Adding Elements Of Innate Human Behavior To Improve System Performance And Safety In The Design Of Complex Systems With Corollaries To Improve Team Performance

by

Mark Jernigan

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

February 2002

Signature of Author____

Mark Jernigan
System Design and Management Program
February 2002

Certified by____

Nancy Leveson
Thesis Supervisor
Professor, Aeronautics and Astronautics

Accepted by____

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

Accepted by____

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

Adding Elements Of Innate Human Behavior To Improve System Performance And Safety In The Design Of Complex Systems With Corollaries To Improve Team Performance

By

Mark Jernigan

Submitted to the System Design and Management Program in Partial Fulfillment o f Requirements for the Degree of Masters of Science in Engineering and Management

Abstract

The top reasons for accidents in complex systems are usually attributable to failures by the design team to address systems safety or human cognition properly in their designs. This thesis explored taking advantage of the innate quality of play in humans to improve human-system performance and project team performance. The framework for the investigation utilizes and builds on Leveson's Intent Specifications and the control theoretic model for system safety. The principal enhancement to the existing intent specification model posed by this thesis is to establish a set of design principles for human system interaction and rules for their application. The framework for the principles is validated by Rasmussen's Ecological Interface Design. The thesis concludes that if the human-machine interface as elements of play in it, the mental model necessary for effective knowledge- based control of a complex system will be enhanced. Aspects of engagement derived from the play paradigm analyzed were: competition, unambiguous rules, requires strategy or skill, tension, and fun. This research assessed the existing design documentation of the Cockpit Avionics Upgrade of the Space Shuttle Program within the framework of intent specification, in order to develop specific recommendations to improve the design of the upgrade. The thesis recommends changing some of the display hierarchies, improving the overall traceability of the operations concepts to the design of the upgrade, and suggests implementation of the engagement techniques. The thesis proposes experiments that will utilize current Space shuttle infrastructure, assessing performance via standard proficiency tests to measure the effectiveness of the techniques in building mental models of the new systems. The work of analyzing and determining the most effective approaches for improving human-system performance naturally gives rise to possible corollaries for use in managing work teams. Deliberate utilization of the elements of play paradigm that improve human-system performance should be applicable for use in improving team performance. The thesis explores these aspects and proposes methods for implementation. The key principle derived from analysis is that no matter what methods are used for enhancing the team performance, the team leader must engender a strong belief in the approach.

Thesis Supervisor: Nancy Leveson
Professor of Aeronautics and Astronautics

Chapter 1

Problem Statement

Introduction

With the advent of the addition of ‘smart controllers’, autonomous agents, machine learning, and other computer software separation of the operator from the actuator in complex systems, the role of the human operator is fundamentally changing. Previously, the operator was someone who physically interacted with the machine, able to get feedback by watching the system actuation, and could understand its operation by observing and learning how to use the controls by direct feedback. With modern complex systems, the operator must monitor the actions of others (intelligent software agents via computer screen), usually well removed from the physical actuation, and recognize when the operations are not proper. The pendulum of complex system interface design has swung from complicated, tedious manual entries of commands, following checklists to completely autonomous designs, which must be retrofitted with manual controls, when the automation does not handle the full range of operating conditions. Since machines do not possess common sense beyond the extent of what has been programmed, the burden of ensuring the system is safe, performing the actions necessary to correct the faults, and restoring the system to operation falls on the humans assigned to that function. As the software systems mature, the demand for attention from the human becomes less and less, and the potential for a human mistake due to distraction greatly increases, especially in cases of an isolated environment such as a long duration space mission.

The Problem

Traditionally in NASA manned space projects, specifications and design considerations leave the human behavioral characteristics as an implicit constraint at best, relying on the particular specifier's sensit ivity as to what works best with historical experience with similar equipment. In software development, a myriad of research and approaches have been tried to improve the interaction between the computers and their human operators. One of the most popular approaches is the "try before you buy" approach where the developer interacts with the operator and puts together an interface based upon the feedback. A version is delivered for the operator to 'play' with, driving out the more obvious bugs and having the operator determine the 'clunky' parts, providing suggestions as to what approaches might help smooth the task flows, and suggest some new features to facilitate improvements in the interaction. This approach is widely accepted, but haphazard.

A substantial amount of research has been performed in the arena of human-system interaction, but no dominant design or standards for complex systems development have emerged. Many complex systems projects have been designed based on legacy experience with previous similar systems. This usually results in a gradual set of improvements and modifications tailored to meet the new environment of the target project. However, research has shown in many cases that designs do not conform to human nature, resulting in systems that have hidden potential for unsafe behavior and which occasionally lead to problems in safely performing the intended functions. Leveson et al. [(1)2001] have characterized the cause of most system level accidents as dysfunctional interactions. For the human-system interface, these dysfunctional interactions manifest themselves as errors attributed to:

- Increased tasks during high workload periods or inexperience of the operator (failure of the human part)
- Difficult interface to use or understand, mode confusion, over-reliance on faulty automation in the control system (failure of the machine part)

Both types of errors are due to either failure of the designer to use human cognition when developing the display/control, or inadequate understanding of how the system really works by the operator. The characterizations of the areas for these dysfunctional interactions are articulation, coordination, and information. Failures between the parts or subsystems in these areas are usually the root of the problem in system accidents.

The fundamental characteristic of a complex system is that it is too complex for a human or group of humans to be able to control and monitor without having a computer or group of computers involved in simplifying and presenting the information needed to effectively operate the system. As the complexity increases, the level of sophistication of the computer architecture and the software also increases, bringing with it both the benefit of a more autonomous system and the liability of the inherent errors that software, by its nature, contains. [Leveson, (2) 1995] The most important aspect the humans must bring to the overall system is the ability to detect the errors when they arise, realize that they are errors, and adjust the system to restore it to as normal as is practical operation.

Therefore, the human must develop both a contextual knowledge of the operation of the system, must have choices in the form of redundant components or processes, and must have the tools necessary to correct undesired behavior in both the hardware and software embedded in the system. The computer in this environment plays a more and more essential role of delivering health and status as well as aiding the humans in both forming and using their mental models of the system. This research is focusing on helping designers in designing an interface between the humans and the system that meets two objectives. The interface must provide the necessary amount of context to show the accomplishment of its defined tasks, but also must have the human involved enough in the operation to realize that problems are arising before they reach a critical undesired state which compromise either the safety, the desired reliability, or the mission objectives.

Human-system interface research early on focused mostly on presentation of information, (i.e. removing information overload and improved system visualization), and control facilitation, (i.e. automating tedious, repetitive tasks, and providing context sensitive information to the operator). While these are important in eliminating a number of cognitive errors, they do not address the problem of vigilance. Examples of these types of ergonomic principles to be used by the designer are presented in chapter three.

Chapter 2

Frameworks to Address the Problem

To address the problem of vigilance, this research is building on the substantial body of research based on holistic system safety principles and utilizing human cognition to improve the interaction between the human operators and the mechanical parts of the system. The frameworks provide the means to assess designs and provide guidance to the designer responsible for developing the complex system. The intent specification design framework has in its hierarchy a section for design principles. This thesis proposes that a set of interface design principles based on the rules of play will help to keep the operator engaged with the system. These attributes appear to be consistent with Rasmussen's Ecological Interface Design, which is also based on human cognition.

Systems Approach to Safety

Since the purpose of this research is to improve the safety of complex systems, a brief discussion of the systems approach to safety is warranted. The basic premise in the system safety methodology is that both humans and computers (because they are programmed by humans and impossible to deterministically verify) are fallible and errors are to be expected, even with a one-of-a kind or few-of-a kind program with huge budgets and redundancies. Errors are expected consequences of long-term operations rather than aberrations to be eliminated, having their origins not in the fallibility of human nature but in the nature of complex systems themselves. Rasmussen discovered in interviews with complex systems operators that in many cases, the operator of a system would intentionally go beyond operating limits occasionally to get feedback from the system to establish their mental model limits or to try to improve operation of the system. [(3), 1987]

Therefore, the system must include recurrent error traps in them, the ability to 'safe' the system, and the organizational and systemic processes required to restore the system to operating condition, if possible. Countermeasures are based on the assumption that organizations should not try to make humans infallible, but to make the system tolerant of both human and machine errors. [Leveson, (1) 2001] The countermeasure that is the focus of this research is that of operator- system engagement. If the human is sufficiently engaged in the operations processes with a highly honed mental model of system functionality and interaction, then error conditions become more recognizable, pinpointing the source of errors is easier, and resolution is arrived at sooner with less compromise to safety. All hazardous technologies possess barriers and safeguards. When an adverse event occurs during development testing or operations, the important issues are not who blundered, but:

1. How and why the safeguards allowed such an error
2. What new safeguards need to be implemented to prevent future similar errors in the system
3. What new constraints must the system operate under given the limited resources available in the isolated situation.

Design Framework

In order to have an effective system safety model, the complex system should have a design framework that captures not only the design of the components, but also has traceability to design decisions and captures the human organizational elements to a certain extent. Leveson's [(4) 2000] Intent Specification is the one chosen as the framework for this research. The Intent Specification model is a three dimensional framework used to capture a living representation of the design of a complex system, including all factors that shape the design and guide the decisions in trade offs. The framework is organized in a left to right (part-whole dimension), top to bottom (intent dimension) hierarchy. The columns are arranged from environment, to human, to system, to components, and rows proceed from goals to design principles to black box behavior, to design representation, to physical representation. The third dimension is refinement. One of the premises of this thesis is that at the lowest levels of the intent specification should necessarily include the above mentioned columns, but the highest two levels, purpose and principals, the column classifications should be abstracted as well to external, system level, and internal (figure 1). At the upper two levels, it is important to retain a system level view, while still facilitating a whole-part hierarchy.

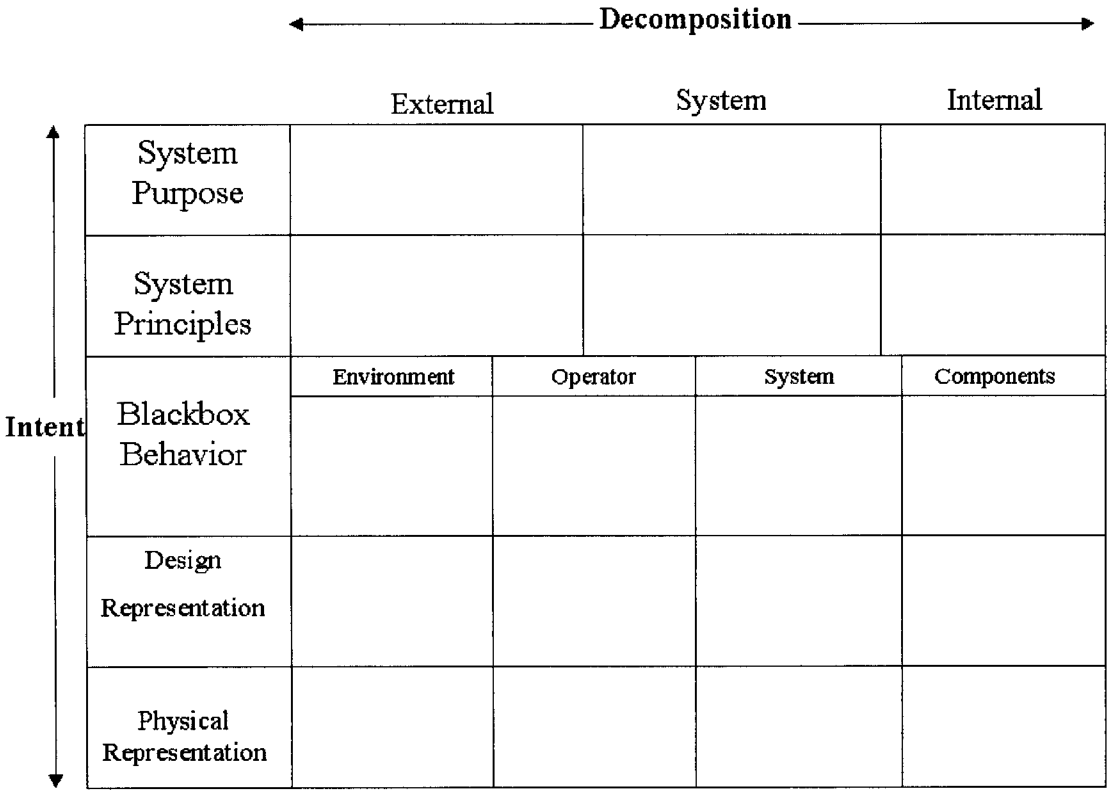


Figure 1: Modified Intent Specification

The main benefit to changing the framework is to avoid a presupposition about which functions should be performed by the machine (and to avoid overly constraining the design to a particular form), the operator, or the organization.

One of the key concepts with Intent specifications is to establish a system framework that will aid the developers of complex systems in both making design trade off decisions and in correctly interpreting the requirements in their baseline designs. This dissertation asserts that the upper levels require additional information for effective development of systems. System specifications need to go beyond those requirements that are intended to be implemented in hardware and software, and should also encompass requirements for the operators, supervisors, maintainers, and all other direct stakeholders that may be involved in the direct operation of the system. So, the specification should also contain requirements for the human organization and should address all aspects of the operation, eventually allocating some requirements to the hardware, some to the software, and the rest to the human elements involved in the operation and delivery of services provided by the system being developed. By adding this extra content, designers can choose to allocate requirements to all three entities and can make choices that effect the number of people involved in a deliberate, proactive, rather than post facto manner. As the hierarchy is traversed downward, the physical allocation is decided, and the hierarchy can resume its present form.

Design Principles

The main enhancement to the existing intent specification framework posed by this thesis is to establish a set of design principles for human system interaction and rules for their application to be included in the design principles level of the framework.

Complex System interface development has begun to take into account models of human cognition in the development of interfaces to systems. Recent research within cognitive ergonomics supports the importance of extending the scope of the interface design beyond the visible user interface to the entire domain [Fischer, (5) 1993]. The human being is not a passive computer user but an active problem solver in the complex system [Woods & Roth, (6) 1988]. By incorporating domain knowledge earlier in the development process and in the methods for analysis, design and evaluation, and by explicit representations of this knowledge, user interface design for specific work activities can be enhanced. The information the users actually use in their work is important for the establishment of the domain model [Neisser, (7) 1987]. By collecting this information to capture both formal and informal aspects of the work that the user might not be aware of and using methods of engagement, the user interface design can be enhanced and the resulting user interfaces can enhance the overall system safety.

A central tool to aid the understanding of user interface design and for deriving prerequisites for the design process is the construction and use of models of human-computer systems [Rasmussen, (8) 1986]. These models aim at understanding why people undertake certain performance patterns and how they can be improved in carrying out a specific work task with computer support. Rasmussen further elaborates this within research on human error. He identifies eight stages of decision making (activation, observation, identification, interpretation, evaluation, goal selection, procedure selection and activation) with possible short-cuts, explaining stereotypical reactions and associative leaps to overcome the laborious and slow knowledge-based processing.

In his 1938 book, *Homo Ludens, A Study of the Play Element in Culture,* Johan Huizinga analyzed the innate human characteristic of play in all facets of human civilization, and concluded that aspects of play are not only present, but essential to human endeavor. [(9) 1938] This thesis will explore taking advantage of this innate quality in humans to improve human-system performance.

Experience with long duration space flight has revealed substantial deterioration in human performance, due to stress, isolation, and unfamiliar living conditions. This research proposes that for any long duration endeavor, incorporating both rules and aspects of play in human-system interaction will improve long term performance. The premise of this research is that a new, deliberate interaction model must be developed that supports the relationship between the operator and the system being controlled. As supervisor/ monitor of the worker (the computer), the operator must understand the status of the system (appropriate feedback), have a mental model of the functions being performed, with detailed knowledge of the inputs that can be made and their effects. In addition, the system must have a deliberately modeled interaction strategy that keeps the human informed and engaged to minimize the hazardous effects of defects in the machine and of lapses by the operator. The interaction structure should balance between engagement and overload, increasing complexity for non real time functions (to improve the operator's mental model) and simplifying for dynamic, time critical functions.

The innovative proposition of this thesis is that if the human-machine interaction has elements of play in it, the mental model necessary for effective knowledge- based control of a complex system will be enhanced. Aspects of engagement derived from analysis of play were: Competition, Unambiguous rules, Strategy or skill, Tension, and Fun.

This research has defined and developed strategies that take advantage of the play paradigm and suggested methods to determine whether a particular strategy has a long term, recognizable benefit. The methods and practices proposed by the research are not only guided by use of human perceptual facilities, but also take advantage of human nature by building on activities that capture the interest of the operator. By developing specific methods of interaction based on these characteristics, it is hoped that the control will be easier to learn and will result in a better operator mental model of the system, which is essential to guide the operator to take appropriate actions when an unanticipated hazardous event manifests itself. These methods should also focus the attention of the operators on the most important information and allow them to manipulate the controls and effectors in a comfortable and interesting fashion, as well.

Rasmussen's Ecological Interface Design (EID) model is based on human cognition and is isomorphic with several aspects of play in each of its levels. The model has had a great impact on human-computer interaction research and has had numerous validating experiments and theoretical corroboration [Rasmussen,(10) 1992]. At a skill-based level of human performance, individuals behave according to stored patterns of pre-programmed actions. The rule-based level applies to the tackling of familiar problems by the application of stored conditional rules. In novel situations, the knowledge-based level is used for on-line planning, using conscious analytic processes and stored knowledge to acquire expertise. The EID requires that complex system operator interfaces contain three levels of interaction, and that [(11), 1983] effective interface designs will provide substantially more information to novice operators while presenting only pertinent cues for effective decisions to experts.

The EID framework contains two basic levels, the skills and rules levels, also known as perceptual processing. The first level requires the operator to interact with the system via time-space signals. Controls at this level provide a virtual representation of the system being controlled, and the actuation of controls provides direct perceptual cues as feedback. Effective interfaces must also contain multiple levels of information in a part- whole hierarchy to accommodate both the inexperienced and expert users and in order for the operator to manage the complexity of the activity being perfomed.

The second level is the rules level, where the interface provides a one to one mapping between the constraints and the cues being provided to the operator. This level requires the operator be able to assess the state of the system and respond with standard predefined actions.

The most complex level requires the operator to have a consistent mental model with that of the actual system as built (2), in order to respond to previously unforeseen states and use the knowledge of the system to take the proper course of action. Huizinga's play model also requires the participant to have a "certain "imagination" of reality" (9) which points to favorable consistency with Rasmussen's EID.

It is important to note at this point that some research has been done on the efficacy of the three levels in interface design. Hammond et al [(12) 1987] discovered that analytical cognition leads to extreme errors and that perceptual processing was superior to analytical thinking in terms of accuracy of judgments. So, it is important that the design of standard interactions with the systems should be limited to the first two levels, despite the fact that the operator's mental model needs to have elements of the third level to be able to handle unanticipated hazardous events. With all complex systems, the operator would quickly become overwhelmed if all functions required total engagement. The system would also have extensive additional complexity to be able to provide engagement functions, so these functions must be chosen judiciously. The decisions designers are faced with is which functions required a fully engaged active human operator presence and which do not.

Chapter 3

Proposed Ergonomic and Engagement Design principles

This chapter presents a set of design principles to be incorporated in the intent specification of a complex system. These principles are proposed to be applicable to the operator interface to most complex systems. The first set is a set of ergonomic principles applicable to the presentation of the information and the design of the control mechanisms. The second set are principles of engagement, followed by a set of rules defining when it is appropriate to apply them.

The following are ergonomic control principles applicable to the development of any interface requiring operator control. The key characteristic of most of the desired attributes is that they are derived from human cognition. If the interface does not follow the principles, it often eventually leads to human errors during operation of the system. These errors are often then blamed on the human when in fact, it is the design of the interface that is truly at fault. The severity of the errors can range from sub optimal operation of the system to loss of critical functions. [Leveson, (2), 1995]

The first principle in interface design is that it must give the operator an unambiguous view into human manageable chunks of information. The rule of seven is a good guideline in this case, which is that humans, in general, are capable of cognitively managing five to nine things at any given time. If the number goes above nine, it will result in either confusion or ignoring some of the essential pieces. [Lind (13) 1991] showed that systems using the short term memory as temporary storage for information sets sequentially, demand a large cognitive load by the user compared with simultaneous presentation. Cognitive load caused by the information system (i.e. by overusing the short term memory) can be a substantial factor when judging the comfort and efficiency of a work situation [Nygren, Johnson, Lind & Sandblad, (14) 1992]. It also can cause stress, anxiety, frustration, and even health problems for the operators [Johnson & Johansson, (15) 1991].Techniques such as pop up information and hierarchies help the interface to keep the information output at the appropriate level.

The control system must take both ergonomics and mental mapping into account. [Kelley (16) 1972] The interface must have a clear mapping of the controls to the devices or effectors. Graphical User Interfaces are based on the idea of direct manipulation [Ziegler & Fähnrich, (17) 1988]. Interface elements are graphical objects of mnemonic shapes in the task domain. User actions have a high degree of direct manipulation if it is illustrated with a visual representation engaging the user in a feeling of immediate control. The degree of direct manipulation is very beneficial to the development of the operators' mental model of the system but eventually comes in conflict with the skilled users' efficiency.

Function overloading in the interest of economies of space or design expediency will generally lead to confusion or errors on the part of the operator. The interface should give some kind of sense of the relationships between the controls. [Singleton (18) 1971]. For example, in a plumbing control system, the system usually has temperatures, pressures, flows, and valves. If the interface clearly shows, though the layout and representation, the locations of each of the sensors and effectors, operation of the system becomes very straightforward and troubleshooting becomes trivial for problems that are anticipated and instrumented by the designer.

The controls must be ergonomically separated to prevent inadvertent actuation. This obvious principle is sometimes compromised due to lack of space, in environments such as spacecraft, cockpits, or submarines where space is at a premium. In such cases, the interface should place additional controls to prevent inadvertent actuation such as arming, or covers. This principle also applies to intuitive placement of controls. The most effective placement for Western systems is left to right, top to bottom, in temporal order. In cases where branching occurs or the temporal order is not predetermined, a top to bottom, ends-means hierarchical order is appropriate.[Singleton (18) 1971]

The instruction for operation of the system should utilize facsimiles for the actual interfaces, where practical. These training displays should have more contextual information in the form of instructions, descriptions of operating principles, and functional interaction information, that can either be displayed or hidden, depending on the expertise of the trainee. [Kelley (16) 1971]

Controls should work in expected ways. Conventions for actuation such as clockwise for opening and counter for closing, up for on, down for off should be carefully considered and consistently applied [Singleton (18) 1971], with a style guide that explicitly defines the conventions to the operators. For binaries, indications such as background lit for “on” and background dark for “off” should be used. In cases where no clear actuation indication is available, the results of each actuation should be clearly marked on the display. In addition, the results of the actuation should display a clear indicator of success (if measurable by the system sensors), such as a bar or pie. Humans are much more capable of processing graphical information than digital, so more graphics mean greater intuitiveness as long as the graphics follow expected conventions.

Engagement Principles

For an activity to be considered play, it must have certain attributes. These attributes of games are innately appealing to humans and their use in system design will henceforth be described as engagement attributes. Humans can spend hours involved in tedious tasks if they are associated with playing a game. This engagement results in both improvement in the skill associated with the game, and an improved mental model of achieving the goals of the game. The following are a few of the characteristics of play derived from Huizinga’s and the author’s analysis, which may be used in human system interface design to increase both the engagement of the humans in the operation of the systems and increase their long term performance with the system.

Belief

The most important aspect of system engagement is “buy in”. Huizinga [(8),1938] cites several instances where lack of belief in the rules or paradigms in a particular engagement situation results in either a breakdown of the engagement or in hostile ostracization of the detractor. It is very important that the operator feel that the processes are essential to the operation of th e system. If the operator thinks that certain required steps are superfluous to the operation of the system or comes to believe that the manual inputs are not essential to the safe, effective operation of the system, then the environment for unsafe operation has been established. This indoctrination step is essential to establishing the environment necessary for continued safe and effective operation of the system. This system level principle may or may not be allocated to the operational machine, but could be allocated to be accomplished to a training system, human organization, or some combination of the three. Having the broad requirements terrain of the Intent Specification is an ideal method of capturing desired emergent behavior, and the allocation exercises require effort in concert from both the designing and operations organization.

Motor Skills-

The most engaging aspect of play is the use of motor skills. Humans are capable of excellent concentration if the play requires use of hand to eye coordination or a consistent, refinable, repetitive skill. Rasmussen captures this characteristic in the basic level of operator control. In Sanders review of tracking controls, however, he notes that some skills which require third and higher order control, result in the same poor performance noted for cognitive based controls. In other words, if the operator must use a cognitive integration or derivative model to decide the actuation of the control device, then the control function is no longer a simple motor skills control.

Competition

One of the principle components of play is competition. Competition can be defined as an agonistic struggle between one or more participants where each of the participants attempts to perform better than the others against a predefined set of performance measurements. In competition, the emphasis is on the outcome of the performance of a task. The usual means of measuring the outcomes is by predetermining a set of metrics, establishing norms or benchmarks to measure against, and developing a comparative report. This simple game technique is a powerful persuader of the competitor to perform and to continue to perform. If the competitor is able to perform a task perfectly, the game evolves from achieving a perfect score to seeing how many times in a row a perfect score can be achieved, to what percent of all tasks have been performed with a perfect score. This goal driven, achievement oriented approach is appropriate for human performance as long as the performance is non attributable, that is to say that the measures are not used externally by some outside entity to measure performance. In this case, the human becomes reluctant to participate, becomes resentful to the measurements, and fosters an environment conducive to cheating or gaming the system to improve external appearances. The context of the game must be avoiding an external audit to maintain the spirit of the game, which keeps the operator engaged.

Components of competition are involved with the ego. Selecting operating strategies that give the operator both a sense of achievement and positive feedback should foster better long-term human performance.

Tension.

Another of the key characteristics of play is the tension derived from the progression and regression of the player to and from an objective. The competitor must overcome impediments in the most efficient manner and make selections, which have both positive and negative outcomes, and the more this random walk to the objective oscillates, the more intense the participant remains engaged. Stanford Statistician Thomas Cover [Selim (19), 2001] has analyzed sporting events and concluded that if a sporting event has a random walk with numerous cycles oscillating between victory and defeat, that the spectator's interest is greatly heightened.

It would not be advisable to intentionally introduce actions with negative outcomes in a safety critical complex system. However, offering different control modes choices so that the operator has the ability to achieve the same desired state via different paths might provide the type of engagement needed in the system.

Requires strategy-

A corollary to the tension and skill characteristics is the strategy required for games. The human becomes mentally engaged when achieving the goal requires formulation of strategy to achieve the objectives. This includes from the ability to select from various control methods outlined above, to selection of a strategy to accomplish mission objectives. Use of these cognitive processes assures the participant's attention is captivated.

Unambiguous rules-

In order to establish a play environment one must establish unambiguous rules constraining the course of play. This can be achieved in the complex system environment by following the principles of good control design. In the manned space environment, considerable effort is placed on defining as many as possible credible scenarios, considering failures and defining rules and procedures for each. These can be overridden by the mission management team, but it is in a collaborative, participative environment.

Fun-

The most difficult aspect of play to characterize is fun. In order to be considered fun, the activity must be stimulating in one or more of the following: intellectually or physically challenging, the activity must stimulate one or more of the 5 senses, or the activity must be physically rewarding. In all cases, if the activity has a positive effect on the ego of the participant, it can be considered fun. This aspect is expected to be achieved through removal of tasks that are tedious, such as substantial data entry and checking, limiting rigid step by step procedures, and providing stimulating feedback to control inputs.

Application

The intent specification should not only contain the enumeration of desired functions of the system, but should generically capture these characteristics as standard functions to be included in systems which meet the following criteria.

These attributes run the gamut of levels of the EID, and fit extremely well with the results of the body of research. Adding these attributes when they are aligned with the intuitive operation of the system such as a control stick and predictor guidance for piloting is trivial. Adding them to the system will add additional complexity to the system and must be carefully considered and judiciously applied. The most obvious controls that attributes of play can be added to are those that have obvious desired performance metrics and where the operator has some flexibility in achieving the desired results. In this case, a scoring and tracking algorithm can be used to assure that the operator is paying attention and gets positive feedback when a task is performed as well or better than in the past. Other attributes are less straightforward, but if the designer keeps the attributes in mind when making decisions about the control interface, the system will be more fun to operate and will naturally tend to keep the operator's attention better and improve the operator's mental model.

Another obvious area for application of the techniques is in the training environment. Many complex systems have a simulator where the operator is allowed to explore the limits of the system without serious repercussions. This environment is tantamount to a play environment for the system and adding complexity to the trainer interface may make it less reliable, but causes no reduction in safety. The techniques must be applied judiciously here as well in order to prevent the interface from being so different from the real interface that it provides bad performance cues.

What other systems should be targeted for this approach? Clearly, simple systems with straightforward functionality should not be augmented with this approach because research has shown that adding complexity results in higher risk of system safety problems.

Rather than specify which operations functions do not require extensive interaction, the designer should have the following criteria when determining whether engagement attributes are warranted. The criteria are as follows:

Tunability.

If control variables that can be modified by the automation or manually are present, then the control interface should include engagement attributes. The interface should include information as to how the control variable fits in the operation of the system and the actuation of the variable should either require some skill development or provide interesting feedback.

Variability.

If the attribute of the system provides variable response to inputs, then the engagement attribute should capture the range of expected response and have alternatives readily available if an unacceptable limit is exceeded.

Skill-

If the function requires fine motor skills, obviously the human must be very involved. To stimulate increased engagement and job performance, the interface should monitor performance, carry benchmarks for key parameters and rate the performance of the function, while maintaining a history of the performance parameters and providing feedback as to comparisons with previous performances of the function.

Understanding –

Rassmussen classifies a whole set of operations in this category. These functions require a detailed knowledge about the operation and response characteristics of the system. The operator must understand both input mechanisms and limits and must be required to make decisions, the result of which have similar consequences. These functions also must be performed outside standard checklists due to the variability of the response.

Complexity or semi autonomous operation-

Complexity is a subjective term defined by Crawley as a system having many interrelated, interconnected or interwoven elements and interfaces. The complexity level can be measured by assessing the number of elements in a system and the degree of interaction between each of them.

- The sophistication or number and sensitivity of the interconnections
- The sensitivity of the interconnections

Semi autonomous operation is simply where the machine has sufficient sophistication to take a series of actions when issued a simple, high level command. This type of control is simpler to use but takes the operator one step further away from the actual actuations needed to achieve the system's objectives.

If the designer anticipates that meeting the desired functionality will require substantial complexity where the human has supervisory responsibility for the performance of the machine, then the interface should incorporate engagement techniques to assure that the operator has sufficient insight into the workings of the system to be able to take the appropriate actions when faced with an unanticipated problem.

The high level specification should not only contain the enumeration of desired functions of the system, but should generically capture these characteristics as standard functions to be included in systems which meet the criteria listed above with traceability to the rationale.

Chapter 4

Example Project The Shuttle Avionics Upgrade

The complex interactions between the machine, the operators, and their organization with its commensurate policies, regulations, and culture all combine to exhibit the emergent behavior of the system under operations. From a systems safety perspective, the goal is to have sufficient controls to prevent an occurrence of accident, which is defined as an undesired release of energy resulting the loss of equipment, personnel, or mission objectives. Also, in long duration programs, the probability of encountering any number of unforeseen external environmental conditions greatly increases. The system, people, and processes must be robust enough to control the emergent properties that arise as a result. Long duration complex systems naturally tend to become less safe over time due to constant cost and performance pressures. (Leveson) In order for organizations to increase the probability of avoiding undesired emergent behavior, deliberate upgrades, training programs, and safety emphasis must be instigated to counterbalance these pressures. Since emergent behavior is not cost effectively deterministic in the case of complex systems, a non-optimum solution that errs on the safe side must be pursued. It is beneficial to be able to utilize an existing project with a significant amount of operational infrastructure to be able to use it as a benchmark from which to base the comparisons and the experimental data. The Cockpit Avionics Upgrade (CAU) of the Space Shuttle Program is a case in point. The Shuttle training program is world class in its depth and fidelity. Program cost pressures are moving the organization to reduce the amount of expensive, customized mission training. Since an adequate level of training is not easily quantifiable, and costs must be lowered to ensure the viability of the program, a controlling (make the operations simpler) upgrade is appropriate, even though it will not provide a return on investment unless an accident is averted that would otherwise not have been, which is problematic to quantify, at best. All of the following concepts and requirements are from the upgrade concepts of operations produced in June of 2001. Each concept has an assessment with respect to the frameworks and applicability of engagement concepts.

The shuttle is one of the most complex systems in existence in the world today, but also has a wealth of operational data. The upgrade project is focused specifically on taking advantage of the new capabilities of the Multifunction Electronic Display System and previous operational experience to improve the command and display capabilities of the shuttle system.

Objectives of the upgrade

- Reduce crew workload by eliminating cumbersome limitations of the legacy system.
- Eliminate the necessity of switching from critical displays during high activity flight phases.
- Provide intuitive, mode tailored trajectory and system displays.

- Implement electronic task sensitive, time-critical, displays that eliminate the need to manually reference some paper products.
- Implement an enhanced caution and warning (ECW) system
- Implement an architecture with sufficient capacity for continued crew-vehicle interface enhancements and safety improvements over the vehicle's expected service life, estimated to be beyond 2020.

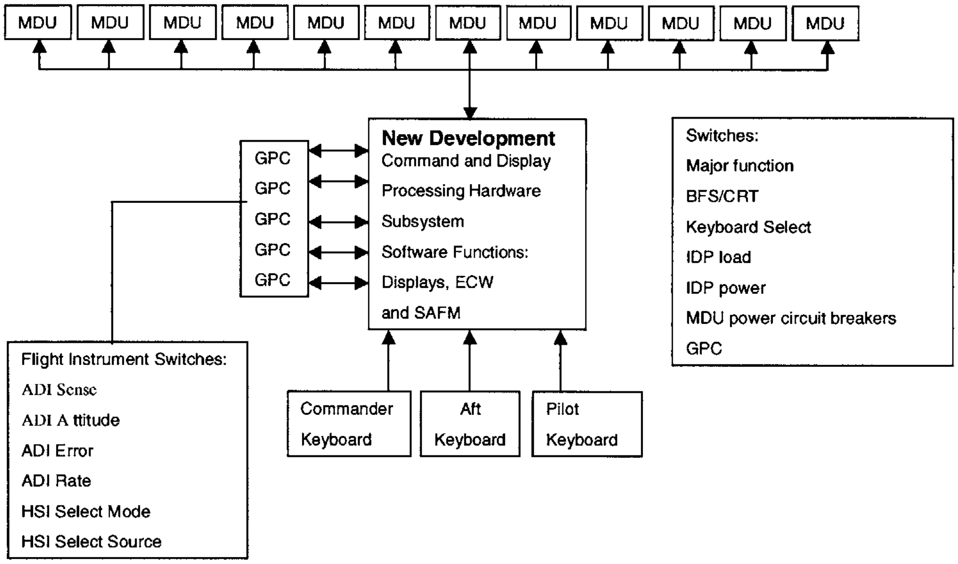
The benefits of fulfilling the prime objectives are reduced crew training time, in both initial and proficiency training, and improving system safety. The Cockpit Avionics Upgrade design is based upon detailed task analyses, subject matter expert interviews, problem definition studies, analysis of commercial and military aviation standards, and cost versus gain trade studies. The new architecture enables the implementation of a streamlined crew-avionics interface, more intuitive task-oriented displays, and enhanced display applications, while reserving a growth path for future enhancements. Although the Cockpit Avionics Upgrade will provide significant improvements in the cockpit, it is not planned to change the fundamental Mission Control Center/Orbiter relationship.

The MCC is responsible for malfunction and/or abort procedure decision-making whenever air-to-ground communication exists between MCC and the Shuttle crew. The relationship will change over time as cost pressures result in reductions to ground support and training. However, the fundamental systems safety model will continue and the avionics upgrade should counterbalance risks being accepted as cost pressures continue on the program. The following sections provide an overview of the top level Avionics Upgrade enabling requirements and an analysis of each in the frameworks of an ends- means hierarchy and a systems safety perspective.

The upgrade objectives are to improve the crew's situational awareness, reduce the crew workload during stressful, high activity periods, and change from a hybrid system/mode system to a more mode oriented system. This paper examines the project's scope, operations concepts and the design methodology using the framework of Leveson's Intent Specification and system safety model. The analysis also provides recommendations for usage of the human system interaction research in the project and proposes experiments to validate the concepts.

Project Scope

The CAU project consists of newly developed Orbiter hardware and software, hardware and software changes made to legacy Orbiter subsystems (e.g., Primary Avionics System Software, Backup Flight Software, or Multifunction Display Unit (MDU) software changes, keyboard keycap modifications, redefinition of cockpit switches), and all interconnecting cabling within newly developed hardware and with Orbiter legacy interfaces. Figure 1 depicts a block functional diagram of the CAU project. The legacy Orbiter hardware that is included in the CAU system consists of the three Orbiter keyboards, eleven Orbiter MDUs, five General Purpose Computers (GPCs), and associated cockpit switches.



Note: Designer is allowed to reassign or delete these switches

MDU FSW changes are allowed

Keycap changes are allowed

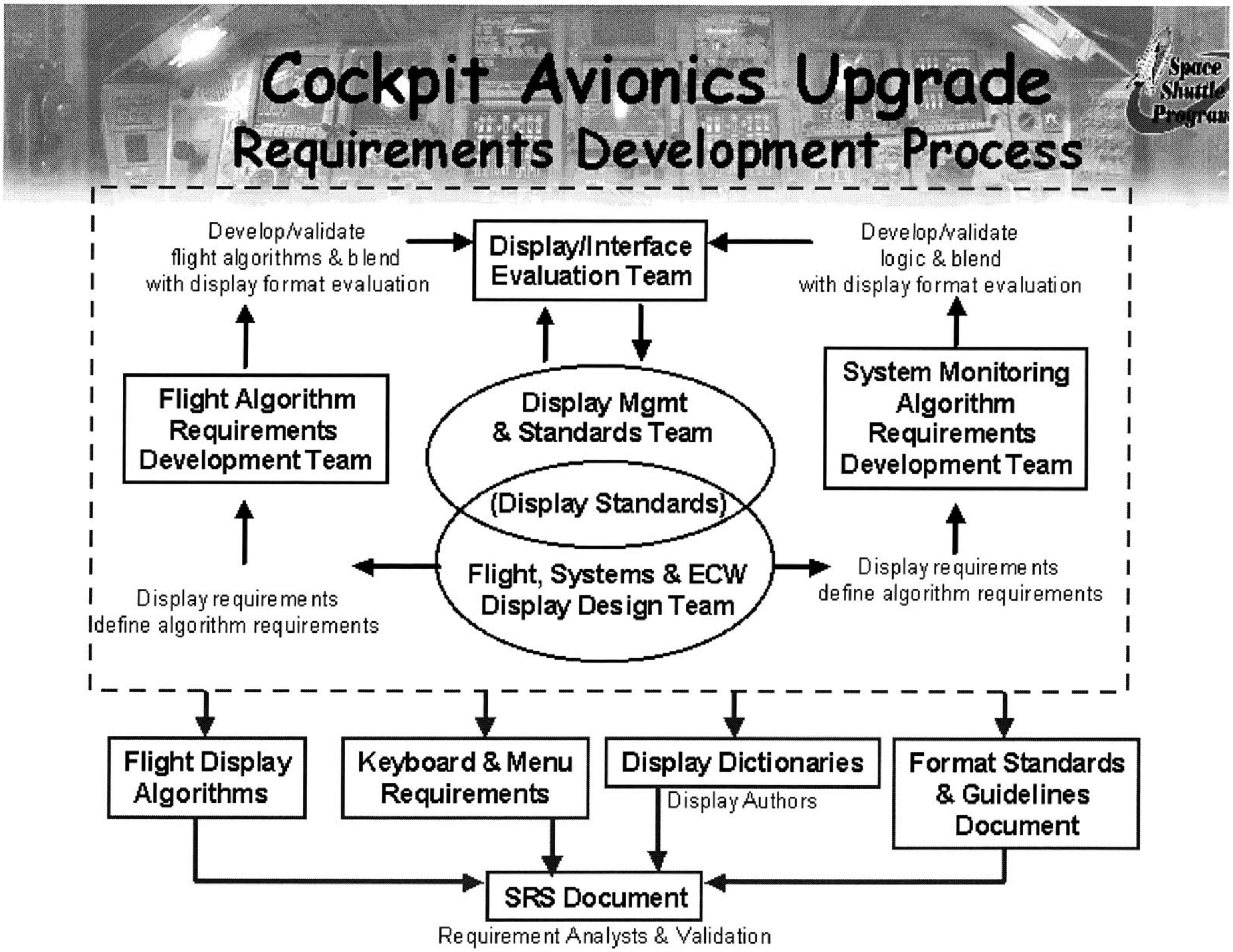
GPC FSW changesare allowed

Figure 1

The operator interacts with the avionics in several different ways, principally via the keyboard. Each keyboard has 32 keys, consisting of a numeric pad and 22 special function keys. Two of the three keyboards are located on the forward flight deck and the third keyboard is located on the aft flight deck. The keyboards issue commands to the GPCs that in turn issue commands to actuate effectors on the shuttle and payloads. The second method is via the MDUs; of which nine are located in the forward flight deck and two are located in the aft flight deck. Each MDU has six edge keys. The edge keys are strictly for commanding display functions. The ground interacts with the CAU via uplink through the Orbiter Interleaver. The final method for control is through actuation of physical switches and circuit breakers. Other command paths such as those via the onboard laptop are out of scope of the upgrade project. All newly developed hardware for the CAU system will interface to the GPCs, keyboards and MDUs.

In addition to the new control and display architecture, the upgrade is planned to include new self-monitoring capabilities, including automated recovery from detected single failures, and provision of enhanced system status. The system will continue to support different modes based on the phase of flight. The system software is planned to be updateable from the ground via uplink command to respond to shuttle in-flight anomalies. For prelaunch processing, ground personnel will access the system via the T-0 interface and the launch data bus. The functional specification for the CAU project is documented in

NSTS 37348. These requirements contain several attributes of intent specifications, including a rationale statement included with every explicit major requirement. The specification provides the system level requirements and constraints but does not explicitly address new software capabilities planned for the upgrade. These are included in each commensurate software requirements specification. The documentation for the upgrade contains much of the information required by the Leveson framework, but lacks the traceability imposed by the framework. As an example, Figures 2 and 3 are important information obtained from a presentation on the upgrade, but not contained anywhere in the formal documentation. Key information such as this should be kept within and traceable to other pieces of the design in order for the builders to have a framework for their design decisions.



Cockpit Avionics Upgrade
Requirements Development Process

Space Shuttle Program

Develop/validate flight algorithms & blend with display format evaluation

Display/Interface Evaluation Team

Develop/validate logic & blend with display format evaluation

Flight Algorithm Requirements Development Team

Display Mgmt & Standards Team

(Display Standards)

Flight, Systems & ECW Display Design Team

System Monitoring Algorithm Requirements Development Team

Display requirements define algorithm requirements

Display requirements define algorithm requirements

Flight Display Algorithms

Keyboard & Menu Requirements

Display Dictionaries

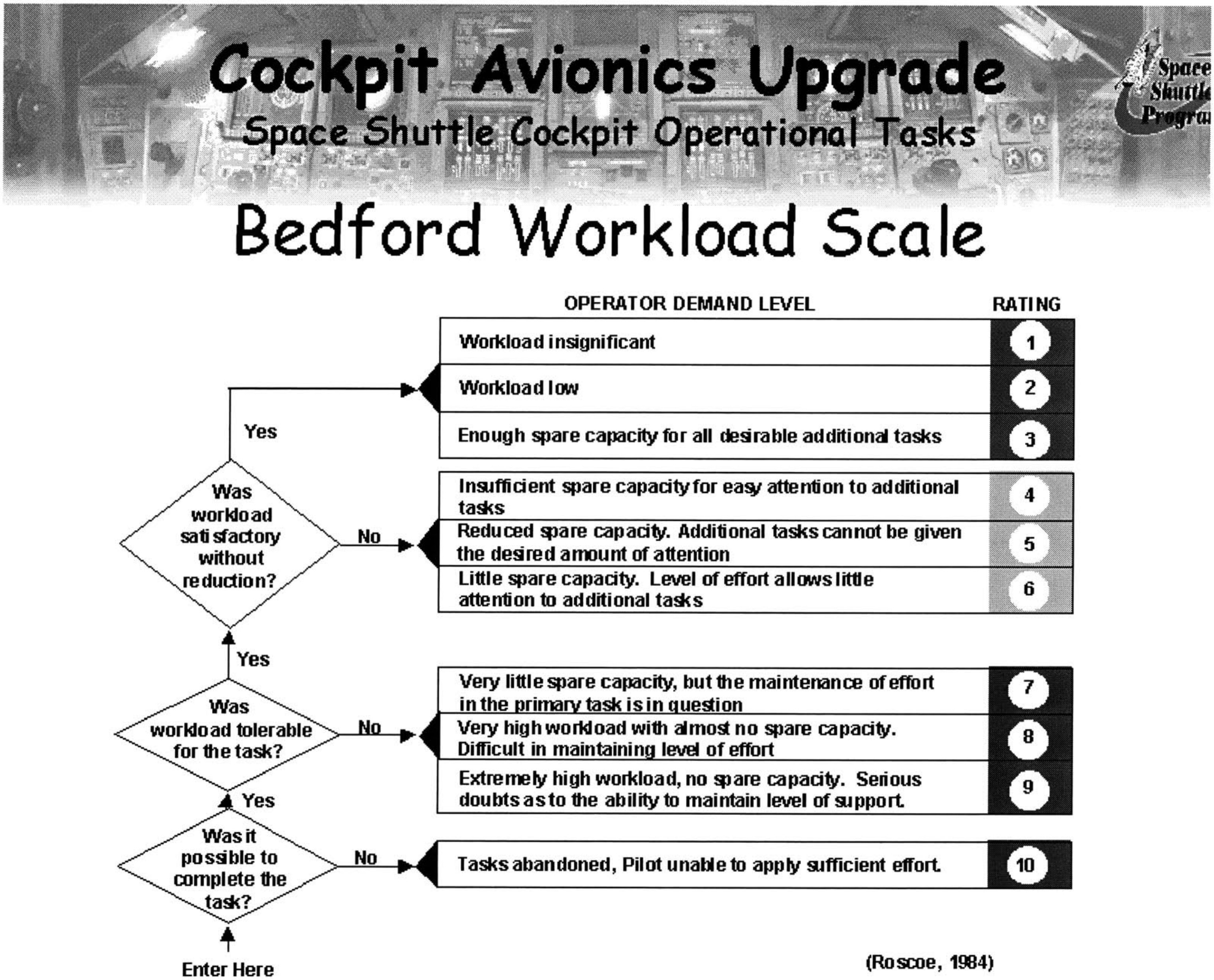
Display Authors

Format Standards & Guidelines Document

SRS Document

Requirement Analysts & Validation

Figure 2



Cockpit Avionics Upgrade

Space Shuttle Cockpit Operational Tasks

Space Shuttle Program

Bedford Workload Scale

OPERATOR DEMAND LEVEL	RATING
Workload insignificant	1
Workload low	2
Enough spare capacity for all desirable additional tasks	3
Insufficient spare capacity for easy attention to additional tasks	4
Reduced spare capacity. Additional tasks cannot be given the desired amount of attention	5
Little spare capacity. Level of effort allows little attention to additional tasks	6
Very little spare capacity, but the maintenance of effort in the primary task is in question	7
Very high workload with almost no spare capacity. Difficult in maintaining level of effort	8
Extremely high workload, no spare capacity. Serious doubts as to the ability to maintain level of support.	9
Tasks abandoned, Pilot unable to apply sufficient effort.	10

Enter Here

Was it possible to complete the task? No → 10; Yes ↑

Was workload tolerable for the task? No → 7–9; Yes ↑

Was workload satisfactory without reduction? No → 4–6; Yes → 1–3

(Roscoe, 1984)

Figure 3

The system is considerably constrained by the legacy hardware and software architectures. Although some enhancement is envisioned for the upgrade, significant hardware changes have been precluded due to cost constraints.

Each General Purpose Computer (GPC) is connected, via a data port, to a converter, which converts the memory map of the respective GPC into a high-speed serial data stream for transfer to each of three Command and Display Processors (CDPs). The CDPs replace the existing four Integrated Display Processors (IDPs), and fit within the same size, weight and power constraints as the IDPs. Each CDP maintains a complete real-time memory map of all five GPCs, without burden to existing GPC input/output capabilities. Additionally, each CDP receives data directly from the existing Orbiter Instrumentation and payload interface (PI) data buses. Each CDP has all the data necessary to generate enhanced displays, with information and commands blended from multiple sources. The CDPs send display information and receive status and edge-key inputs from the existing Multifunction Display Unit (MDU). Each MDU display is generated from a primary CDP. Each MDU has connectivity with a secondary CDP in the event of a primary CDP or transmission path failure. This is an improvement over the existing IDP-MDU connectivity which has only a single IDP for each of the four CRT MDUs.

The CDPs execute display software for each of the specific displays that it is generating e.g. change display colors, display shapes, de-clutter, etc. Additionally, each CDP simultaneously executes a limited set of display applications that run continuously over one or more flight phases, independent of what displays are being generated. These continuous applications include Shuttle Abort Flight Management (SAFM), which computes real-time abort boundaries and site selection during powered ascent, and energy versus range and landing site options during glided flight, and Enhance Caution and Warning (ECW), which provides intelligent, mode tailored fault diagnosis, failure management, and elimination of nuisance alarms. The upgrade is planned in delivery increments

Increment 1

Increment 1 will provide the core Cockpit Avionics Upgrade architecture and the replacement of the 1970's era "green screen" user interface with a streamlined, intuitive, task-based crew interface.

The operations concepts were derived to address the current fundamental user interface problems that exist in the Space Shuttle cockpit and provide the growth path for follow-on enhancements.

- The hardware architecture described above
- An enhanced, mode tailored display suite, with priority given to convert from a hybrid system/ mode display set to more function oriented flight, systems and fault display formats. These include the associated display logic and computations to generate graphics, trigger color and status changes, clutter and de-clutter particular display fields (mode tailoring), and compute local parameters. Detailed, lower level display formats will generally be "ported" copies of the current displays, modified slightly to conform with the Avionics Upgrade display standards, and will have limited display logic.

- A limited suite of display-independent applications that run continuously over one or more flight phases, regardless of which displays are called up on an MDU. These applications include the powered flight abort boundary determination and site selection, and vehicle glided flight energy assessment to reach landing sites and GPC set split diagnoses.
- A select set of Electrical Power System bus modules that use GPC and OI parameters with "and"/"or" Boolean logic for sub-bus loss diagnosis. These modules will be used for the **EPS Sum** and other system summary displays that depict EPS sub-bus loss impacts. These modules will not be used to annunciate alerts in Increment 1.

Increment 1 will not include changes to the existing class 0, 1, and 2 software and hardware caution and warning systems, with the following exceptions:

- New monitoring and software driven text annunciations will be added as necessary for the new hardware (for example, alerts for CDP anomalies).
- Some unused software driven text alerts will be deleted (for example, some of the currents MEDS alerts are currently not used by crew, or will not be required in the new architecture).

Some of the text annunciations for software alerts will be modified to more clearly indicate the failure or to conform with Avionics Upgrade display standards.

Increment 2

Increment 2 builds upon the Increment 1 display suite by providing an initial implementation of ECW. Increment 2 includes:

- Baseline ECW application or “engine.”
- ECW for critical systems only (priority given to system failures that do not have obvious failure recognition cues), triggered from a combination of GPC fault messages and OI discretes, with ECW applications to drive fault suppression and inhibition for the subset of critical system fault annunciations.
- Baseline ECW displays (main ECW, status, history and consequences displays).
- Format and application enhancements that were not within cost guidelines for Increment 1 or identified after Increment 1 design (based on priorities and cost constraints).

Increment 3

Increment 3 will complete the Cockpit Avionics Upgrade by providing the full ECW application applied to all shuttle systems. It may also include additional format and application enhancements identified in the development of Increments 1 and 2.

Follow-on Increments

Follow-on changes will occur in regular Orbiter Flight Software Increments (OI releases), utilizing the same processes that are currently in place for Shuttle flight software. The content of these increments will be based on priorities and funding. They may include expansion of the ECW core application to include all of the shuttle systems, and any additional display and application enhancements or fixes identified during the development or after the implementation of Increments 1 and 2.

The same processes, organizations and facilities used in the Cockpit Avionics Upgrade design, prototyping and verification of display requirements, the implementation of the requirements, and the validation of the display implementation will remain in place for the sustaining growth of the Shuttle cockpit avionics.

One of the most significant and beneficial features of the Cockpit Avionics Upgrade architecture is the consolidation of information and commands from multiple sources (Primary Avionics System Software (PASS), Backup Flight Software (BFS), Command and Display Processor (CDP), and Orbiter Instrumentation (OI)) onto a single display. This includes the ability to blend information from multiple GPCs and GPC major functions (guidance, navigation and control (GNC), system monitoring (SM) and payload (PL)) onto a single display, transforming information displays from sets of compartmentalized subsystem or mode data to a display which contains all of the necessary information needed to perform a specific task or management function. Coupled with the consolidation of information and commands is a more cognitively compatible display navigation. In the current cockpit, crew is required to memorize assigned display numbers and allowable major functions, must reference separate PASS and BFS displays for the same system, and must reference multiple formats to gather information or issue commands for a single system or task.

The new approach will give the crew easier access to most of the needed information references for their mental model, which will eliminate, or substantially reduce, the necessity for the crew to reference multiple displays to gather information or make commands associated with a single task or system management function. The upgrade does not intend to replace all paper procedures and checklists due to costs and the commensurate additional complexity that would be added to the orbiter display software. This intent is in line with the EID, in that it removes a significant amount of unnecessary cognitive load on the crew and makes most of the actions either a skill or rules based action, arranged based on the particular task being performed.

The consolidation of information and commands greatly simplifies display navigation. After completion of the Avionics Upgrade cockpit, the crew will not have to memorize superfluous information related to the limitations of the current display constraints.

In the current architecture, for example, Auxiliary Power Unit (APU) information is found on the **BFS SM SYS SUMM 2** display during ascent and entry (i.e., crew members must use a "green screen" multi-function display unit (MDU) assigned to the BFS, select the SM major function on that MDU, and then use the keyboard to call up "SYS SUMM 2"). On orbit, however, APU information is found on the **PASS SM SYS SUMM 2**, **SM SPEC 86**, **SM SPEC 87**, and **SM SPEC 88**. The on-orbit displays are not available during ascent and entry.

Successful operation of this management function requires many hours of practice in both private and group sessions for a crewmember t o perform without the need of detailed checklists, which must be constantly re-verified each flight as changes in the vehicle and software are implemented. Even with today's extensive training, it is obvious that time critical failures are significantly more likely to evoke procedural errors with the existing system than with the proposed enhancements.

The upgrade allows crews to navigate via an ends- means hierarchy menu available in all flight modes. In the example above, the crew would select (the menu via MDU edge-keys or keyboard entry, without using "SPEC" numbers), a single APU Hyd summary display to gather all the top level APU information required to accomplish routine nominal and time-critical off-nominal procedures, alleviating the need for the crew to memorize which GPC is providing the data.

Note that with in this particular instance, the crew's mental model of the actual physical interconnections of the system is eroded, and should be augmented via training or captured in a further APU/Hyd data system detail display. This approach also keeps the control interface at the Rules level of the EID, with straightforward procedural processing to accomplish the tasks.

This problem with the legacy system is prevalent through all flight modes, and has resulted in a long training template and expensive procedures verification process. The controlling factors preventing the limitations thus far from not causing an accident, are the extensive refurbishment and maintenance and therefore relatively trouble free systems performance of the shuttle, the extensive training, the caliber of the people entrusted to fly the vehicle and the tight team process with a substantial number of system experts following every step of the processes. As pressure to reduce the control staff, training templates, and refurbishment templates increases, the CAU project is expected to help mitigate the losses.

The upgrade also intends to consolidate mode information. In order to monitor vehicle ascent performance and execute time critical abort procedures the present system requires switching from primary and backup systems to follow the vehicle through that phase of the flight. The **PASS ASCENT TRAJ** is used to monitor primary guidance (but only during a limited portion of the phase), monitor contingency abort regions, command single engine roll control (SERC) and command a contingency abort. The **BFS ASCENT TRAJ** was designed by a separate design team and provides a different representation of the same information different from the **PASS ASCENT TRAJ**, but supports the same guidance monitoring task as the **PASS ASCENT TRAJ** (from the BFS perspective). The BFS display serves as the prime display for trajectory monitoring because it provides information during the entire powered ascent flight phase at level of fidelity that is more useful to the crew than the **PASS ASCENT TRAJ** display. The **SPEC 51 OVERRIDE** display is used to command main engine throttle levels, command orbiter maneuvering system (OMS) dumps that are required for aborts, and as an alternate means to command an abort in the event of a failure of the commander's abort rotary knob or push-button.

The **OMS/MPS Sub-system Status** display is used to monitor main engine and orbital boost/ deorbit engine status. During powered flight, a high stress, high activity mode, 4 displays are required, on 4 MDUs, including all three available "green screen" MDUs, in order to accomplish a single abort procedure.

The Cockpit Avionics Upgrade powered ascent **Traj** display consolidates all the necessary trajectory monitoring information and abort commands from the four PASS and BFS **ASCENT TRAJ**, **SPEC 51 OVERRIDE** and **OMS/MPS Sub-system Status** displays onto a single display and organizes it in an ends – means hierarchy.

Main engine chamber pressure tapes, flags to indicate main engine anomalies, and PASS/BFS commanded throttle levels provide an overall assessment of main engine health, including detected failures. The flight design trajectory monitoring line is mode tailored and automatically changes to reflect the current flight mode, which is displayed at the top of the screen. The display also includes predictor mode technique for the flight dynamics trajectory with current and future states displayed for either the primary or backup guidance, allowing the crew to manually fly the vehicle via BFS guidance without engaging BFS, providing operator choice for optimum control. The display also provides graphic indicators that depict when an OMS assist or dump is in progress and with commensurate detected falure indications.

The current shuttle requires multiple system summary formats, in both PASS and BFS, as well as GNC and SM, to gather situational awareness regarding the status of the vehicle systems, because the displays are organized via system rather than via operator function or process. During ascent and entry, crews cycle through **PASS SYS SUMM 1**, **BFS GNC SYS SUMM 1**, **BFS GNC SYS SUMM 2**, **BFS SM SYS SUMM 1** and **BFS SM SYS SUMM 2,** depending on which flight mode, (called for by checklist) or depending on failures detected.

The Avionics Upgrade, on the other hand, will have a single **Fault Summary** display, which consolidates information from PASS and BFS (both GNC and SM) with OI data to provide crews a mental model enhancing status of the vehicle. The display provides system health, and an indication of vehicle systems that have parameter values that exceed software caution and warning limits or are missing (communications faulted). This display provides a means to troubleshoot problems and gives the operators more insight as to the potential effects of detected failures, and may be used to direct crews to top level system summary displays, when necessary, to perform the appropriate malfunction procedure(s). The increment 1 phase of the upgrade will not be fully ends-means. The display will be oriented via a system- subsystem hierarchy, which enhances the mental model, but does not necessarily guide the crew through procedures.

The display provides both detected failures with unambiguous indicators and a "subdued dark" philosophy, which provides no indications other than the gray labels and dark gray symbols, unless a parameter related to that system exceeds software caution and warning limits. The lower portion of the display keeps track of most recent PASS and BFS fault messages. The crew can also view a time-ordered list of the most recent fault messages by selecting a log **display**.

The Cockpit Avionics Upgrade architecture will allow for customization of the forward displays by the crew. The current shuttle has a restricted view with three interactive displays and six information only displays. This results in the crew having to time-share the three interactive GPC generated "green screen" formats in performing all the tasks associated with monitoring and managing each of the vehicle systems, as well as the vehicle trajectory, guidance and navigation. Crews are often forced to replace critical trajectory formats for system display formats, and vice versa. This problem is especially prevalent during ascent and entry when the crews must time share the central MDU among all of the BFS trajectory and systems monitoring formats. The current system also, in come cases, requires commands to be instantiated from different displays than those critical to monitoring the progress of the flight. This display "juggling" is high workload and results in lost situational awareness during the most dynamic flight phases.

The ops concept provides this example:

" For example, the **SPEC 51 OVERRIDE** display is a "green screen" format that the crews use to make throttle command entries. The main engine throttle levels, however, which are used to determine the need for making the **SPEC 51 OVERRIDE** throttle commands and verification of the commands, are monitored by the crew using the **OMS/MPS Sub-system** display, which has no command interface."

Commands are issued by shifting the operator's keyboard assignment to the desired display via switch, followed by the appropriate item entry key strokes (item entries are made in the Avionics Upgrade cockpit similar to the way they are made in the current cockpit). The commands are issued by typing an item number that is associated with a particular function. This method of command entry is effective because it eliminates ambiguity and inadvertent commanding. The development and deployment of a new command interface has significant risk as well as little tangible benefit. Using the existing command structure provides an interface that is familiar and simple to use.

With the upgrade, crews will also be able to customize the layout of displays, depending on flight phase and failure situations, allowing for concentration on the problems at hand rather than remembering which displays are needed and moving back and forth. This will also allow particular crews to decide layouts during training, making the layout as user specific as possible without the verification difficulties associated with software customization.

If the crew is alerted to a malfunction for a system that does not have a display called up, the display navigation tree is instantiated via a single edge key. For example, if the crew needs an OMS display to respond to an OMS malfunction, the pilot can replace the current system summary display with the **OMS Sum** display via a single MDU edge-key push or keyboard entry, without dropping the vehicle trajectory, fault summary or main propulsion system (MPS) displays.

The Avionics Upgrade architecture will allow for multi-color graphics with logical information and command groupings on any display, consistent with human factors standards and modern aviation display design. This eliminates the current monochromatic, text-based restrictions associated with the GPC generated “green screen” displays, enabling displays functions to be grouped and differentiated, improving the operator mental model. The new graphics capabilities allow greater relationship indicators and reduces clutter, reducing mental workload in interpreting cryptic and cluttered displays.

The current display has textual references to valve positions and fault statuses, requiring a mental visualization of the system layouts and interactions. Key parameters are easily lost in columns of monochromatic, single font numbers, and split among multiple formats. The crew must also interpret some sensor indicators to glean a fault and perform cognitive analysis to properly assign the effects of the fault. The new displays provide a virtual representation of the physical interactions of the subsystems and components, and use color schemes to provide instant visualization of system condition, consolidated on a single display addressing the current function being performed, as well as effects from other subsystems on the subsystem being displayed.

The Cockpit Avionics Upgrade architecture will allow for the tailoring of display information and commands to the current flight mode. As an example of display mode tailoring, the current **SPEC 50 HORIZ SIT** display is used to manage navigation sensors and landing site selection, and for an overhead depiction of the vehicle’s relative location to the selected landing site.

The only portions of this display used during ascent are the landing site selection item entries on the left side. Since the overhead view does not function until the entry flight phase, the display provides no situational awareness of horizontal trajectory, abort region boundaries and relative position to potential abort sites.

Additionally, the navigation sensor fields are not functional   Crews use procedure cue cards and voice communication with the Mission Control Center (MCC) for abort boundary determination, adjustments to abort boundaries for staggered engine failures, and abort landing site selection. Manual look-up using paper tables during the very dynamic, time critical phase of powered ascent can cause temporary loss of awareness of critical vehicle health parameters and increases workload at very critical phases of the flight. Adding this information to the horiz sit display prevents fumbling through paper checklists and provides a dynamic view of the flight situation.

The new display consists of a static map with a moving orbiter and a magenta target insertion plane. There are two selectable scales: **H Sit 1** for east coast abort landing (ECAL) sites, and **H Sit 2** for transoceanic abort landing (TAL) sites. The display contains all the information and commands used by the commander in making landing site selections, determining abort regions and selecting an abort when the abort rotary knob or the push button fails. This display replaces the no communication abort boundary, staggered engine TAL and ECAL re-designation, and the two and three engine out contingency site selection cue cards. The new display will provide an intuitive display of the abort options for all engine failure possibilities on board, similar to what's available in the control center. Although the control center will retain responsibility for abort region determination during periods with good vehicle-ground communication, the new display will decrease the possibility of vehicle and ground miscommunication by providing the on board operators situational insight.

The display will use the Shuttle Abort Flight Management (SAFM) application to replace the manual procedure cue table look-ups. The display uses tables and colors to guide the crew to make the proper selections depending on engine failure and timeline parameters. The **SPEC 50 HORIZ SIT** commands that are not used during ascent are removed from the mode tailored Avionics Upgrade **H Sit 1** and **H Sit 2** displays. Additionally, the abort execution item entries, which currently reside on the **SPEC 51 OVERRIDE** display are appropriately consolidated onto the task-based Avionics Upgrade display, designed to support the CDR in the abort region determination and execution tasks.

It is the same **SPEC 50 HORIZ SIT**, but with an active overhead view, that provides useful information to the crew only during the terminal area energy management (TAEM) flight phase (the final portion of the entry profile). During the earlier phases of entry, this display provides very little useful information. The bottom portion of the display is used to manage incorporation of navigation sensor data.

This new display is tailored to the crew pre-TAEM tasks: determination of vehicle capability to reach available landing sites, landing site selection, and delta azimuth management (roll reversals). The display provides an overhead view of the vehicle position, azimuth deviation and bank angle relative to the selected and alternative landing sites. The top left portion of the display uses the

SAFM application to provide an energy assessment to the selected landing site and the next best two alternative sites. Potential sites are listed and guidance modes to reach them are specifically enumerated.

The **SPEC 50 HORIZ SIT** navigation sensor management information and commands are moved onto a phase tailored sensors display (which consolidates the PASS and BFS navigation sensor information and commands onto a single display).

The TAEM version of the prototype Avionics Upgrade horizontal situation display, looks very similar to the current SPEC 50, which is well suited for the TAEM flight phase.

These examples illustrate how the Avionics Upgrade architecture will allow for mode tailoring of displays, which will eliminate unused fields, reduce potential mode confusion, and provide the appropriate information and commands to the crew at the appropriate time. These displays are oriented in an ends means hierarchy and well suited to guiding the operator according to the Rasmussen interface model. Most of the interaction is at the skills level, with a few items at the rules level, making these critical phases of the flight high in engagement.

The current GPC display generation capability lacks the processing speed and memory capacity for implementation of displays consistent with modern aviation technology. The Cockpit Avionics Upgrade architecture will expand the avionics processing and memory capabilities for the implementation of enhanced display applications and logic. The processor and memory will be sized to include all of the proposed Cockpit Avionics Upgrade displays and associated applications, plus reserve for follow-on growth. Expanding the display processing capabilities opens the door for the implementation of modern displays and support applications that will reduce crew workload and increase crew situational awareness, but also has the potential to increase the risks through increasing software complexity and verification problems. The plan is to add functions incrementally, but no method currently exists to assess the cost versus benefit for these changes.

The Cockpit Avionics Upgrade architecture will segregate the display generation software from the GPCs. This axiomatic principle is one of the big advantages of the upgrade project. Although the display software is now logically separated from the command, instrumentation, and control software. The physical separation should streamline the development, prototyping, verification and implementation of display software by making it independent of the guidance, navigation and control (GNC) and system monitoring (SM) flight software, resident in the GPC's. Segregation of display software from the GPC hardware that executes the GNC and SM flight software reduces the risks and level of verification associated with display updates. Additionally, it frees memory and processing in the GPCs, which are currently at near capacity levels, reducing risks associated with faults that occur when computers are near their performance boundaries.

Crew display interface is via the existing three keyboards, which will be updated to be more intuitive with the displays. Each keyboard is connected to all three CDPs via existing 1553 data buses. This enables the use of any CDP from any keyboard for single CDP operations.

Although the location and size of the physical keyboards remain unchanged, the mapping of the keys is changed to facilitate the streamlined display navigation, keyboard focus and command entry.

Each of the two forward cockpit keyboards is assigned to a particular MDU via the DU key followed by a number 1 through 9, representing the nine forward cockpit MDUs, numbered left to right. The aft keyboard can be assigned focus only to the aft two MDUs, designated 1 and 2 when using the aft keyboard and the DU key.

Keyboard commands are transmitted via the prime CDP for the assigned MDU to the appropriate command recipient(s). For example, a keyboard item entry to deselect an inertial measuring unit (IMU) in the BFS is directed by the CDP only to the BFS GPC; a keyboard entry for a PASS OPS transition, on the other hand, is transmitted simultaneously to all PASS GPCs.

The existing MDU edge-keys are used for display navigation only. No vehicle commands are issued via the MDU edge-keys. Display navigation may also be accomplished using the A through F keys on the keyboards. These keys equate to the six MDU edge-keys (lettered A through F from left to right) for the MDU to which the keyboard is assigned.

Minor modifications to the cockpit panels will be required since the crew will no longer assign CRT's to specific major functions, assign the BFS to a specific cathode ray tube (CRT), or use a switch to assign keyboard focus to the center CRT's. These changes are not expected to have a significant interface design effect.

Summary Analysis

The following is an analysis of the upgrade with respect to engagement techniques. Increment 1 of the upgrade deals with the high engagement phases of flight. Pilot skills tasks are effectively modeled using a predictor mode display and joystick for the control. This type of display is very effective in preventing pilot induced oscillations and has a good track record of performance both in flight and even in simulations, where the cognitive load is intentionally stressed in order to sharpen the crew's mental model of the design of the shuttle. The other mode oriented displays do not require engagement techniques as these phases of flight are not tedious or long duration and now follow an ends-means hierarchy with rule based behavior for control.

Increment 2 and beyond, on the other hand, have the potential for utilization of engagement techniques. The final two aspects of the upgrade are systems management and ECW. Systems management has been given the lowest priority of the upgrade. All of the detailed systems management displays are planned to be simply the ported green screen displays of the current shuttle. These are rows of text based displays, that can change intensity when out of limits. The upgrade project plans to slowly develop more human intuitive displays as a part of the sustaining effort for the project. While these have the potential for engagement techniques, their low priority, coupled with a higher cost for added engagement techniques, do not make them a good candidate for further analysis.

This part of the project does not follow the task based, ends-means paradigm of increment one and should merit reconsideration of the current approach.

The longer duration of the orbit phase and the likelihood of infrequent use of the ECW system make it more suitable for engagement techniques. A combination of the techniques are applicable and a discussion follows. ECW already has some innate characteristics of engagement. A natural tension ensues when an alarm sound, because it signals the failure of some of the vehicle's equipment and the resolution usually process follows the random walk between resolution and further trouble. The rules for troubleshooting are also clear and unambiguous. The steps are identify, safe, isolate, and restore to operations. The troubleshooting procedures are usually well documented, depending on the tyoe of alarm. The two major goals when encountering a failure are to ensure the vehicle is safe and return to normal operations as quickly as possible. The metrics to be tracked are clearly quantifiable for most systems, with time usually being the most important metric. For consumables, tracking of the losses due to the failures are also an ideal tracking metric. Since the shuttle is an incredibly complex machine with substantial redundancies, fault isolation and restoration can be a very challenging problem and usually requires development and execution of a strategy for resolution, which is in direct alignment with the play paradigm.

The proposed design of the engagement techniques would first be implemented in the single systems trainer. This is an ideal environment where facsimiles of the actual flight displays are implemented. These would be augmented with a tracking and scoring adjunct to the display, giving performance statistics with respect to the desired goals of the isolation exercises. The trainer can also be augmented with pop up storyboarding, providing immediate feedback for inappropriate responses to the injected failure and providing aids to improving the crews' mental model of the operation of the vehicle.

Whether these adjuncts would be kept for use on the flight vehicle may be debatable, and a set of tests to determine whether they are an enhancement or detraction to performance should be performed. Assessment of the effectiveness of the new approaches will be performed by experiment. The experiments will utilize current Space shuttle instructors, taking the lessons both with the display enhancements and without, and assessing their performance via standard proficiency tests to measure the effectiveness of their mental models of the new systems derived from their training. Even if these do indicate a clear performance advantage of the new approach, Shuttle managers may be reluctant to add the applications to the vehicle displays because of distraction and complexity concerns. In this case, the tracking application might be added to the shuttle laptop, providing the crew with an in flight familiarization tool, without adding risk to the flight displays.

Chapter 5

Application to the Management of High Performance Teams

The work of analyzing and determining the most effective approaches for improving human-system performance naturally gives rise to possible corollaries for use in managing work teams. Since the advent of the utilization of the team paradigm for accomplishing work, the literature abounds with sports analogies and various aspects of play for improving team performance. Therefore, deliberate utilization of the elements of play paradigm that improve human-system performance should be applicable for use in improving team performance.

The key principle derived from analysis of the tenets of play is that no matter what methods are used for enhancing the team performance, the team leader must engender a strong belief in the approach and must ensure that all members of the team are 'playing by the rules'. Most of the methods for improving team performance involve an intense indoctrination period, and recommend getting rid of naysayers in order for the system to work. This methodology is exactly in line with the principles of play. If one player begins to blatantly break the rules, the game immediately comes to a halt and can not proceed until the rule breaker is removed from the game environment. However, if the player goes along with the game, but breaks the rules, the game can continue, although somewhat corrupted by the cheater. Therefore, the key tenet that can be derived from this is that it is the responsibility of the team leader to understand the extent of 'buy in' of each member and to make sure that if some members are not fully engaged with the methodology, that they be coached to participate in the methodology and to refrain from creating non constructive dissention during the start up phase.

Another component of the play paradigm in use today is competition. Management practitioners have found that using the balanced scorecard method for managing work is very effective in increasing the productivity of teams. This method is most effective when it becomes a game where teams are competing with each other to achieve the best scores and when recognition is plainly evident and occurs at regular time intervals. The downside to this approach is that referees must be appointed to assure scoring integrity and the output may be sub-optimal if the metrics used in scoring are misaligned with firm's strategic direction. Nonetheless, judicious use of the competition attribute can be a powerful motivator and its success is well documented in management literature.

The use of tension is also in line with current management practice. The methodology that uses this principle effectively is the use of stretch goals. If a team has an appropriate stretch goal, natural tension arises because the team's normal expectation is that the stretch goal can not be achieved. The manager in this case should use the stretch goals to achieve short-term objectives, rather than establishing long-term stretch objectives, because the aggregated goals will often appear too difficult and can result in disillusionment with the processes, which is potentially catastrophic, resulting in the loss of buy in and the subsequent loss of belief in the process.

Finally, every development project requires an effective strategy and plan in order to achieve success. The key tenet that the play paradigm brings to this situation is again the well documented need for each member of the team to participate in its formulation. If team members participate in the strategy formulation, it not only engenders the needed buy in, but also facilitates engagement by the participants. Team leaders should be very vigilant in assuring that each member of the team has gone beyond the skills and rules levels of cognition and applied the knowledge level cognitive processes to the particular project being addressed. By assuring this level of participation, the leader increases the engagement of the team member and therefore improves the probability of successfully delivering the project's objectives within the constraints.

Chapter 6

Summary and Conclusions

The purpose of this research was to help developers of complex systems, by building on the Systems Safety and Intent Specification framework for complex systems design developed at MIT. The principal enhancements to the existing intent specification model posed by this thesis are to modify the framework at the higher levels and establish a set of design principles for human system interaction to be selected by the designer and included as part of their design documentation. The principles are isomorphic to Rasmussen's Ecological Interface Design, which contains a Skills, Rules, and Knowledge Hierarchy. A set of principles for the Skills and Rules levels for complex system control design are proposed and validated by a survey of current research. The innovative key proposition of this thesis is that if the human-machine interaction has elements of play in it, the mental model necessary for effective knowledge- based control of a complex system will be enhanced. Aspects of engagement derived from the play paradigm analyzed were: Belief Competition, Unambiguous rules, Requires strategy or skill, Tension, and Fun.

This research assessed the existing design documentation of the Cockpit Avionics Upgrade of the Space Shuttle Program within the framework of intent specification, in order to develop specific recommendations to improve the design of the upgrade. The research applies proposed heuristics to the

Upgrade's new displays and proposes design enhancements incorporating selected aspects of play to control of the spacecraft to assess whether they have any long-term benefits.

The thesis recommends changing some of the display hierarchies and improving the overall traceability of the operations concepts to the design of the upgrade. The analysis also recommends applying pop up story boarding to training displays, establishing performance times and quantitative metrics in the display, as well as a tracking application to be included on the orbiter laptop.

If research on the human-systems interaction that takes advantage of the play paradigm proves viable, it might also be extended to take advantage of natural human communication characteristics. Techniques such as reducing the challenge level during high stress periods in order maintain the human-system performance, providing interesting and interactive problems during non-operational hours, and allowing for tuning to suit the particular personality of the operator should also be investigated. Since the target environment for this research is limited to only a few individuals, some sort of matching to personality should not only be feasible but appropriate.

The conclusion of the analysis is that engagement techniques should be applied not in the actual performance of time critical tasks, but only in test and checkout functions that allow the operator to explore the functionality and limits of the systems. While these activities may increase the wear and tear on the system, the additional knowledge garnered by the operator should make the system safer.

Perhaps the most interesting avenue for further research has to do with tailoring the engagement techniques to fit certain personality types. The great range of personality types seems naturally to lead to the conclusion that different engagement techniques are applicable to different people. For complex systems, rather than have the systems customizable to the individual operator, the most logical approach would be to have some sort of efficacy test to determine which person would be ideal for operation of the system.

In summary, use of the play paradigm does appear to be in line with current research on improving the human interface to complex systems. If designers know the principles of play and judiciously apply them to the correct control situations, these techniques may prove effective in making complex systems safer, and more enjoyable for the operations community.

References:

1. Leveson, N., (2001) A Control Theoretic Model of Accident Causation, draft, p21-22
2. Leveson, N., (1995) Safeware: System Safety and Computers Published by Addison Wesley. Leveson, N.,
3. Rasmussen, J. (1987). The Definition of Human Error and a taxonomy for Technical System Design, In Rasmussen, Duncan, and Leplat, (eds.) New Technology and Human Error, p 25, Wiley & Sons, ltd. Chichester, UK.
4. Intent Specifications: An Approach to Building Human-Centered Specifications, IEEE Trans. on Software Engineering, January 2000
5. Fischer, G. (1993). Beyond Human-Computer Interaction: Designing Useful and Usable Computational Environments. In J. Alty, D. Diaper & S. Guest (eds.) People and Computers VIII, Proceedings of the BCSHCI' 93 conference, Cambridge University Press, Cambridge, UK
6. Woods, D.D., & Roth, E.M. (1988). Cognitive Systems Engineering. In M. Helander, (ed.) Handbook of Human-Computer Interaction. Elsevier: North-Holland..
7. Neisser, U. (1976). Cognition and Reality. San Francisco: W H Freeman
8. Rasmussen, J. (1986). Information Processing and Human-Machine Interaction. An Approach to Cognitive Engineering. A.P. Sage (ed.) North-Holland Series in System Science and Engineering. Elsevier Science Publishing Co., Inc., Amsterdam.

9. Huizinga, Johann, Homo Ludens, A Study of the Play Element in Culture, Beacon Press, Boston, 1955, English translation of the 1944 German version of the original published in 1938.

10. Vicente, K, & Rasmussen, J, Ecological Interface Design: Theoretical Foundations, IEEE Transactions on Systems, Man, and Cybernetics,V22 1992

11. Rasmussen, J. (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man, and Cybernetics, Vol. 13, No. 3, pp. 257-266.

12. Hammond, KR, Hamm, RM, Grassia, J, Pearson, J, Direct comparison of intuitive and analytical cognition in expert judgement" IEEE Trans. Syst. Man Cybern. Vol SMC-17 pp 753-770, 1987

13. Lind, M. (1991). Effects of Sequential and Simultaneous Presentation of Information. Report no. 19, CMD, Uppsala University.

14. Nygren, E., Johnson, M., Lind, M. & Sandblad, B. (1992). The Art of the Obvious. Automatically Processed Components of the Task of Reading Frequently Used Documents. Implications for Task Analysis and Interface Design. J.P. Baursefeld, J. Bennett & G. Lynch (eds.) Proceedings of Human Factors in Computing Systems, CHI '92, Monterey, California, Ma y 1992, ACM, pp. 235-239

15. Johnson, J.V. & Johansson, G. (Eds.) (1991). The Psychosocial Work Environment: Work Organisation, Democratization, and Health. Baywood Publishing Company, Inc., Amityville, New York.

16. Kelley, CR, (1971) Display Layout, In Display and Controls p 41-52, Swets and Zeitlinger, NV Amsterdam,1972

17. Ziegler, J.E. & Fähnrich, K.P. (1988). Direct Manipulation. In M. Helander (ed.) Handbook of Human-Computer Interaction, Elsevier Science Publishers B.V.

18. Singleton, WT (1971) General theory of Presentation of Information, In Display and Controls p 81, Swets and Zeitlinger, NV Amsterdam,1972

19. *Selim, Jocelyn,* Soccer or Nascar, It' s All the Same*by* DISCOVER Vol. 22 No. 6 (June 2001

20. Space Shuttle Cockpit Avionics Upgrade, Concepts of operations, Volumes 1-3, June,2001

21. NSTS 37348, NASA Space Shuttle Cockpit Avionics Upgrade Functional Specification