of electromagnetic interference control measures.

Hazardous Fluids:

Provide preliminary design to contain hazardous fluids.

Crew Contact Hazards:

Review initial design to preclude sharp edges and pinch points.

Battery:

Produce preliminary battery circuit design to incorporate controls for short circuit, overcharging, temperature extremes and electrolyte leakage. Review preliminary thermal analyses for thermal environment at battery location.

Thermal:

Perform preliminary thermal analysis.

Electrical Shock:

Select connectors to ensure crew cannot contact powered components.

Electrical Power Distribution:

Incorporate wire size, and appropriate circuit protection into preliminary design.

Pressurized Systems:

Incorporate appropriate Factors Of Safety, proper materials selection, and safe release of gases in the event of a single-point failure into preliminary pressure systems design.

Rotating Equipment:

Include rotating parts in Fracture Control Plan. Design system to limit excess rotation rates and to containment fan blades should breakage occur.

Lasers:

Design system for appropriate containment of LASER.

Pyrotechnics:

Design pyrotechnic devices to incorporate fault tolerance for inadvertent firing.

Jettison/Payload release:

Define electrical/mechanical measures to preclude inadvertent or premature payload release.

Radio frequency radiation interfering with STS circuitry:

Assess RF emissions and define inhibits should levels exceed allowable limits.

Safety Engineer participates in design meetings to continually assess design attributes as applicable to NASA safety standards.

Design team responds with periodic design re-iterations throughout Preliminary Design Phase.

Safety Engineer establishes relationship with JSC subsystem safety engineers for feedback on safety-relevant design features; Support meetings/Technical Interchange Meetings (TIMs); Redesign as necessary.

Primary Payload Safety Review Panel Representative:

Safety Engineer submits all safety data to assigned NASA Payload Safety Engineer.

NASA PSRP Rep provides general direction as well as establishes contact with NASA subsystem engineers

Materials:

Safety Engineer submits preliminary materials list:

NASA materials scientist analyzes composition of materials, and begins analysis/test on materials which have no established NASA test data; provides feedback.

Structures:

Safety Engineer submits preliminary structural analyses

NASA structural engineer analyzes preliminary design and provides feedback.

EMI:

Safety Engineer submits preliminary system design and EMI mitigation measures

NASA Battery Rep provides feedback

Toxicologist:

Safety Engineer submits preliminary list of potentially toxic fluids

Toxicologist assesses fluids for toxicity level

Battery:

Safety Engineer submits preliminary battery design

NASA Battery Rep provides feedback

Crew Representative:

Crew Rep provides feedback on crew interface design

Pressurized Systems:

Safety Engineer submits preliminary battery design

NASA Battery Rep provides feedback

Safety Engineer writes Payload Safety Data Package to outline safety critical subsystems and address all potential hazards.

Safety Engineer submits Payload Safety Data Package to JSC Payload Safety Review Panel (PSRP)

Safety Engineer and Engineering Team support Phase 0/1 Payload Safety Review at JSC.

Safety Engineer presents Safety Critical Design at Preliminary Design Review.

If Ground Processing Safety is required, Safety Engineer engages in KSC Safety Process in parallel with JSC Safety.

Critical Design Phase

As conceptual design materializes, Safety Engineer reanalyzes design for susceptibility to suite of potential safety hazards.

Materials:

Re-assess materials used in custom and commercially purchased components for flammability, toxic outgassing, and ability to withstand thermal extremes and vacuum; Ensure preferable materials used in design or appropriately contained, cured or coated.

Structures:

Re-analyze structural design to withstand launch, re-entry and landing loads; Assess materials for stress corrosion potential, fatigue or improper fastener use. Review design for appropriate Factors Of Safety. Update Fracture Control Plan.

EMI:

Review matured design and re-assess electromagnetic emissions from payload. Ensure that EMI control measures are sufficient to meet NASA safety requirements.

Hazardous Fluids:

Review hazardous fluids list for completeness. Review design for appropriate containment scenarios. Submit new fluids to JSC as necessary.

Crew Contact Hazards:

Review design for sharp edges, rotating parts and potential pinch hazards. Ensure that design meets NASA requirements.

Battery:

Review battery design for compliance with NASA requirements. Submit design modifications to JSC as necessary.

Thermal:

Review/update thermal analyses.

Electrical Shock:

Review design for proper configuration of connectors.

Electrical Power Distribution:

Review design for proper wire size and appropriate circuit protection.

Pressurized Systems:

Review design for appropriate Factors Of Safety, proper materials selection, and safe release of gases in the event of a single-point failure.

Rotating Equipment:

Ensure rotating parts are included in Fracture Control Plan. Review design for appropriate rotation rates and containment of broken fragments.

Lasers;

Review design for appropriate containment of LASER to preclude hazard to crew.

Pyrotechnics:

Review design for fault tolerance to inadvertent firing.

Jettison/Payload release

Review electrical/mechanical measures to preclude inadvertent or premature payload release.

Radio frequency radiation interfering with STS circuitry:

Review RF emissions and inhibits to meet allowable limits.

Engineering team modifies hardware as necessary.

Safety Engineer furthers relationship with JSC subsystem safety engineers to get feedback on safety-relevant design features.

Safety Engineer revises Payload Safety Data Package to include all design and safety critical subsystem modifications.

Safety Engineer submits Payload Safety Data Package to JSC PSRP.

Safety Engineer supports Phase 2 Payload Safety Review at JSC.

Safety Engineer presents Safety Critical features at Critical design Review.

Fabrication and Testing Phase

Verify all safety hazard controls by test, inspection, analyses, or demonstration.

Materials:

Perform offgas test
Perform flammability tests as required

Structure:

Perform vibration testing to withstand launch, re-entry and landing loads (in addition to factors of safety.)

EMI:

Perform system level, integrated EMI test at JSC to ensure that EMI control measures are sufficient to meet NASA safety requirements.

Hazardous Fluids:

Perform ground testing to verify containment design.

Crew Contact Hazards:

Inspect flight hardware for compliance with design.

Battery:

Perform vacuum test as required; Inspect flight hardware for cell reversal and proper containment.

Thermal:

Perform system level thermal cycling test.

Electrical Shock:

Inspect flight hardware for proper configuration of connectors.

Electrical Power Distribution:

Inspect flight hardware for proper wire size and circuit protection in compliance with design.

Pressurized Systems:

Inspect flight hardware for compliance with design.

Rotating Equipment:

Inspect flight hardware for appropriate rotation rates and containment should breakage occur.

Lasers:

Inspect flight hardware for appropriate containment of LASER.

Pyrotechnics:

Inspect flight hardware for compliance with design.

Jettison/Payload release :
Inspect flight hardware for compliance with design.

Radio frequency radiation:
Test flight hardware for acceptable RF emissions.

Submit test and inspection results to JSC subsystem safety engineers and attain written approvals accordingly.

Write Phase 3 Payload Safety Data Package to outline safety critical subsystems and address all potential hazards, including all hazard control verification reports.

Submit Payload Safety Data Package to JSC PSRP.

Support Phase 3 Payload Safety Review at JSC.

Pre-Delivery Phase

Safety Engineer maintains Verification Tracking Log

Finalize testing and verification activities

Final VTL close-out

THIS PAGE INTENTIONALLY LEFT BLANK



Appendix C:
Presentation for the Payload Safety Review Panel

The following pages contain the slides that were presented to the NASA Payload Safety Review Panel on January 31, 2003.

Questions for Discussion
Can Lean Enterprise Principles be Applied to the Phase Safety Process?



Jeff Hoffman
Javier de Luis

Massachusetts Institute of Technology (MIT)
Systems Design and Management (SDM)
in cooperation with the
Lean Aerospace Initiative (LAI)



Background

- Lean principles and techniques have been applied to a wide range of processes
- NASA Safety poses unique constraints and requirements
- But...more payloads, less resources will strain the system
- Can "Lean" help?



Some Lean Principles and Techniques

(that may be applicable)

- Reduce or eliminate "inventory" that isn't used (in our case, information):
 - Overproduction
 - Timeliness
 - Travel and reviews
- "Pull"
 - Data produced only when it is needed by the reviewing personnel
 - If data is not needed, then it is not produced
- "Monuments"
 - Institutions, facilities, or organizations that may need to change to support ISS more efficiently.
- "Work Cells"
 - Do payload developers have the right skill mix to have a successful safety process.
 - If not, how can we provide them with the right people/knowledge?



Approach

- Start from a perspective of experience in the safety process.
- Gather information from stakeholders
 - Payload Developers
 - Safety Panel
 - International Partners?
- Map process, identify potential for Lean savings
- Report back to stakeholders



Safety Panel Input

- There are three specific areas we would like to obtain inputs from:
 - The “standard” payload developer process
 - The roles and responsibilities of the international partners
 - The safety approach for in-house and crew equipment
- We would welcome inputs in other areas that we may have missed.



Payload Developers

- From the Panel’s perspective, what is the main stumbling block that payload developers face in order to achieve a successful safety review?
- Do the data packages that are submitted contain too much superfluous information, from the perspective of what is needed to satisfy the safety requirements? Or would you prefer even more background information?
- Is it feasible for more payloads to skip or do reviews out of board? What would be required to make that happen? In the future, do you foresee that a payload will be able to submit and be reviewed completely electronically, with no reviews?
- Are there special issues or concerns with reflow or facility hardware that you feel tend to not be properly addressed by the developers at this time?



International Partners

- Do the other ISS partners have authority to certify payloads as being safe to fly on-board ISS? If so, how is NASA safety oversight maintained with ESA, NASDA or the other international partners? (We understand that the Russian partners are handled differently)
- Is there a certification/training program that other agencies safety representatives go through before they can review and sign-off on data packages?



In-House and Crew Equipment

- The perception is that in-house developed equipment undergoes a different process for safety certification than payloads. If so, what are the differences?
- What would prevent some of these different procedures from being applied across the board?
- Does crew equipment, such as miscellaneous personal items, watches, personal stereos, etc., undergo the same safety process?



References

- ¹ NASA Consolidated Launch Manifest, <http://spaceflight.nasa.gov/shuttle/future/index.html>
- ² NASA document FS-2003-02-28-MSFC, Feb., 2003, <http://www1.msfc.nasa.gov/NEWSROOM/background/facts/slifactstext.html>
- ³ NASA Press Release, 02-108, February, 2002, <http://www1.msfc.nasa.gov/NEWSROOM/news/releases/2002/02-108.html>
- ⁴ Mars Program home page, <http://mars.jpl.nasa.gov/>
- ⁵ NASA Space Telescope Science Institute press release, STScI-2002-20, Sept., 2002, available at <http://hubblesite.org/newscenter/archive/2002/20/text>
- ⁶ J.P. Womack, D.T. Jones, and D. Roos, *The Machine That Changed The World: The Story of Lean Production*, New York: Harper Perennial, 1991
- ⁷ J.P. Womack, D.T. Jones, *Lean Thinking*, New York: Simon & Schuster, 1996
- ⁸ T. Ohno, *Toyota Production System: Beyond Large-Scale Production*, Productivity Press, 1998.
- ⁹ Enterprise Level Waste, lecture notes from MIT's graduate level course 16.852J "Integrating the Lean Enterprise"
- ¹⁰ E. Murman *et al.*, *Lean Enterprise Value*, New York: Palgrave, 2002
- ¹¹ A History of US Space Stations, NASA Facts, IS-1997-06-ISS009JSC, June, 1997
- ¹² C. M. Vest, *et al.*, Advisory Committee on the Redesign of the Space Station: Final Report to the President, NASA-TM 108760, 1993
- ¹³ N.G. Levenson, *Safeware: System Safety and Computers*, Addison-Wesley Pub Co; 1st Ed., April, 1995
- ¹⁴ Transition to Lean Roadmap is available at the MIT Lean Aerospace Initiative website, <http://lean.mit.edu/>
- ¹⁵ T. Seitz, *Lean Enterprise Integration*, MIT Master of Science Thesis, June 2003
- ¹⁶ I. Grossi, *Stakeholder Analysis in the Context of the Lean Enterprise*, MIT Master of Science Thesis, June 2003

-
- ¹⁷ S. Nahmias, *Production and Operations Analysis*, 4th Ed., McGraw-Hill, 2001
- ¹⁸ One NASA Program, <http://www.onenasa.nasa.gov/>
- ¹⁹ J.B. Fussell, G.R. Burdick, G. R., *Nuclear Systems Reliability Engineering and Risk Assessment*, Electric Power Research Institute, Energy Research and Development Administration., University of Tennessee Knoxville. Department of Nuclear Engineering, Society for Industrial and Applied Mathematics, 1977
- ²⁰ *Failure Modes and Effects Analysis (FEMA) : A Bibliography*, National Aeronautics and Space Administration, NASA Scientific and Technical Information Program, 2000
- ²¹ J-L, Lions, *et al.*, ARIANE 5 Flight 501 Failure, Report by the Inquiry Board [originally appeared at <http://www.esrin.esa.it/htdocs/tidc/Press/Press96/ariane5rep.html>]
- ²² G. Le Lann, "The Ariane 5 Flight 501 Failure - A Case Study in System Engineering for Computing Systems", INRIA Research Report 3079, Dec. 1996, 26 p [<http://www.inria.fr/RRRT/publications-fra.html>]
- ²³ E.S. Pearson, B.P. Dudding, W.J. Jennett., *Quality Control Charts*. London,: British Standards Institution, 1942
- ²⁴ C.W. Adams, P. Gupta, C.E. Wilson, *Six Sigma Deployment*. Amsterdam ; Boston: Butterworth-Heinemann, 2003
- ²⁵ T. Pyzdek, *The Six Sigma Handbook : A Complete Guide for Greenbelts, Blackbelts, and Managers at All Levels*. New York: McGraw-Hill, 2001
- ²⁶ J.M. Utterback, *Mastering the Dynamics of Innovation*, Harvard Business School Press, September 1996.
- ²⁷ S. Shiba, D. Walden, *Four Practical Revolutions in Management*, Productivity Press, The Center for Quality Management, 2001
- ²⁸ D.L. Goetsch , S.B.. Davis, *Quality Management: Introduction to Total Quality Management for Production, Processing, and Services*, Prentice Hall College Div; 4th Ed., April 2002.
- ²⁹ E.M. Goldratt, J. Cox, *The Goal: A Process of Ongoing Improvement*, North River Press Publishing Corporation; 2nd Rev. Ed., May 1992.
- ³⁰ NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements for Payloads using the ISS
- ³¹ M. Hammer, J. Champy, *Reengineering the Corporation*, HarperBusiness, 2001