MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Demonstration of a New Dynamic Approach to Risk Analysis for NASA's Constellation Program

MIT CSRL Final Report to the NASA ESMD Associate Administrator*

March 2007

Dr. Nicolas Dulac[1]
Brandon Owens[2]
Prof. Nancy Leveson (PI)[1,2]

Dr. Betty Barrett[2]
Prof. John Carroll[2,3]
Dr. Joel Cutcher-Gershenfeld[2,3]
Stephen Friedenthal[2]
Joseph Laracy[2]
Prof. Joseph Sussman[2,4]

Complex Systems Research Laboratory
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

[1] Department of Aeronautics and Astronautics
[2] Engineering Systems Division
[3] Sloan School of Management
[4] Department of Civil and Environmental Engineering

* This research was supported by grants from ESMD, USRA/NASA APPL, and NSF. The NASA ESMD points of contact for this research are David Lengyel, Garry Lyles, and Dr. Fred Bickley

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

The authors would like to thank the 44 NASA employees at Headquarters, Marshall Space Flight Center, Johnson Space Center, and Langley Research Center who participated in face-to-face interviews with the authors throughout the project. These employees represented the following offices and directorates:

- Office of the Administrator
- Office of the Chief Engineer
- Office of Safety and Mission Assurance
- Office of Program Analysis and Evaluation
- Office of Institutions and Management
- ESMD Directorate Offices
- Program Offices
- Project Offices
- NASA Engineering and Safety Center
- Center Safety and Mission Assurance Directorates
- Center Engineering Directorates
- Center Mission Operations Directorates
- The Astronaut Office.

Additionally, we would like to thank the following individuals for organizing and supervising the interviews: David Lengyel, Dr. Fred Bickley, Maria Dee, Thomas Diegelman, Garry Lyles, John McIntyre, Cindy Offermann, and Dr. Jeevan Perera. Finally, we would like to thank Walter Hussey for answering our initial questions on the organizational structure of NASA (particularly regarding "Technical Authority"), Prof. Jeffrey Hoffman for his assistance in interview protocol development, and Margaret Stringfellow Herring for her editorial comments on draft versions of this document.

This research was supported by USRA Cooperative Agreements 05115-C1P1-03 and 05115-C1P2-01, NASA Grant NNG04GB43G, and NSF Grant SES-0527660.

EXECUTIVE SUMMARY

Introduction

The *Challenger* and *Columbia* accident reports both identified factors in the losses related to budget and schedule pressures and aspects of the safety culture that led to flawed decision-making by managers and engineers.[1,2] While it is easy to see these flawed decisions after the fact, making better decisions requires up-front access to risk-related information.

Effective risk management in the development of complex aerospace systems requires the balancing of multiple risk components including safety, cost, performance, and schedule. Safety considerations are especially critical during system development because it is very difficult to design or "inspect" safety into a system during operation. Because the consequences of improperly addressing safety during development are not as immediately visible as those of cost, schedule, and performance considerations, project managers may be tempted to satisfy the latter three goals at the expense of safety.

Research Objective

This report summarizes a MIT Complex Systems Research Laboratory (MIT CSRL) study conducted at the request of the NASA Exploration Systems Mission Directorate (ESMD) to evaluate the usefulness of systems theoretic analysis and modeling of safety risk in the development of exploration systems. In addition to fulfilling the specific needs of ESMD, this study is part of an ongoing effort by the MIT CSRL to develop and refine techniques for modeling and treating organizational safety culture as a dynamic control problem.

Approach

STAMP or Systems-Theoretic Accident Modeling and Processes is a new, more powerful model of accident causation that integrates all aspects of risk, including organizational and social aspects. STAMP can be used as a foundation for new and improved approaches to accident investigation and analysis, hazard analysis and accident prevention, risk assessment and risk management, and derivation of risk metrics and performance monitoring strategies. The methodology used in the research described in this report melds static STAMP structural models with system dynamics modeling to create a novel and powerful new approach to risk modeling and risk management.

STAMP-based system dynamics models are executable and simulation runs can identify decisions that outperform others with respect to cost, schedule, final system scope, and safety; to recognize conditions and decisions that are desirable at first yet harmful over time; and to identify variables that provide leading indicators of increasing risk. Combining the qualitative insights derived from the model about relative performance of policy options, the existence of tipping points, and leading/lagging indicators of risk or success sheds light on the "intended rationality" of decisions and their efficacy and assistance in identifying ways in which organizational and programmatic risks can be controlled.

Accomplishments

Over the course of this study, the MIT CSRL team:

[1] William P. Rogers (Chair) (1986), *Report of the Presidential Commission on the Space Shuttle Challenger Accident.* Government Accounting Office, June.

[2] Harold Gehman (Chair) (2003), *Columbia Accident Investigation Report*, Government Accounting Office, August.

Created an executable model, using input from the NASA workforce, to analyze relative effects of management strategies on schedule, cost, safety, and performance: The model takes into account the impact of decision-making at every level of the socio-technical system involved in the development of the space exploration system. In all, 44 NASA employees at NASA HQ, JSC, MSFC, and LaRC contributed to the development and validation of the model.

Developed scenarios to analyze risks identified by the Agency's workforce: In order to make the model more conceptually accessible to the NASA ESMD workforce and relevant to ESMD risk management, we asked a number of NASA employees to describe the risks they viewed as the most important to address in the development of new spacecraft systems. Inputs from the workforce were used as the basis for the development of dynamic scenarios to analyze the risks identified and create associated mitigation strategies. The scenarios address issues such as:

1) The effects of hiring constraints and workforce planning on system development and risk management capabilities: In the scenario developed to analyze this issue, we demonstrated that ESMD's eventual inheritance of the Space Shuttle Program's budget and its workforce will also lead ESMD to inherit the Space Shuttle Program's civil-servant to support-contractor ratio if it does not increase its hiring rates. This insight raises the following question:

   "Will having a low civil-servant to support-contractor ratio in the development environment of ESMD work as well as having a low ratio in the operations-oriented environment of the Space Shuttle Program?"

   With the current set of assumptions and parameters used in the model, our analysis indicates that there will be a relative increase in the ultimate safety of the operational systems developed by ESMD if it maintains a civil-servant to support-contractor ratio higher than that of the Space Shuttle Program.

2) The impact of management reserves (schedule and resources) on risk management and uncertainty mitigation: In one of the scenarios that we developed, we looked into ways in which management reserves might be used to mitigate the uncertainties of developing exploration systems. The results of the scenario indicate a strong link between the amount of reserves and both development schedule and ultimate safety of the system when it becomes operational. That is, large schedule reserves significantly decreased development time while improving safety and vice versa.

3) The effect of schedule pressure and safety priority: Schedule pressure was a common thread of discussion following both Space Shuttle accidents. Not surprisingly, it was also a frequently discussed topic in our interviews for both its positive and negative attributes. A scenario was developed to investigate the impact of schedule pressure and enforcement in exploration systems development. Our results indicated that overly aggressive schedule enforcement has surprisingly little effect on completion time (less than two percent) and cost, but has a large negative impact on safety. Inversely, analysis of our risk models showed that increasing the priority of safety activities has a large positive impact, including a reduction in cost. The cost reduction stems from reduced rework due to the high quality of safety inputs to design decisions in the early stages of development.

4) The consequence of high influence and power of the safety organization on decision-making: There is a natural tendency for cost, schedule, safety, and performance considerations to conflict in system development. Each consideration has its advocates and balancing the power in design decision-making among these stakeholders is crucial to ensure that critical considerations are not neglected in the system design. This paradox of power distribution was analyzed in one of our analysis scenarios. As expected, high influence and power of safety advocates has a large positive impact on safety while having a slightly negative impact on cost and schedule. However, our results indicate that there are ways in which even the small negative impact on schedule and cost can be dampened, for example, by allocating more resources to system integration and carefully planning and anticipating safety engineering resource requirements.

5) The assignment of respected leaders to safety engineering activities: When highly regarded people in an organization are assigned to address a certain problem, a message is sent to the rest of the workforce—either intentionally or unintentionally—that the organization's management considers the problem to be important. In one of the scenarios, we demonstrated how the assignment of respected leaders to safety engineering activities throughout system development has a large impact on the safety of the system when it becomes operational while having a minimal impact on development costs and schedule.

6) The impact of scope and requirements change on system safety: In one scenario we reaffirmed the largely accepted concept that scope and requirements changes in development negatively impact program cost, schedule, and safety. Our approach was unique, however, in that we analyzed this concept deductively (as opposed to inductively analyzing past experience) and were thus able to produce somewhat surprising results. For example, small frequent changes had almost as much of a negative impact on cost, schedule, and safety as large, infrequent changes.

Derived preliminary recommendations to mitigate and monitor program-level risks: Based on the scenario analyses**,** preliminary mitigation strategies and policy recommendations were provided to improve risk management practices at NASA ESMD. Additionally, preliminary metrics for evaluating and monitoring the health of safety related decision-making were identified.

Conclusions and Future Plans

This preliminary research study demonstrated the viability and potential power and benefits of our unique new approach to risk analysis. The model we produced and the insights developed in our preliminary analysis should serve as a starting point for future analysis and iteration of the decision rules inherent in exploration system development and for possible improvements in the ESMD organizational structure to reduce risk. However, modeling of complex systems is an iterative process that usually has no natural ending. There are almost always parts of any model that can be refined as well as parts that will eventually become obsolete as the system evolves. Thus, the end products of this study should not be viewed as the final word on the system dynamics of exploration systems development. Several collaborative opportunities between ESMD and MIT CSRL exist in further validation and enhancement of the model, evaluation of ESMD organizational design and safety culture, knowledge capture through expert interviews and modeling about complex system development (including risk mitigation, and the development of risk management tools and simulators to support management decision making and management training).

1. INTRODUCTION

The *Challenger* and *Columbia* accident reports both identified factors in the losses related to budget and schedule pressures and aspects of the safety culture that led to flawed decision-making by managers and engineers.[3,4] While it is easy to see these flawed decisions after the fact, making better decisions requires access to risk-related information and risk management tools.

As part of a USRA and NASA Exploration Systems Mission Directorate (ESMD) research grant, we created an executable risk model of ESMD based on new safety modeling techniques where safety is viewed as a dynamic control problem. Using input from the NASA workforce and a model we created of risk in ESMD, we performed a preliminary analysis of the relative impact of various ESMD management strategies on schedule, cost, safety, and performance. The analysis looked at the effects of scenarios involving workforce planning, management of schedule reserves, schedule pressure and safety priority, the influence of safety analysis on engineering and management decision-making, assignment of respected leaders to safety engineering tasks, and various levels of project scope and requirements changes. This document describes the approach used, the results of the research project, and how the model (or similar models) could be used in a program management simulator where various program management variables can be varied to identify their impact on program and project risk.

1.1 Research Objectives and Accomplishments

The research summarized in this report is part of an ongoing effort by the MIT Complex Systems Research Laboratory (CSRL) to develop and refine techniques for modeling and treating organizational safety culture[5] as a dynamic control problem. The motivation behind this effort is described in the following research hypothesis:

> *Safety culture can be modeled, analyzed, and engineered using the same logic and techniques as in physical systems. The models will be useful in designing and validating improvements to risk management and safety culture, in evaluating the potential impact of changes and policy decisions, in assessing risk, in detecting when risk is increasing to unacceptable levels, and in performing root cause analysis.*

This hypothesis is derived from a growing record of accidents in complex, socio-technical systems that suggest that the current risk mitigation techniques centered on treating safety as a technical, reliability problem rather than a socio-technical control problem are being stressed beyond their limits by the dynamic complexity of these systems.[6,7] In fact, the problems with risk mitigation in complex systems are so evident and have such potentially catastrophic implications that there is a school of thought that suggests that such systems should be abandoned because accidents in them are "normal," not so much for their frequency, but for their inevitability.[8] While we do agree with *some* of the observations of these "Normal Accident Theorists," we feel that these complex systems do have a place in our future and can even exist safely if we develop safety control systems with the same sophistication that we use to develop control systems for other attributes of system performance.

[3] William P. Rogers (Chair) (1986), *Report of the Presidential Commission on the Space Shuttle Challenger Accident.* Government Accounting Office, June.

[4] Harold Gehman (Chair) (2003), *Columbia Accident Investigation Report*, Government Accounting Office, August.

[5] Refer to Appendix B of this report for a definition of safety culture as it relates to NASA.

[6] Nancy G. Leveson (1995), *Safeware: System Safety and Computer,* Addison-Wesley Publishing Co.

[7] Nancy G. Leveson (2002), *System Safety Engineering: Back to the Future.* Cambridge, MA. Available online at <http://sunnyday.mit.edu/book2.html>.

[8] Charles Perrow (1999), *Normal Accidents: Living with High-Risk Technologies.* 1999 Edition. Princeton Books.

The first application of MIT CSRL safety culture evaluation techniques on NASA's safety culture began shortly after the *Columbia* Accident when we formed an interdisciplinary working group to create a dynamic model of this culture.[9] Initially, we used our findings in the modeling effort in a two-phase competition for a two-year USRA CPMR research grant. As part of the competition, which ultimately led to MIT CSRL being awarded the grant, we made presentations on a number of simulation scenarios analyzed with the model, including one that evaluated the efficacy of an Independent Technical Authority (ITA) function at NASA.[10] After reviewing our presentation, the NASA Office of the Chief Engineer (OCE) asked MIT CSRL to perform a risk analysis of NASA's planned implementation of ITA. The goal of this study, conducted in the summer of 2005, was to identify and evaluate the risks associated with this new organizational structure. The results of this study, along with each of the two theoretical foundations upon which the analysis was based—STAMP and system dynamics—will be described in the following sections. In the spring of 2006, MIT CSRL was asked by NASA ESMD to demonstrate the application of this new risk analysis and management approach to ESMD. The following Statement of Work (SOW) was provided by ESMD:

> *MIT will develop an ESMD Systems Dynamics Model based on previous work with the NASA Office of the Chief Engineer model for Independent Technical Authority. This model will consider the work done by the CAIB regarding influences and effects on Systems Risks and Safety.*
>
> *Organizational entities in the system model will include Congress, regulatory agencies, industry associations, unions, courts, NASA HQ, ESMD, SOMD, Office of Safety and Mission Assurance, Constellation Program, Shuttle and Station Programs, Johnson/Marshall/Kennedy Space Centers, CEV, CLV, RLEP, and Advanced Technology. The process models must contain: required relationships among process variables, current state and the ways the process can change state. Process models shall be iterated during development with NASA personnel to ensure their accuracy. A formal report and presentation shall be developed for the Associate Administrator for ESMD.*
>
> *Deliverable C1: A final report and presentation will be developed for the Associate Administrator for ESMD.*
>
> *Deliverable C2: The ESMD Systems Dynamic Software Model.*

Inherent in this SOW are three challenges:

- **To validate the applicability of new system safety approaches for modeling, analyzing, and engineering safety culture:** Models of the behavior of a specific organization must be derived from a deep knowledge of general organizational theory and the structure of the specific organization at all levels. This involves the engagement of multiple individuals from the various levels of the organization in the model validation process.
- **To create a system dynamics model of safety for NASA ESMD, an organization involved primarily in human spaceflight system development:** The formulation of a system dynamics model of the development process of complex systems is a challenge in

[9] This group, which contains faculty and research staff from the MIT Schools of Engineering, Sloan School of Management, and Engineering Systems Division, still meets regularly to investigate safety culture in NASA and a variety of other organizations.

[10] As part of the Space Shuttle return-to-flight effort following the *Columbia* Accident, the CAIB recommended that NASA prepare and implement Independent Technical Authority.

and of itself. In this case, the difficulty of the task at hand is amplified by the fact that NASA has not developed human-rated launch and landing systems since the 1970s and thus there is little up-to-date data and documentation on human spaceflight system development.

- **To demonstrate the usefulness of our model for risk management in ESMD:** Because the model is intended for use by NASA ESMD in risk management, it will be underutilized if: 1) it is only possible for MIT CSRL personnel to run the model and interpret its results and 2) the model's concepts are too abstract to be applied in ESMD risk management.

By the end of study, the MIT CSRL team accomplished the following:

- **Creation of an executable model, using input from the NASA workforce, to analyze relative effects of management strategies on schedule, cost, safety, and performance:** The system dynamics model accounts for the effects of actions from the Presidential/Congressional level to the engineering level and can be run and subjected to sensitivity analysis on a standard laptop or desktop personal computer. Forty-four NASA employees contributed to the development and validation of the model.
- **Development of scenarios to analyze risks identified by the Agency's workforce:** In order to make the model more conceptually accessible to the NASA ESMD workforce and relevant to ESMD risk management, we asked a number of NASA employees to describe the risks they viewed as the most important to address in the development of new spacecraft systems. We then used their responses to build features into the model that would allow the analysis of these specific issues.
- **Derivation of preliminary recommendations to mitigate and monitor program-level risks:** Preliminary analysis was performed on the effects of hiring constraints, management reserves, independence, requirements changes, etc. on safety-related decision-making. In this analysis, organizational policy options relating to these items were identified and compared. Additionally, metrics for evaluating the health of safety-related decision-making were identified.

Throughout this report, the details of these accomplishments will be summarized along with the process through which they were achieved.

1.2 Systems-Theoretic Accident Model and Processes (STAMP)

STAMP or Systems-Theoretic Accident Modeling and Processes is a new way of thinking about accidents that integrates all aspects of risk, including organizational and social aspects. STAMP can be used as a foundation for new and improved approaches to accident investigation and analysis, hazard analysis and accident prevention, risk assessment and risk management, and derivation of risk metrics and performance monitoring strategies. One unique aspect of this approach to risk management is the emphasis on the use of visualization and building shared mental models of complex system behavior among those responsible for managing risk. The techniques integral to STAMP can assist in achieving more effective organizational decision-making.

STAMP is constructed from three fundamental concepts: constraints, hierarchical levels of control, and process models. These concepts, in turn, give rise to a classification of control flaws that can lead to accidents. Each of these is described only briefly here; for more information see Leveson.[11]

[11] Nancy G. Leveson (2004), "A New Accident Model for Engineering Safer Systems", *Safety Science*, Vol. 42, No. 4, April 2004. pp. 237-270.

The most basic component of STAMP is not an event, but a constraint. In systems theory and control theory, systems are viewed as hierarchical structures where each level imposes constraints on the activity of the level below it—that is, constraints or a lack of constraints at a higher level allow or control lower-level behavior.

Safety-related constraints specify those relationships among system variables that constitute the non-hazardous or safe system states—for example, the power must never be on when the access to the high-voltage power source is open, the descent engines on the lander must remain on until the spacecraft reaches the planet surface, and two aircraft must never violate minimum separation requirements.

Instead of viewing accidents as the result of an initiating (root cause) event in a chain of events leading to a loss, accidents are viewed as resulting from interactions among components that violate the system safety constraints. The control processes that enforce these constraints must limit system behavior to the safe changes and adaptations implied by the constraints. Preventing accidents requires the design of a control structure encompassing the entire socio-technical system that will enforce the necessary constraints on development and operations. Figure 1 shows a generic hierarchical safety control structure. Accidents result from inadequate enforcement of constraints on behavior (e.g. the physical system, engineering design, management, and regulatory behavior) at each level of the socio-technical system. Inadequate control may result from missing safety constraints, inadequately communicated constraints, or from constraints that are not enforced correctly at a lower level. Feedback during operations is critical here. For example, the safety analysis process that generates constraints always involves some basic assumptions about the operating environment of the process. When the environment changes such that those assumptions are no longer true, the controls in place may become inadequate.

The model in Figure 1 has two basic hierarchical control structures—one for system development (on the left) and one for system operation (on the right)—with interactions between them. A spacecraft manufacturer, for example, might only have system development under its immediate control, but safety involves both development and operational use of the spacecraft, and neither can be accomplished successfully in isolation: safety must be designed into the physical system, and safety during operation depends partly on the original system design and partly on effective control over operations. Manufacturers must communicate to their customers the assumptions about the operational environment upon which their safety analysis and design was based, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations.

Between the hierarchical levels of each control structure, effective communication channels are needed, both a downward *reference* channel providing the information necessary to impose constraints on the level below and a *measuring* channel to provide feedback about how effectively the constraints were enforced. For example, company management in the development process structure may provide a safety policy, standards, and resources to project management and in return receive status reports, risk assessment, and incident reports as feedback about the status of the project with respect to the safety constraints.

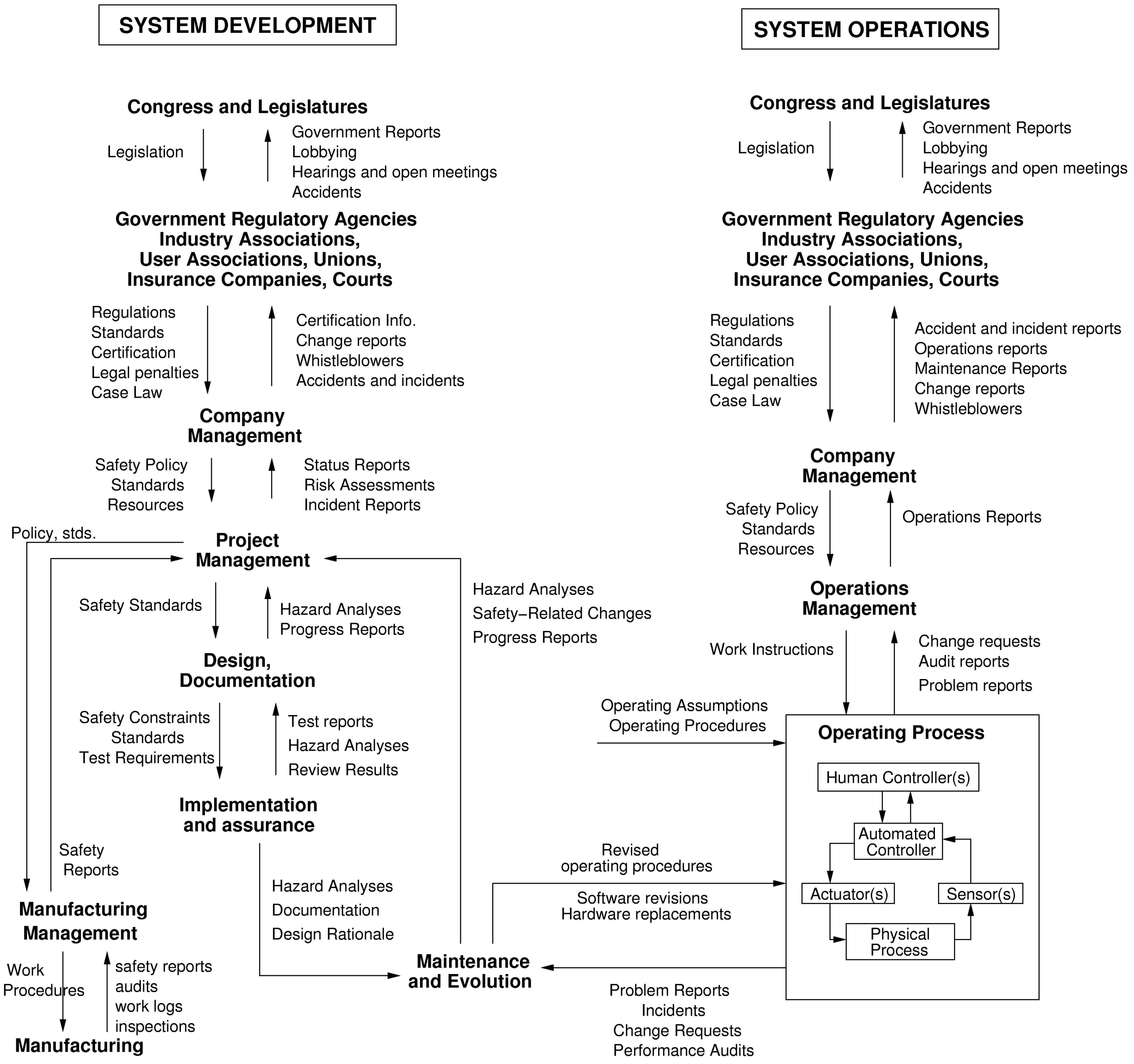


Figure 1. The general form of a model of socio-technical safety control.

The safety control structure often changes over time, which accounts for the observation that accidents in complex systems frequently involve a migration of the system toward a state where a small deviation (in the physical system or in human behavior) can lead to a catastrophe. The foundation for an accident is often laid years before it occurs. One event may trigger the loss, but if that event had not happened, another one would have. As an example, Figure 3 shows the changes over time that led to a water contamination accident in Canada where 2,400 people became ill and 7 died (most of them children). The reasons why this accident occurred would take too many pages to explain and only a small part of the overall STAMP model is shown in Figure 3. Each component of the water quality control structure played a role in the accident. The upper portion of the figure shows the control structure for water quality in Ontario, Canada as designed. The lower portion of the figure shows the control structure as it existed at the time of the accident. One of the important changes that contributed to the accident was the elimination of a government water-testing laboratory. The private companies that were substituted were not required to report instances of bacterial contamination to the appropriate government ministries. Essentially, the elimination of the feedback loops made it impossible for the government agencies and public utility managers to perform their oversight duties effectively. Note that the goal here is not to identify individuals to blame for the accident but to understand why they made the mistakes they made (none were evil or wanted children to die) and what changes are needed in the culture and water quality control structure to reduce risk in the future.

In this accident, and in most accidents, degradation in the safety margin occurred over time and without any particular single decision to do so but simply as a series of decisions that individually seemed safe but together resulted in the gradual movement of the water quality control system structure toward a situation where any slight error would lead to a major accident. Preventing accidents requires ensuring that controls do not degrade despite the inevitable changes that occur over time or that such degradation is detected and corrected before a loss occurs.

Figure 3 shows static models of the safety control structure, but models are also needed to understand *why* the structure changed over time in order to build in protection against unsafe changes (see Section 1.3). For this goal, we use system dynamics models. It is often the case that the degradation of the control structure involves *asynchronous evolution* where one part of a system changes without the necessary changes in other related parts. Changes to subsystems may be carefully designed, but consideration of their effects on other parts of the system, including the control aspects, may be neglected or inadequate. Asynchronous evolution may also occur when one part of a properly designed system deteriorates. The Ariane 5 trajectory changed from that of the Ariane 4, but the inertial reference system software did not. One factor in the loss of contact with the SOHO (Solar Heliospheric Observatory) spacecraft in 1998 was the failure to communicate to operators that a functional change had been made in a procedure to perform a gyroscope spin-down.

Besides constraints and hierarchical levels of control, a third basic concept in STAMP is that of process models. *Any* controller—human or automated—must contain a model of the system being controlled. For humans, this model is generally referred to as their *mental model* of the process being controlled, see Figure 2 below.

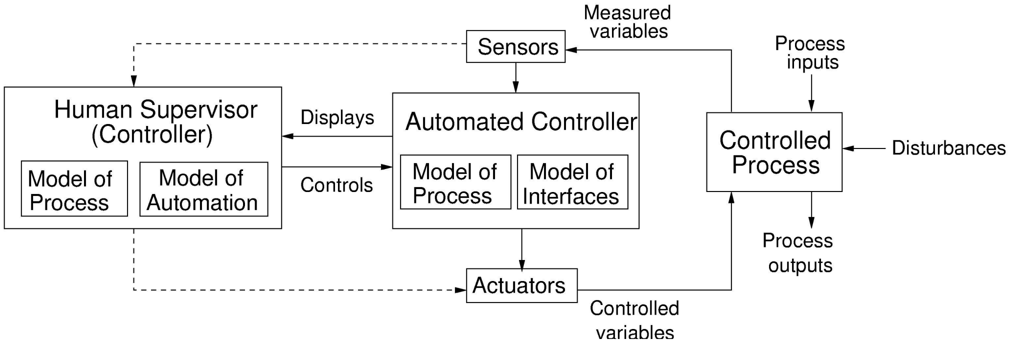


Figure 2. A control structure involving human supervision of an automated controller that can directly issue commands.

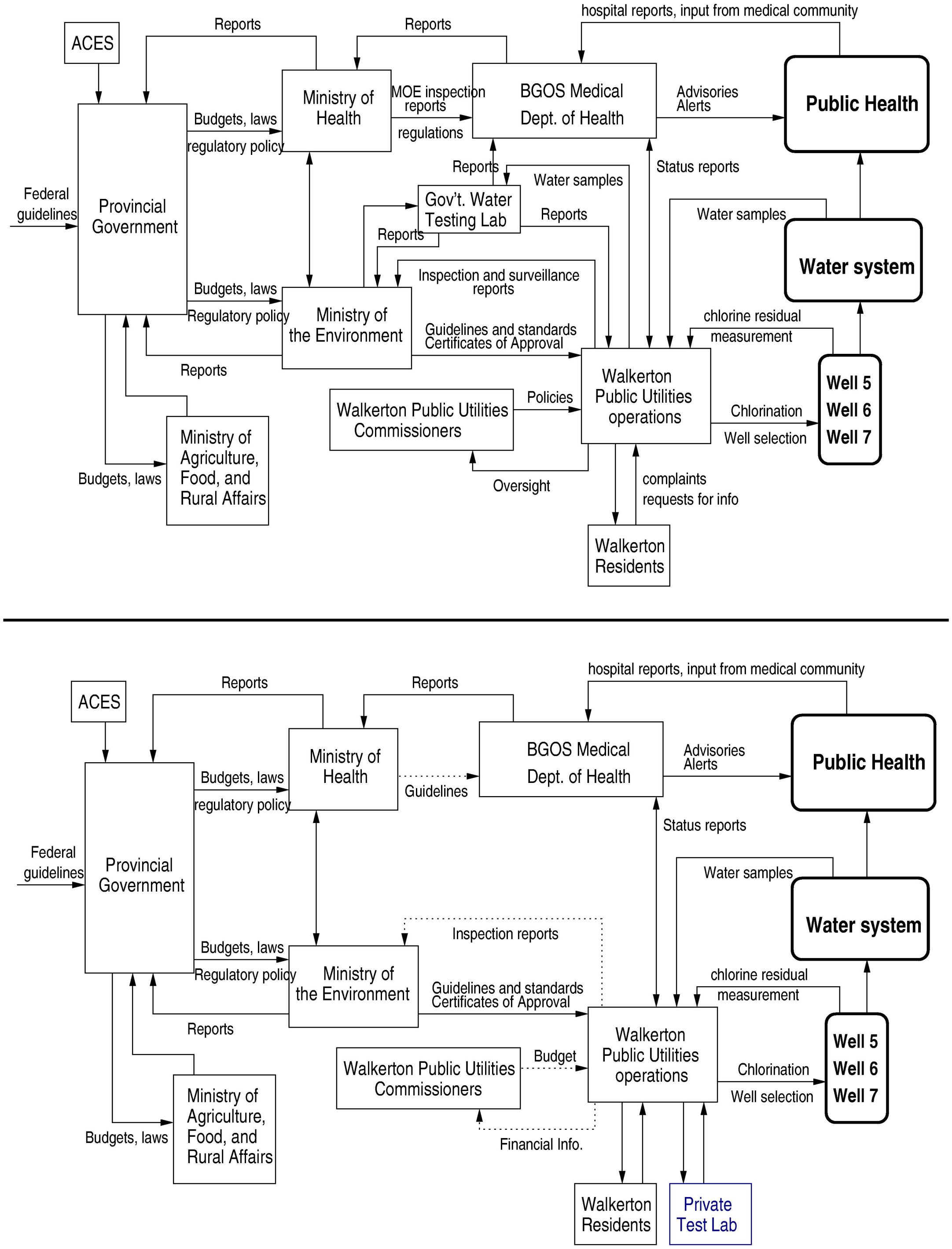


Figure 3. The safety control structure in the Walkerton Water Contamination Accident.[12]

[12] The structure is drawn in the form commonly used for control loops. Lines going into the left of a box are control lines. Lines from or to the top or bottom of a box represent information, feedback, or a physical flow. Rectangles with sharp corners are controllers while rectangles with rounded corners represent physical processes. The dotted lines on the bottom half of the figure represent changes from the original structure.

For effective control, the process models must contain the following: (1) the current state of the system being controlled, (2) the required relationship between system variables, and (3) the ways the process can change state. Accidents, particularly system accidents, frequently result from inconsistencies between the model of the process used by the controllers and the actual process state: for example, the lander software thinks the lander has reached the surface and shuts down the descent engine; the Minister of Health has received no reports about water quality problems and believes the state of water quality in the town is better than it actually is; or a mission manager believes that foam shedding is a maintenance or turnaround issue only. Part of our modeling efforts involve creating the process models, examining the ways that they can become inconsistent with the actual state (e.g., missing or incorrect feedback), and determining what feedback loops are necessary to maintain the safety constraints.

When there are multiple controllers and decision makers, system accidents may also involve inadequate control actions and unexpected side effects of decisions or actions, again often the result of inconsistent process models. For example, two controllers may both think the other is making the required control action (both Canadian government ministries responsible for the water supply and public health thought the other had followed up on the previous poor water quality reports), or they make control actions that conflict with each other. Communication plays an important role here: accidents are most likely in *boundary* or *overlap* areas where two or more controllers control the same process.[13]

A STAMP modeling and analysis effort involves the creation of a model of the organizational safety structure that includes the static safety control structure and safety constraints that each component is responsible for maintaining, process models representing the view of the process by those controlling it, and a model of the dynamics and pressures that can lead to degradation of this structure over time. These models and analysis procedures can be used to investigate accidents and incidents to determine the role played by the different components of the safety control structure, to learn how to prevent related accidents in the future, to proactively perform hazard analysis by designing to reduce risk throughout the life of the system, and to support a continuous risk management program where risk is monitored and controlled.

1.3 System Dynamics

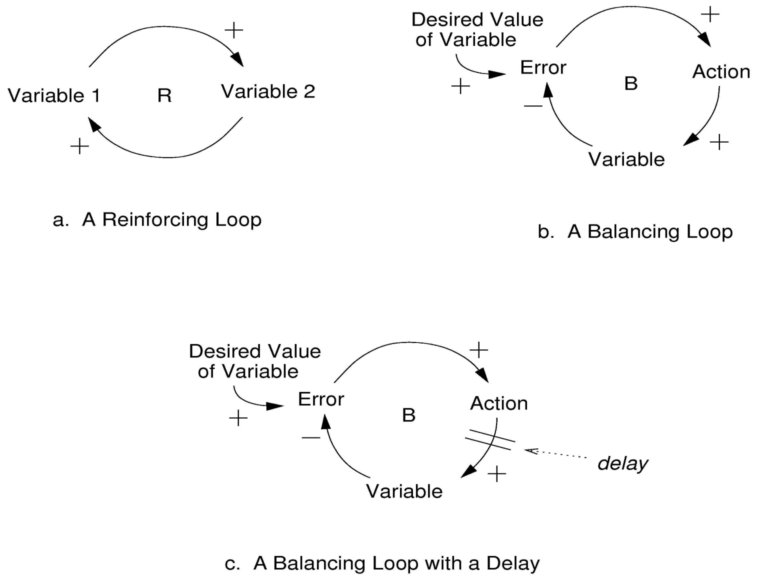
> *"While it's hard to define what system dynamics is, I don't have any trouble answering why it is valuable. As the world changes ever faster, thoughtful leaders increasingly recognize that we are not only failing to solve the persistent problems we face, but are in fact causing them. All too often, well-intentioned efforts to solve pressing problems create unanticipated 'side effects.' Our decisions provoke reactions we did not foresee. Today's solutions become tomorrow's problems. The result is policy resistance, the tendency for interventions to be defeated by the response of the system to the intervention itself. From California's failed electricity reforms, to road building programs that create suburban sprawl and actually increase traffic congestion, to pathogens that evolve resistance to antibiotics, our best efforts to solve problems often make them worse.*
>
> *At the root of this phenomenon lies the narrow, event-oriented, reductionist worldview most people live by. We have been trained to see the world as a series of events, to view our situation as the result of forces outside ourselves, forces largely unpredictable and*

[13] Jacques Leplat (1987), Occupational Accident Research and Systems Approach, in Jens Rasmussen, Keith Duncan, and Jacques Leplat (editors), *New Technology and Human Error*, pp. 181-191, John Wiley & Sons, New York.

> *uncontrollable…System dynamics helps us expand the boundaries of our mental models so that we become aware of and take responsibility for the feedbacks created by our decisions."* –John Sterman[14]

The field of system dynamics, created at MIT in the 1950s by computer pioneer Jay Forrester,[15] is designed to help decision-makers learn about the structure and dynamics of complex systems, to design high leverage policies for sustained improvement, and to catalyze successful implementation and change. System dynamics provides a framework for dealing with dynamic complexity, where cause and effect are not obviously related. It is grounded in the theory of non-linear dynamics and feedback control, but also draws on cognitive and social psychology, organization theory, economics, and other social sciences.[16]

System behavior in system dynamics is modeled by using feedback (causal) loops, stocks and flows (levels and rates), and the non-linearities created by interactions among system components. In this view of the world, behavior over time (the dynamics of the system) can be explained by the interaction of positive and negative feedback loops.[17] The models are constructed from three basic building blocks: positive feedback or reinforcing loops, negative feedback or balancing loops, and delays. Positive loops (called reinforcing loops) are self-reinforcing while negative loops (called balancing loops) tend to counteract change. Delays introduce potential instability into the system.



a. A Reinforcing Loop

b. A Balancing Loop

c. A Balancing Loop with a Delay

Figure 4. The three basic components of system dynamics models.

Figure 4a shows a *reinforcing loop*, which is a structure that feeds on itself to produce growth or decline. Reinforcing loops correspond to positive feedback loops in control theory. An increase in variable 1 leads to an increase in variable 2 (as indicated by the "+" sign) that leads to an additional

[14] John Sterman (2002), "All models are wrong: reflections on becoming a systems scientist," *System Dynamics Review*, Vol. 18, No. 4, Winter 2002. pp. 501-531.

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

[16] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill.

[17] Peter M. Senge (1990), *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday Currency, New York.

increase in variable 1 and so on. The “+” does not mean the values necessarily increase, only that variable 1 and variable 2 will change in the same direction (polarity). If variable 1 decreases, then variable 2 will decrease. In the absence of external influences, both variable 1 and variable 2 will clearly grow or decline exponentially. Reinforcing loops generate growth, amplify deviations, and reinforce change.

A *balancing loop* (Figure 4b) is a structure that changes the current value of a system variable or a desired or reference variable through some action. It corresponds to a negative feedback loop in control theory. A “-“ indicates that the values of the variables change in opposite directions. The difference between the current value and the desired value is perceived as an error. An action proportional to the error is taken to decrease the error so that, over time, the current value approaches the desired value.

The third basic element is a delay, which is used to model the time that elapses between cause and effect. A delay is indicated by a double line, as shown in Figure 4c. Delays make it difficult to link cause and effect (dynamic complexity) and may result in unstable system behavior. For example, in steering a ship there is a delay between a change in the rudder position and a corresponding course change, often leading to over-correction and instability.

The simple “News Sharing” model in Figure 5 is helpful in understanding the stock and flow syntax in system dynamics models. The model shows the flow of information through a population over time. The total population is fixed and includes 100 people. Initially, only one person knows the news, the other 99 people do not know it. Accordingly, there are two *stocks* in the model: *People who know* and *People who don’t know*. The initial value for the *People who know* stock is 1 and that for the *People who don’t know* stock is 99. Once a person learns the news, he or she moves from the left-hand stock to the right-hand stock through the double arrow flow called the *rate of sharing the news*. The *rate of sharing the news* at any point in time depends on the number of *Contacts between people who know and people who don’t*, which is a function of the value of the two stocks at that time. This function uses a differential equation (i.e. the rate of change of variable V or dV/dt, at time t depends on the value of V(t)). The results for each stock and variable as a function of time are obtained through numerical integration. The formulas used in the News Sharing model are:

$$\textit{People who know(t)} = \int_0^t \textit{Rate of sharing the news}$$

$$\textit{People who know(}\,0\,\textit{)} = 1$$

$$\textit{People who don't know(}\,0\,\textit{)} = 99$$

$$\textit{People who don't know(t)} = \int_0^t -\textit{Rate of sharing the news}$$

$$\textit{Total People} \;=\; \textit{People who don't know(t)} \;+\; \textit{People who know(t)}$$

$$\textit{Rate of sharing the news(t)} \;=\; \textit{Contacts between people who know and people who don't(t)}$$

$$\textit{Contacts between people who know and people who don't}(t) = \frac{\textit{People who don't know}(t) \times \textit{People who know}(t)}{\textit{Total People}}$$

The graph in Figure 5 shows the numerical simulation output for the number of *People who know*, the number of *People who don’t know*, and the *Rate of sharing the news* as a function of time.

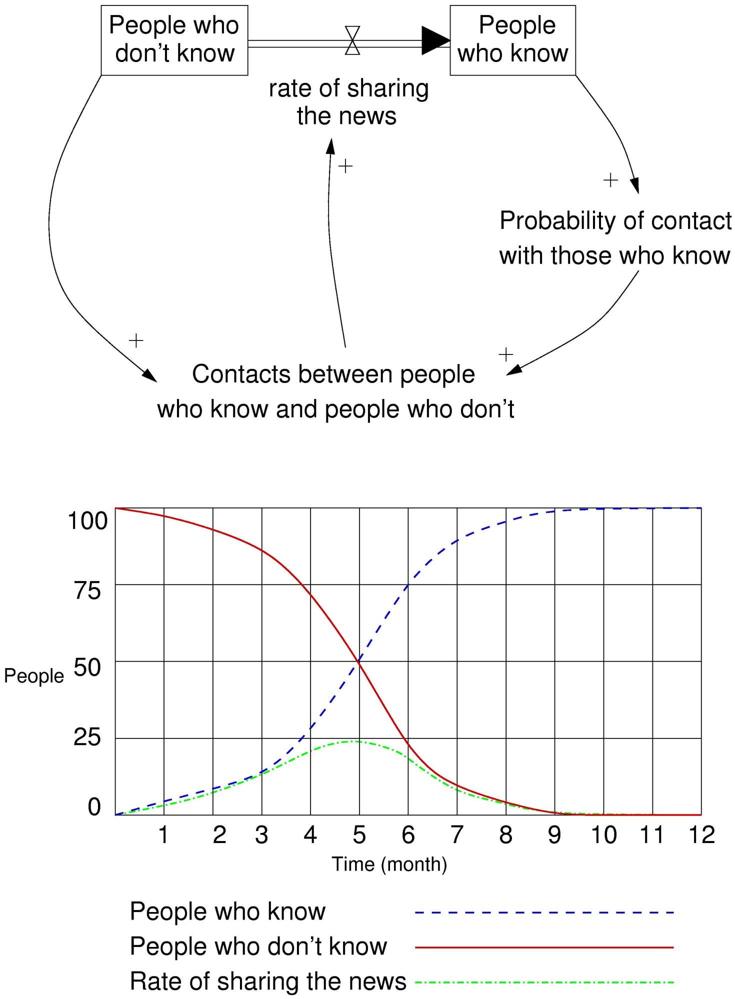


Figure 5. An example of a system dynamics model and its output.

System dynamics is particularly relevant for complex systems. System dynamics makes it possible, for example, to understand and predict instances of policy resistance or the tendency for well-intentioned interventions to be defeated by the response of the system to the intervention itself. Figure 6 shows a high-level abstraction of a system dynamics model of the *Columbia* Accident developed by the MIT CSRL.[18] The actual model contains many more variables and relationships

[18] Due to the complexity of system dynamics models, it is sometimes necessary to abstract the models themselves for the purpose of presentation. Section 3 provides a taxonomy for abstractions of system dynamics models. Under this taxonomy, the abstraction in Figure 6 is a Level 1 abstraction of a system dynamics model created by MIT CSRL.

than are shown in the figure; however, the causal structure presented here is illustrative of the high-level dynamics at work in the model and is useful in understanding this type of model. There are three main variables in the causal structure: safety, complacency, and success in meeting launch rate expectations.

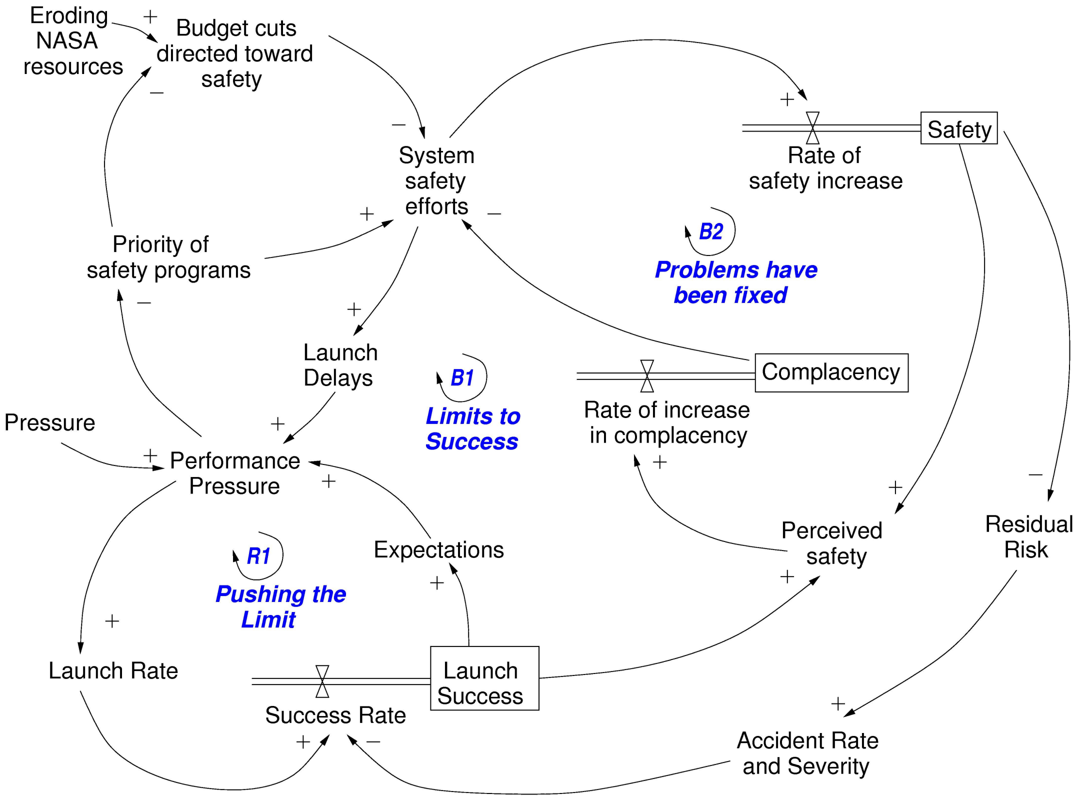


Figure 6. Simplified model of the dynamics behind the Space Shuttle *Columbia* loss.

The control loop in the lower left corner of Figure 6, labeled R1 or *Pushing the Limit*, shows how performance pressures increased as external expectations grew, which led to increased launch rates and thus success in meeting the launch rate expectations, which in turn led to increased expectations and further increases in performance pressures. This, of course, is an unstable system and cannot be maintained indefinitely—note the larger control loop, B1, in which this loop is embedded, is labeled *Limits to Success*. The upper left loop represents part of the safety program loop. The external influences of budget cuts and increasing performance pressures that reduced the priority of safety procedures led to a decrease in system safety efforts. The combination of this decrease along with loop B2 in which fixing problems increased complacency, which also contributed to reduction of system safety efforts, eventually led to a situation of (unrecognized) high risk. There is one other important factor shown in the model: increasing system safety efforts led to launch delays, another reason for reduction in priority of the safety efforts in the face of increasing launch pressures.

The diagram does not show the delays in the system. While reduction in safety efforts and lower prioritization of safety concerns may lead to accidents, accidents usually do not occur for a while so false confidence is created that the reductions are having no impact on safety and therefore pressures increase to reduce the efforts and priority even further as the external performance pressures mount.

The models can be used to devise and validate fixes for the problems and to design systems with lower risk. For example, one way to eliminate the instability of the model in Figure 6 is to anchor the safety efforts by, perhaps, externally enforcing standards in order to prevent schedule and budget pressures from leading to reductions in the safety program. Other solutions are also possible. Alternatives can be evaluated for their potential effects and impact on risk using a more complete system dynamics model, as described in this report.

1.4 Previous System Dynamics and STAMP Modeling Effort on the NASA Independent Technical Authority

As mentioned above, MIT CSRL was asked, following the completion of a two-phase USRA grant competition, to perform a study of NASA's planned implementation of ITA. We followed a traditional systems engineering and system safety engineering approach for this study, but adapted it to the task at hand (organizational risk analysis) as depicted in the following diagram:

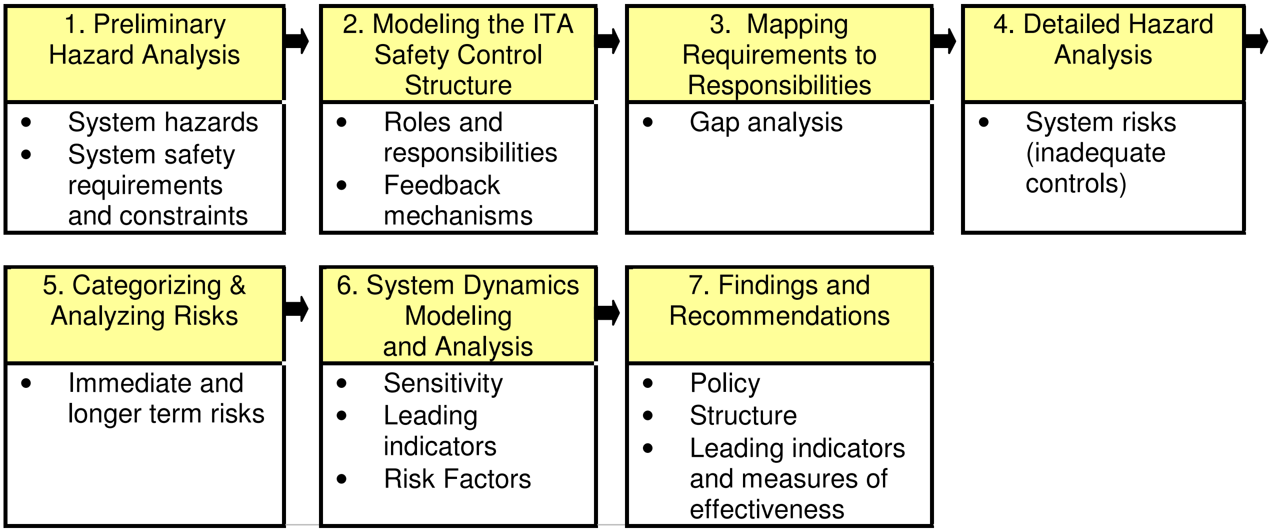

1. Preliminary Hazard Analysis
• System hazards
• System safety requirements and constraints
2. Modeling the ITA Safety Control Structure
• Roles and responsibilities
• Feedback mechanisms
3. Mapping Requirements to Responsibilities
• Gap analysis
4. Detailed Hazard Analysis
• System risks (inadequate controls)
5. Categorizing & Analyzing Risks
• Immediate and longer term risks
6. System Dynamics Modeling and Analysis
• Sensitivity
• Leading indicators
• Risk Factors
7. Findings and Recommendations
• Policy
• Structure
• Leading indicators and measures of effectiveness

Figure 7. The hazard analysis process used in the study of the NASA ITA.

Step 1: Preliminary Hazard Analysis

The first step in our STAMP-based risk analysis was a preliminary hazard analysis to identify the high-level hazard(s) ITA was designed to control and the general requirements and constraints necessary to eliminate the hazard(s):

System Hazard: ***Poor engineering and management decision-making leading to an accident (loss)***

System Safety Requirements and Constraints

1. ***Safety considerations must be first and foremost in technical decision-making.***
   a. State-of-the art safety standards and requirements for NASA missions must be established, implemented, enforced, and maintained that protect the astronauts, the workforce, and the public.
   b. Safety-related technical decision-making must be independent from programmatic considerations, including cost and schedule.

c. Safety-related decision-making must be based on correct, complete, and up-to-date information.
d. Overall (final) decision-making must include transparent and explicit consideration of both safety and programmatic concerns.
e. The Agency must provide for effective assessment and improvement in safety-related decision-making.

2. ***Safety-related technical decision-making must be done by eminently qualified experts, with broad participation of the full workforce.***
   a. Technical decision-making must be credible (executed using credible personnel, technical requirements, and decision-making tools).
   b. Technical decision-making must be clear and unambiguous with respect to authority, responsibility, and accountability.
   c. All safety-related technical decisions, before being implemented by the Program, must have the approval of the technical decision-maker assigned responsibility for that class of decisions.
   d. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making.

3. ***Safety analyses must be available and used starting in the early acquisition, requirements development, and design processes and continuing through the system lifecycle.***
   a. High-quality system hazard analyses must be created.
   b. Personnel must have the capability to produce high-quality safety analyses.
   c. Engineers and managers must be trained to use the results of hazard analyses in their decision-making.
   d. Adequate resources must be applied to the hazard analysis process.
   e. Hazard analysis results must be communicated in a timely manner to those who need them. A communication structure must be established that includes contractors and allows communication downward, upward, and sideways (e.g., among those building subsystems).
   f. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves and test experience is acquired.
   g. During operations, hazard logs must be maintained and used as experience is acquired. All in-flight anomalies must be evaluated for their potential to contribute to hazards.

4. ***The Agency must provide avenues for the full expression of technical conscience (for safety-related technical concerns) and provide a process for full and adequate resolution of technical conflicts as well as conflicts between programmatic and technical concerns.***
   a. Communication channels, resolution processes, and adjudication procedures must be created to handle expressions of technical conscience.
   b. Appeals channels must be established to surface complaints and concerns about aspects of the safety-related decision making and technical conscience structures that are not functioning appropriately.

Step 2: Modeling the ITA-Augmented Safety Control Structure

The next step was to create a model of the safety control structure in the NASA manned space program, augmented with the ITA function as designed. This model includes the roles and responsibilities of each organizational component with respect to safety, inputs and outputs, potential inadequate control actions, and feedback requirements. For most components, we also included the environmental and behavior-shaping factors (context), mental model requirements, and available controls. As an example, according to the ITA implementation plan[19], one responsibility of the System Technical Warrant Holder is:

1. Establish and maintain technical policy, technical standards, requirements, and processes for a particular system or systems.
   a. STWH shall ensure the program identifies and imposes appropriate technical requirements at program/project formation to ensure safe and reliable operations.
   b. STWH shall ensure inclusion of the consideration of risk, failure, and hazards in technical requirements.
   c. STWH shall approve the set of technical requirements and any changes to them.
   d. STWH shall approve verification plans for the system(s).

Step 3: Mapping Requirements to Responsibilities

We then traced each of the above system safety requirements and constraints to those components responsible for their implementation and enforcement. In this process, we identified some omissions in the organizational design and places where overlapping control responsibilities could lead to conflicts or require careful coordination and communication and we recommended additions and changes.[20]

Step 4: Detailed Hazard Analysis using STPA

Next we performed a hazard analysis on the safety control structure, using a new hazard analysis technique (STPA) based on STAMP. STPA works on both the technical (physical) and the organizational (social) aspects of systems. There are four general types of risks in the ITA concept:

1. Unsafe decisions are made by or approved by the ITA,
2. Safe decisions are disallowed (i.e., overly conservative decision-making that undermines the goals of NASA and long-term support for the ITA),
3. Decision-making takes too long, minimizing impact and also reducing support for the ITA,
4. The ITA makes good decisions, but they do not have adequate impact on system design, construction, and operation.

The hazard analysis applied each of these types of risk to the NASA organizational components and functions involved in safety-related decision-making and identified the risks (inadequate control) associated with each. As an example, consider the Chief Engineer's responsibility under the ITA structure to develop, monitor, and maintain technical standards and policy. Using the general risks above and instantiating them for this particular responsibility leads to the following programmatic/organizational risks:

1. General technical and safety standards and requirements are not created.
2. Inadequate standards and requirements are created.
3. Standards degrade as they are changed over time due to external pressures to weaken them. The process for approving changes is flawed.
4. Standards are not changed or updated over time as the environment changes.

[19] NASA Office of the Chief Engineer (2005), *Technical Authority Implementation Guidance: Review #1*, Internal Document.

[20] One caveat is in order when reviewing the results of our ITA study in the summer of 2005: changes are occurring so rapidly at NASA that our models, although based on the ITA implementation plan of March 2005, require updating to match the current structure.

Step 5: Categorizing and Analyzing Risks

The resulting list of risks was quite long (250 risks) and most appeared to be important and not easily dismissed. To reduce the list to one that could feasibly be assessed, we categorized each risk as either an immediate and substantial concern, a longer-term concern, or capable of being handled through standard processes and not needing a special assessment.

Step 6: System Dynamics Modeling and Analysis

The next step was to take the NASA Space Shuttle program system dynamics model developed for Phase 1 of the USRA grant competition (September 2004 to February 2005) and alter it to reflect the addition of an ITA function. The original model was constructed using both Leveson's personal long-term association with NASA as well as informal interviews with current and former employees, books on NASA's safety culture (such as McCurdy[21]), books on the *Challenger* and *Columbia* accidents, NASA mishap reports (CAIB[22], Mars Polar Lander[23], Mars Climate Orbiter[24], WIRE[25], SOHO[26], Huygens[27], etc.), other NASA reports on the manned space program (SIAT[28] and others) as well as many of the better researched magazine and newspaper articles. The additions for ITA reflect information we obtained from the ITA Implementation Plan and our personal experiences at NASA.

Analysis of ITA Function Behavior Modes:

Using this model, we performed a 200-run Monte-Carlo sensitivity analysis on the parameters we used to model the ITA function in order to identify behavior modes of this function. In this analysis, we randomly varied the exogenous variables (i.e. those parameters that are input into model) for the ITA function by ±30% of the baseline values and injected a discrete safety incident/accident near the end of the simulations. Figure 8 shows the values of the *Indicator of Effectiveness and Credibility of ITA*—a multi-attribute utility function for the effectiveness and credibility of the ITA function—throughout the 200 individual simulation runs.

The initial sensitivity analysis shows that at least two qualitatively different system behavior modes can occur. The first behavior mode (Behavior Mode 1, Figure 8) is representative of a successful ITA program implementation where risk is adequately mitigated for a relatively long period of time (Behavior Mode 1 in Figure 8). More than 75% of the runs fall in that category. The second behavior mode (Behavior Mode 2 in Figure 8) is representative of a rapid rise and then collapse in ITA effectiveness associated with an unsuccessful ITA program implementation. In this mode, the *Level of Risk* increases rapidly, resulting in frequent hazardous events (serious incidents) and accidents (Behavior Mode 2 in Figure 9).

Behavior Mode 1 (i.e. the successful implementation of an ITA function) includes a short-term initial transient where all runs quickly reach the maximum effectiveness and credibility of the ITA. This behavior is representative of an initial excitement phase, where the ITA is implemented and shows great promise to reduce the level of risk. After a period of very high success, the effectiveness and credibility of the ITA slowly starts to decline. Looking at the model helps to explain these results, i.e., the decline is mainly due to the effects of complacency: the quality of

[21] Howard McCurdy (1994), *Inside NASA: High Technology and Organizational Change in the U.S. Space Program*, Johns Hopkins University Press.

[22] Harold Gehman (Chair) (2003), Columbia Accident Investigation Report, August.

[23] Tom Young (Chair) (2000), Mars Program Independent Investigation Board Report, NASA, 14 March 2000

[24] A. Stephenson (Chair) (1999), Mars Climate Orbiter Mishap Investigation Board Report, NASA 10 Nov. 1999.

[25] D.R Branscome (Chair) (1999), WIRE Mishap Investigation Board Report, NASA, 8 June 1999.

[26] NASA/ESA Investigation Board (1998), SOHO Mission Interruption, NASA, 31 August 1998.

[27] D.C.R. Link (2000), Report of the Huygens Communications System Inquiry Board, NASA, December 2000.

[28] Harry McDonald (2000), Shuttle Independent Assessment Team (SIAT) Report, February 2000.

safety analyses starts to erode as the program is highly successful and safety is increasingly seen as a solved problem. When this decline occurs, resources are reallocated to more urgent performance-related matters and safety efforts start to suffer.

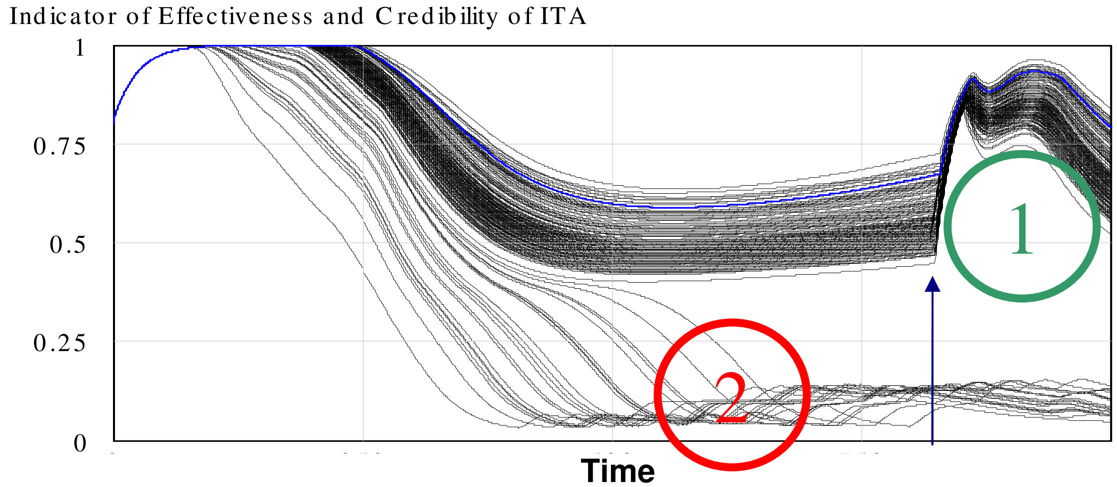


Figure 8. The effectiveness and credibility of the ITA function in a Monte-Carlo sensitivity analysis of ITA parameters.

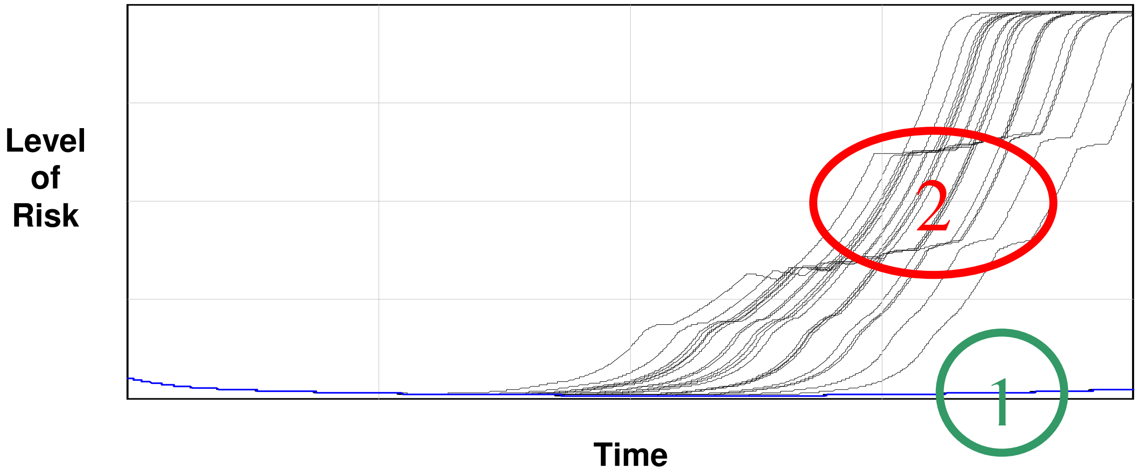


Figure 9. The level of risk in a Monte-Carlo sensitivity analysis of ITA parameters.

In Behavior Mode 1, the effectiveness and credibility of the ITA declines and then stabilizes until the injected incident/accident occurs. This incident/accident creates a discontinuous rise in the Agency's perception of safety as problem and therefore, it looks to ITA for solutions (see Figure 8). Overall, this behavior mode is characterized by an extended period of nearly steady-state equilibrium where risk remains at very low levels (see Figure 9).

In the second behavior mode (Behavior Mode 2 in Figure 8), the effectiveness and credibility of the ITA increases in the initial transient, then quickly starts to decline to equilibrium at a low value.

In examining the model, we found that this behavior mode represents cases where a combination of ITA parameters (e.g. insufficient resources, no power to affect operational decisions, etc.) creates conditions where the ITA structure is unable to have a sustained effect on the system. As ITA decline reaches a tipping point, reinforcing loops cause the system to migrate toward a high-risk state where accidents and serious incidents occur frequently.

In the unsuccessful implementations of ITA represented by Behavior Mode 2, as risk increases, accidents start to occur and create shock changes in the system. Safety is increasingly perceived as an urgent problem and more resources are allocated for safety analyses. The ITA function, however, loses so much credibility that they are not able to significantly contribute to risk mitigation anymore. As a result, risk increases dramatically, and the ITA personnel and safety staff become overwhelmed with safety problems and start to issue a large number of waivers in order to continue flying.

Identification of Leading and Lagging Indicators of Risk:

We also used the model to identify which variables were the most important to measure and assess, i.e., which provided the best measure of the current level of organizational risk and were the most likely to detect increasing risk early enough to prevent significant losses. This analysis led to a list of the best leading indicators of increasing and unacceptable risk. Figure 10 and Figure 11 show examples. The accumulation of waivers to technical requirements, shown in Figure 10, increases as the level of technical risk in the system increases and is a good indicator of increased risk. It lags behind any increase in system risk, however, casting doubt on its usefulness as an effective early warning metric. In comparison, the number of incidents/problems under investigation by the ITA, shown in Figure 11, increases at the same time as technical risk and thus shows promise as an effective leading indicator that the system is migrating towards a state of high risk.

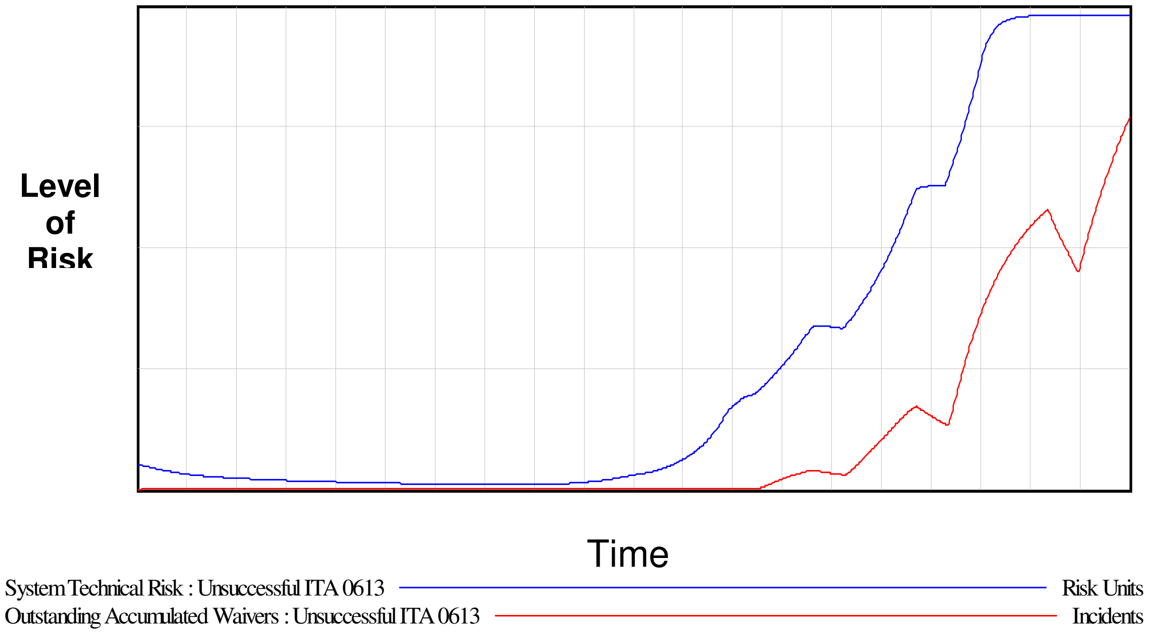


Figure 10. Level of risk and outstanding accumulated waivers in the Space Shuttle Program over time as simulated by MIT CSRL.

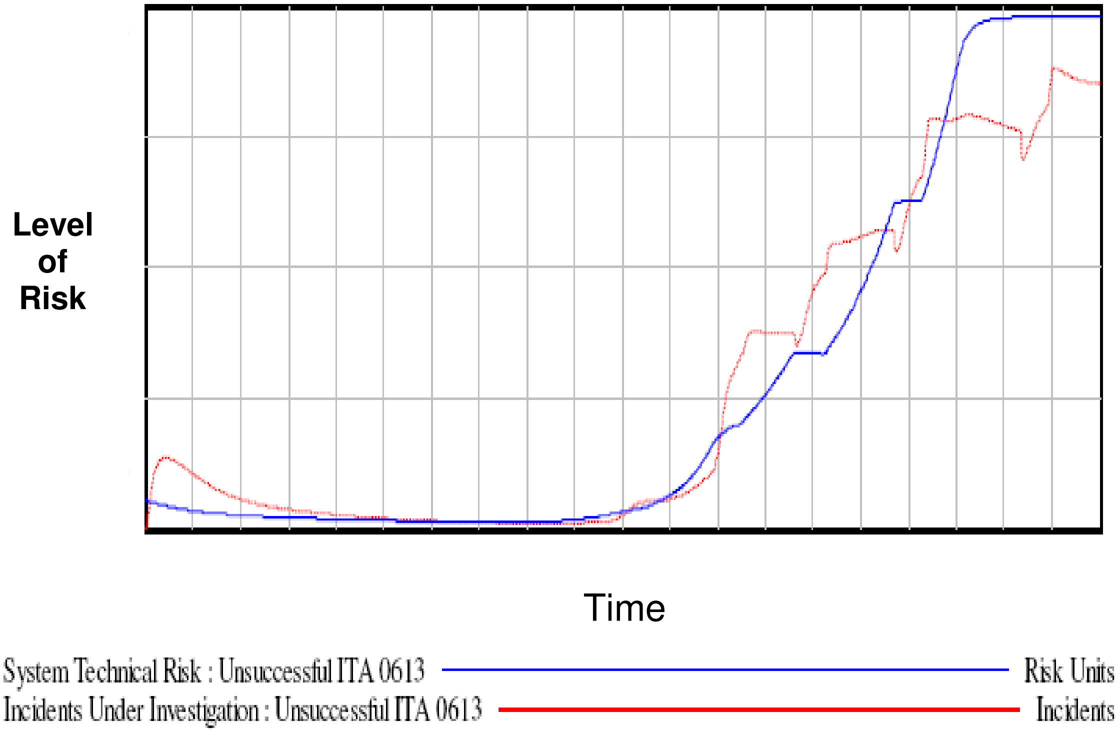


Figure 11. The coincident increases in level of risk and number of incidents under investigation in the Space Shuttle Program as simulated by MIT CSRL.

Step 7: Findings and Recommendations

The completed organizational analysis process resulted in a list of recommended policy and structural changes to the ITA organizational design as well as a list of leading indicators and measures of effectiveness to monitor safety risk in the manned space program. The full list of findings and recommendations from the ITA study can be found in the formal report that was delivered to NASA.[29]

Development of an ITA Model Interface Prototype:

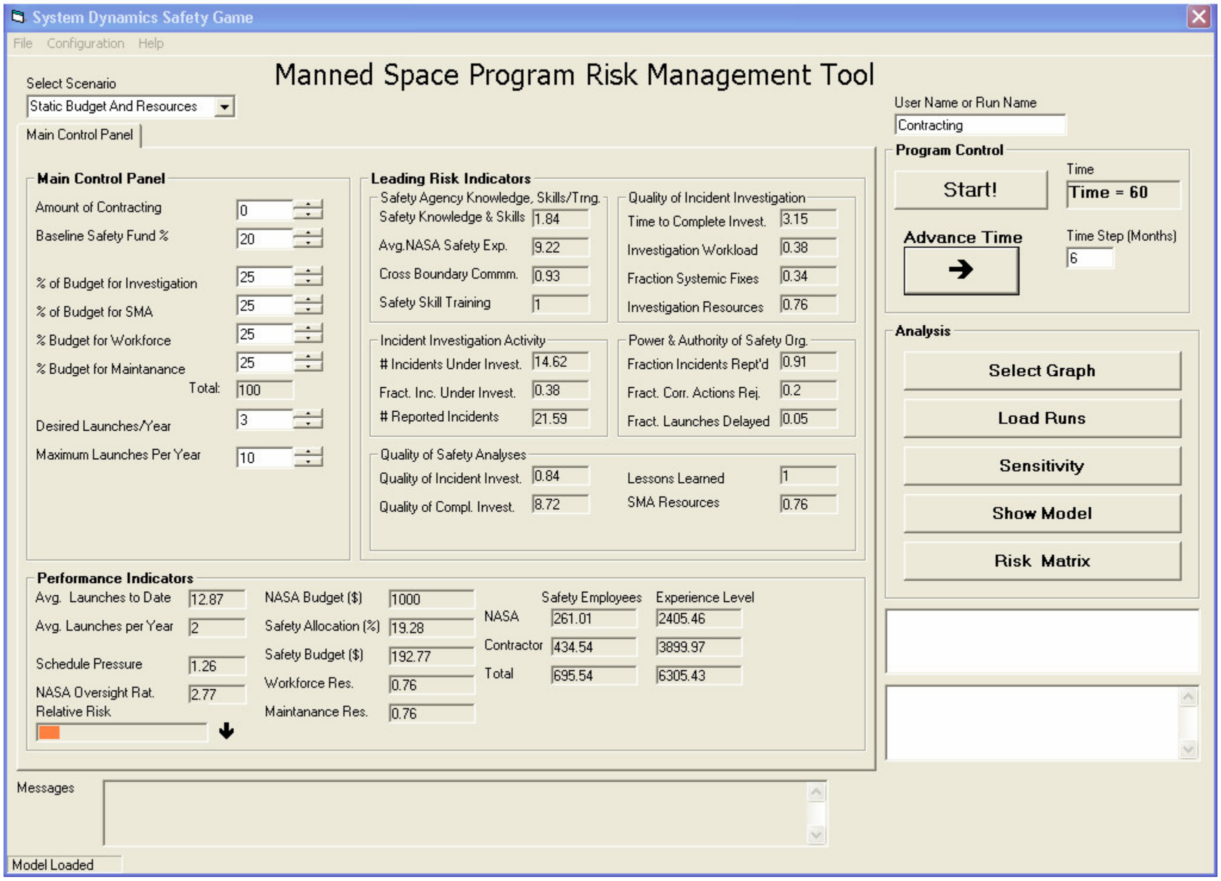
Shortly after the ITA study, a graduate student in CSRL developed a prototype software interface to that system dynamics model to explore how such models may be folded into risk management tools.[30]

Figure 12 through Figure 17 below contain screenshots of the prototype design developed. The main menu of the interface is shown in Figure 12. It contains the interface inputs for simulation runs along with performance and risk indicators and buttons for accessing additional interface displays. Because the hundreds of variables and dozens of loops in the model are sure to be

[29] Nancy Leveson, Nicolas Dulac, Joel Cutcher-Gershenfeld, John Carroll, Betty Barrett and Stephen Friedenthal (2005), *Risk Analysis of NASA Independent Technical Authority*. Report Submitted to NASA Office of the Chief Engineer. June 2005. Available at MIT CSRL's publications website <http://sunnyday.mit.edu/papers.html>

[30] Stephen R. Friedenthal (2006), *Developing a Risk Management "Flight Simulator" for Manned Space Programs: A User Interface to a Systems Dynamic Simulation of System Safety at NASA*. S. M. Thesis, Engineering and Management, Massachusetts Institute of Technology.

overwhelming to novice users of the model, a high-level abstraction[31] of the model can be accessed in the tool. This structure is somewhat complicated in and of itself and thus it is broken into pieces—refer to Figure 13 to Figure 15—that can be sequentially added to the display to allow the user to explore the structure in a stepwise manner. The interface also contains tools for plotting user-selected variables throughout the simulation (Figure 16), and tracking the status of the leading indicators on a 4x3 risk matrix (Figure 17).



Manned Space Program Risk Management Tool

Select Scenario Static Budget And Resources

Main Control Panel

User Name or Run Name Contracting

Main Control Panel

Amount of Contracting 0
Baseline Safety Fund % 20
% of Budget for Investigation 25
% of Budget for SMA 25
% Budget for Workforce 25
% Budget for Maintanance 25
Total: 100
Desired Launches/Year 3
Maximum Launches Per Year 10

Leading Risk Indicators

Safety Agency Knowledge, Skills/Trng.
Safety Knowledge & Skills 1.84
Avg.NASA Safety Exp. 9.22
Cross Boundary Comm. 0.93
Safety Skill Training 1

Quality of Incident Investigation
Time to Complete Invest. 3.15
Investigation Workload 0.38
Fraction Systemic Fixes 0.34
Investigation Resources 0.76

Incident Investigation Activity
Incidents Under Invest. 14.62
Fract. Inc. Under Invest. 0.38
Reported Incidents 21.59

Power & Authority of Safety Org.
Fraction Incidents Rept'd 0.91
Fract. Corr. Actions Rej. 0.2
Fract. Launches Delayed 0.05

Quality of Safety Analyses
Quality of Incident Invest. 0.84
Quality of Compl. Invest. 8.72
Lessons Learned 1
SMA Resources 0.76

Program Control

Time Time = 60
Time Step (Months) 6

Analysis

Performance Indicators

Avg. Launches to Date 12.87
Avg. Launches per Year 2
Schedule Pressure 1.26
NASA Oversight Rat. 2.77
Relative Risk

NASA Budget ($) 1000
Safety Allocation (%) 19.28
Safety Budget ($) 192.77
Workforce Res. 0.76
Maintanance Res. 0.76

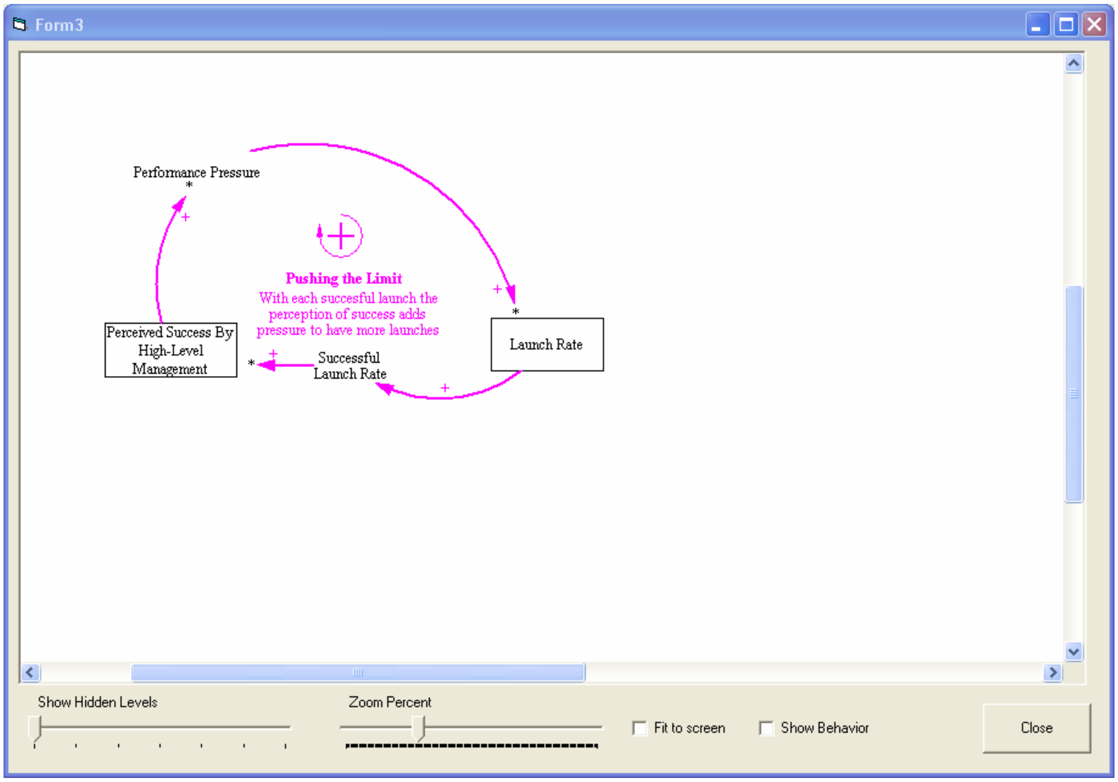
	Safety Employees	Experience Level
NASA	261.01	2405.46
Contractor	434.54	3899.97
Total	695.54	6305.43

Messages

Model Loaded

Figure 12. Screen image of the main interface menu.

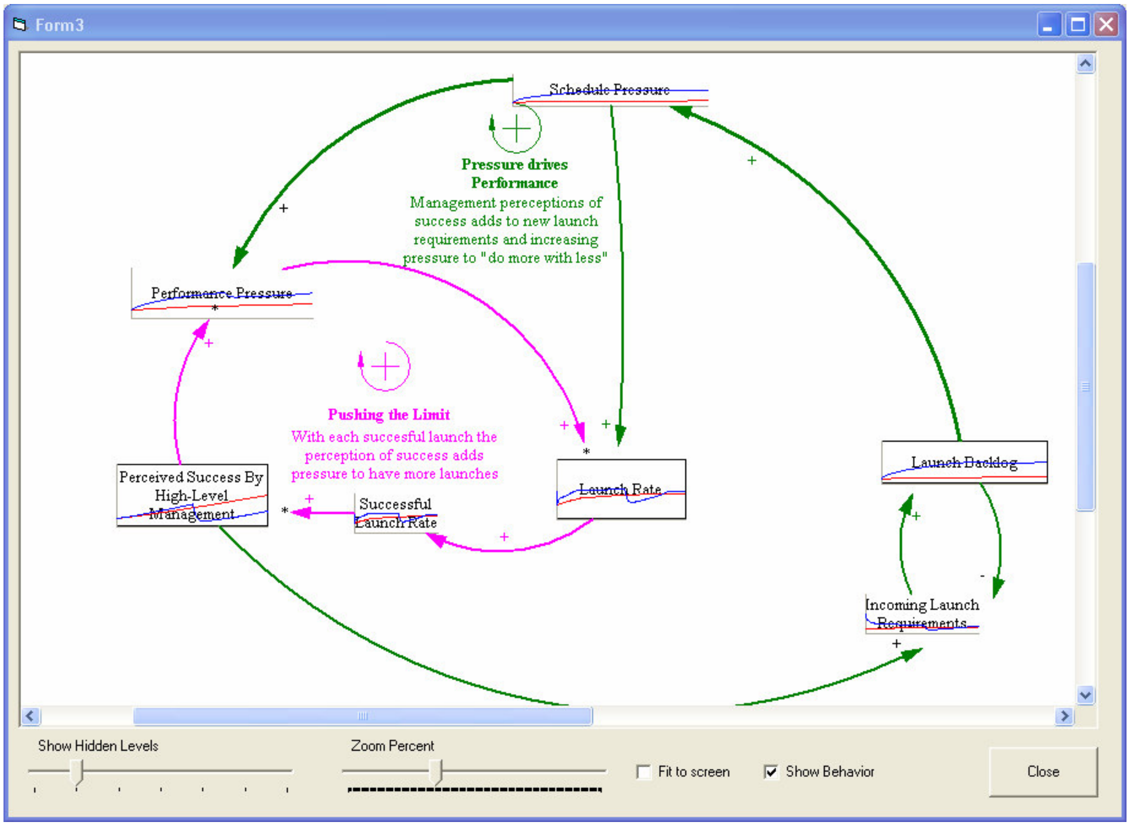
[31] Due to the complexity of system dynamics models, it is sometimes necessary to abstract the models themselves for the purpose of presentation. Section 3 provides a taxonomy for abstractions of system dynamics models. Under this taxonomy, the abstraction in Figure 13 through Figure 15 is a Level 1 abstraction of the ITA model created by MIT CSRL.



Pushing the Limit
With each succesful launch the perception of success adds pressure to have more launches

□ Fit to screen
□ Show Behavior

Figure 13. Screen image of the first layer of the ITA model high-level structure.



Pressure drives Performance
Management pereceptions of success adds to new launch requirements and increasing pressure to "do more with less"

Pushing the Limit
With each succesful launch the perception of success adds pressure to have more launches

□ Fit to screen
☑ Show Behavior

Figure 14. Screen image of the second layer of the ITA model high-level structure.

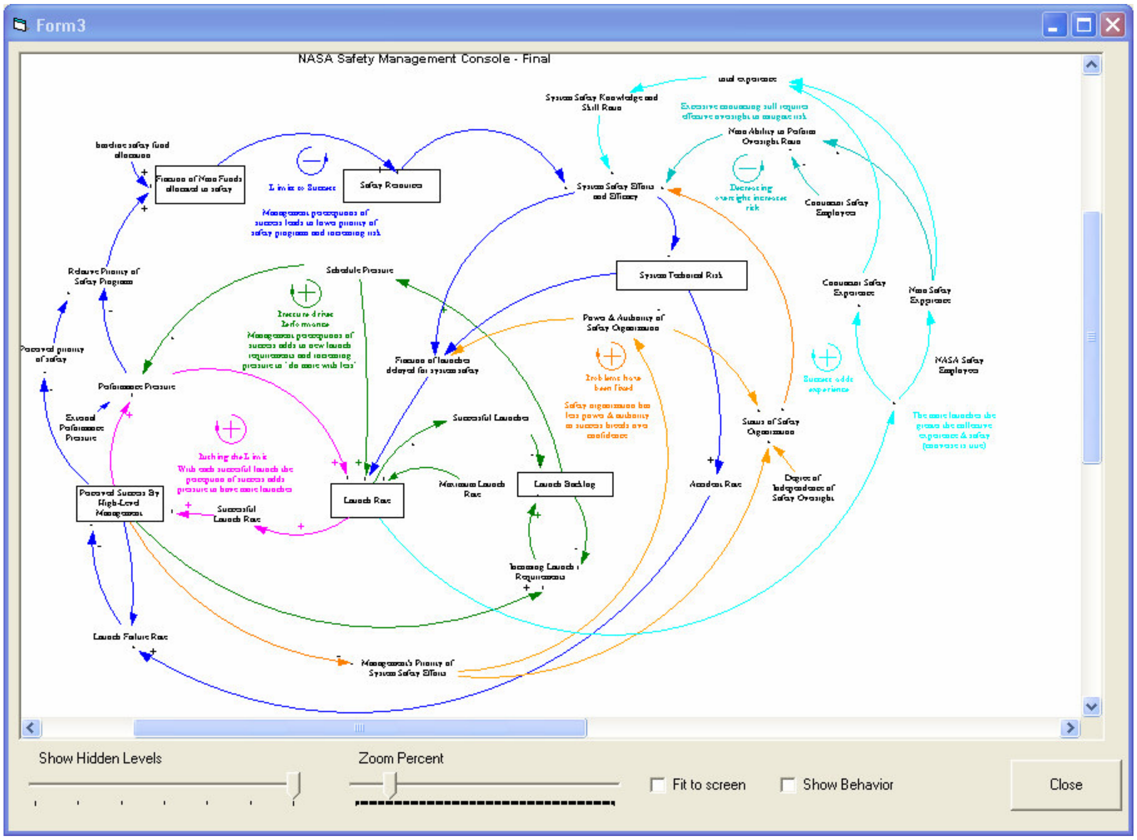

Form3
NASA Safety Management Console - Final
baseline safety fund allocation
Fraction of Nasa Funds allocated to safety
Limits to Success
Safety Resources
Management perception of success leads to lower priority of safety programs and increasing risk
System Safety Knowledge and Skill Ratio
total experience
Excessive contracting still requires effective oversight to mitigate risk
Nasa Ability to Perform Oversight Ratio
System Safety Efforts and Efficacy
Decreasing oversight increases risk
Contractor Safety Employees
Relative Priority of Safety Programs
Schedule Pressure
Pressure drives Performance
Management perception of success adds to new launch requirements and increasing pressure to 'do more with less'
System Technical Risk
Contractor Safety Experience
Nasa Safety Experience
Perceived priority of safety
Performance Pressure
Fraction of launches delayed for system safety
Power & Authority of Safety Organization
Problems have been fixed
Safety organization has less power & authority as success breeds overconfidence
Success adds experience
NASA Safety Employees
External Performance Pressure
Pushing the Limit
With each successful launch the perception of success adds pressure to have more launches
Successful Launches
Status of Safety Organization
The more launches the greater the collective experience & safety (converse is true)
Perceived Success By High-Level Management
Successful Launch Rate
Launch Rate
Maximum Launch Rate
Launch Backlog
Accident Rate
Degree of Independence of Safety Oversight
Incoming Launch Requirements
Launch Failure Rate
Management's Priority of System Safety Efforts
Show Hidden Levels
Zoom Percent
□ Fit to screen
□ Show Behavior
Close

Figure 15. Screen image of the final layer of the ITA model high-level structure.

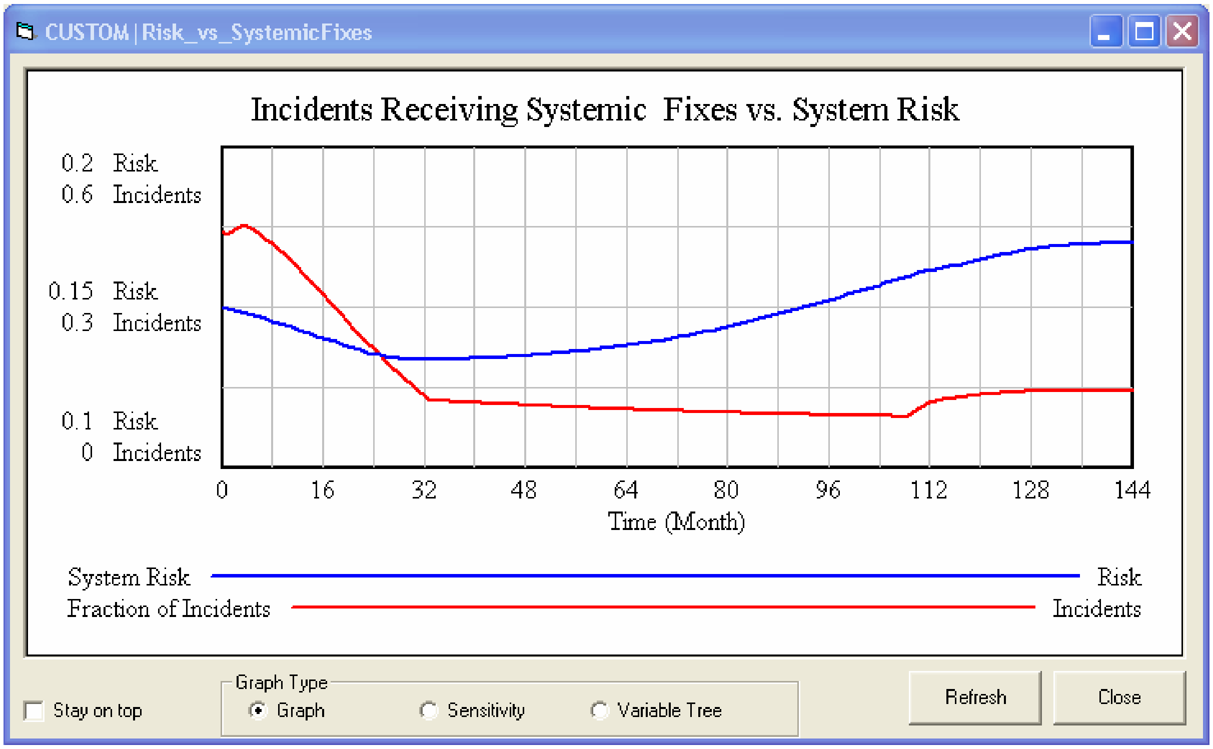
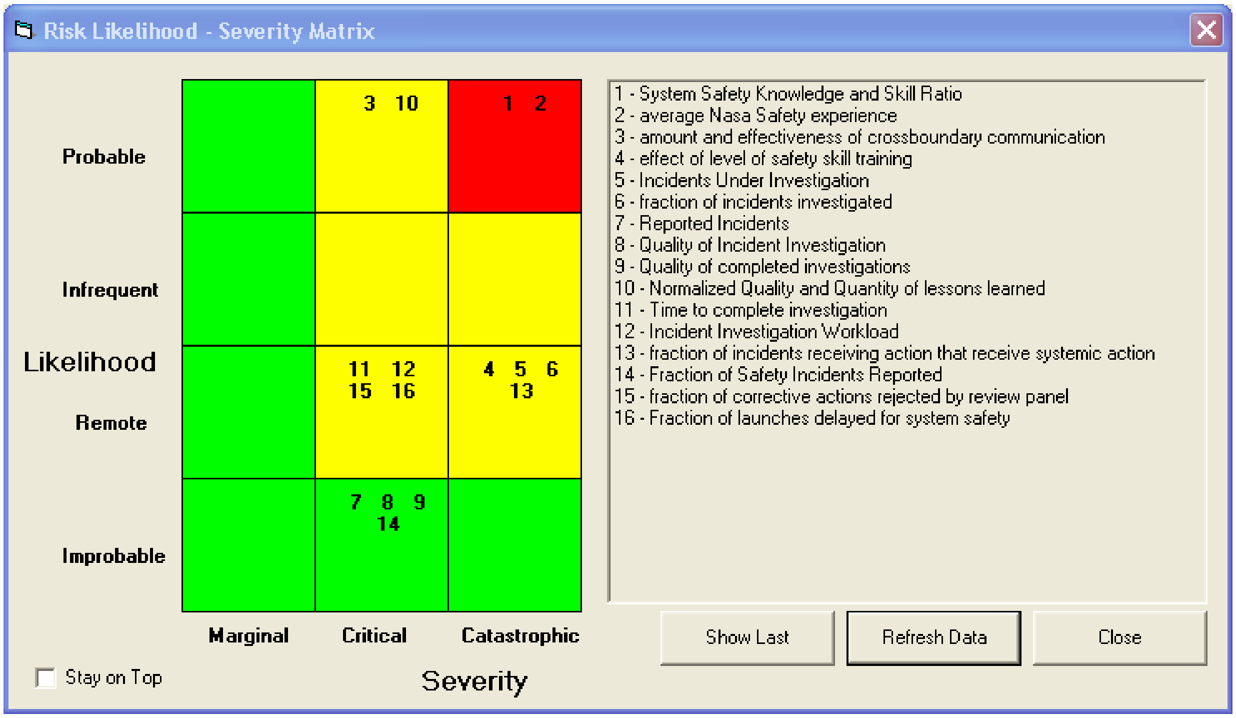


Figure 16. Screen image of the variable plotting tool.



	Marginal	Critical	Catastrophic
Probable	🟩	🟨 3 10	🟥 1 2
Infrequent	🟩	🟨	🟨
Remote	🟩	🟨 11 12 15 16	🟨 4 5 6 13
Improbable	🟩	🟩 7 8 9 14	🟩

1 - System Safety Knowledge and Skill Ratio
2 - average Nasa Safety experience
3 - amount and effectiveness of crossboundary communication
4 - effect of level of safety skill training
5 - Incidents Under Investigation
6 - fraction of incidents investigated
7 - Reported Incidents
8 - Quality of Incident Investigation
9 - Quality of completed investigations
10 - Normalized Quality and Quantity of lessons learned
11 - Time to complete investigation
12 - Incident Investigation Workload
13 - fraction of incidents receiving action that receive systemic action
14 - Fraction of Safety Incidents Reported
15 - fraction of corrective actions rejected by review panel
16 - Fraction of launches delayed for system safety

Figure 17. Screen image of the 4x3 risk matrix for tracking the risk scores of the leading indicators.

2. METHODOLOGY

For the current study described in this report, our goal was to demonstrate a novel and powerful new approach to risk management that combines STAMP-based and system dynamics modeling. This study differed in three important ways from that performed in the ITA risk analysis described above.

First, the Space Shuttle program is basically an operational program while ESMD will be focused for many years on development rather than operations. Second, the Space Shuttle program has been in existence for decades with its safety control structures well defined (with the exception of the new ITA structure). In contrast, ESMD is currently trying to define an effective safety control structure. While the application of our new methodology in the first research study evaluated the risks in making a significant change to the current Space Shuttle (SOMD) organizational structure, the goal of the second was to assist in creating a new structure and to demonstrate how our approach could assist in managing risks and in general risk-related decision-making for a new program.

Finally, in the ITA study we were primarily concerned with determining whether our approach worked for a real, complex organization. After we had demonstrated feasibility and effectiveness with the ITA risk analysis, we were more concerned in the second study with improving the methodology from what we had learned and making it more practical and easy to apply and use by people with limited expertise in system dynamics modeling.[32] Two significant additions to the methodology were (1) the association of system dynamics modeling components with the STAMP

[32] Nicolas Dulac (2007), *A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems*, Ph.D. Dissertation, Aeronautics and Astronautics, Massachusetts Institute of Technology.

safety control structure components and (2) the development of generic system dynamics model components that can be tailored and used for other organizations.

At the same time, schedule and budget restrictions for the ESMD study limited the detailed completion of the STAMP control structure model component responsibilities and thus the generation of a complete list of project risks. We had demonstrated and proven this project risk generation process in the ITA study and instead for ESMD used a more classic (and less complete) identification process involving interviews of experts. The next section describes the interview process used to gather information (including potential risks). Section 2.3 then describes how this information was used to create and validate the model. The rest of the report describes the model itself and the example risk analyses we performed on it.

2.1 Employee Interviews

We relied on interviews with NASA officials as a primary source of information throughout the study for a number of reasons. First, because each organization is unique and many elements of its functions are unwritten or even guarded closely at times, the amount of information that can be gathered through a review of internal documentation and the broader literature in the public domain is limited even under normal circumstances. At the time of this study the scarcity of such documentation was exacerbated by the fact that NASA was in the midst of a dramatic reorganization in response to the *Columbia* Accident, the appointment of a new Administrator, and the Vision for Space Exploration, that, among other things, will require NASA to develop human-rated launch and landing systems for the first time since the 1970s.

An additional consideration in the collection of data through interviews is that a primary goal of system dynamics modeling is to capture the "intended rationality" of the key decision-makers in the system.[33,34] When presented with imperfect information, time limitations, and/or complexities that exceed the limits of human cognitive abilities, people act with a rationality that is said to be "bounded" rather than perfect.[35,36] This is not to say that people act in an unintelligent manner, rather, it is meant to indicate that the bases on which people make decisions is "intendedly" rational, that is, that their decisions would produce sensible results if their model of the relevant system is correct.[37] People rely on heuristics or rules of thumb and satisficing—a practice where instead of evaluating all options, the analyst stops whenever he or she finds a solution that is "good enough"—for decision-making and thus, when studying a system, it is imperative to include both the heuristics and satisficing criteria in the models to accurately explain decision-making in the system.[38,39] Typically, information on these heuristics and criteria can only be obtained through discussions with decision-makers in the organization.

In all, 44 people were interviewed during 41 interviews conducted over a three-month period at NASA Headquarters, the Marshall Space Flight Center, the Johnson Space Center, and the Langley Research Center.[40] Many of the interviewees worked in the Exploration Systems Mission Directorate, but a number worked above the directorate-level and still others worked in the other

[33] John D. W. Morecroft (1983), "System Dynamics: Portraying Bounded Rationality," *Omega-The International Journal of Management Science*, Vol. 11, No. 2, pp. 131-142.

[34] Herbert Simon (1979), *Models of Thought*, Yale University Press, pg. 3-19.

[35] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, pp. 597-629.

[36] Simon, ibid, pp. 3-19.

[37] Sterman, ibid, pp. 597-629.

[38] Sterman, ibid.

[39] Simon, ibid, pp. 3-19.

[40] In three of the interview sessions, two people were interviewed simultaneously. In all of the other sessions only one person was interviewed at a time.

mission directorates, particularly the Space Operations Mission Directorate (refer to Appendix C for an overview of NASA's organizational structure). Overall, we interviewed representatives from the Office of the Administrator, the Office of the Chief Engineer, the Office of Safety and Mission Assurance, the NASA Engineering and Safety Center, the Office of Program Analysis and Evaluation, Mission Directorate Offices, ESMD Directorate Offices, Program Offices, Project Offices, the Office of Institutions and Management, Center Safety and Mission Assurance Directorates, Center Engineering Directorates, Center Mission Operations Directorates, and the Astronaut Office.

In order to get the most out of the interview time that we were allotted, we developed an interview protocol employing state-of-the-art interview techniques in the social sciences. Upfront, we recognized that our interviews were going to be staged over a period of months and that the simulation model that we would ultimately create would require some degree of debugging to expunge logic as well as syntax errors. With that said, we knew that creating and debugging the model after the interview process was complete would be a misuse of both the interview time and the time between interviews (i.e. it would leave us with idle time between interviews and exclude our interviewees from the debugging process). Therefore, we selected a research process that would allow us to collect interview data, develop the model, and debug it in a concurrent fashion rather than a serial one. The iterative process that we adopted is formally referred to as a grounded theory building approach,[41,42,43] supplemented by causal loop diagramming and formal simulation model building.[44] This process involved the creation of a draft qualitative structure of the model before the first interview and a succession of revisions to the model based on the comments provided by each set of interviewees. The interview protocol that we selected is best described as *semi-structured in-depth*, which means that there was a set of questions for consistency, but the interviewees were allowed to elaborate on any topic. This technique is typically used in the development of system dynamics models[45] and allows the interviewee to provide information that the interviewer might have unintentionally suppressed with a more rigid set of questions.

The standard duration for an interview session was one hour, though some were as short as approximately twenty minutes or as long as approximately one hundred minutes. At the beginning of each session, the interviewee was briefed on system dynamics and STAMP from a set of introductory slides and asked to both sign a consent form and give verbal consent to the voice recording of the session (see Appendix F for copies of these slides and the consent form).[46,47] After the signing of the consent form, the session consisted of up to four major sections based on time constraints and interviewee expertise: 1) Discussion of NASA's Organizational Structure, 2) Responsibilities Survey, 3) Safety Risk Survey, and 4) Review of a Specific Component of the

[41] A grounded theory building approach is a qualitative research method that involves multiple stages of data collection and the refinement of categories of information (Strauss & Corbin, 1990). This type of approach is typically characterized by the constant comparison of data with emerging categories and theoretical sampling of various groups to maximize the similarities and the differences of information (Creswell, 1994).

[42] Creswell, John W. (1994), *Research Design: Qualitative and Quantitative Approaches.* Thousand Oaks, CA: Sage.

[43] Strauss, A. and J. Corbin (1994), "Grounded Theory Methodology: An Overview." In N. K. Denzin and Y. S. Lincoln (eds.), *Handbook of Qualitative Research:* 273-285. Thousand Oaks, CA: Sage.

[44] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill.

[45] Sterman, ibid, pg. 157.

[46] To protect interviewee confidentially, interviewee names were not included in notes and transcripts from the sessions and are not included in this report.

[47] Recordings of the interviews were partially transcribed into a collection over 220 pages in length and used internally for review of the key concepts discussed.

System Dynamics Model. Each of these portions of the interviews is described in the subsections below.

Discussion of NASA's Organizational Structure:

NASA's organizational structure was briefly discussed with each interviewee in order to clarify our questions and identify both the interviewee's vantage point on organizational issues and discrepancies in what interviewees viewed as the roles of the organization elements. We presented the chart in Figure 18 to each interviewee and asked him/her to describe his/her expertise and where his/her position fit in the organizational structure. Then we asked the interviewee how resources and information flowed across the elements of the organizational structure. Finally, before moving on to the responsibilities survey, we asked each interviewee to describe his/her role in safety during the development of space exploration systems.

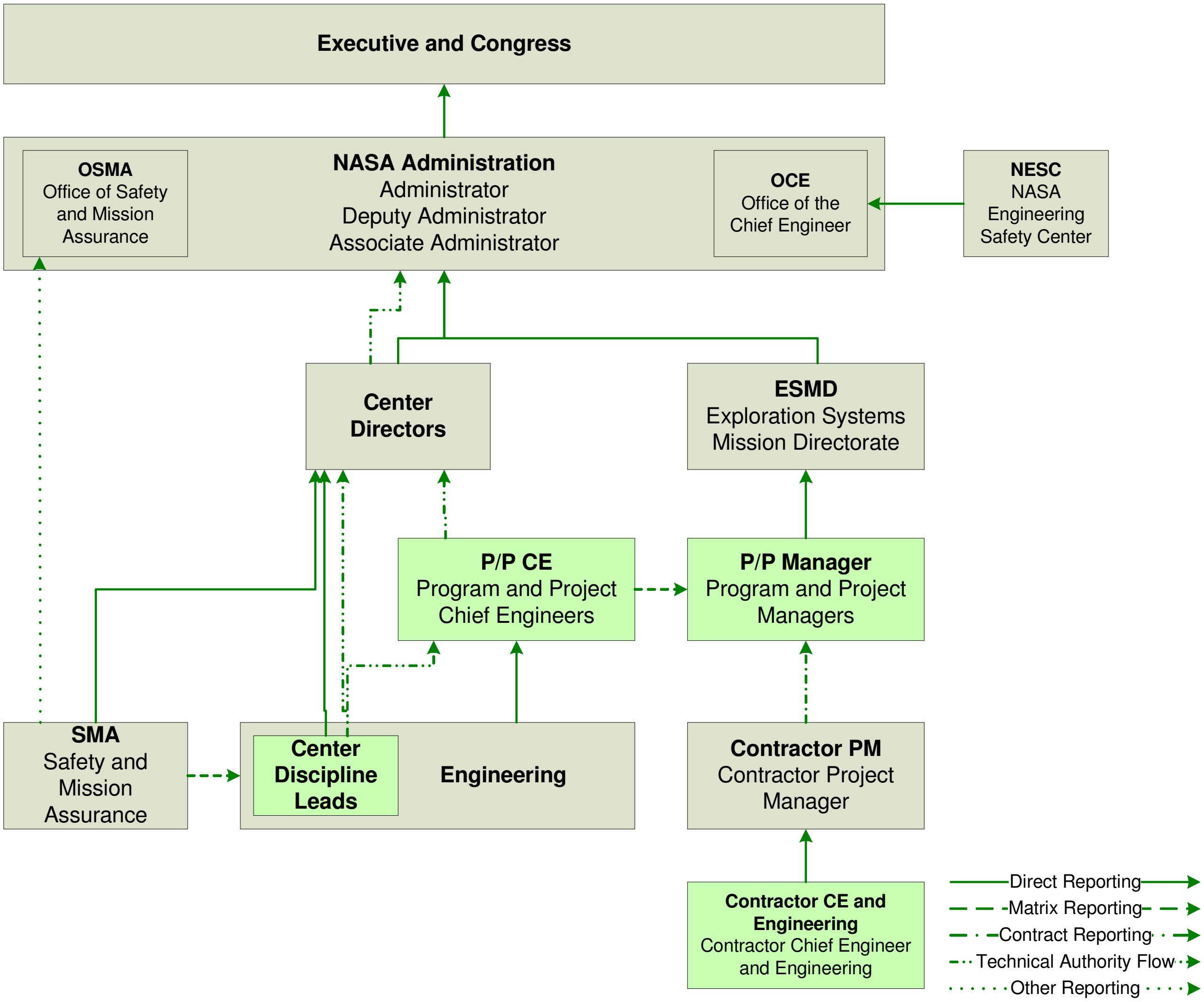

Executive and Congress
OSMA
Office of Safety and Mission Assurance
NASA Administration
Administrator
Deputy Administrator
Associate Administrator
OCE
Office of the Chief Engineer
NESC
NASA Engineering Safety Center
Center Directors
ESMD
Exploration Systems Mission Directorate
P/P CE
Program and Project Chief Engineers
P/P Manager
Program and Project Managers
SMA
Safety and Mission Assurance
Center Discipline Leads
Engineering
Contractor PM
Contractor Project Manager
Contractor CE and Engineering
Contractor Chief Engineer and Engineering
Direct Reporting
Matrix Reporting
Contract Reporting
Technical Authority Flow
Other Reporting

Figure 18. NASA's organizational control structure.[48]

[48] This diagram was developed based on discussions with Walter Hussey, Director of the Independent Technical Authority Implementation in NASA OCE. Because NASA was in the midst of organizational changes, certain subtleties of this structure changed even within the time span that the interviews were being conducted. Therefore the diagram is somewhat outdated; however, the basic concept of the Executive and Legislative Branches of U.S.

Responsibilities Survey:
Control theory is a foundational element of both system dynamics and STAMP. In both frameworks, system parameters are viewed as evolving within the confines of certain control laws that may even evolve themselves. In the vernacular of organizational dynamics, policies and processes (formal and informal) constitute the control laws that regulate organizational behavior in areas such as safety-related decision making. Thus, whenever time and the interviewee's expertise permitted, we asked the interviewee where the following responsibilities should be allocated in order to ferret out whatever organizational control laws are at play:

- Adjudication of differences between the mission directorate associate administrators and the center directors
- Provision of the directives and procedural requirements that define technical excellence
- Implementation of technical excellence
- Maintenance of the effectiveness of the Technical Authority program
- Preservation of Program/Project Chief Engineer and Center Discipline Lead financial and managerial independence at the centers
- Safety trend analysis
- Incorporation of the hazard analysis results into the system or component design, development, and operation
- Hazard and risk analysis, system safety design, FMEA, and identification of critical items for in-house activities
- Evaluation of contractor produced analyses and their incorporation into contractor products
- Approval of the FMEA, CIL, and hazard and risk analyses
- Ownership of the processes and systems for FMEA and hazard reporting
- Ownership of the integrated hazard process
- Conflict resolution at the Project/Program management level
- Determination of what is and is not an anomalous event
- Determination of whether a design satisfies the technical requirements and/or approval of any variances written against them
- Approval of the Program/Project Chief Engineers.

Ultimately we were able to collect responses in this survey from all but fifteen interviewees because some were either not asked or had no opinion when asked about these responsibilities. As expected, there was some level of disagreement among the interviewees on the allocation of each of the responsibilities; in these cases, however, the responses themselves were usually not as informative to the modeling process as the discussion that they generated.

Safety Risk Survey:
In order to identify the risks in the development of the new exploration systems that were raising the most concerns among NASA employees, we asked each interviewee to list what they feel will be the three to five most important factors affecting safety-related risk in the development of space exploration systems. Ultimately, there were a number of recurring items mentioned in the responses that the interviewees gave. These items include (in no particular order):

Government influencing the NASA Administration that in turn influences the "Three Legs of the Stool" (i.e. S&MA, Engineering, and Project Management) remained unchanged.

- Having a system's view, strong systems engineering, and getting requirements right
- Proper management of risk, ensuring that each risk gets the attention that it deserves
- Building and maintaining a workforce with the right skill sets at the right time
- Information sharing and lessons learned (knowledge capture); Center cooperation
- S&MA having necessary prestige, influence, skills, and independence
- Preventing schedule pressure from getting too high or too low; having a realistic alignment of cost, schedule, resources with technical work to be done
- Promoting a culture of speaking up whenever people identify problems
- Finding problems early; including hazard analysis results in design
- Adequately overseeing contractors
- Making safety an important part of risk management[49]
- Developing and executing a robust test program
- Ensuring program stability
- Shifting from an operations-oriented to a development-oriented organization
- Receiving adequate support and funding from Congress (particularly after accidents/incidents)
- Planning for operations during development.

These items are not meant to represent things that the interviewees view as current problems at NASA; instead, they represent the things that they feel would be most detrimental to safety if NASA did not do them properly. Therefore, it was important to our modeling effort to ensure that there were mechanisms in the model—whenever possible—to show how well these things are being done at any given time in our simulations and what, if anything, might lead to poor performance in these areas.

Review of a Specific Module of the System Dynamics Model:

Towards the end of almost every interview, the interviewee was asked to review the causal structure of a module of the model that was closely related to his or her area of expertise. These modules, which were printed on a large sheet of paper and laid out in front of the interviewee, were sometimes difficult for the interviewee to review at first due to their complexity and/or the interviewee's lack of experience with system dynamics. Thus, it was often necessary to guide the interviewee through the review process by asking questions on specific relationships and variables that we had hoped to get more information on prior to the interview or ones that had come up in discussion earlier in the interview. Usually, after the first few questions were asked, the interviewee was able to review other relationships and variables in the model and provide comments on them without further prompting.

In all, the interviewees in 38 of the 41 interviews reviewed model modules and both the qualitative and quantitative inputs that they provided led to a number of changes in the causal structure of model and the equations behind it.

[49] Risk management includes management of schedule risk, cost risk, and performance risk in addition to safety risk. Unfortunately, actions to control one or more of these risks will not necessarily have positive impacts on the other risks. In fact, actions to control one risk may lead to increases in the other risks.

2.2 Additional Data Collection

While interviews served as our primary source of qualitative data, we obtained most of our quantitative data from a number of sources in the public domain. These sources, which mostly contained budget and personnel data, are summarized in Table 1. Of these, the most noteworthy source of data was the workforce data cubes on the NASAPeople Website. This data source is highly interactive in that it allows for the customization of data reports and the ability to get even the most obscure statistics on the NASA civil servant workforce (e.g. the resignation rate of NASA civil servants with less than nine years of experience). The data from this and the other sources in Table 1 provided a quantitative foundation for the workforce planning and budget estimation algorithms in the model.

SOURCE	TYPES OF DATA
Workforce Data Cubes on the NASAPeople Website[50]	• Center support contractor headcounts for FY 2002 • Headcounts of civil servant workforce in Science and Engineering (S&E) positions • S&E civil servant workforce age, experience, hiring counts, attrition counts, retirement eligibility • Age of civil servant new hires • Etc.
FY 2004 to FY 2007 NASA Budget Requests[51]	• Budget breakdowns to the program level (historical and forecast) for FY 2002 to FY 2011 • Estimates of civil servant unfunded capacity
FY 2002 to FY 2004 NASA Procurement Reports[52]	• Total procurement dollars for FY 2002 to FY 2004 • Procurement Awards by type of effort for FY 2002 to FY 2004
Columbia Accident Investigation Board Report	• Space Shuttle Program civil servant and support contractor workforce for FY 1993 to FY 2002 • Space Shuttle Program budget for FY 1993 to FY 2002

Table 1. Budget and personnel data sources and the types of data used from them in the model.

2.3 System Dynamics Model Development, Testing, and Preliminary Utilization

A system dynamics model of the safety-related decision-making in the development of exploration systems was a primary deliverable for this project. Accordingly, the majority of the effort centered on the logical and syntactical encoding of real-world behavior in the development of exploration systems into a software model executable from a laptop or desktop personal computer.[53] As mentioned earlier, this process began prior to the first interview and was conducted concurrently throughout and beyond the interview time frame. Overall, the model went through dozens of revisions to both its qualitative and quantitative structure and was tested by an individual who was not involved in the model development process.

[50] Available at <http://nasapeople.nasa.gov/Workforce/data/page8.htm>.

[51] Available at <http://www.nasa.gov/about/budget/index.html>.

[52] Available at <http://ec.msfc.nasa.gov/hq/library/procreport/index.html>.

[53] The system dynamics software tool used in this effort was Vensim® Windows Version 5.5d.

Development of the Model's Causal Structure:

Our system dynamics model structure and creation process differs from that which is traditional in system dynamics as our model-creation process and structure is tied to the STAMP accident causality model. Consequently, an important part of the module-based model creation was to create the STAMP control structure. For system development projects, the initial qualitative structure will be similar to the left-hand column of Figure 1 while models of system operation will resemble the right-hand column. Because the model produced for the previous study of NASA ITA primarily focused on the Space Shuttle Program—an operational, rather than developmental program—many of its elements were not directly transferable to the ESMD model. Therefore, it was necessary to begin by creating a STAMP model of the NASA ESMD system development organizational structure.

To do this, we started with the organizational structure (shown in Figure 18) of safety-related decision-making for the new exploration system. The model was slightly modified a few times during model refinement and validation based on the input of the domain experts interviewed. The final configuration of the control structure can be seen in Figure 19. The complete model would include much more information, such as the defined responsibilities of each module in the model, the possible control actions, feedback information, etc. An example can be found in the final report on the ITA analysis.[54] As mentioned earlier, our methodology and the use of STPA (a new hazard analysis technique) provides the ability to generate a comprehensive list of project risks from the model. Budget and time limitations for this study precluded us from being able to accomplish this for ESMD, but the feasibility and effectiveness of the process was demonstrated in the ITA study (and compared to a classic risk analysis process performed in parallel by NASA). For this current study, we instead used the risks identified in our expert interviews.

[54] Nancy Leveson, Nicolas Dulac, Joel Cutcher-Gershenfeld, John Carroll, Betty Barrett and Stephen Friedenthal (2005), *Risk Analysis of NASA Independent Technical Authorit*y. Report Submitted to NASA Office of the Chief Engineer. June 2005. Available at MIT CSRL's publications website <http://sunnyday.mit.edu/papers.html>

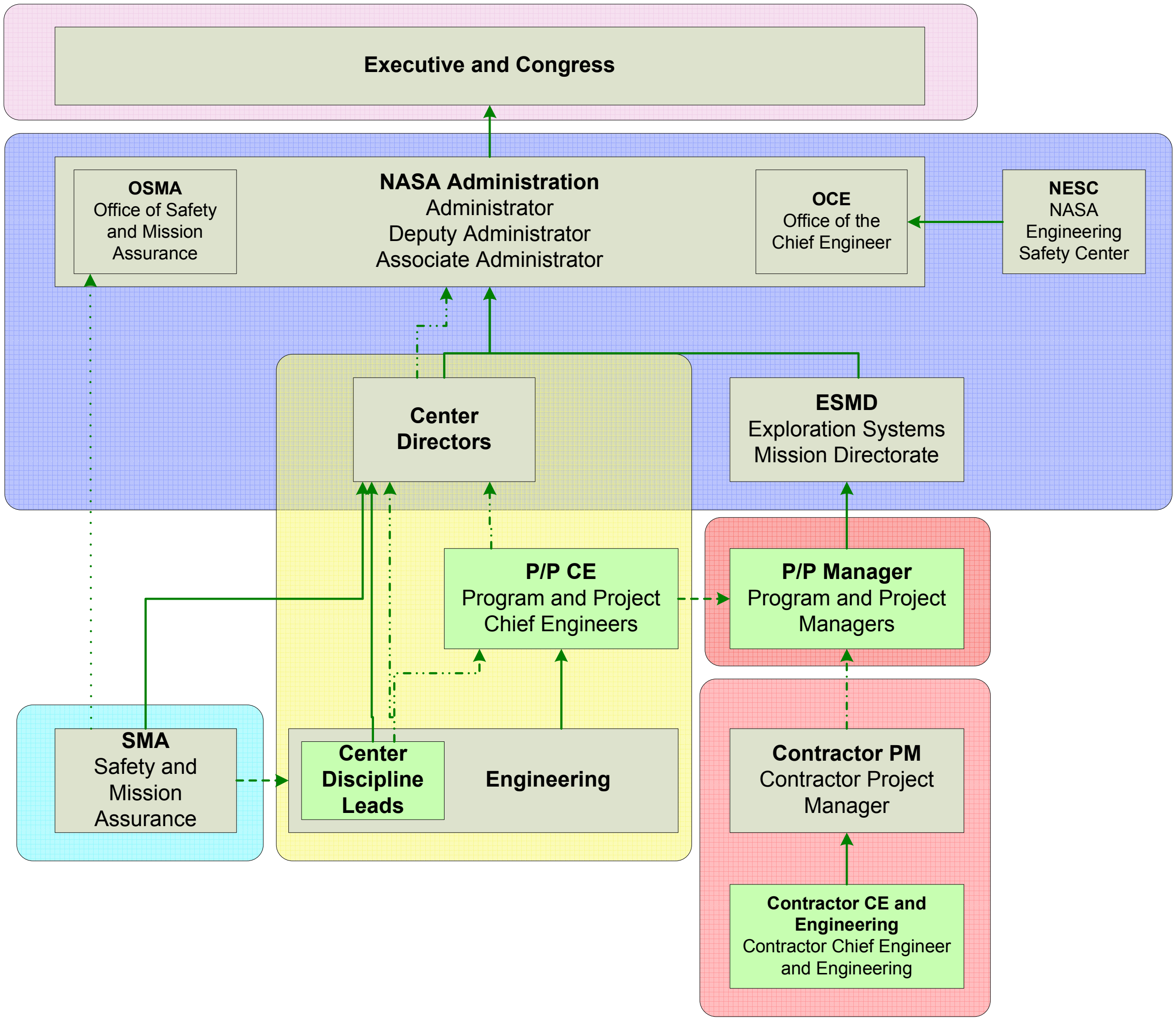

Executive and Congress
OSMA
Office of Safety and Mission Assurance
NASA Administration
Administrator
Deputy Administrator
Associate Administrator
OCE
Office of the Chief Engineer
NESC
NASA Engineering Safety Center
Center Directors
ESMD
Exploration Systems Mission Directorate
P/P CE
Program and Project Chief Engineers
P/P Manager
Program and Project Managers
SMA
Safety and Mission Assurance
Center Discipline Leads
Engineering
Contractor PM
Contractor Project Manager
Contractor CE and Engineering
Contractor Chief Engineer and Engineering

Figure 19. The mapping of NASA's organizational structure to the generic STAMP structure of organizational control.

Because one research goal of this study was to make the methodology easily accessible to a wide range of non-expert users, we have defined generic system modules that can be tailored to fit specific projects.[55] Accordingly, after defining the NASA control structure shown in Figure 19, an overall model structure was created by assembling generic sections corresponding to the real system participants. The resulting model structure is shown in Figure 20. In general, upward arrows represent feedback channels, while downward arrows represent control actions. The operating principle of the model is that of the STAMP accident model, that is, safety is achieved by performing the control actions necessary to ensure that safety constraints will be enforced throughout the system lifecycle. In addition to feedback and control channels, information is passed across module boundaries as needed to allow the model to execute. For example, project management may not receive continuous feedback about the number of NASA employees working

[55] Nicholas Dulac (2007), *A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems,* Ph.D. Dissertation, Aeronautics and Astronautics, Massachusetts Institute of Technology.

in particular areas, but the amount of work performed in an area per time period is a good indicator of the resources allocated to this particular area. In short, some information may be available indirectly without being explicitly included in a reporting/feedback channel.

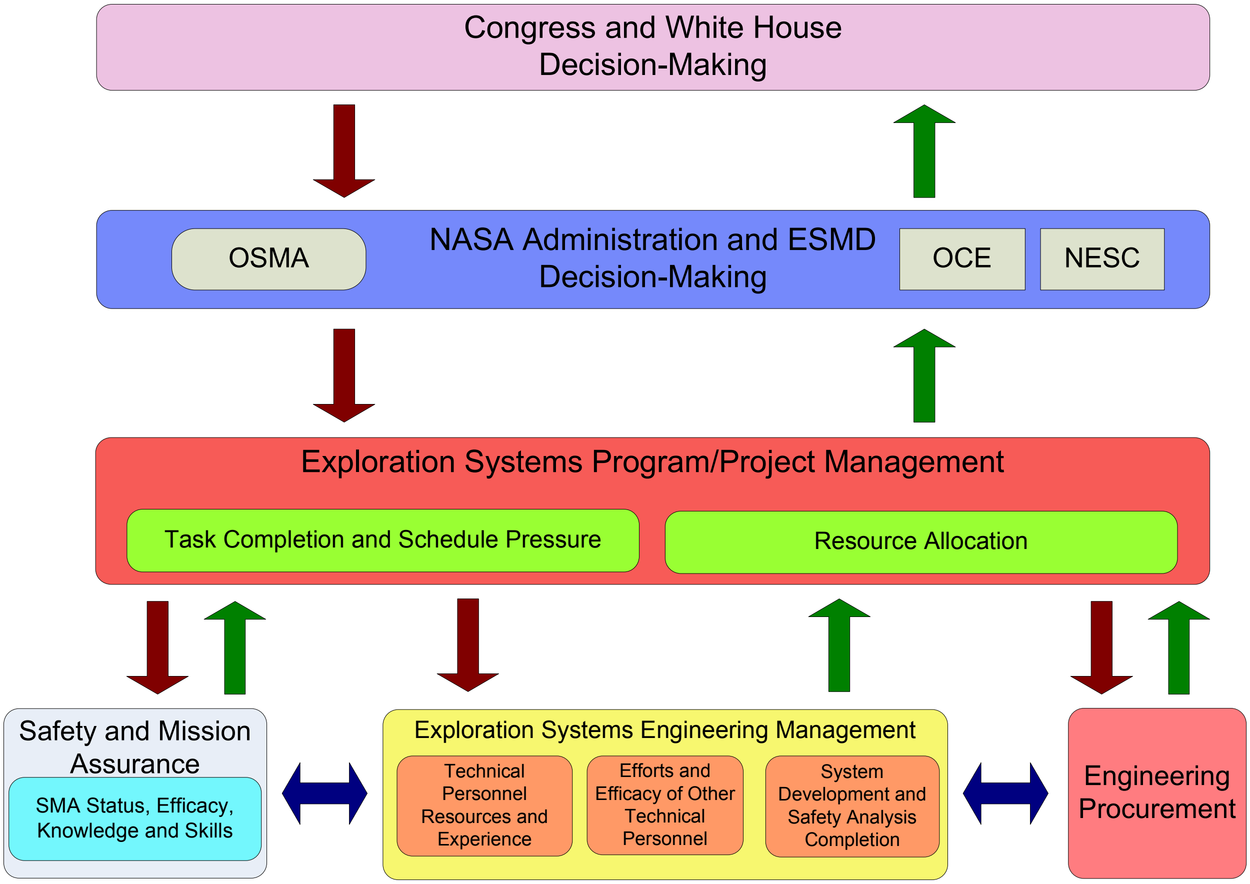

Congress and White House
Decision-Making
OSMA
NASA Administration and ESMD
Decision-Making
OCE
NESC
Exploration Systems Program/Project Management
Task Completion and Schedule Pressure
Resource Allocation
Safety and Mission Assurance
SMA Status, Efficacy, Knowledge and Skills
Exploration Systems Engineering Management
Technical Personnel Resources and Experience
Efforts and Efficacy of Other Technical Personnel
System Development and Safety Analysis Completion
Engineering Procurement

Figure 20. The sections of the ESMD System Dynamics Model.

The initial structure of individual model modules was derived from existing data in NASA literature and accident reports, from our knowledge of system safety, and previously documented system development dynamics structures and archetypes. For example, the "Rework Cycle" in the model—which will be explained in a later section—was derived from a portion of a system dynamics model that was used for the out-of-court settlement of a lawsuit involving the Navy and one of its contractors.[56] The structure was then modified and refined based on inputs and discussion with NASA domain experts (as described above) until we converged on a structure deemed acceptable to a majority of domain experts interviewed.

[56] Ingalls, a ship builder for the Navy, sued the Navy to recover losses from significant cost overruns that it encountered in fulfilling one of its contracts. Ingalls contended that the overruns were due to frequent design changes imposed by the Navy. The Navy was skeptical of Ingalls' claim until it was shown a system dynamics model of the effects of these design changes and given the opportunity to incorporate its critiques of the model. In June of 1978 the parties settled out of court Described in John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, pg. 55-66.

Testing:

Before using the model in a prescriptive manner to suggest organizational changes or policy recommendations, an analysis was performed to ensure the prescribed recommendations are robust to parameter and structural uncertainty. In areas where there was uncertainty or disagreement on parts of the structure and decision rules, the model developers and an individual who did not participate in the modeling process performed sensitivity analyses in order to determine the impact of the uncertainty and/or disagreement. In these analyses, many of the parameters in the model were varied to extreme values in terms of magnitude and/or frequency either individually or in groups. In some of the cases, this process revealed that several areas that were debated before the analyses actually had little impact on the overall model and did not warrant further scrutiny. In other cases, the opposite was true. Additionally, some test cases revealed subtle logic errors in the model by magnifying them to the point where they could be identified and corrected.

Scenario Development, Testing, and Execution:

Shortly before the model configuration was frozen, a number of potential model simulation scenarios were identified for a preliminary analysis of NASA ESMD that would ultimately serve as a demonstration of the model's capabilities. The scenarios chosen for the preliminary analysis were derived primarily from interviewee comments, particularly those that occurred during the Safety Risk Survey. In reviewing the results of that survey, we noticed that there were a number of recurring themes in the interviewee responses. Once these themes were identified, we sorted the interview comments by theme and reviewed them to generate ideas for the scenarios. This led to a list of potential scenarios that was far too long to completely explore within the time span of this study. Of these, some were not well suited for analysis through system dynamics while others were perceived as higher priority than others. Therefore, we selected a handful to use in our final tests of the overall model structure. After incorporating the necessary updates to the model after this round of testing, we froze the model's configuration and explored the scenarios more deeply in our preliminary analysis of risk in the NASA ESMD. The results of this analysis and brief descriptions of these model simulation scenarios are provided in section 4.

3. THE MODEL

In discussing the ESMD System Dynamics Model, it is helpful to refer to the levels of abstraction defined in Figure 21. Moving from top to bottom, each successive level of abstraction contains more detailed information on the structure of the model. At the highest level, there are seven major feedback loops. These loops are implemented in the model through seven major modules (Level 2), each containing dozens of variables and low-level loops (Level 3). Each of these variables and low-level loops were derived from assumptions and conventions (Level 4) that were implemented through equations and data (Level 5). Due to the large scale of the model and the data collection effort, a comprehensive description of all of levels of abstraction is worthy of its own document. Therefore, the discussion in this section is limited to the major feedback loops in the model and the structure of the modules in which these loops are implemented (Levels 1 and 2). In other words, this section describes the model on the major causal-loop level and module level. Readers that are interested in the structure of the model on the variable and minor loop-level are advised to refer to Appendix D while readers interested in the assumptions and conventions-level should refer to Appendix E. A description of the data and equations-level of the model is not provided in this document, but is available online at <http://sunnyday.mit.edu/ESMD-model/> along with the model and a reader for viewing Vensim files.

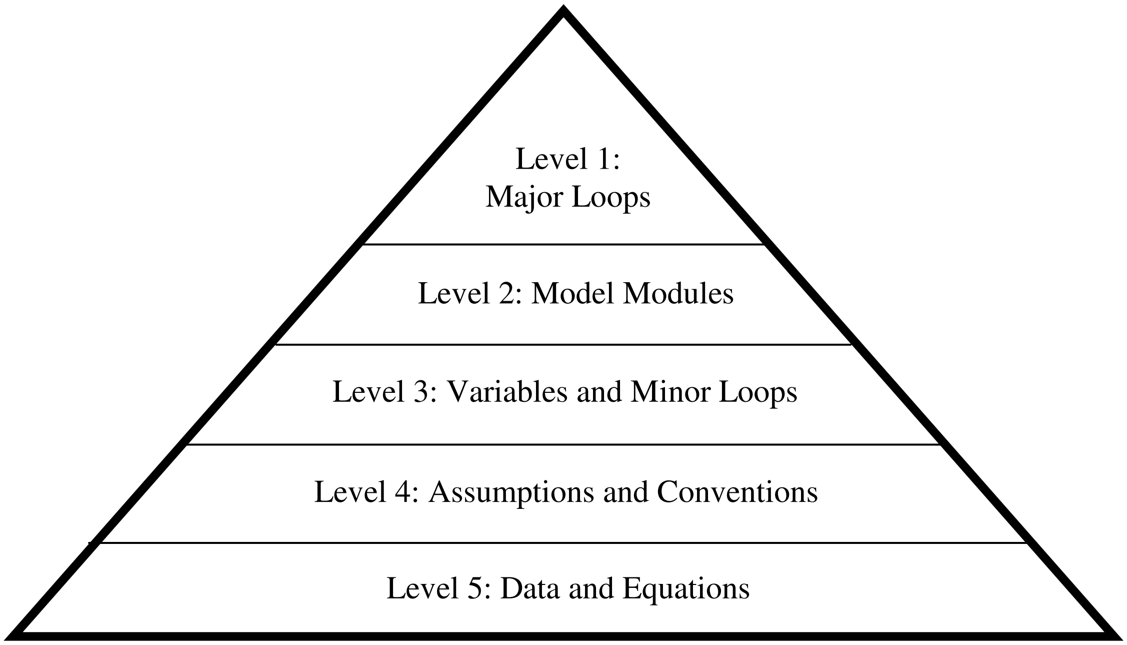

Level 1:
Major Loops
Level 2: Model Modules
Level 3: Variables and Minor Loops
Level 4: Assumptions and Conventions
Level 5: Data and Equations

Figure 21. The levels of abstraction for discussing the ESMD System Dynamics Model.

3.1 Overview

The safety engineering techniques we have created based on the STAMP accident causality model consider safety starting from the very beginning of system conceptual development and continuing through system design, implementation, and operation. The impact of the entire socio-technical structure on system safety is considered from the start. However, building safety into a new system and attempting to mitigate potential hazards during system development is very different from attempting to safely operate an existing system. This is one of the main reasons why the generic STAMP safety control structure is divided in two distinct columns, called System Development and System Operations, see Figure 1 and Figure 22. The two distinct columns "connect" at the bottom, near the Operating Process, where safety will be enforced during the operation of the physical system. For most systems, however, development and operation happen on different time scales simply because a system must be developed and implemented before it is operated. There may be exceptions to this rule, such as systems developed entirely through an incremental process where the development and operation are performed concurrently by starting with a very simple system and adding functions and capabilities while operating the system. However, for the type of complex systems with which we are concerned (i.e., large scale complex socio-technical systems), we assume that system development and operation will be mostly performed on different timescales, while allowing for overlap periods during transition from development to operations during partial or timed system deployment and during system maintenance and evolution.

3.2 Abstraction Level 1: Major Feedback Loops in the Model

The focus of our ESMD System Dynamics Model is on the dynamics occurring within the left column (system development) of the generic STAMP safety control structure (Figure 22). The most important high-level feedback loops in the model are shown in Figure 23. These loops were derived from the existing literature on the dynamics of project management and system development, as well as from dynamic safety archetypes and on the authors' direct interactions and interviews with project management professionals in NASA.

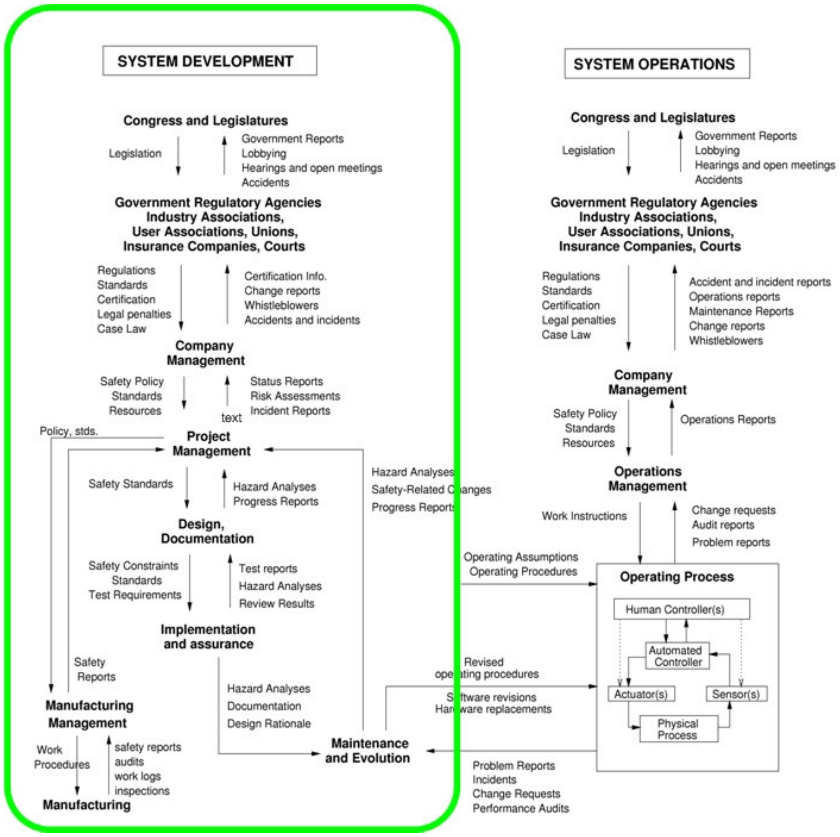


Figure 22. The generic STAMP system development and system operation structures.

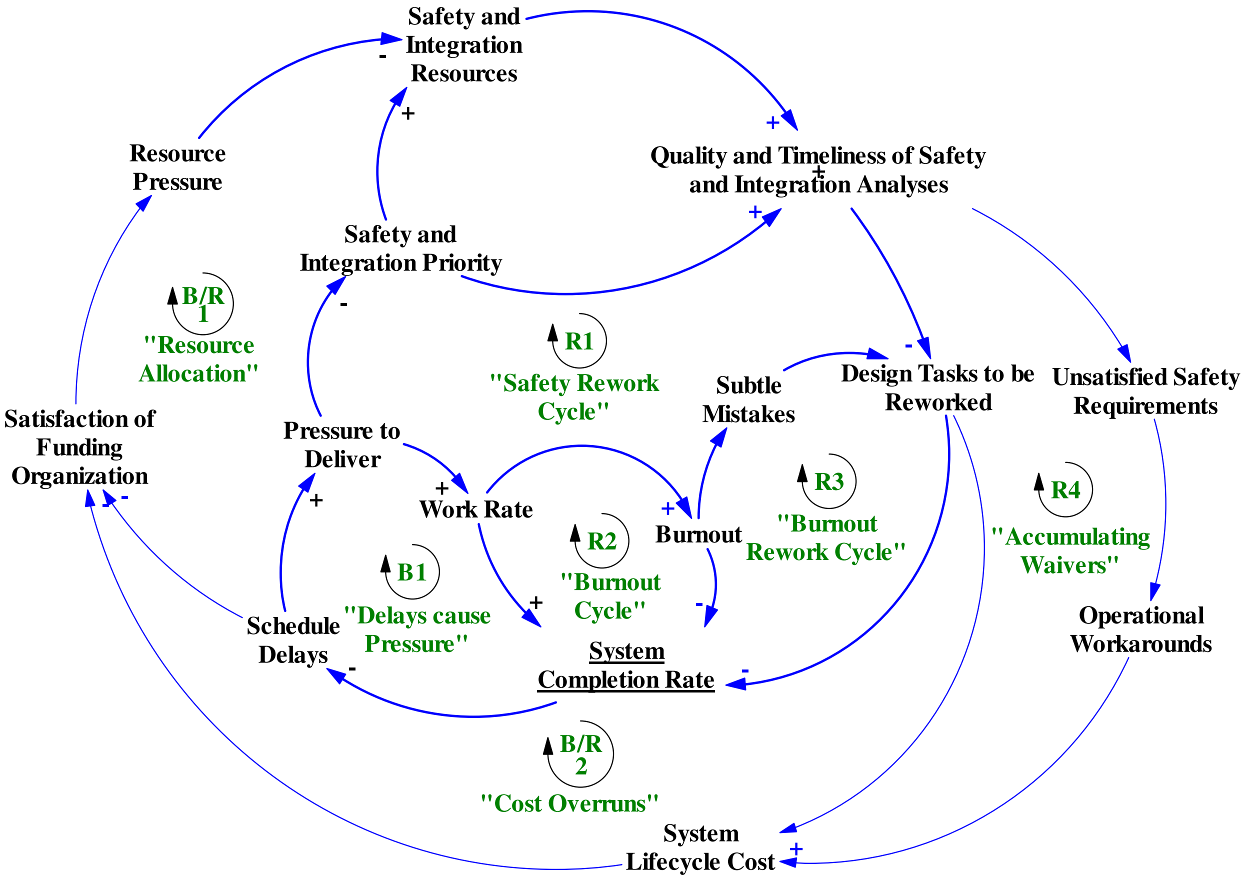


Figure 23. Simplified structure (i.e., Level 1 abstraction) of the ESMD System Dynamics Model.

The dynamics of these major loops (each of which is implemented by minor loops using a hierarchical approach to manage model complexity) are controlled in the model by dozens of additional variables (not shown in the figure) that track real system characteristics, such as the amount of resources (material and human) allocated to a particular project, as well as the number of tasks allocated, the number of tasks completed, and the number of safety analyses completed and used in design. In the remaining paragraphs of this subsection, each of these major loops is examined individually and in the following subsection the modules in which these loops are implemented are discussed.

Loop B1 - Delays Cause Pressure:

The first and arguably most critical balancing loop is Loop B1 labeled “Delays Cause Pressure”, which is the balancing loop for schedule pressure, shown in Figure 24.

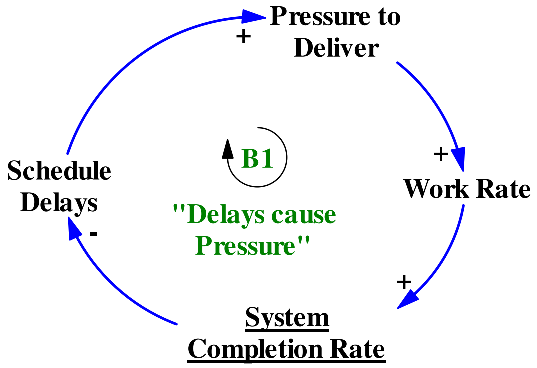


Figure 24. Loop B1: "Delays cause Pressure"

Loop B1 is responsible for system development being completed on or near schedule. As the system development completion falls behind, schedule delays start to accumulate, which leads to more pressure to accelerate system development and a faster work rate which eventually allows the system development to catch up with desired or planned completion rates and deadlines. As is, this simple structure allows the development to remain within schedule. For instance, if we assume a perfectly planned and executed project with 1,000 development tasks[57] to be completed within 100 months at a constant rate, the fraction of completed design tasks for this theoretical project should follow a pattern similar to that of Figure 25.

[57] The term "development tasks" is a generic term used here that includes all tasks required to develop and deliver a system, including requirements planning and definition, design, review, manufacturing, testing, and approval. Further iterations of the model will make distinctions between some of these activities and will have an increased resolution.

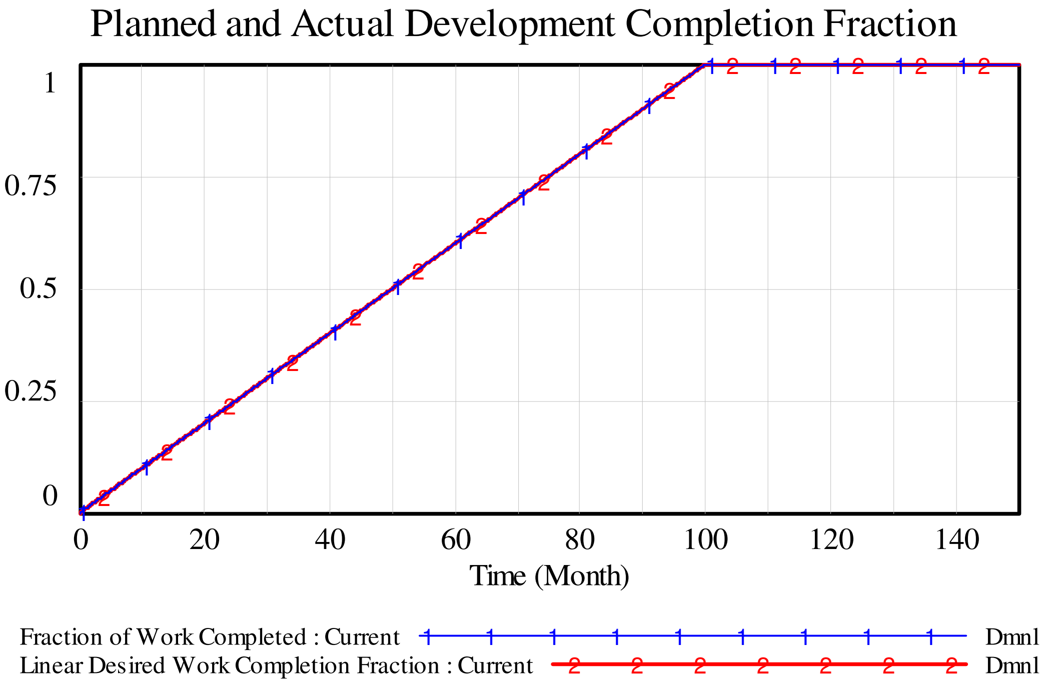


Figure 25. Planned and actual fraction of completed development task assuming perfect and linear system development rates.

However, if external disturbances such as a change in requirements or a change in workforce capacity affect this equilibrium condition, the B1 balancing loop for schedule pressure will act to restore the system to its equilibrium position. As a first approximation, the balancing loop can be seen as a simple proportional controller.[58] If the actual completion fraction falls behind the desired completion fraction, schedule pressure will be applied to restore equilibrium. The amount of schedule pressure applied depends on the proportional gain—P gain—of the controller.[59] For example, let's assume an externally applied decrease of 20% in workforce capacity at time t = 30 months. In the case where no proportional control is applied, the completion fraction starts to diverge at time t = 30 months and the divergence increases until the project is finished, see Figure 26.

[58] In control theory, a controller is a device or entity (e.g. electro-mechanical actuator, digital computer, human operator) in a system that imposes an action on the system in order to drive a system variable to a desired value and/or maintain it at that value. The magnitudes of the actions imposed by a simple proportional controller are linearly related to the difference between the current value of the controlled variable and the desired value of the variable. In other words, a simple proportional controller exerts more "effort" or "gain" to control the variable as the value of the variable moves farther away from its desired value. Thus, if one were to consider a manager as a controller using a proportional control law to keep his team on schedule, the amount of schedule pressure the manager would put on his employees at any given time would directly depend on how far the team is behind schedule at that time.

[59] Gain is a term used in control theory to scale the response of the controller to a given difference between the current and desired value of the controlled parameter.

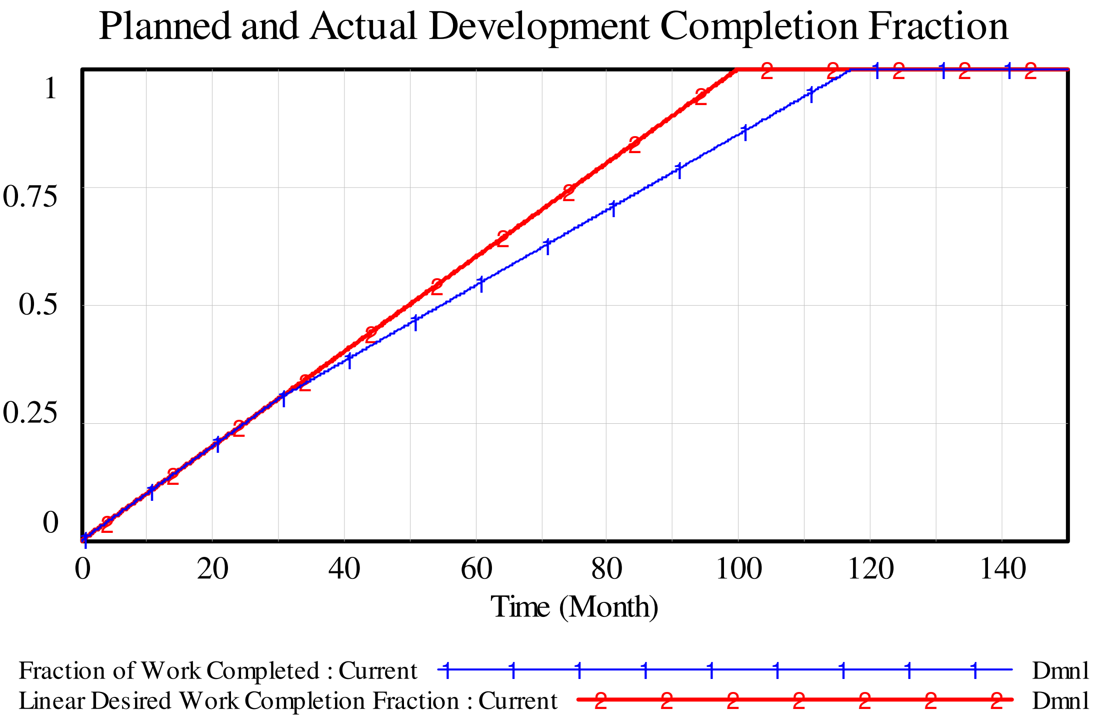


Figure 26. The impact of a disturbance to the design task completion rate at time t = 30 months if P gain = 0.

When proportional control is present (i.e. P gain > 0), the controller applies schedule pressure to reduce the schedule delays. The more schedule pressure that is applied (i.e. the higher the P gain), the more schedule delays are reduced. However, it should be noted that once the equilibrium is disturbed, proportional control is not sufficient to completely bring the project back on schedule. This can be easily explained in terms of control theory because the steady state error to a ramp input—which is similar to a perfectly planned linear project—does not converge to zero with proportional control alone (see Figure 27). In other words, because proportional control only considers the current state of the system and does not account for issues such as future changes in the desired value of the controlled variable—in this case, the fraction of design tasks completed—there will always be an "error" or difference between the current and desired value of the controlled variable if the desired value continuously changes.[60]

[60] Proportional control also does not account for delays in the response of the system to control actions and the physical limitations on the minimum amount of gain that the controller can impose on the system. Therefore, even if the desired value of the controlled parameter is constant, proportional control will lead to a situation where an error always exists because the system will overshoot and oscillate around the desired value or decrease the error to a level that is both non-zero and below what can physically be removed by the controller (e.g. one Newton of force is required to eliminate the error, but the controller is only able to apply five Newtons of force on the system).

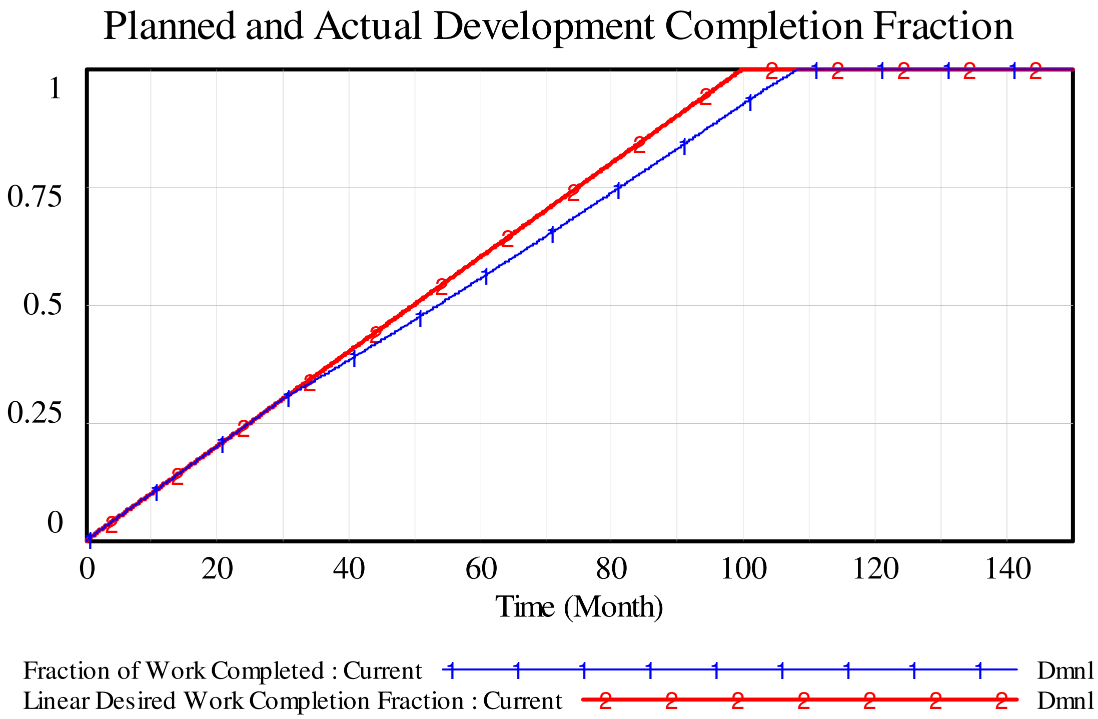


Figure 27. The completion fraction over time with a disturbance at time t = 30 months and a P Gain greater than zero.

Adding integral control (I gain) is a slightly more sophisticated and realistic way of bringing a project back on schedule. In determining the appropriate magnitude of its control actions, an integral controller considers the cumulative difference between the desired value of the controlled variable and its actual value over time. In other words, unlike a proportional controller, an integral controller uses information from the past performance of the overall control system. In the context of schedule pressure, a manager utilizing both proportional and integral control might apply more or less schedule pressure than a manager that only uses proportional control because he/she "learns" from past experience that proportional control is not sufficient to properly bring the project back on schedule. The result of this compensation is shown in Figure 28, where integral control has been added to the system represented in Figure 27 the steady state error is reduced to zero (i.e., the project eventually gets back on schedule after the initial disturbance) because the integral controller effectively compensates for the failings of the proportional controller.

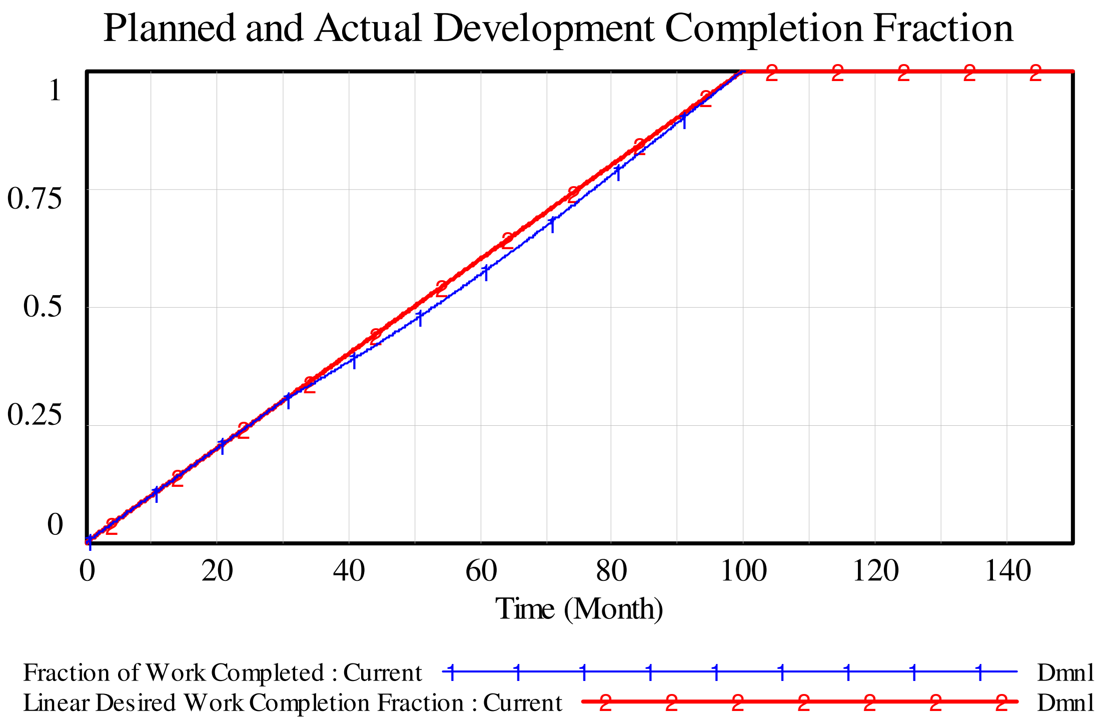


Figure 28. The completion fraction over time with a disturbance at time t = 30 months and nonzero P and I Gains.

Loop R2 - The Burnout Cycle:

The "Delays cause Pressure" balancing loop is the main feedback mechanism responsible for keeping the project on schedule. However, other reinforcing mechanisms may reduce the actual impact of this loop on schedule completion. One important loop is the "Burnout Cycle" loop that limits the impact of the "Delays cause Pressure" loop as shown in Figure 29.

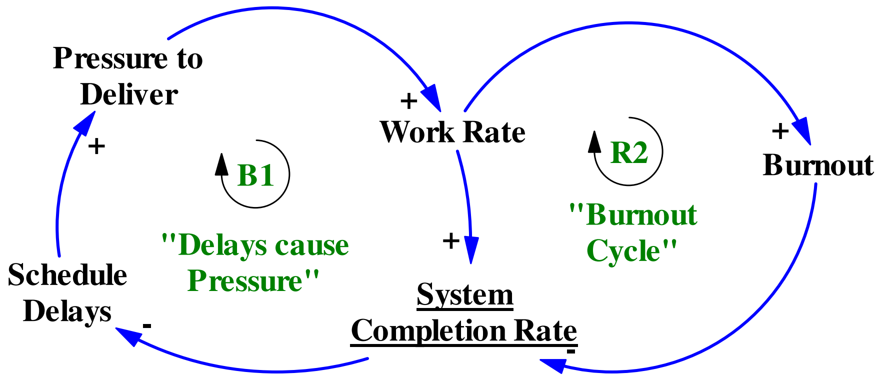


Figure 29. The "Burnout Cycle" loop added to the "Delays cause Pressure" loop.

The burnout loop mitigates the impact of schedule pressure on completion rate because as the employees are asked to perform more work, burnout starts to occur and productivity decreases over time when employees become tired and overwhelmed. Consequently, as shown in Figure 30, adding the burnout loop to the previous structure reduces the impact of the "Delays cause Pressure" balancing loop, preventing the project from getting back on schedule, despite the planning efforts (i.e. proportional and integral control) of the project managers.

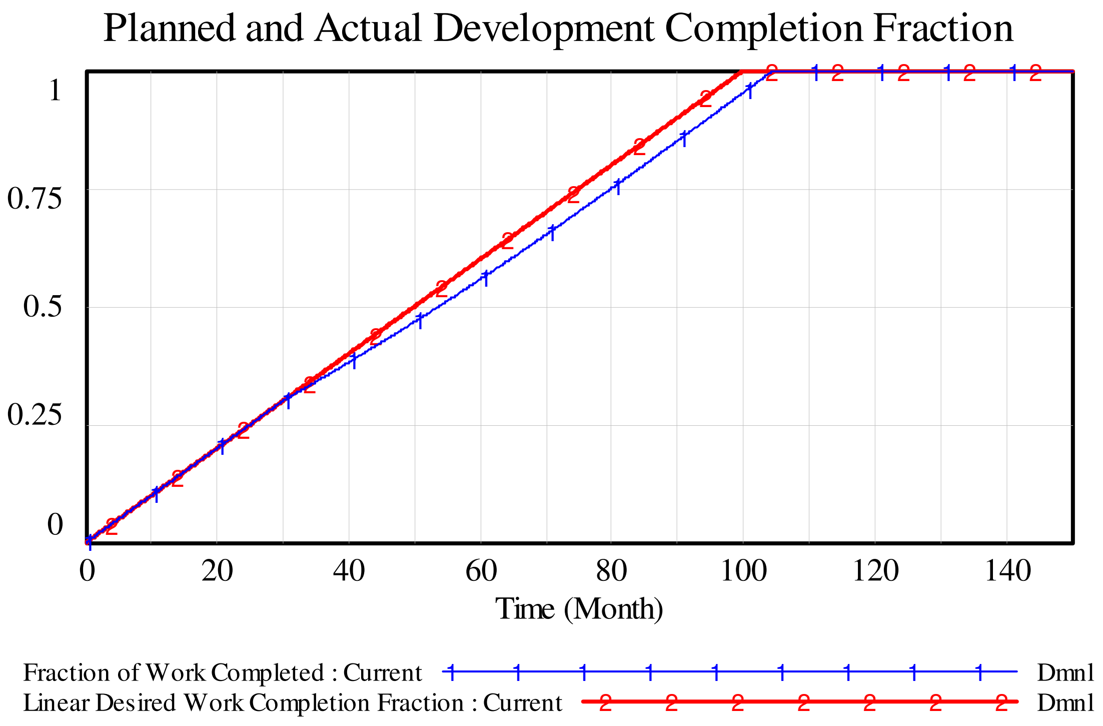


Figure 30. The fraction of work completed over time when the "Burnout Cycle" is added to the model.

Loop R3 - The Burnout Rework Cycle:

Another reinforcing loop affecting development completion is the basic "Rework Cycle". The "Rework Cycle" is a standard component of development dynamics and has been discussed in great detail in the project dynamics literature.[61,62,63,64] The dynamics behind this loop were also described by several of the NASA employees interviewed. As burnout increases, people are overwhelmed and while burning the midnight oil to remain on schedule, they make subtle mistakes that create the need for more rework. In Figure 31, this reinforcing loop, the "Burnout Rework Cycle" loop, is added to loops B1 and R2.

[61] David Ford (1995), *The Dynamics of Project Management: An Investigation of the Impacts of Project Process and Coordination on Performance*. Ph.D. Dissertation, Dynamic Engineering Systems, Massachusetts Institute of Technology.

[62] Kimberly Reichelt and James Lyneis (1999), "The Dynamics of Project Performance: Benchmarking the Drivers of Cost and Schedule Overrun." *European Management Journal*. Vol. 17, No. 2, April 1999. pp. 135-150.

[63] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, pg. 55-66.

[64] James Lyneis, Kenneth Cooper, and Sharon Els (2001), "Strategic management of complex projects: a case study using system dynamics." *System Dynamics Review*. Vol. 17, No. 3, Fall 2001, pp. 237-260.

There is strong evidence that the relationship between the "pressure to deliver" and subtle flaws and mistakes is not linear; several NASA employees noted that schedule pressure can have a positive effect on the workforce if it is applied correctly. In other words, these employees believed that too little schedule pressure would lead to an unmotivated workforce and too much schedule pressure would lead to a burned out workforce susceptible to making subtle mistakes. This claim effectively describes the classical Yerkes-Dodson Law, which states that performance is increased up to a point by cognitive arousal/stress and decreased by arousal/stress levels beyond that point.[65]

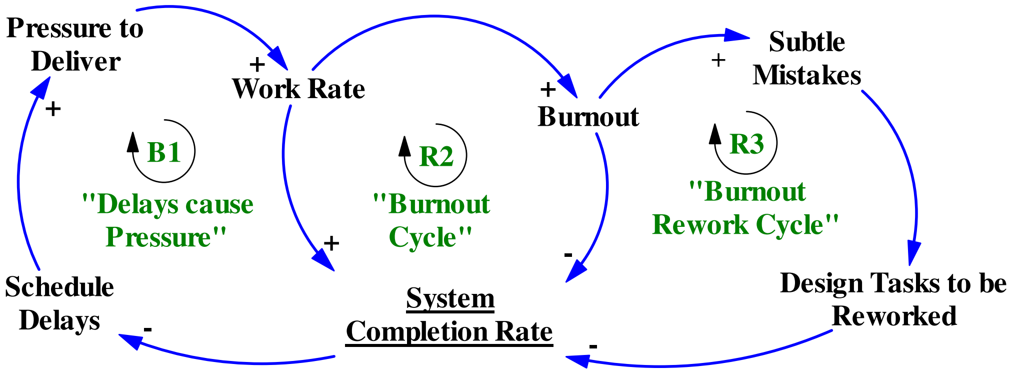


Figure 31. The "Burnout Rework Cycle" loop added to loops B1 and R2.

Figure 32 and Figure 33 show the impact of the "Burnout Rework Cycle" (Loop R3) on the fraction of development tasks that need to be reworked because of subtle mistakes and the fraction of work completed over time. As workload increases beyond the optimal point and burnout starts to take effect, the fraction of tasks requiring rework increases until the project is completed. Ultimately, this process increases the overall cost of system development by stretching out the development cycle and thus creating inefficiencies in it.

[65] Yerkes, R.M. and Dodson, J.D. (1908), "The relation of strength of stimulus to rapidity of habit-formation." *Journal of Comparative Neurology and Psychology*, Vol. 18, pp. 459-482

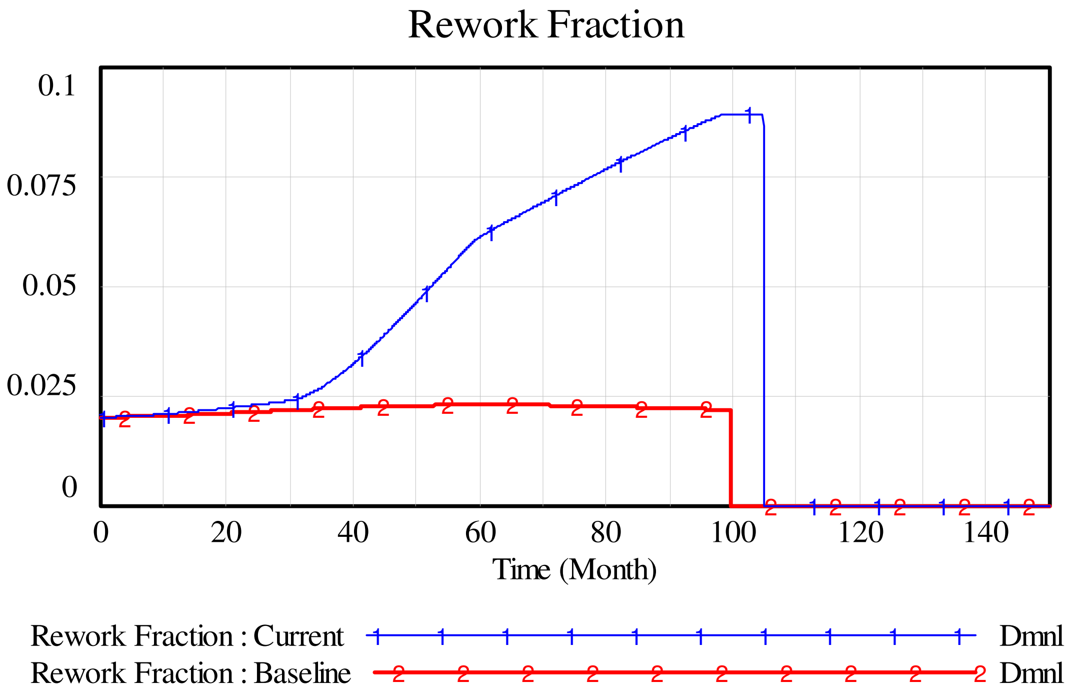


Figure 32. The impact of the "Burnout Rework Cycle" on the fraction of design tasks that must be reworked.

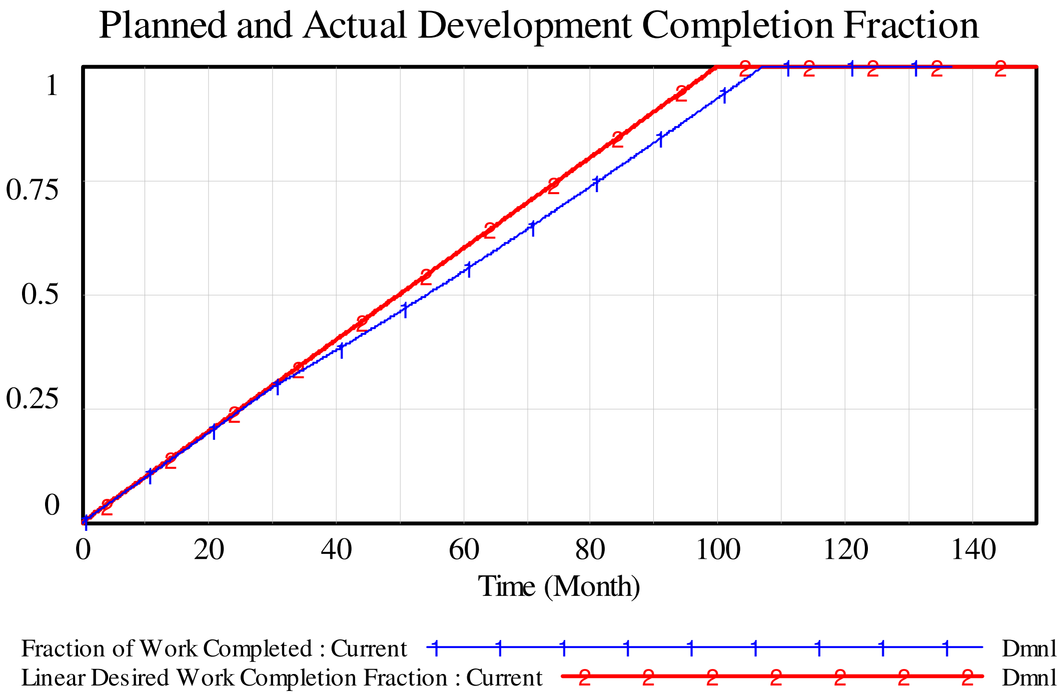


Figure 33. The impact of burnout and rework on the fraction of work completed over time.

Loops R1 and R1b - Safety and Integration:

Other loops having an impact on system development are related to the "Quality and Timeliness of Safety and Integration Activities". As schedule pressure increases because of disturbances or development delays, the effective priority of safety and integration activities decreases. As schedule pressure increases because of development delays or overoptimistic planning, more effective priority is allocated to getting the hardware built and delivered, at the expense of less visible activities such as safety and integration. At a high level, lower priority of safety and integration activities reduces the impact, quality, and timeliness of analyses through soft factors such as a loss of influence and power of the safety and integration activities and reduced scope of these activities as most of the effort and resources are allocated toward product delivery. Similarly, the inevitable resource pressure coming from Congress or the NASA administration will be aimed primarily at activities not directly and immediately critical to system delivery. Those two reinforcing feedback loops are shown respectively as the "Safety Rework Cycle" and "Resource Rework Cycle" loops—loops R1 and R1b, respectively—in Figure 34.

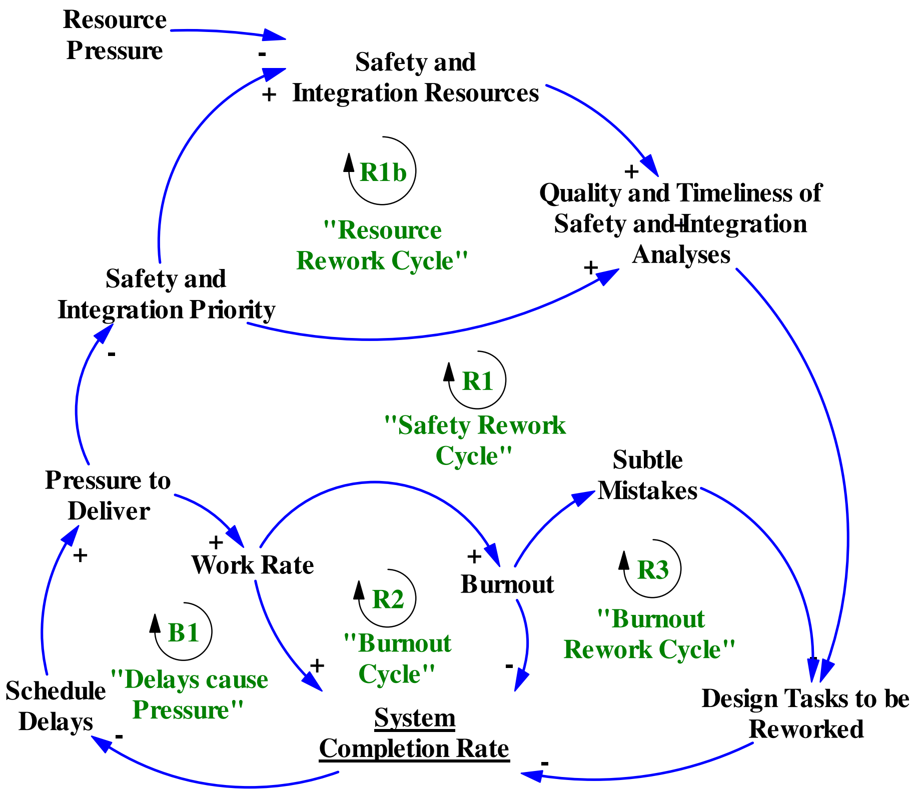


Figure 34. Loops R1 and R1b added to Loops B1, R2, and R3.

Comments that we collected during the interviews support this claim. One high-level NASA manager described a dynamic where resource pressure from Congress causes project managers to scope their projects such that they must accept considerable cost and schedule risks. These risks typically result in cost overruns and delays that upset Congress and create pressure to de-scope the project and/or cut back on employee training and other safety-critical functions.

The impact of the R1 and R1b outer loops on the development dynamics is significant—perhaps even more than the reinforcing loops documented previously. While the impact of development task sequencing, overwork, burnout, and mistakes during a project has been addressed extensively in the literature, the impact of the safety and integration activities on the strength of the rework cycle has not been the focus of attention. This lack of attention exists despite the fact that for the development of complex safety-critical systems, safety, integration, and software development activities are likely to be the bottleneck. Consequently, the thoroughness, quality, and timing of safety and integration activities must be modeled as accurately as possible in order to improve complex systems development processes. Figure 35 and Figure 36 show the cumulative impact of adding the effect of the R1 and R1b loops to the previous feedback structure. The cumulative impact is significant, creating an order of magnitude increase in the fraction of tasks requiring rework, which in turn cause large development delays, with associated cost overruns. The high-level formulations used for this model could be further refined, but in the end, the cumulative effects of the three reinforcing loops create significant delays, cost overruns, and safety and quality problems.

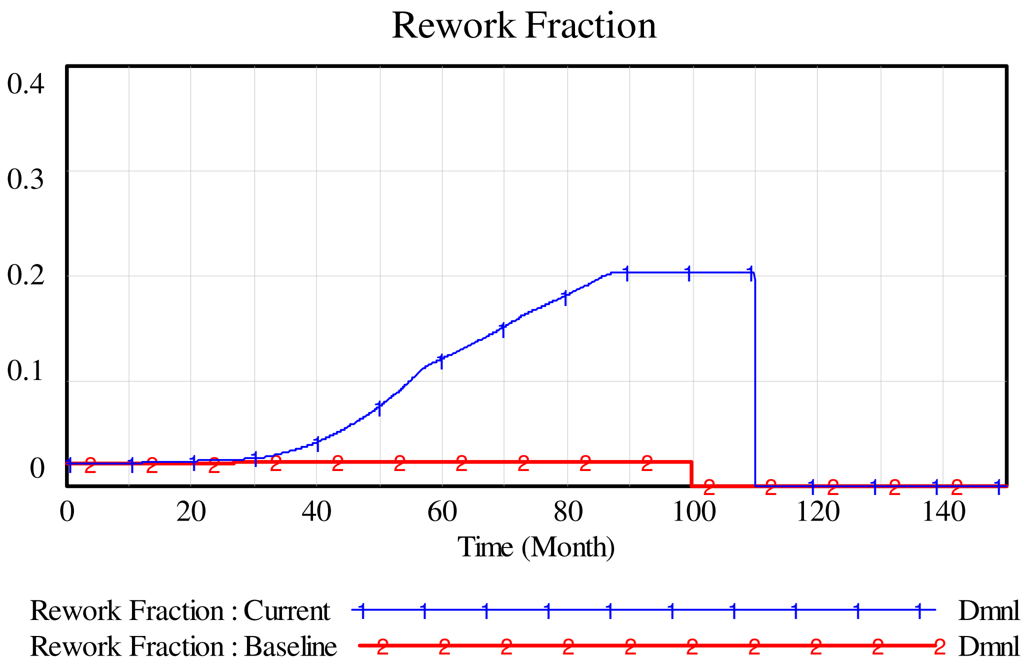


Figure 35. The impact of Loops R1 and R1b on the fraction of development tasks that must be reworked.

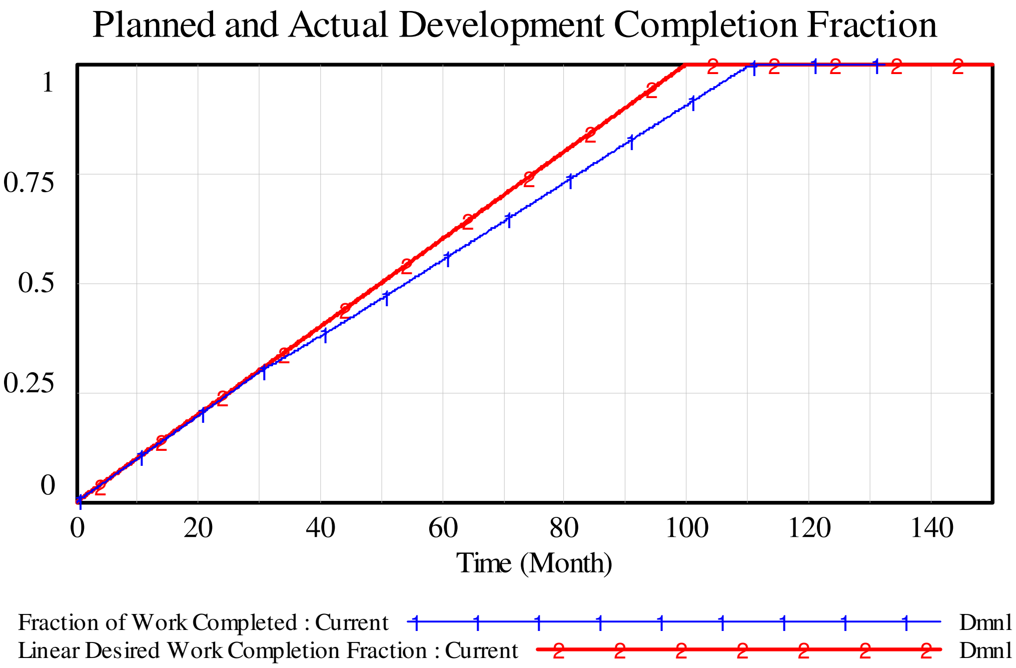


Figure 36. The impact of Loops R1 and R1b on the fraction of work completed over time.

Outer loops - Waivers, cost, and resources:

The main high-level loops that create the system development dynamics were described in the previous subsections. Outer loops that may not necessarily have an impact on the system during development but might impact operational characteristics are shown in Figure 37 using dotted causal links. Lifecycle cost was a recurrent theme during interviews. It is often the case that lifecycle cost is informally defined by system designers and manufacturers as the costs incurred from the start of system development up to hardware delivery. In many instances, operating cost is not explicitly included in lifecycle cost. The rationale is that it is very difficult to estimate operating cost before the system is delivered and operated. Indeed, cost estimation is very difficult and data intensive, especially for radically new, large-scale complex systems including a good deal of software and new technologies. Nevertheless, an attempt is made in our model to develop a metric for relative lifecycle cost because NASA's space exploration system will be operated for a long period of time and with limited reuse between missions.

The usual method for evaluating cost is to divide the work to be performed according to a standard work breakdown structure, evaluate cost for the development and/or acquisition of each component or subsystem, and assemble the cost of subsystems, while allowing for system engineering and integration costs, as well as management and overhead. At our level of analysis, the resolution of standard cost estimation methods is too high to be useful. Instead, we create a system lifecycle cost variable based on a few proxy variables. According to interview data, two main factors will influence the cost overruns for a project. The first factor is the amount of work done to correct mistakes and problems found at any stage of system development. The second factor is the project or program completion time relative to planned time. Those two factors are correlated. Unless enough management reserves are available to allow for additional development work, there are two possible options whenever a problem is discovered: either (1) the problem will be accepted and requirements that define it as a problem will be waived or (2) the program completion will be delayed in order to use the resources budgeted for the following fiscal cycle.

Cost overruns and schedule delays have an impact on the satisfaction of project sponsors or funding organizations. This impact is very important because it can switch the polarity of outer loops from reinforcing to balancing or vice versa. If the project sponsor reacts negatively to delays and overruns by adding more resource pressure, the polarity of the loop will be reinforcing, creating more delays and problems. On the other hand, if the sponsor reacts by adding resources to alleviate delays and problems, the outer loops are balancing and pressures are diminished. The response of project sponsors and funding organizations usually depends on project context and criticality, as well as on the magnitude of delays and overruns.

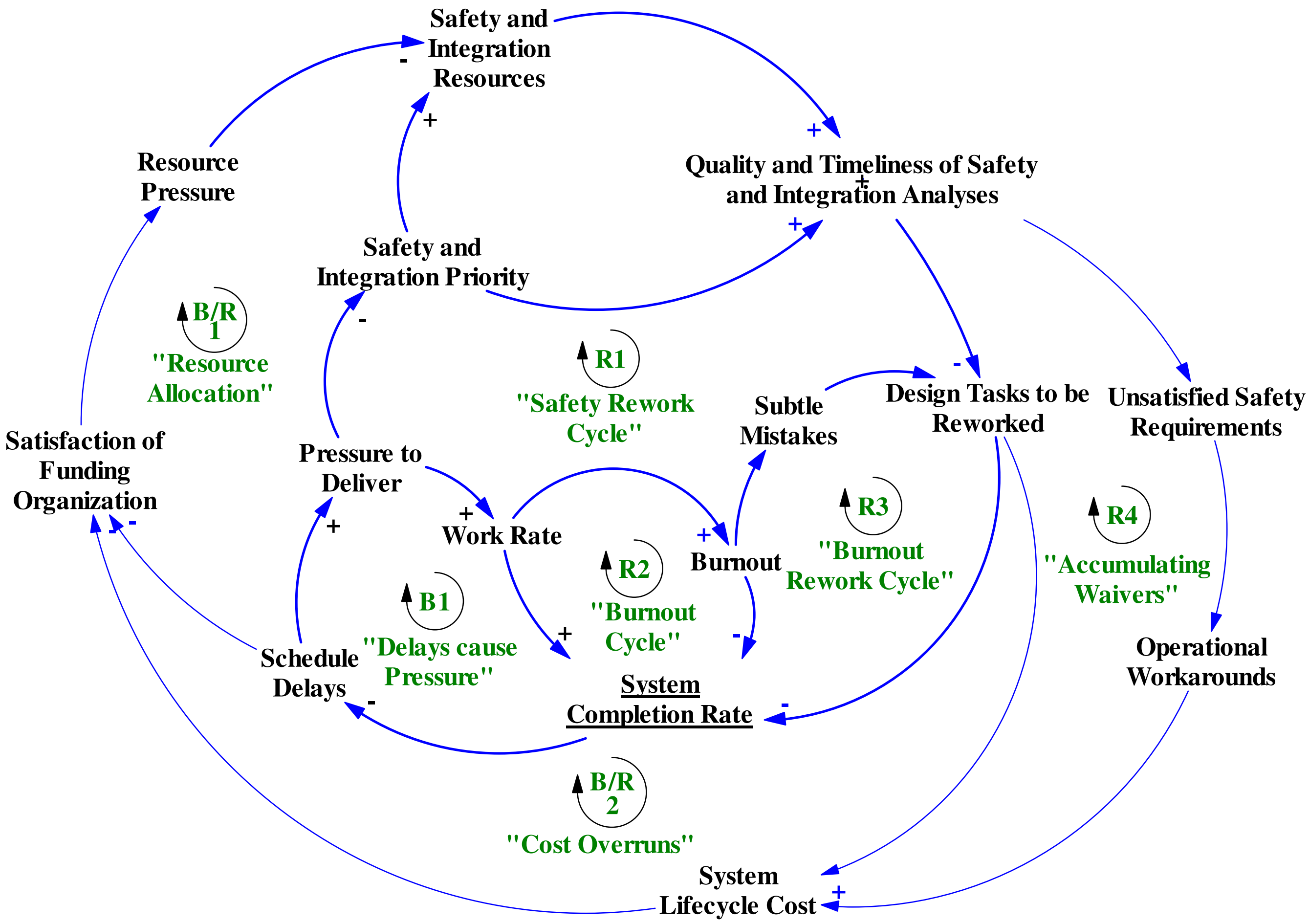


Figure 37. The complete Level 1 abstraction of the ESMD System Dynamics Model.

3.3 Abstraction Level 2: Modules of the Model

The model created for the ESMD project includes seven independent structural modules, some of which are tightly connected and grouped under a common area. The model modules are:

1. Congress and Executive (White House)
2. NASA Administration and ESMD
3. Exploration Program and Project Management
4. Engineering – Technical Personnel Resources and Experience
5. Engineering – Effort and Efficacy of Technical Personnel

6. Engineering – System Development Completion
7. Safety and Mission Assurance - Effort and Efficacy of System Safety Analysts

The following subsections provide a description of the individual modules included in the complete model. The model structure of each individual module is provided in Appendix D and online at <http://sunnyday.mit.edu/ESMD-model/>.

.

Congress and Executive (White House) Module:

The Congress and Executive module is responsible for defining the vision for the U.S. space exploration enterprise, as well as providing the level of funding necessary to develop and operate a safe exploration system. Many external factors affect the ability and willingness of the Congress and Executive to define and implement a realistic and safe system. Some of these external factors include: political uncertainty, time horizon of political objectives, and the Executive Branch initial leadership and vision for the program. These three external factors influence the initial compromises in system design along with the criticality of the program. In turn, the initial compromises in system design will have an impact on the life cycle cost of the system. This latter model variable, when combined with technology uncertainty, will increase the operational costs of the system.

In addition, technology uncertainty affects the stability of system scope and requirements. The coherence and consistency of program policy can counterbalance this effect. The ability of NASA to market the space exploration program will influence the effective criticality of the program. This ability is very important because a program perceived as being critical is less likely to be canceled, compromised, or subjected to budget cuts. Uncertainty in the development environment is a factor that affects the amount of outside contracting desired by the Agency. Uncertainty in a development environment is caused by a combination of technology uncertainty and likelihood of program cancellation. While we were not able to find hard quantitative evidence that uncertainty in the development environment affects the amount of reliance on private contractors, many of the interviewees confirmed that a relation exists. The Congressional and Executive module receives project cost and performance reports from NASA. Cost overruns have a negative impact on Congressional satisfaction with the program. Similarly, constituency support can also be influenced by cost overruns. However, other factors also play a role, including the visibility of the program and the Congress and Executive ability to market the program to constituents. In addition to cost, the perceived program performance also has an impact on Congressional satisfaction with the program. A highly visible project perceived to be on schedule and within cost budgets and providing quality jobs in selected congressional districts is likely to be perceived as highly successful and be strongly supported by members of Congress. On the other hand, if Congress becomes dissatisfied with a project not perceived to be critical to national objectives, inevitable budget cuts are likely to be directed toward this particular project.

Another theme often mentioned by interviewees (and included in our model) is that of Congressional risk tolerance and risk perception. Space flight is a risky business. While every effort must be put in place to mitigate hazards and improve safety as much as possible, many interviewees mentioned a mismatch between risk perception at the Congress and Agency levels. Interviewees felt that this mismatch could lead to unrealistic safety, cost, and schedule expectations from Congress.

Assumptions and Conventions:

Congressional and Executive dynamics are highly complex. In this module, we did not attempt to precisely quantify the relationships between different variables. Instead, we merely tried to improve our confidence in the existence of these relationships. In the baseline model, the variables in this module are in equilibrium, that is, unless the values of external variables in this module are modified, the module will have negligible effect on the dynamics of the system. Nevertheless, all the relationships have been implemented in the model, thus allowing us to test Congressional and Executive policies as well as scenarios where external events affect national priorities and Agency funding. Similarly, in the baseline model, NASA's budget is exogenous, that is, based on existing predictions and is not affected by national priorities and future Congressional satisfaction. The model is equipped to relax this assumption by making part of NASA's budget allocation dependent on Congressional satisfaction with the program.

NASA Administration and ESMD Module

Overview:

The purpose of the NASA administration and ESMD module is to identify the agency level policies, requirements, and guidelines that will enable the development of a safe and successful exploration system. The Agency receives directives and funding from Congress and then allocates resources according to program needs. However, NASA has limited flexibility in resource allocation because some of the budgets associated with larger programs are dictated at the Congressional level. For example, by the mandate of the President, the US space shuttle program has to be supported until it is retired around 2010. This and other constraints on resource allocation flexibility take up a significant portion of NASA’s approximately $17 billion annual budget. The primary function of the NASA Administration and ESMD module is to allocate resources (human and material) to different programs while respecting the constraints imposed by Congress and presidential administrations.

Detailed Description:

In addition to dealing with budget and financial matters, the Agency and its directorates are also responsible for providing programs and projects with a highly qualified and trained civil servant workforce. This workforce is drawn mostly from the individual NASA centers, which provide the institutional technical knowledge and skills necessary for a safe and successful exploration enterprise. The technical workforce available at the centers is then matrixed to the individual programs and projects based on technical needs and the availability of funding.

ESMD monitors the progress and cost of the individual programs under its responsibility. The incoming resource pressure from Congress affects NASA and ESMD by reducing resources available for safety training and improvements, as well as potentially compromising the quality of safety oversight provided to individual programs and projects by NASA/OSMA and ESMD. In addition to these effects on safety, budget pressure flows downstream and affects the resources available to develop the exploration system.

The NASA Administration and ESMD module has very few exogenous inputs. One of these external inputs is the technology uncertainty variable included in the Congress and Executive module. This exogenous input influences the management and technical personnel’s understanding of the physical process and system development environment. The technology uncertainty variable is not meant to have a precise numerical value. Instead, it is used to investigate scenarios where the chosen system architecture includes completely proven or field-tested technologies versus scenarios with new, undeveloped technologies. Another external input is the planned profile of work completion. Projects are usually not completed in a linear way. There are project phases that require a larger workforce and project managers can have varying levels of flexibility in hiring support and procurement contractors to supplement their workforce during critical phases. For the

ESMD baseline model, we made the work completion profile proportional to the total ESMD budget allocation (confirmed and projected) at any point in time. This budget-weighted profile is a first order estimate that may not be entirely accurate, but we believe it is a better approximation of work completion than a linear profile.

The NASA Administration and ESMD module monitors the amount of reported safety problems throughout system development and adjusts safety budgets and policies accordingly.[66] An increase in the occurrence of system safety problems creates more NASA Administration perceived system risk and a shift of NASA Administration safety priority, resulting in increased efforts to improve safety through training and additional resources. The strength of this balancing feedback may be variable, and a slow adaptation may occur that creates desensitization to increases in safety problems. This phenomenon can be modeled through an anchoring and adjustment dynamic scheme,[67] where increases in problem reports are relative to the recent usual number of problems reported. This natural adaptation tendency occurs unless there is an independent outside anchor to the number of problem reports. Benchmarking other industries might be a way to approach the adaptation problem.

Exploration Systems Program Management Module

Overview:

The purpose of the Exploration Systems Program Management module is to mimic the behavior of program and project managers during real systems development. Program managers have to ensure that the system under development meets technical requirements, including both safety and performance requirements while remaining within budget and on schedule. Program managers use multiple levers to achieve these objectives, including reshuffling schedules, reallocating resources (human and material), and applying various pressures to lower-level managers, engineers and other technical workers.

The program management module is essentially a control system trying to regulate system development. In general, the task assigned to program management is a multi-objective control problem that may require trade-offs between different system qualities. In most cases, the overall objectives will be dictated by higher-level elements of the control structure such as the NASA Administration, the Executive Branch, or Congress, but the implementation details will be the responsibility of the programs and projects. For example, the system scope and high level technical requirements as well as the budget and workforce available are usually constraints applied by the Agency or the directorate, which are based on desires, requirements, and constraints at the Congressional and Executive level. Program managers have to report to the administration at various system development milestones. Another potential constraint is the amount of contracting desired by Congress or the agency. In this model, resources are allocated to five different bins: technology development, system integration, safety analyses, system design, and other ESMD projects.[68] The total amount of in-house resources available has a large impact on system

[66] System safety problems in development are different from safety problems in operations, such as accidents. A system safety problem in development is defined here to be a realization by the development team that a design will not satisfy safety requirements as specified and will thus necessitate a redesign or the acceptance of reduced capability to enforce safety constraints.

[67] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, pp. 532-535.

[68] *Other ESMD Projects* is a model variable in which to place ESMD employees that are not working on the development project(s) being tracked in a given simulation run (e.g. if the development of the CEV and CLV is being tracked in a given simulation run, but not the CaLV, then employees working on the CaLV should be placed in the other ESMD projects bin).

development. It allows project managers to allocate sufficient resources into the five different bins while keeping management reserves to account for uncertainty, disturbances, and unplanned events. In case of a high likelihood of missing a development deadline, program management can place requests for deadline extension or in some cases request a decrease in system scope, which translates into either dropped or waived requirements.

Another way to alleviate the likelihood of missing schedule is to improve the rate of design completion. This improvement in design completion rate can be achieved through the allocation of more resources to design or by applying pressure to work faster. If the project is perceived to be over budget, management can place requests for additional resources or deadline extensions (which ultimately translate into more resources) or try to improve completion rate, which also reduces fixed costs.

Just as at the Agency level, the amount and severity of safety and integration problem reports will have an impact on the amount of energy and resources expended by project management to improve system safety. If the safety analysis completion rate falls behind the development completion rate, more resources might be allocated to safety in order to catch up. Resources are limited, however, and allocating more resources to safety means that fewer resources will be available for other activities such as design or integration and vice versa. The impacts of various resource allocation strategies are discussed in a scenario presented later.

System Development Completion and Safety Analyses Module

Overview:

The System Development Completion and Safety Analyses module is at the core of our ESMD system dynamics model. It includes three different flows that have to be synchronized and coordinated to produce a final integrated product. The three flows are: technology development, system development tasks, and safety analyses. The timing of these flows is critical. Late technologies cannot be used in the design without significant development delays. Similarly, late safety analyses might delay design or might not be used in design decisions, resulting in an unsafe system. In addition, some development work might have to be redone if problems are found along the way. This rework causes delays in both the design and safety activities, and thus further increases schedule pressure. System engineering and integration is responsible for making sure that the three flows of technology, design, and safety merge in a synchronized and coordinated manner.

Detailed Description:

The three flows of technology, design, and safety are illustrated below in Figure 38.

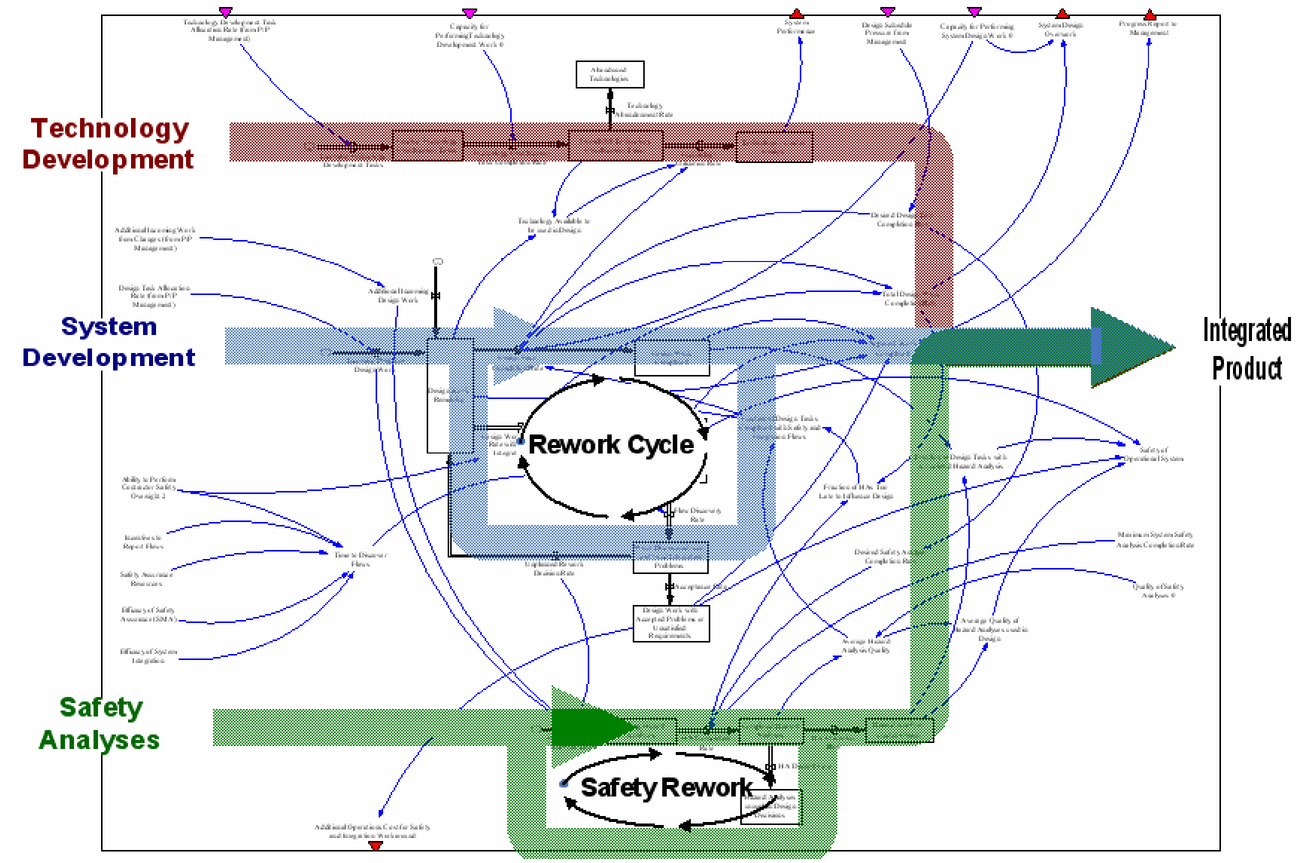


Figure 38. The flow of technology development, system development, and safety analysis in the System Development Completion and Safety Analysis module.

The first flow is that of technology development. Once technology requirements have been defined, technology development work has to be completed on time for a specific technology to be available in design. Some technologies might be abandoned along the way because of changing requirements or external factors. Other technologies might not be ready on time for design or deployment. In some cases, a technology might not live up to its promises, thus requiring more investments, resources, or time. Some of these technologies might have to be abandoned or replaced by an already available technology. Good technology requirements planning should include "off-ramps" to minimize the impact of technology abandonment.

The second flow is that of development tasks. Initial system requirements get transformed into the development tasks to be accomplished. Development tasks get completed according to the current development capacity, which is a function of the resources and workforce available as well as the workforce productivity. These factors, in turn, affect workforce experience, training, overwork, and schedule pressure. Once development tasks are completed, they are submitted for review, testing and approval. Subsequently, some tasks will be completed, while others will be found to have safety or integration problems that will require changes and rework—hence the *Rework Cycle*. The percentage of tasks to be reworked will depend on many factors including: availability of information from hazard analyses, efficacy of system integration, ability to perform contractor safety oversight, efficacy of testing, efficacy of safety assurance, design schedule pressure from management, mistakes made by overworked or burned out development personnel, and incentives to report problems. At any point in the development cycle, changes in requirements may necessitate the abandonment of some requirements or completed designs, as well as the introduction of new requirements to be transformed into development tasks. A scenario to be discussed later addresses the impact of changes along the system development life cycle.

The completion of safety analysis tasks mirrors the completion of development tasks through what is referred to as a *non-conserved coflow structure.*[69] However, the timing of the two flows may not be synchronized in every case. If the information from safety analyses is not available at the time when design decisions have to be made, two outcomes are possible: either (1) a decision will be made without the proper safety information or (2) development will be delayed while waiting for safety analyses to be completed.[70] Neither outcome is optimal. If safety analysts work hand-in-hand with engineering and system engineering and integration is performed correctly, the safety and development flows should be tightly connected and the safety analyses should be performed at the same time as development tasks. While this synchronization of safety analysis and design task completion is an ideal situation, it may not always reflect the way things are done in the ESMD or in typical system development activities. Because it is very difficult to have the safety information available exactly when it is needed, a good approach is to try to anticipate safety analysis needs in order to have a head start on development tasks. Anticipating needs may not always be possible because of the highly iterative nature of development activities, but it should be attempted when possible. Otherwise, the workforce may choose to accelerate the completion of safety analyses by cutting corners and reducing the fidelity and quality of safety analyses performed. In addition to keeping track of safety analyses performed, a coflow structure is used to monitor the quality of safety analyses performed and the average quality of safety analyses in the completed design.

One of the major variables calculated in the System Development Completion and Safety Analyses module is the ultimate *Safety of the Operational System.* This variable is a dimensionless, multi-attribute utility function that is meant to characterize how safe the operational will be. Its inputs are the *Average Fraction of Hazard Analyses used in the Approved Design*, the *Fraction of Completed Designs Completely Meeting Safety Requirements*, and the *Average Quality of Hazard Analyses used in the Completed Design*. This function is not meant to be inversely proportional to the likelihood of accidents (i.e. if *Safety of the Operational System* is 1, the system will not necessarily have twice as many incidents/accidents than it would if *Safety of the Operational System* were 2). Instead, it is meant to serve as a relative measure between simulation runs of how well tasks crucial to the safety of the system are performed in the design process. Alternative factors (or alternative weightings of the factors) can be chosen by those who want to reflect their judgment on the value of certain tasks throughout the design process in the model.

Engineering – Technical Personnel Resources and Experience Module

Overview:

The purpose of the Engineering (Technical Personnel Resources and Experience) module is to keep track of the human resources working on ESMD projects. This module was initialized and calibrated using employment data available on the NASA web site. The objective is to monitor the

[69] A coflow is a structure used in system dynamics to track multiple attributes of stock in the model (e.g. quantity, age, cost, etc.). It involves at least two separate stock-and-flow structures, where the flows of one structure are regulated to some extent by the flows of the other structure. When all the flows in the second stock mirror the flows of the original stock, the coflow is conserved; in all other cases, the coflow is non-conserved. See John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, pp. 469-512.

[70] This lack of synchronization in design task and hazard analysis task completion creates a flow in the hazard analysis stock-and-flow structure (an exit flow for hazard analyses that are not used) that does not mirror any flow in the design task completion stock-and-flow structure and is thus the reason that the coflow is non-conserved.

availability and characteristics of the technical workforce responsible for the development of the exploration system. The module considers the number of people hired for entry-level positions and for experienced positions, as well as transfers between ESMD and other NASA directorates such as the Space Operations Mission Directorates (SOMD). It also keeps track of the experience of NASA technical employees as well as attrition rates, retirements, and employees choosing to use their early retirement option in order to work as consultants or as contractor employees. The scope of this module includes a NASA in-house technical workforce (i.e., NASA technical civil servants) and support contractors working at NASA centers. Employees working for the procurement contractors are not explicitly modeled.[71] All these factors have a critical impact on NASA's ability to develop a safe and successful exploration system.

Detailed Description:

This module receives inputs from higher-level modules, such as the desired size of the civil servant technical workforce and the budget available to hire support contractors. The allocation of technical human resources into the five different bins discussed previously is also provided as an input. The difference between the desired workforce size and the current workforce size drives the hiring rate. Civil servants can either be hired at the entry-level or at the experienced level. Additionally, if civil servants from another NASA directorate are available, they will be transferred to ESMD and have priority over new hires. Once civil servants are hired or transferred to ESMD, it takes time for them to become fully productive. According to interview data, it takes approximately three months for an experienced hire to become productive, while it takes up to two years for entry-level hires to become productive. The employment data shows that once civil servants become productive, they will leave the NASA workforce in one of two ways: either (1) they will stay at NASA until they retire or (2) they will stay for a few years and then make an early career decision to work in the private sector or to work for a different government agency. The data shows that very few mid-career NASA employees leave the civil servant workforce. NASA employees, however, are regularly transferred to and from projects and directorates. The model accounts for this possibility and allows us to investigate the impact of various types of transfers on system development. The module also takes into account the fact that hiring civil servants is more difficult than hiring support contractors. The only requirement to hire a support contractor is to have the budget available. More important, laying off support contractors is much easier. Civil servants are frequently transferred, but firing a civil servant is rare and reductions in workforce are very difficult to do on the government side, which is a disadvantage in large-scale system development. This reality, combined with the fact that recent administrations have had a desire to reduce the size of the government workforces, creates a strong bias toward hiring more contractors.

The output of this module includes the number of in-house technical employees working in the five areas mentioned previously: technology, integration, safety, development tasks, and other ESMD projects. The output also includes the average ESMD civil servant experience and average support contractor experience, both of which have impacts on productivity and the capability to oversee support contractors and the capability to oversee procurement work.

Engineering – Effort and Efficacy of Technical Personnel Module

The purpose of the Engineering (Effort and Efficacy of Technical Personnel) module is simply to collect information from various sources in the model and output the total capacity of in-house workforce to perform development work in areas of technology development, system integration,

[71] The budget allocations for procurement are explicitly modeled in the NASA Administration and ESMD module of the model.

and system development. To provide this output, the module uses such inputs as the number of employees assigned to different areas, the overwork of employees in those areas and other variables that affect the motivation and productivity of employees such as the likelihood of program cancellation, requirements and design changes, and project abandonment. This module also computes a value for the average quality of system integration work, which is a function of many factors such as the ability to perform contractor oversight, the quality of the system engineering and integration process, and the quality and quantity of communication across NASA centers and contractor offices.

Safety and Mission Assurance - Effort and Efficacy of System Safety Activities Module

The focus of the Safety and Mission Assurance module is on the effort and efficacy of in-house employees working on safety activities. The purpose of the module is to determine the capacity of safety personnel to work hand-in-hand with other engineers and technical people in order to produce high quality, useful safety information to be used in making design decisions. Many soft factors such as the power and authority, status, and credibility of system safety personnel will largely determine the impact the system safety engineers have on the safety of the final system. Consequently, all of these factors have to be included, even though they are difficult to quantify and their influence might not be completely understood. The outputs of this module include the capacity for performing safety activities, current quality of the safety analyses and other safety engineering products, and the influence and prestige of the safety organization and their authority to delay system development for safety concerns and to detect system safety and integration problems.

4. PRELIMINARY ANALYSIS AND RESULTS

We performed a preliminary analysis of safety-related decision-making at ESMD to provide both a demonstration of the model's capabilities and preliminary results upon which to base further analyses to be performed on the delivered model. In the subsections below, these analyses and their results are discussed following preliminary remarks on how the results derived from this and other CSRL system dynamics models should be interpreted.

4.1 Interpreting Results from the Model

"All models are wrong, some are useful." –George E.P. Box[72]

"If being absolute is impossible in estimating system risks, then be relative." –Eberhardt Rechtin[73]

The most important thing for individuals to take away from the use of a STAMP-based system dynamics model is a deep, qualitative understanding of the overall system's response to its various inputs. Model users and those who review the model results are advised not to focus too intently on the specific numeric values produced in the model, as they only tell a small part of the story that we have tried to capture in the models. The actual numeric values that are generated in the simulation are not always as important as the qualitative learning opportunities presented by the model. For instance, one can use the model to hone in on decision rules that outperform others in terms of cost,

[72] George E. P. Box (1979), "Robustness in the strategy of scientific model building," in *Robustness in Statistics*, R. L. Launer and G. N. Wilkinson, Editors. Academic Press, New York.

[73] Eberhardt Rechtin (1991), *Systems Architecting, Creating and Building Complex Systems,* Prentice-Hall, Englewood Cliffs, NJ. pp. 177.

schedule, final system scope, and/or safety; to recognize that a specific input to the system produces results that are desirable at first yet exponentially harmful over time; or to identify variables that provide leading indications or "warnings" of undesirable trends to follow. Knowledge of concepts such as these is the key to identifying ways in which organizational and programmatic risks can be controlled.

As mentioned earlier, there are several variables in the models that are meant to serve as relative performance indicators. One example in the ESMD System Dynamics Model is the variable *Safety of the Operational System*. The numeric value of this variable is not linearly related to the likelihood of accidents. Instead, it provides a reference variable for the comparison of multiple simulation runs, that is, if the final value of *Safety of the Operational System* is higher at the end of one simulation run than it was at the end of another, the product of the design process from that run is better in terms of the attributes that have been explicitly identified as important to the safety of the operational system. Such reference variables allow the model user to evaluate the relative importance of parameters and decision rules in the model.

Additionally, these models are useful in the identification of tipping points or unstable equilibriums in the system. Tipping points are points beyond which the stabilizing forces of the balancing loops in the system are overwhelmed by the destabilizing forces of the reinforcing loops of the system.[74] The example almost universally used to explain the concept of a tipping point or unstable equilibrium is that of a ball resting on the top of a hill or upside-down bowl. If the ball receives enough of a perturbation to dislodge it from its resting position, it will quickly roll down the hill. Similarly, processes and/or groups within an organization may be stable until they receive just the right type of perturbation to send them into upward or downward spirals. Through sensitivity analyses of the parameters in the model, these tipping points can be identified and policies to avoid or exploit them can be evaluated through the addition of feedback loops to the affected elements of the model.[75]

Combining the qualitative insights derived from the model about relative performance of policy options, the existence of tipping points, and leading/lagging indications of risk or success sheds light on the "intended rationality" of the decision rules in place in the system and their efficacy. In other words, the model should be instructive in informing the answers to questions of hazard and risk controllability on the technical and the organizational levels of the system. These questions include, but are not limited to the following:

- Which actions will be relevant in addressing the issues that need to be addressed?
- Will the decision-maker have the appropriate feedback to make a sound decision?
- Will this policy action have an immediate or delayed effect?
- Will this policy action have the intended effect, and if so, how long will this effect last?
- What, if any, indications will be available if the policy action does not work out?
- Where are the bottlenecks in the system that might or will prevent the intended effect of the policy action?
- Over time, how will one policy perform relative to another?

[74] John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill. pp. 306.

[75] Once again, knowledge of the numeric value that moves the system past the tipping point is not necessarily as important as the mere recognition that a tipping point exists and that a given policy can be implemented to exploit or avoid it.

Though the simulation is run with numeric parameters and produces numeric results, it is these qualitative insights that will be of the most importance in risk management.

4.2 Scenario 1: Workforce Planning

Scenario Motivation

The first scenario that was analyzed was inspired by concerns raised in a number of interviews about the current and future skill sets of the workforce. The following quote from a recent report by the National Academies of Science Space Studies Board summarizes many of the long-term issues raised in the interviews:

> *"NASA is not currently experiencing a supply problem in terms of overall available personnel. But the agency is experiencing a more complex and subtle problem that will grow over time. Like other government agencies and aerospace contractors, NASA is experiencing difficulty finding experienced personnel in certain areas, such as systems engineers and project managers. NASA's workforce also has a skewed age distribution arising from hiring policies first implemented in the 1990s. The agency did not experience a hiring freeze during that time, but it adopted policies whereby it filled specific positions but did not hire younger people and 'grow' them into positions. As a result the agency's mean age has continued to rise over time, and it lacks younger employees with necessary skills. As the agency embarks on new human and robotic exploration programs, problems in fulfilling demand will likely increase because the agency has not been developing the necessary employees from within."*[76]

Additionally, NASA is struggling with a short-term workforce problem referred to as "unfunded capacity". This problem stems from programmatic changes across the agency in response to the Vision for Space Exploration (VSE). Whenever a NASA project or program ends or gets restructured—either through the planned conclusion of the project/program or due to cancellation—the employees that work on that project/program have to find another one to work on. Unfortunately, this process does not always work out because some projects/programs effectively get replaced by ones that require vastly different employee skill sets than the ones that they succeed. Additionally, the employees sometimes do not get to transfer into the new projects/programs even when they have the appropriate skill sets because the successor project/programs occasionally are assigned to different NASA centers—refer to Appendix C for a discussion on NASA's organizational structure. Thus, there is bound to be a contingent of the NASA civil servant workforce at any given time that is not assigned to an Agency project/program. This contingent is referred to as the unfunded capacity. In the wake of the programmatic changes made for the VSE, there are roughly 900 civil servant positions that are unfunded.[77]

Scenario Description and Results

With the impending retirement of the Space Shuttle in 2010, workforce retirements due to the high mean age of the Agency civil servants, and a planned two-to-four year gap in human spaceflight launch operations; NASA will be challenged to keep its workforce skill set problems under control. To study this problem, we developed a simulation scenario in the model to explore ESMD's workforce needs between 2004 and 2016. The results are shown below in Figure 39

[76] National Academies of Science (2006), "Issues Affecting the Future of the U.S. Space Science and Engineering Workforce: Interim Report," *The National Academies Press*, Washington, D.C. pp. 2-3.

[77] National Academies of Science, ibid, pp. 13.

through Figure 41. Figure 39 shows the results of a sensitivity analysis of the *ESMD Employee Gap* for a case where transfers are accepted from the Space Shuttle Program and the initial unfunded capacity—Figure 39a—and a case where transfers are not accepted from other directorates in the Agency—Figure 39b. The contours in the figure represent different levels of hiring and transfers from the Space Shuttle Program (the blue contour, which should appear darker than the others on a black and white printout, represents the largest monthly hiring rate of science and engineering personnel for the entire Agency since at least 1993[78]). In both of these cases, the *ESMD Employee Gap*—which is the number of sufficiently experienced technical civil servants that ESMD wants minus the number that it has—increases dramatically shortly before the Space Shuttle is retired and then tapers off towards the end of the simulation. This tapering occurs because funds from the Space Shuttle Program in the Space Operations Mission Directorate (SOMD) are transferred to ESMD, thus creating a need for ESMD to hire new employees and/or transfer employees in from unfunded capacity.[79] Unfortunately, transferring civil servants in from SOMD is only slightly effective because the Space Shuttle Program is comprised of a civil-servant to support-contractor ratio that is much lower than the Agency average. Figure 40 shows that when the *ESMD Employee Gap* is filled through the hiring of support contractors using a simple proportional control law (i.e. as the gap increases more support contractors are hired instead of civil servants) the ratio of civil-servants to support-contractors in ESMD trends down towards the Space Shuttle's ratio of civil-servants to support-contractors.

With that said, the conclusion from this simulation is that if ESMD inherits the Space Shuttle Program's budget and its workforce, it will also inherit the Space Shuttle Program's civil-servant to support-contractor ratio unless it increases hiring rates. Because the Space Shuttle Program is an operational program, however, and ESMD is involved in development efforts, the following question must be raised:

> *"Will having a low civil-servant to support-contractor ratio in the development environment of ESMD work as well as having a low ratio in the operations environment of the Space Shuttle Program?"*

To gain insights into this question, we looked into the *Safety of the Operational System* variable in the model. Figure 41 shows that with the assumptions built into the model, *Safety of the Operational System* will decrease as the ratio of civil-servants to support-contractors decreases. This decrease is due to the increased difficulty of contractor oversight when the ratio is low and an effective decrease in the total number of people that can be hired.[80]

In all, this scenario challenges the "intended rationality" of using ratios of civil servants to support contractors in system development that are as low as those seen in system operations. While the specific numbers shown in the figures are likely to be less accurate than those that will be produced by NASA when they use higher fidelity data than we were able to obtain, the qualitative lesson is clear:

[78] This rate of 60 Science and Engineering civil servants per month was derived from FY 2004 data in the workforce data cubes on the NASAPeople website.

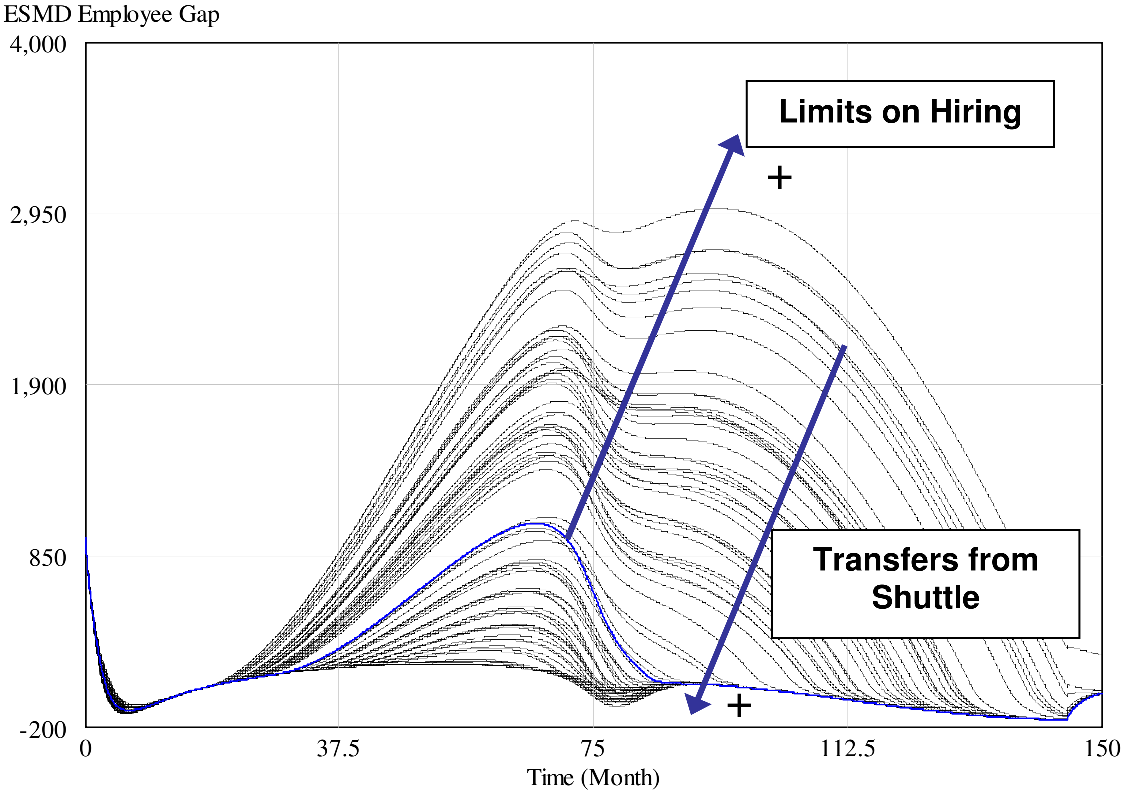
[79] Towards the end of the simulation, the *ESMD Employee Gap* decreases mainly due to the fact that a portion of its budget gets transferred back to SOMD when the CEV/CLV is deployed for operations.

[80] In the model, it was assumed that with all things being equal, a civil servant would cost less than a support contractor because a support contractor's employer would have to add its profit margin on top of the support contractor's salary. While some of the people at NASA who have seen the results of the model did not approve of this assumption due to the overhead involved in employing civil servants, it can easily be changed by ESMD.

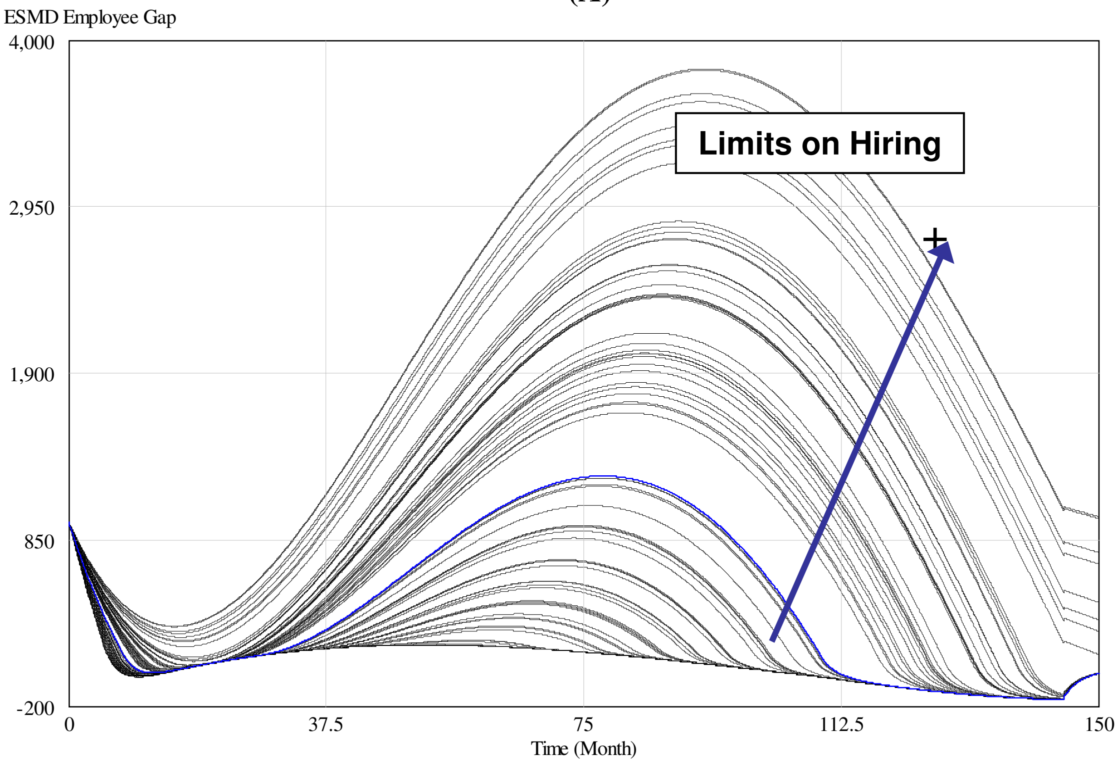
> *The safety of the operational systems developed by ESMD will depend partially on its ability to determine an acceptable ratio of civil servants-to-support contractors and alter its hiring practices to maintain that ratio.*

Recommendations

The results of this scenario point towards a possible connection between safety and the civil-servant to support-contractor ratio in system development, which may warrant monitoring and/or control of personnel decisions from the program or directorate levels. Specifically, it is recommended that ESMD determine an acceptable, time-dependent ratio of civil-servants to support-contractors and structure its hiring and SOMD-to-ESMD transfer rates around the maintenance of that ratio throughout development.



(A)



(B)

Figure 39. The Increase in Demand for ESMD Technical Civil Servants (Civil Servant to Contractor Ratio Held Fixed).

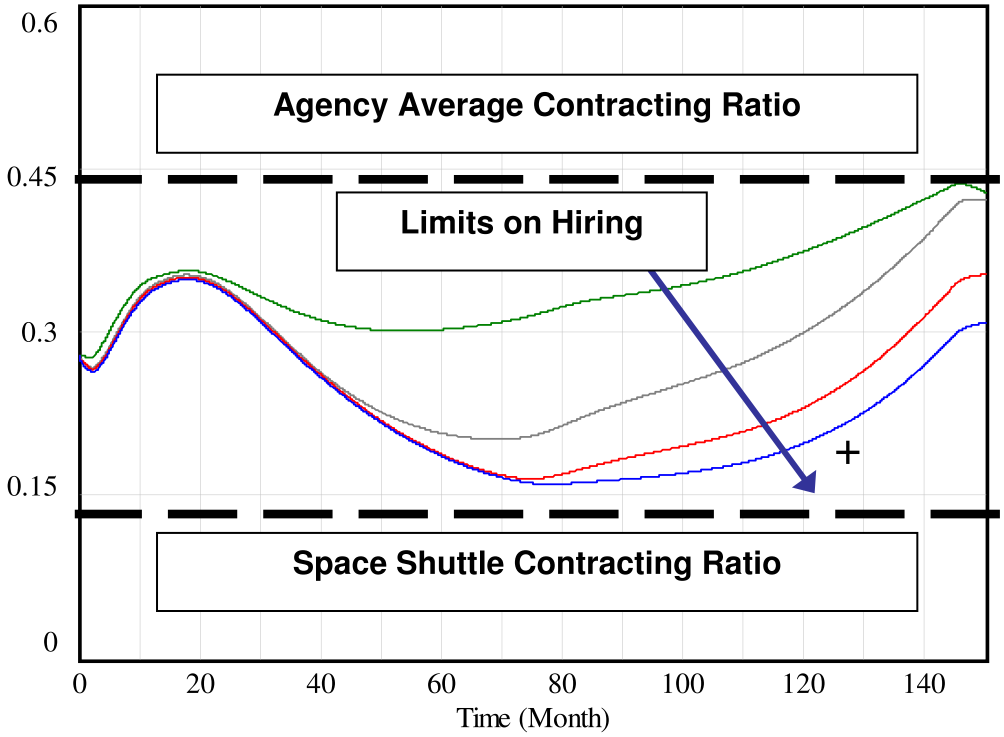


Figure 40. Ratio of Productive, Technical Civil Servants to Productive, Technical Support Contractors.

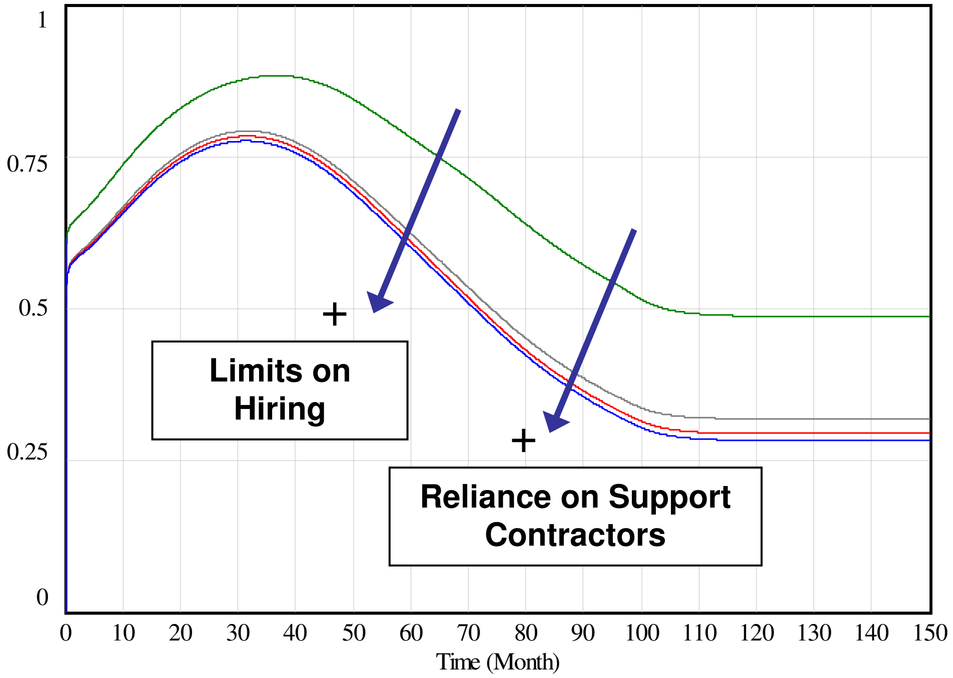


Figure 41. The Ultimate Safety of the Operational System as Dependence on Support Contractors Increases.

4.3 Scenario 2: Investigating Management Reserves

Scenario Motivation

Many interviewees stressed the importance of a realistic alignment of system requirements with available resources, combined with program management leadership that is able to secure and manage sufficient reserve resources to mitigate programmatic uncertainties and complete system development on schedule.

Scenario Description and Results

We created a scenario to investigate the impact of system requirements planning and management reserves on development completion and the overall safety of the system (as defined by the relative system safety indicator). In the baseline scenario, the requirements are calibrated based on a planned system development time of 8 years (96 months) in order to hit the 2012 CEV launch deadline. The resources available are calibrated according to planned ESMD budgets and workforce data.[81]

A sensitivity analysis was performed using these baseline parameters. The number of system requirements were randomly varied ± 25% of the baseline value of 8 years worth of requirements; that is, requirements for 6 to 10 years of development. Given that the planned development deadline is fixed at 2012, the simulation run involving 6 years worth of requirements is associated with more reserve because the system could be theoretically completed in 2010 while the simulation run with 10 years worth of requirements is overoptimistic because, given baseline resources and realistic pressure, the system could not be completed until 2014.

In a similar manner, the resources (budget and workforce) available were varied ± 20% of the baseline value. The upper limit of the resources (120% of the baseline value) represents a conservative management case with 20% management reserve, while the lower limit of 80% represents the overoptimistic planning case with insufficient baseline resources to perform the work on time.[82]

Figure 42 and Figure 43 provide some scenario results for the baseline and envelope cases, namely the overoptimistic planning case (10 years requirements, 80% resources), and the sufficient reserves case (6 years requirements, 120% resources). As can be observed, the management reserves have a significant impact on completion time and relative system safety. Longer completion time is having more work to do and fewer resources to do it. Lower safety can be explained through the side effect loops shown in Figure 37: because there is more to do with fewer resources, managers apply additional schedule pressure, resulting in lower safety priority, lower quality safety analyses, more unsatisfied safety requirements, and consequently lower overall system safety of the final system.

[81] Budget data are available at <http://www.nasa.gov/about/budget/index.html> and workforce data are available at <http://nasapeople.nasa.gov/Workforce/data/page8.htm>.

[82] The baseline does not include explicit reserves.

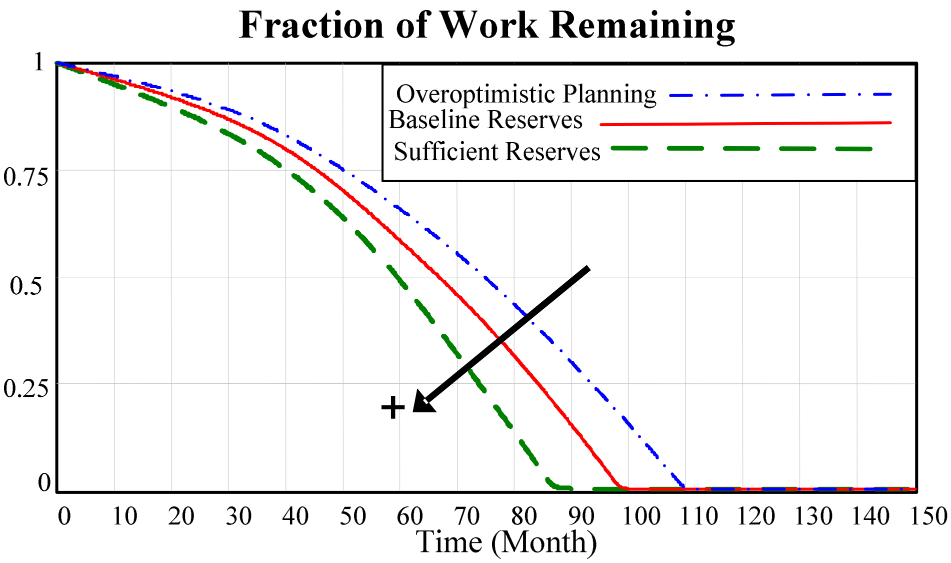


Figure 42. Fraction of work remaining for the baseline and envelope scenarios.

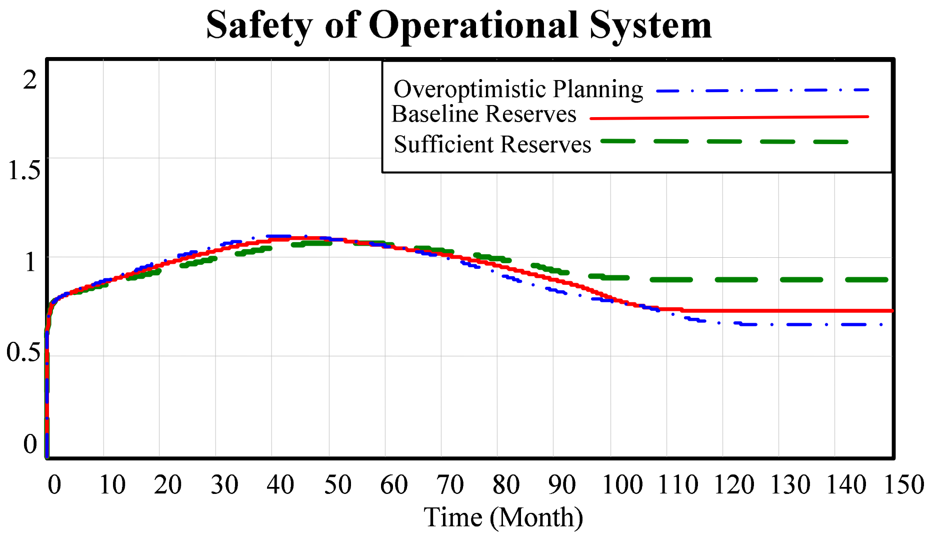


Figure 43: Relative safety of the final system for the baseline and envelope scenarios.

In addition to envelope results, the scenario sensitivity analysis allows the generation of outcome distributions. Using a random variation of the parameters described above, the final system development outcomes were collected and arranged by frequency interval to obtain the distributions of Figure 44 for completion time (in years) and (final) system safety. There are many advantages of this approach, including that the best (or worse) final outcomes can be traced back to the specific parameters that produced them and the runs can be analyzed individually. The runs at the tail of the distribution in Figure 44 correspond to the envelope values; in other cases, however, extreme outcomes may be associated with less obvious model parameters.

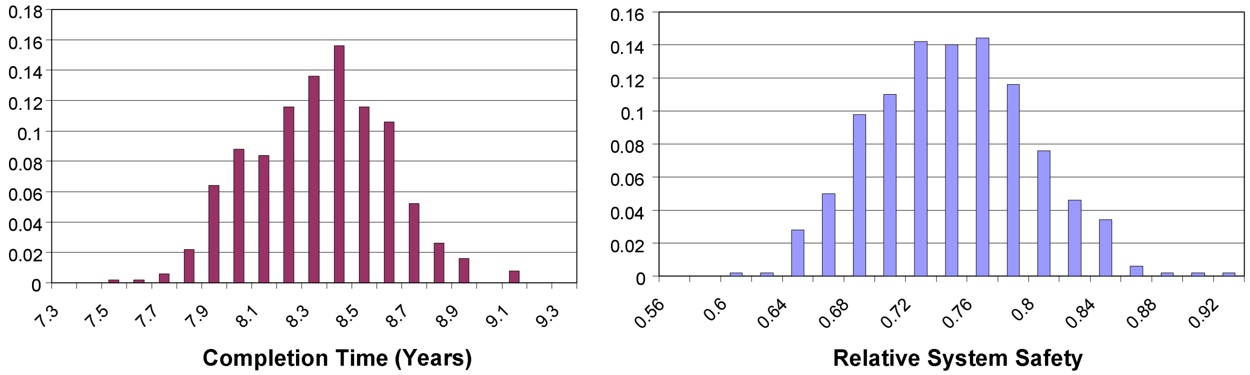


Figure 44: Outcome distributions (completion time and safety) for the sensitivity analysis.

Recommendations

Based on this scenario, it appears that careful planning and reserve utilization, management, and monitoring are critical to dampen disturbances in workforce, budget, and technology availability. One of the indicators that planning or reserves may be inadequate is the workload of the ESMD workforce. This should be especially true in the critical employment areas of system engineering and integration, safety engineering, and safety assurance, as these areas control the strength of the rework cycle. A common sentiment that was echoed by one of our interviewees is that doing things wrong the first time costs you more in the long run. Based on the scenario results, one could add that you also get a lower quality, less safe system in the end.

4.4 Scenario 3: Effect of Schedule Pressure and Safety Priority

Scenario Motivation

Schedule (and budget) pressure ended up being one of the most common factors of risk management discussed by interviewees. The CAIB made it clear that the managers and engineers of the Space Shuttle Program were under tremendous pressure from the NASA administration to meet the February 2004 deadline for the International Space Station to reach "core complete" configuration.[83] As a result, the CAIB recommended the implementation of measures (such as an ITA) to ensure that schedule pressure does not negatively affect safety-related decisions. Nevertheless, some of these recommendations (including ITA as it was initially designed) are encountering *policy resistance*[84] in the development of the new exploration systems, only three years after the *Columbia* Accident.

Scenario Description and Results

A scenario was developed to investigate the impact of schedule pressure and enforcement in exploration systems development. As mentioned previously in Section 3.2, management pressures were implemented in the model as a simple PID controller. Essentially, the profile for the desired fraction of completed development was created based on actual and forecasted yearly budget allocations. The schedule pressure applied at the program management and administration level is a function of the difference between the measured work completed and the desired work completed

[83] Harold Gehman (Chair) (2003), *Columbia Accident Investigation Report*, Government Accounting Office, August.

[84] *Policy resistance* is a phenomenon in which well-intentioned efforts to solve pressing problems are delayed, diluted, or defeated by unanticipated side effects in the system. It is a common area of system dynamics research. For more detail and examples, see John Sterman (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill. pp. 3-20.

at any point in time. This simple controller framework was applied to the desired system development completion profile, as well as to the desired safety analyses completion profile.

In the scenario, the proportional gain responsible for the application of pressure at the program management level (when development falls behind schedule) was varied from a value of 0 to 10. Consequently, the pressure applied is simply equal to the gap in schedule completion multiplied by a proportional gain (K). The same variation (0 to 10) applies to the safety pressure gain, that is, the pressure used to ensure that safety analyses are performed early enough to be used in design decisions.

Figure 45 shows the estimated project outcomes for safety, schedule, and cost as a function of extreme values (0:Low, 10:High) of schedule pressure and safety priority gains. As can be observed, overly aggressive schedule enforcement has little effect on completion time (<2%) and cost, but has a large negative impact on safety. Inversely, priority of safety activities has a large positive impact, including a reduction in cost, as less safety-related rework is required due to the high quality of safety analyses used to influence design decisions in the early stages of development.

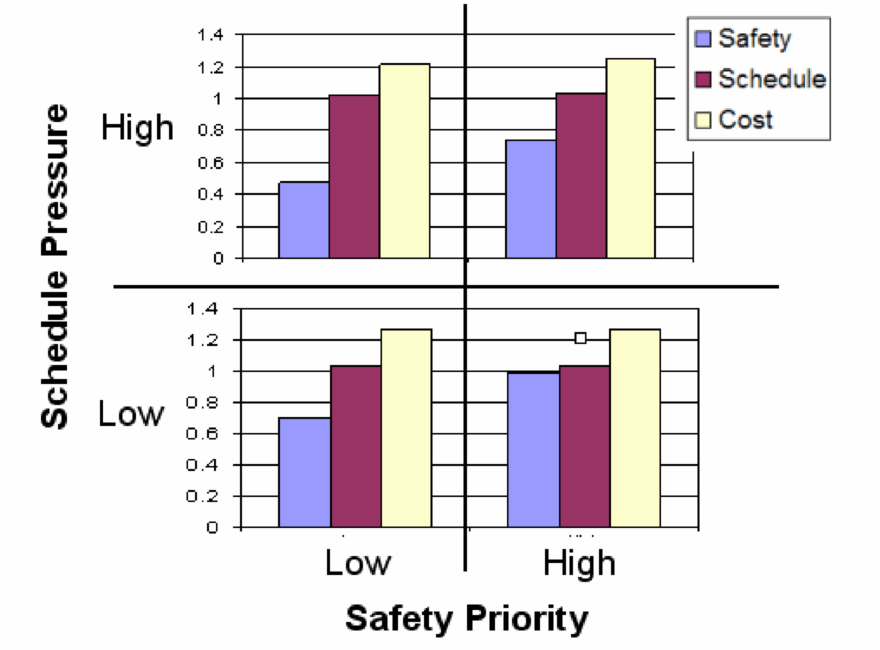


Figure 45: Outcomes (Safety, Schedule, Cost) as a function of schedule and safety pressure (low, high).

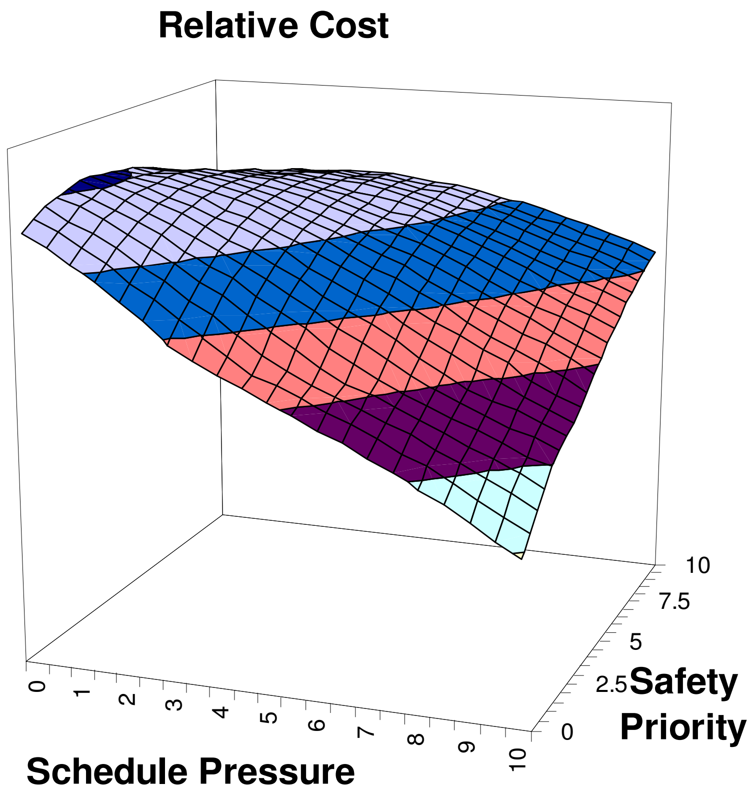


Figure 46: Estimated relative cost as a continuous function of schedule pressure and safety priority.

Figure 46 shows the estimated effects on cost of a more continuous variation of the schedule and safety gains from 0 to 10. The improvement in cost observed when the schedule gain is low and the safety gain is high is achieved because less rework (associated with variable and fixed costs) is necessary as the safety work was done correctly and on time. The improvement in cost associated with high schedule pressure and low safety priority is achieved at the detriment of safety, which means development is finished earlier (lower fixed costs) but the final system is less safe.

Recommendations

Recommendations from this scenario include the monitoring of workforce workload, as extreme workload and employee burnout allow for more mistakes, which necessitate more rework. In addition, ensuring that safety analyses are used in design decisions is a good way to verify the synchronization of the design and safety flows. Controlling safety requirements waivers and operational workarounds is another way of ensuring that schedule pressure does not take undue priority over safety concerns.

4.5 Scenario 4: Consequence of High Safety Influence and Power on Decision-Making

Scenario Motivation

A number of interviewees commented on the natural tendency for considerations of the various types of risk (i.e. cost, schedule, performance, and safety risk) to conflict in design tradeoffs. As they explained, a key element to ensuring that these conflicting considerations are addressed in a reasonable manner is to ensure that the influence and power in design decision-making is appropriately distributed among the advocates of the many considerations. Many of the interviewees agreed with the CAIB's assertion that at the time of the *Columbia* Accident, program management had the power to essentially "buy" as much or little advocacy for safety considerations as they desired.[85] These interviewees also noted that the resolution of this issue is still a work in progress and a hotly contest topic. Thus, this issue was flagged as an area for further investigation.

Scenario Description and Results

A scenario was created to investigate the impact that the level of influence and power held by the safety organization has in design decision-making. In the system safety module of the model, the variables *Power and Authority of System Safety Analysts*, as well as *Status and Credibility of System Safety Analysts* were varied ± 50% about baseline values. The results in Figure 47 show the potential impact of safety influence and power on system development. High safety influence and power has a large positive impact on safety (see bottom-left of Figure 47) because it effectively removes the "relief valve" of accepting design problems, unsatisfied requirements, and operational workarounds (see bottom right of Figure 47). On the other hand, not accepting these problems may necessitate additional rework, which has slight negative impact on cost and schedule (see top of Figure 47). The negative impact on schedule and cost can be dampened by allocating more resources to system integration, and by carefully planning and anticipating safety analysis requirements. Indicators of safety influence and power on decision-making were identified in the model and include: 1) Safety-based design changes, 2) Overruling of safety decisions, 3) Adequacy and stability of safety resources, 4) Review time allocated to safety analyses, and 5) Unsatisfied safety requirements.

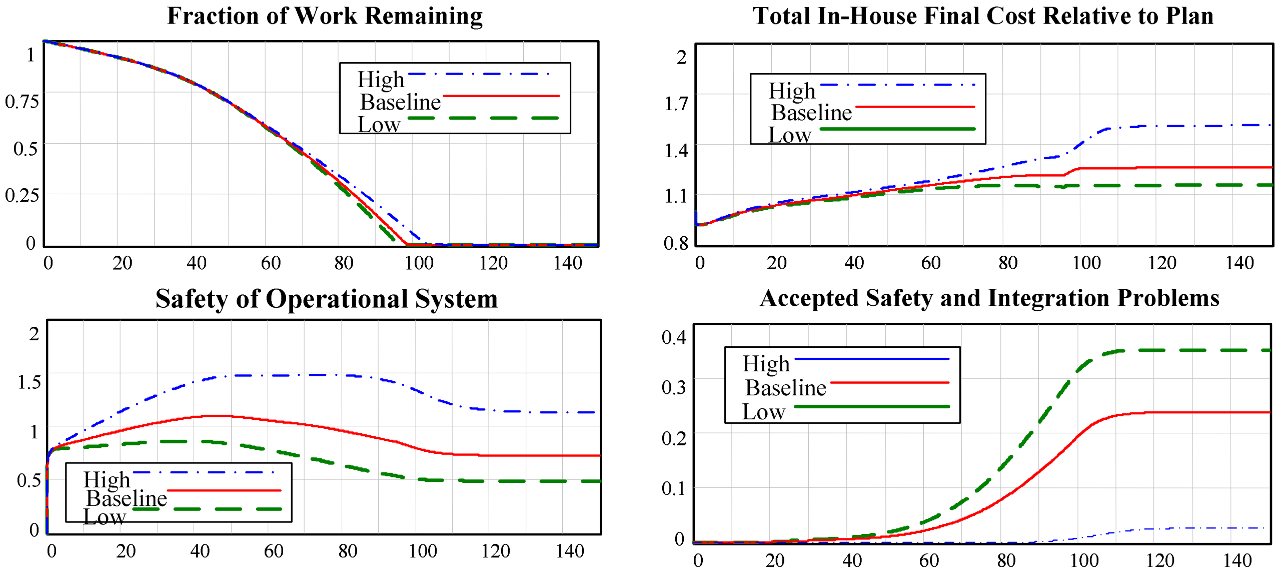


Figure 47: Impact of safety influence and power on project dynamics.

Recommendations

The results of this scenario underscore the importance of the recommendation by the CAIB for a powerful and active technical authority to advocate safety considerations in situations where they conflict with other programmatic considerations. Ensuring that system safety analysts have high

[85] Harold Gehman (Chair) (2003), Columbia Accident Investigation Report, August, pp. 181.

influence and power on decision-making, as well as high credibility and status is a very effective way to improve the safety of the system with minimal impact on cost and schedule.

4.6 Scenario 5: Assignment of Highly Regarded Technical Leaders to Safety Engineering Roles

Scenario Motivation

As mentioned in the previous scenario description, the natural tension between safety considerations and other programmatic considerations can be detrimental to safety if the influence of those advocating safety is marginalized. According to several of our interviewees, the ultimate influence that these safety advocates hold is not just determined by the formal decision processes of the organization, but also by the perception of these advocates by the workforce at large. Many interviewees asserted that the assignment of the most highly regarded people to solve a problem sends a strong signal to the workforce at large that management considers the problem to be important. They also claimed that, conversely, the assignment of people that are held in comparatively low regard to a problem sends a signal that management considers that problem to be less relevant. Unfortunately, many interviewees agreed with the CAIB's assertion that at the time of the *Columbia* Accident, careers in safety had lost organizational prestige.[86] Some partially attributed this to practices of safety advocates that many people are now keen on changing, namely, the tendency to identify problems without offering solutions. Others claimed that the negative perceptions were instigated by perceived shortcomings in the technical and leadership capabilities of those who advocated safety. In any case, it will take the advocacy of highly respected and skilled individuals to reverse any negative perceptions of careers in safety within the organization.

Scenario Description and Results

Leadership capability and technical expertise of an individual is closely related to his or her influence and power in decision-making. Consequently, a scenario was created to investigate the impact of the assignment of highly regarded technical leaders to safety roles. The results (see Figure 48) show that such assignments have a very high impact on safety, with a minimal impact on cost and schedule. One of the main reasons for this positive impact is that these highly regarded technical leaders will have the capability to deliver high-quality safety products on time, as well as the status and credibility necessary to influence design decisions (see right side of Figure 48). The effective result is a high quality system with safety "designed-in" that meets schedule and budget by virtue of avoiding costly rework throughout development. Indicators of the assignment of technical leaders to safety were identified in the model and include: 1) Attractiveness of safety positions, 2) Experience and skills of current and incoming workforce, and 3) Impact of safety advocates and analyses on design.

[86] Harold Gehman (Chair) (2003), Columbia Accident Investigation Report, August, pp. 181.

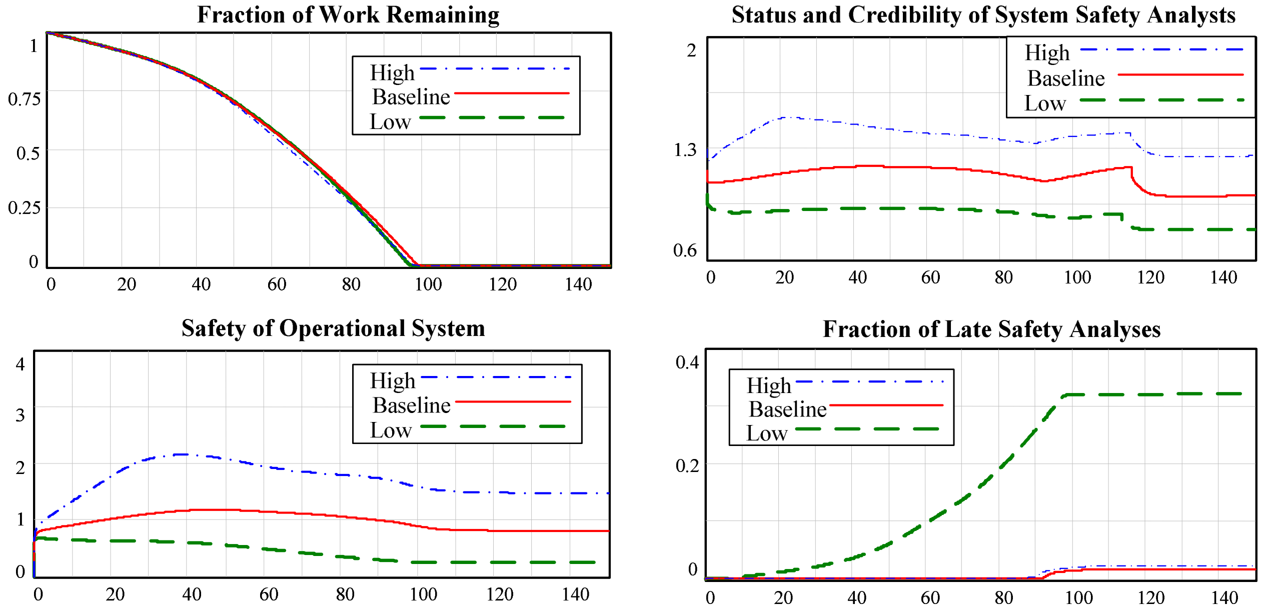


Figure 48: Impact of high-level technical leaders on project dynamics.

Recommendations

High priority should be given to the assignment of highly regarded technical leaders to safety roles (possibly through the rotation of technical leaders and "rising stars" into these positions). This personnel management strategy can be a relatively effortless way to positively impact the status, credibility, and impact of the system safety engineers.

4.7 Scenario 6: Effect of Scope and Requirements Changes

Scenario Motivation

Having a fixed set of clear requirements from the beginning is arguably the most effective way to ensure the system will be developed on time and on schedule. Several of the interviewees even suggested that the effects of poorly defined (i.e. too detailed at too high of a level or not detailed enough at the low levels) and changing requirements extends to safety. Indeed, from a project management perspective, frozen requirements are a huge advantage. However, for a very large development environment such as the exploration system, freezing requirements early is very difficult because of the complexity of the system and the low maturity of the technology. This creates large difficulties and opens the door to changes in requirements and system scope later in the development cycle.

Scenario Description and Results

A scenario was created to investigate the impact of requirements and scope change on project dynamics and system characteristics. In this scenario, the baseline simulation corresponds to requirements that are well defined and frozen from the beginning of system development. A second simulation was run where very small requirements changes (less then two percent of the total requirements) are made at a 12-month regular interval. Finally, a third simulation was run where large requirements and scope changes (less than twenty percent of the total requirements) are made at a 60-month regular interval (see top-left of Figure 49). Upward changes in scope and requirements (in top-left of Figure 49) indicate added requirements, while downward changes indicate abandoned requirements. Consequently, an entire cycle of downward/upward changes is associated with a replacement of requirements even if the total net change in the number of requirements and tasks is zero.

It is well understood and accepted that large requirements and scope changes will have significant negative consequences on project cost, schedule, and system characteristics. Not surprisingly, the scenario reproduces these expected results (see Figure 49) as large changes have a disastrous impact on schedule and system safety. Also, not surprisingly, the later the changes, the more negative impact they have. Another not so intuitive result, however, is that small but more frequent changes can have a similar negative impact on the system.

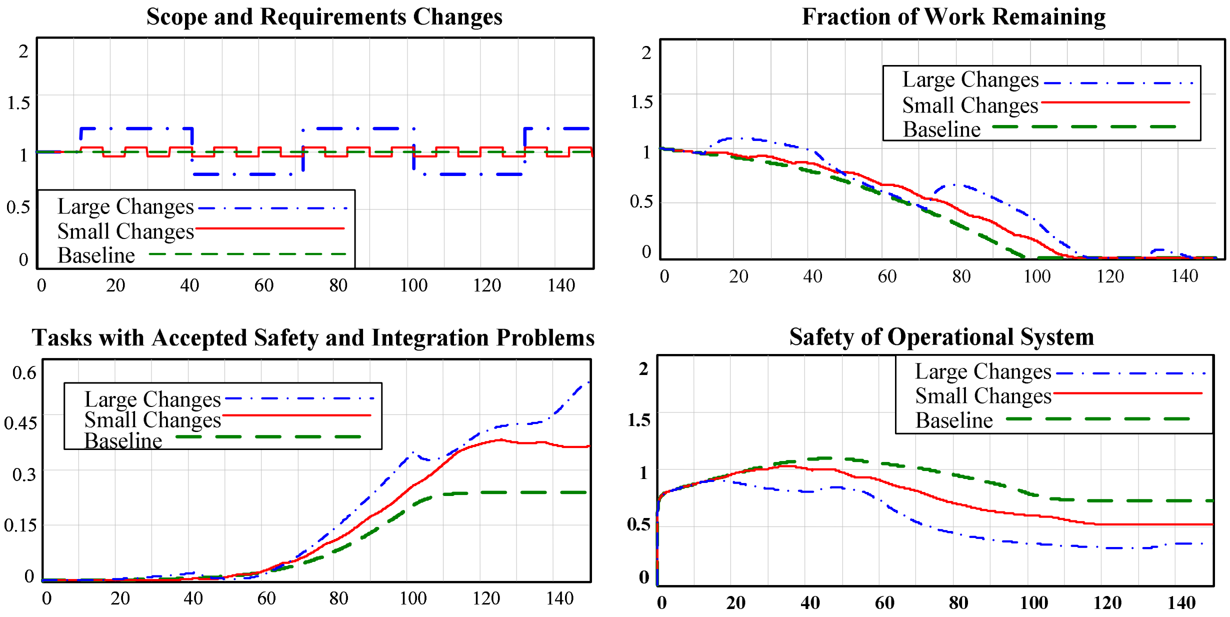


Figure 49: Effect of scope and requirements change on project dynamics and outcome.

Detailed planning is necessary to limit requirement changes (even small ones) and their negative impact on system development. Many potential mitigation strategies were identified to lessen the impact of some amount of (inevitable) changes later in the development cycle. These mitigation strategies include: 1) the use of additional management reserves, 2) design and planning for operations, 3) on/off-ramps for technologies and design, and 4) improved system engineering and integration.

Recommendations

In a perfect world, requirements would be well defined and frozen at the very beginning of a development project. However, this is rarely the case, particularly for new and complex engineering systems using unproven technologies that are developed and tested as the system is designed. The scenario presented in this section demonstrated that small, frequent changes can have a negative impact similar to larger, less frequent changes. Careful and complete requirements specification, combined with the mitigation strategies mentioned above, can help lessen the negative impact of changes. The following metrics were identified to monitor the amount of smaller, more subtle requirements changes: 1) the number of discarded or otherwise performed but unused design tasks, safety analyses, and technology items and 2) the number of accepted unsatisfied requirements and operational workarounds.

5. CONCLUSIONS AND FUTURE PLANS

> *"I feel that the emphasis on 'The' model is not only unrealistic, but probably also alarming to the reader…I believe we are proposing the 'Process' of modeling rather than particular frozen and final models…we are suggesting that models will help to clarify our processes of thought; they will help to make explicit the assumptions we are already making; and they will show the consequences of the assumptions. But as our understanding, our assumptions, and our goals change, so can the models."* – Jay Forrester[87]

> *"Model revision usually continues nearly to the end of the project. Do not expect the refinement process to come to a natural halt, nor the modeling team to feel comfortable at any point in freezing the model. One usually faces a tradeoff toward the end of a project, in which additional model refinement will cut into the time available for policy and scenario testing. This tradeoff should be faced squarely by modeler and client and settled with the goal of maximizing the model's effectiveness while accepting certain limitations."* – Jack B. Homer[88]

Effective risk management in aerospace systems requires the balancing of multiple risk components including safety, cost, performance, and schedule. Safety considerations are especially critical during system development because it is very difficult to design or "inspect" safety into these systems during system operations. Because the consequences of improperly addressing safety during development are not as immediately visible as those of cost, schedule, and performance considerations, project managers may be tempted to satisfy the latter three goals at the expense of safety. A goal of this modeling effort was to show how safety and programmatic considerations interact during the development of space exploration systems.

While the executable simulation model created in this study can provide insights such as those shown in our example analyses, there are additional opportunities to learn from this type of risk management modeling. As the quotes above indicate, the modeling of complex systems is an iterative process that usually has no natural ending. There are almost always portions of the model that can be refined as well as portions that will eventually become obsolete as the system evolves. These portions are especially prone to exist when decision rules and their "intended rationality" are modeled, as they are subject to both change and subtleties that can rarely be captured exhaustively in a one-time effort. Thus, the end products of this study should not be viewed as the final word on the system dynamics of exploration systems development. Instead, the model and the insights developed in the preliminary analysis should serve as a starting point for future analysis, iteration of the decision rules inherent in exploration system development, and possible improvements in the ESMD organizational structure.

The six-month research effort documented in this report illustrates the preliminary results of what an extended collaboration between MIT CSRL and NASA could provide to ESMD, including:

Further Validation and Enhancement of the Model:

The hypothesis of this research, as discussed earlier, is:

[87] Jay W. Forrester (1985), "'The' model versus a modeling 'process'." *System Dynamics Review*, Vol. 1, No. 1, Summer 1985. pp. 133-134.

[88] Jack B. Homer (1996), "Why we iterate: scientific modeling in theory and practice." *System Dynamics Review*, Vol. 12, No. 1, Spring 1996. pp. 1-19.

> *Safety culture can be modeled, analyzed, and engineered using the same logic and techniques as in physical systems. The models will be useful in designing and validating improvements to risk management and safety culture, in evaluating the potential impact of changes and policy decisions, in assessing risk, in detecting when risk is increasing to unacceptable levels, and in performing root cause analysis.*

While we feel that this hypothesis has been validated in both this and the previous (i.e. ITA) modeling efforts, we recognize that all models have varying levels of accuracy and usefulness and that there are almost always opportunities to improve these qualities in any given model. This model is no exception to this generalization, and therefore we see ways in which it will be possible to enhance the accuracy and usefulness of this model in attempts to effectively engineer the ESMD safety culture. First, we anticipate further model refinement through discussions with the end users of the model, once they have had a chance to use it themselves. Furthermore, because the model can now be run on a standard desktop or laptop computer, additional rounds of NASA employee interviewing can be conducted with real-time execution and update of the model incorporated into our interview protocol. Both of these measures will allow NASA employees and model end users at NASA to improve the quality of data input into the model, challenge the assumptions of the model, and identify ways in which model can be extended and restructured to provide key insights into the system dynamics of exploration systems development.

Knowledge Capture of Interviewee Comments on Complex System Development and How to Mitigate Risks:

Due to the high-level perspectives and collective experience of individuals interviewed throughout this study, the authors collected a wealth of information on complex system development. Partial transcription of the interviews has already yielded over 220 pages of quotations and notes. After some level of abstraction to preserve the confidentiality of the interviewee, these quotations and notes could be formally analyzed, documented, and annotated for their relevance to the broader management and systems engineering knowledge.

Complete Evaluation of ESMD Organizational Design through STPA:

As mentioned earlier, a complete STPA was not performed for ESMD as it was for the NASA ITA in 2005. We used only a selection of risks mentioned in the interviews. A complete programmatic risk identification and programmatic and organizational risk analysis could be derived from the STPA analysis of the ESMD organizational structure.

Development of Risk Management Tools and Simulators for Management Training:

A hindrance in the utilization of the CSRL's system dynamics models by the NASA workforce at large is their complexity and the subtleties of the system dynamics modeling conventions and software tools. Ultimately, without a custom user interface, the models are unusable by those who are unfamiliar with system dynamics. Along with assisting in risk management on projects, tool sets similar to the prototype interface for the ITA model might be developed for training in ESMD and other mission directorates.

APPENDICES

Appendix A: Acronyms

AA	Associate Administrator
ARC	Ames Research Center
CAIB	*Columbia* Accident Investigation Board
CaLV	Cargo Launch Vehicle
CD	Center Director
CDL	Center Discipline Lead
CEV	Crew Exploration Vehicle
CIL	Critical Items List
CLV	Crew Launch Vehicle
CSRL	Complex System Research Laboratory
DFRC	Dryden Flight Research Center
ESD	Engineering Systems Division
ESMD	Exploration Systems Mission Directorate
FMEA	Failure Modes and Effects Analysis
FTE	Full-Time Equivalent
FY	Fiscal Year
GRC	Glenn Research Center
GSFC	Goddard Spaceflight Center
HA	Hazard Analysis
HQ	Headquarters
ISS	International Space Station
ITA	Independent Technical Authority
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LaRC	Langley Research Center
LPRP	Lunar Precursor and Robotics Program
MDAA	Mission Directorate Associate Administrator
MIT	Massachusetts Institute of Technology
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NSF	National Science Foundation
OCE	Office of the Chief Engineer
OSMA	Office of Safety and Mission Assurance
PA&E	Program Analysis and Evaluation
P/PM	Program/Project Management
P/PM CE	Program/Project Chief Engineer
PID	Proportional-Integral-Derivative
RLEP	Robotic Lunar Exploration Program
S&MA	Safety and Mission Assurance
S&E	Science and Engineering
S.M.	Master of Science
Sc.D.	Doctor of Science

SE&I	System Engineering and Integration
SA	Safety Analysis
SOMD	Space Operations Mission Directorate
SOW	Statement of Work
SR&QA	Safety, Reliability, and Quality Assurance
SSC	Stennis Space Center
STAMP	Systems-Theoretic Accident Model and Process
STPA	STAMP Analysis
USRA CPMR	Universities Space Research Association Center for Program/Project Management Research
USRA/NASA APPL	Universities Space Research Association/NASA Academy for Program/Project Leadership
VSE	Vision for Space Exploration
WYE	Work Year Equivalent

Appendix B: Defining Safety Culture at NASA

Modeling something requires first defining it. Sociologists commonly define culture as the shared set of norms and values that govern appropriate behavior. Safety culture is the subset of organizational culture that reflects the general attitude and approaches to safety and risk management.

Culture is embedded in and arises from the routine aspects of everyday practice as well as organizational structures and rules. It includes the underlying or embedded operating assumptions under which actions are taken and decisions are made. Management, resources, capabilities, and culture are intertwined, and trying to change the culture without changing the environment within which the culture operates is doomed to failure. At the same time, simply changing the organizational structures—including policies, goals, missions, job descriptions, and standard operating procedures related to safety—may lower risk over the short term but superficial fixes that do not address the set of shared values and social norms are very likely to be undone over time. The changes and protections instituted at NASA after the *Challenger* accident slowly degraded to the point where the same performance pressures and unrealistic expectations implicated in the *Challenger* loss contributed also to the loss of *Columbia*. To achieve lasting results requires making broad changes that provide protection from and appropriate responses to the continuing environmental influences and pressures that tend to degrade the safety culture. "Sloganeering" is not enough—all aspects of the culture that affect safety must be engineered to be in alignment with the organizational safety principles.

We believe the following are all important social system aspects of a strong safety culture and they can be included in our models:

- The *formal organizational safety structure* including safety groups, such as the headquarters Office of the Chief Engineer, the Office of Safety and Mission Assurance, the S&MA offices at each of the NASA centers and facilities, NESC (the NASA Engineering and Safety Center), as well as the formal safety roles and responsibilities of managers, engineers, civil servants, contractors, etc. This formal structure has to be approached not as a static organization chart, but as a dynamic, constantly evolving set of formal relationships.
- *Organizational subsystems* impacting the safety culture and risk management including open and multi-directional communication systems; safety information systems to support planning, analysis, and decision making; reward and reinforcement systems that promote safety-related decision-making and organizational learning; selection and retention systems that promote safety knowledge, skills, and ability; learning and feedback systems from incidents or hazardous events, in-flight anomalies (IFA's), and other aspects of operational experience; and channels and procedures for expressing safety concerns and resolving conflicts.
- *Individual behavior*, including knowledge, skills, and ability; motivation and group dynamics; and many psychological factors including fear of surfacing safety concerns, learning from mistakes without blame, commitment to safety values, and so on.
- *Rules and procedures* that effectively support risk mitigation and are understood and accepted by system stakeholders.
- Values and assumptions that support a clearly articulated system safety vision. The vision must be shared among all the stakeholders, not just expressed by the leaders.

There are several assumptions about the NASA safety culture that underlie our ITA and ESMD risk analyses:

The Gap Between Vision and Reality: NASA as an organization has always had high expectations for safety and appropriately visible safety values and goals. Unfortunately, the operational practices have at times deviated from the stated organizational principles due to political pressures (both internal and external), unrealistic expectations, and other social factors. Several of the findings in the CAIB and Rogers Commission reports involve what might be termed a "culture of denial" where risk assessment was unrealistic and where credible risks and warnings were dismissed without appropriate investigation. Such a culture is common where embedded operating assumptions do not match the stated organizational policies. To "engineer" a safety culture, or, in other words, to bring the operational practices and values into alignment with the stated safety values, requires first identifying the desired organizational safety principles and values and then establishing and engineering the organizational infrastructure to achieve those values and to sustain them over time. Successfully achieving this alignment process requires understanding why the organization's operational practices have deviated from the stated principles and not only making the appropriate adjustments but also instituting protections against future misalignments. A goal of our risk analysis is to provide the information necessary to achieve this goal.

No One Single Safety Culture: NASA (and any other large organization) does not have a single "culture." Each of the centers, programs, projects, engineering disciplines within projects, and workforce groupings have their own subcultures. Understanding and modeling efforts must be capable of differentiating among subcultures.

Do No Harm: An inherent danger or risk in attempting to change cultures is that the unique aspects of an organization that contribute to, or are essential for, its success are changed or negatively influenced by the attempts to make the culture "safer." Culture change efforts must not negatively impact those aspects of NASA's culture that has made it great.

Mitigation of Risk, Not Elimination of Risk: Risk is an inherent part of space flight and exploration and other NASA missions. While risk cannot be eliminated from these activities, some practices involving *unnecessary* risk can be eliminated without impacting on NASA's success. The problem is to walk a tightrope between (1) a culture that thrives on and necessarily involves risks by the unique nature of its mission and (2) eliminating unnecessary risk that is detrimental to the overall NASA goals. Neither the *Challenger* nor the *Columbia* accidents involved *unknown unknowns*, but simply failure to handle known risks adequately. The goal should be to create a culture and organizational infrastructure that can resist pressures that militate against applying good safety engineering practices and procedures without requiring the elimination of the necessary risks of space flight. Most major accidents do not result from a unique set of proximal events but rather from the drift of the organization to a state of heightened risk over time as safeguards and controls are relaxed due to conflicting goals and tradeoffs. The challenge in preventing accidents is to establish safeguards and metrics to prevent and detect such changes before an accident occurs. NASA must establish the structures and procedures to ensure a healthy safety culture is established and sustained.

Appendix C: NASA's Organizational Structure

Though NASA's organizational structure is evolving in subtle ways, much can be learned from an overview of the basic function of organizational elements and where they are located. Figure 50 below is a graphical representation of this information, derived from discussions with interviewees, element websites, and other sources. Note that the list of elements shown in the figure and described below is not exhaustive as it focuses primarily on the elements relevant to development, rather than operations. Also, the lines connecting elements to each other are not meant to represent reporting and funding paths in every case; instead, they are meant to represent 1) a similarity of function between elements at different levels when they cross level boundaries or 2) paths of direct support when they do not cross level boundaries. Examples for each respective type of relationship are as follows: 1) OSMA represents the Center S&MAs on Level I[89] and 2) PA&E directly supports the Office of the Administrator. Additionally, it is worth noting that an element's vertical position on the chart does not always indicate its level of influence and even prestige within the Agency. For example, while the Center Directors are located on Level II, they are among the most powerful individuals in the Agency and according to the most recent iteration of the Technical Authority function, the heads of the Mission Directorate Offices (otherwise known as Mission Directorate Associate Administrators) cannot overrule them on matters of Technical Authority.

The levels and elements within them can be described as follows:

- **Level I: The Corporate Level** - includes corporate and enterprise management
    - Office of the Administrator: The Office of the Administrator assumes overall responsibility for the fulfillment of NASA's missions.
    - PA&E – The Office of Program Analysis and Evaluation: PA&E "provides objective, transparent, and multidisciplinary analysis of NASA programs to inform strategic decision-making." PA&E also leads the Agency's strategic planning efforts.[90]
    - OSMA – The Office of Safety and Mission Assurance: OSMA "assures the safety and enhances the success of all NASA activities through the development, implementation, and oversight of Agency-wide safety, reliability, maintainability, and quality assurance (SRM&QA) policies and procedures."[91] OSMA is located at NASA Headquarters
    - OCE – The Office of the Chief Engineer: OCE "assures that the development efforts and missions operations of NASA are being planned and conducted on a sound engineering basis with proper controls and management."[92] OCE is located at NASA Headquarters.
    - Mission Directorate Offices: The Mission Directorate Offices manage the Agency's efforts to fulfill the missions of NASA. Each directorate is divided into programs, which are further divided into projects. There are four mission directorates: Aeronautics Research, Exploration Systems, Science, and Space Operations.
    - Mission Support Offices: The Mission Support Offices provide support to the Mission Directorates and the Centers in the areas of: strategic communications, human capital management, procurement, etc.

[89] It is important to note that OSMA does not provide funding to the Center S&MAs.

[90] <http://www.nasa.gov/offices/pae/home/index.html>

[91] <http://www.hq.nasa.gov/office/codeq/>

[92] <http://www.nasa.gov/about/highlights/scolese_bio.html>

- OIG – Office of the Inspector General: OIG "prevents and detects crime, fraud, waste, abuse, and mismanagement and promotes efficiency, effectiveness, and economy throughout NASA."[93] OIG's auditors, investigators, analysts, specialists, attorneys, and administrative staff are located at NASA Headquarters and the NASA Centers.
- NESC – The NASA Engineering and Safety Center: NESC is an Agency-wide technical resource funded by the OCE to perform independent technical assessments for NASA Centers, programs, and other organizations. NESC is headquartered at the Langley Research Center, but has a technical presence at all of the Centers.[94]

- **Level II: The Program Level** – includes institutional management and program management
  - Center Directors: The Center Directors provide an institution—in terms of facilities and technical expertise—in which the programs and projects operate. There are ten Centers: Ames Research Center, Dryden Flight Research Center, Glenn Research Center, Goddard Space Flight Center, Jet Propulsion Laboratory, Johnson Space Center, Kennedy Space Center, Langley Research Center, Marshall Space Flight Center, and Stennis Space Center.
  - Program Offices: Each program office, under the direction of its Mission Directorate Office, manages a number of project offices. While each program office is located at a specific Center, it may oversee project offices at multiple Centers. An example of a program office in the Space Operations Mission Directorate is the Space Shuttle Program Office, which oversees project offices such as the Space Shuttle Orbiter Project Office, the Space Shuttle External Tank Project Office, etc.

- **Level III: The Project Level** – includes project management
  - Project Offices: The project offices can best be described as the Working Level of the Mission Directorates. Each project office, under the direction of its program office, manages the functions necessary to complete the projects of each Mission Directorate. The project offices acquire technical personnel (either civil servants or contractors based on-site at the Centers) from the Center S&MA and Engineering Directorates to perform in-house functions. The advantage of this arrangement is that the employees and institutional knowledge gained on each program/project can be transitioned to new programs/projects at the conclusion of each program/project. The drawback to this arrangement is that civil servants might exist within the institution without being assigned to a project.[95,96] The project offices also procure equipment and services from off-site contractors whenever the necessary in-house expertise to perform that function is not available.
  - Center S&MA Directorates: The Center S&MA Directorates are the institutional elements from which the project offices acquire Center personnel (either civil

[93] < http://www.hq.nasa.gov/office/oig/hq/mission.html>

[94] <http://www.nesc.nasa.gov/index.cfm?linkfrom=home>

[95] This problem typically arises when employee skill sets do not translate well from project to project. For example, an astrophysics project may conclude and be replaced by an aeronautics project. Consequently, the highly specialized astrophysicists that worked on the original project may not have the knowledge or interest necessary to gain assignment to the aeronautics project.

[96] NASA refers to the civil servants that fall under this category as "Unfunded Capacity." In the 2007 Budget Request, NASA estimated that the "Unfunded Capacity" was roughly 1000 civil servants.

servants or contractors based on-site at the Centers) to perform functions defined by OSMA to be "Safety and Mission Assurance" functions.

  - Center Engineering Directorates: The Center Engineering Directorates are the institutional elements from which the project offices acquire Center personnel (either civil servants or contractors based on-site at the Centers) to perform functions defined by OCE to be Engineering functions.

- **Level IV: The Contractor/Subcontractor Level** – includes activities of the off-site contractors and subcontractors

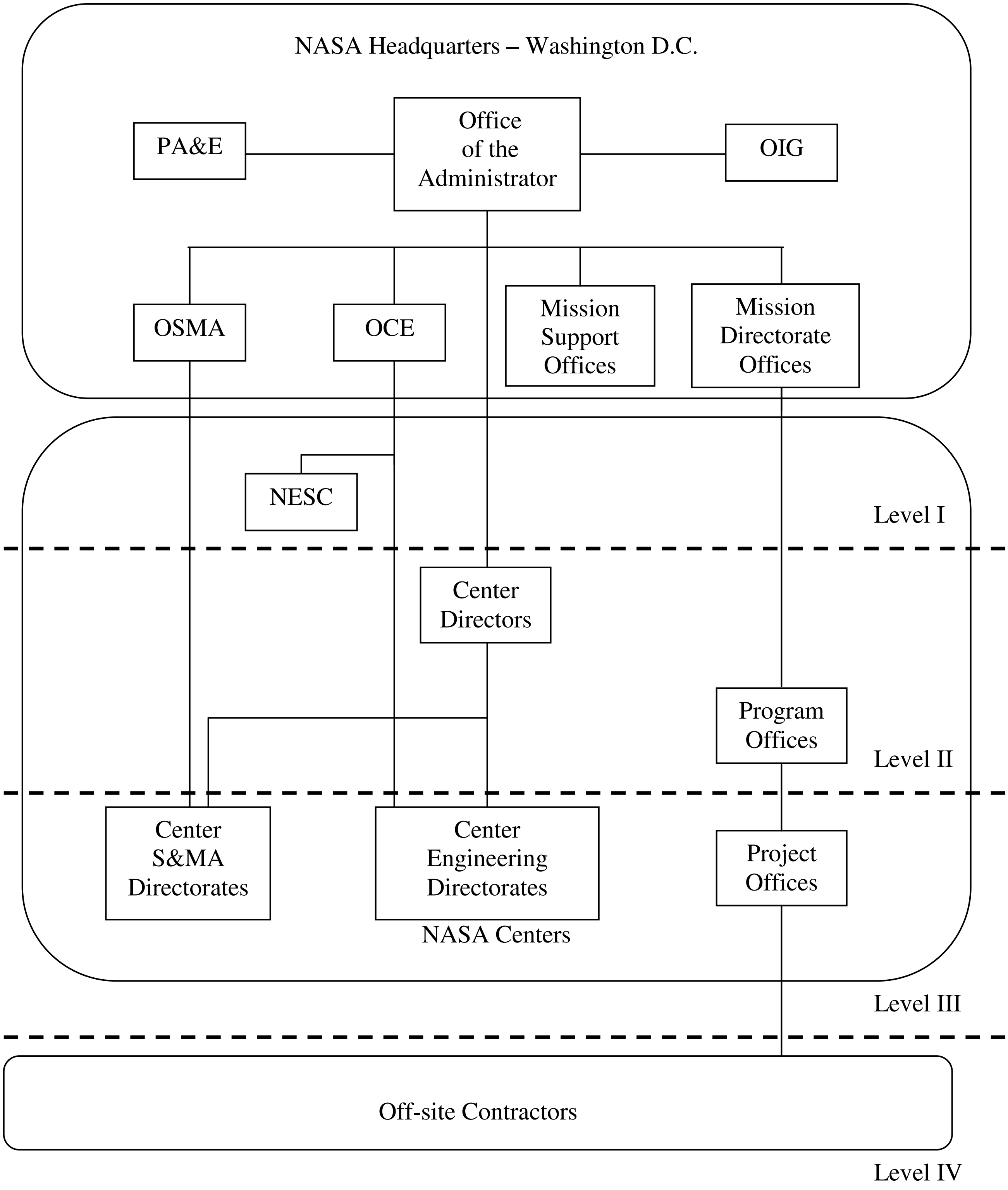


Figure 50. NASA's Organizational Structure (Summer of 2006).

Appendix D: Abstraction Level 3 of the Model (Variables and Minor Loops)

This Appendix contains causal loop diagrams for each module in the model, as well as an associated list of inputs, internal variables, and outputs.

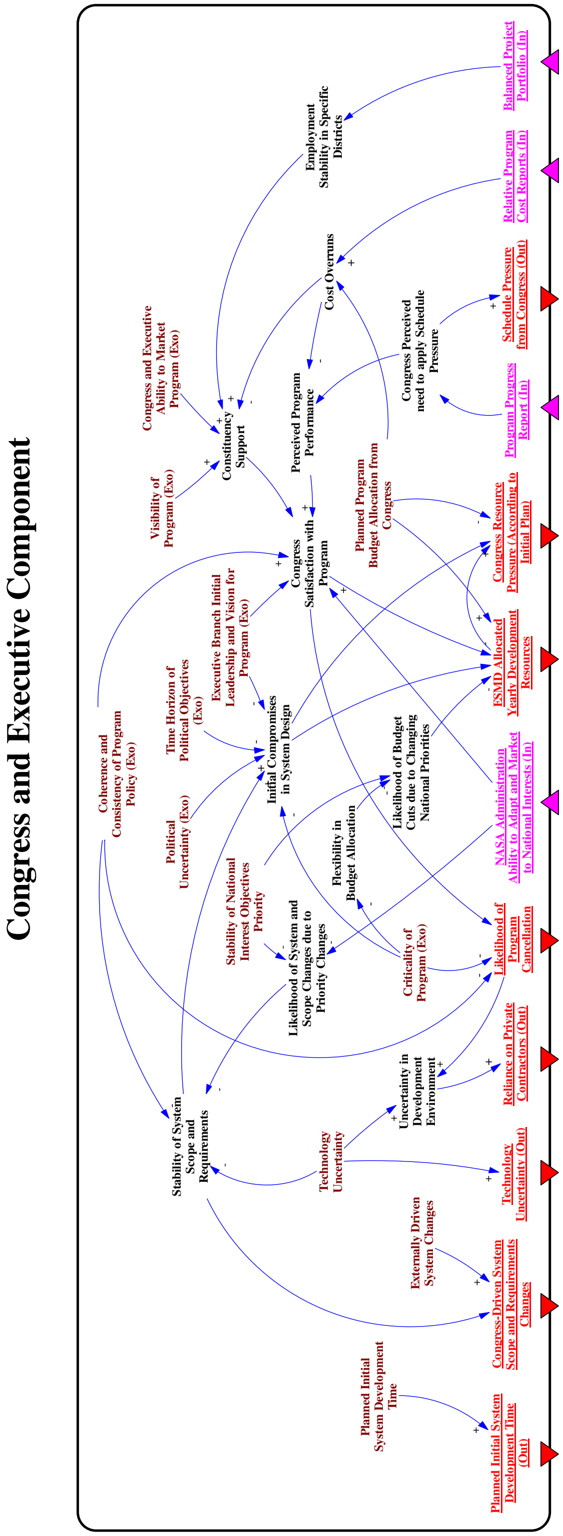

Congress and Executive Component
Coherence and Consistency of Program Policy (Exo)
Stability of System Scope and Requirements
Political Uncertainty (Exo)
Time Horizon of Political Objectives (Exo)
Visibility of Program (Exo)
Congress and Executive Ability to Market Program (Exo)
Executive Branch Initial Leadership and Vision for Program (Exo)
Stability of National Interest Objectives Priority
Initial Compromises in System Design
Constituency Support
Likelihood of System and Scope Changes due to Priority Changes
Congress Satisfaction with Program
Perceived Program Performance
Cost Overruns
Employment Stability in Specific Districts
Technology Uncertainty
Flexibility in Budget Allocation
Planned Program Budget Allocation from Congress
Planned Initial System Development Time
Uncertainty in Development Environment
Likelihood of Budget Cuts due to Changing National Priorities
Criticality of Program (Exo)
Externally Driven System Changes
Congress Perceived need to apply Schedule Pressure
Planned Initial System Development Time (Out)
Congress-Driven System Scope and Requirements Changes
Technology Uncertainty (Out)
Reliance on Private Contractors (Out)
Likelihood of Program Cancellation
NASA Administration Ability to Adapt and Market to National Interests (In)
ESMD Allocated Yearly Development Resources
Congress Resource Pressure (According to Initial Plan)
Program Progress Report (In)
Schedule Pressure from Congress (Out)
Relative Program Cost Reports (In)
Balanced Project Portfolio (In)
+
-

Figure 51. Congress and Executive (White House) module of the model.

Congress and Executive Module Variables:

Inputs (from NASA):
- NASA administration ability to adapt and market in national interests
- Program progress reports
- Relative program cost reports
- Balanced project portfolio

Internal variables:
- Planned initial system development time
- Externally driven system changes
- Stability of system scope and requirements
- Technology Uncertainty
- Uncertainty in development environment
- Stability of national interest objectives priority
- Likelihood of system and scope changes due to priority changes
- Criticality of program (exogenous)
- Flexibility in budget allocation
- Political uncertainty (exogenous)
- Coherence and consistency of program policy (exogenous)
- Time horizon of political objectives (exogenous)
- Executive branch initial leadership and vision for program (exogenous)
- Initial compromises in system design
- Likelihood of budget cuts due to changing national priorities
- Congress satisfaction with program
- Visibility of program (exogenous)
- Congress and executive ability to market program (exogenous)
- Constituency support
- Planned Program Budget Allocation from Congress
- Perceived program performance
- Congress Perceived need to apply schedule pressure
- Cost overruns
- Employment stability in specific districts

Outputs (to NASA):
- Planned initial system development time
- Congress-driven system scope and requirements changes
- Technology uncertainty
- Reliance on private contractors
- Likelihood of program cancellation
- ESMD allocated yearly development resources
- Congress resource pressure (according to initial plan)
- Schedule pressure from Congress

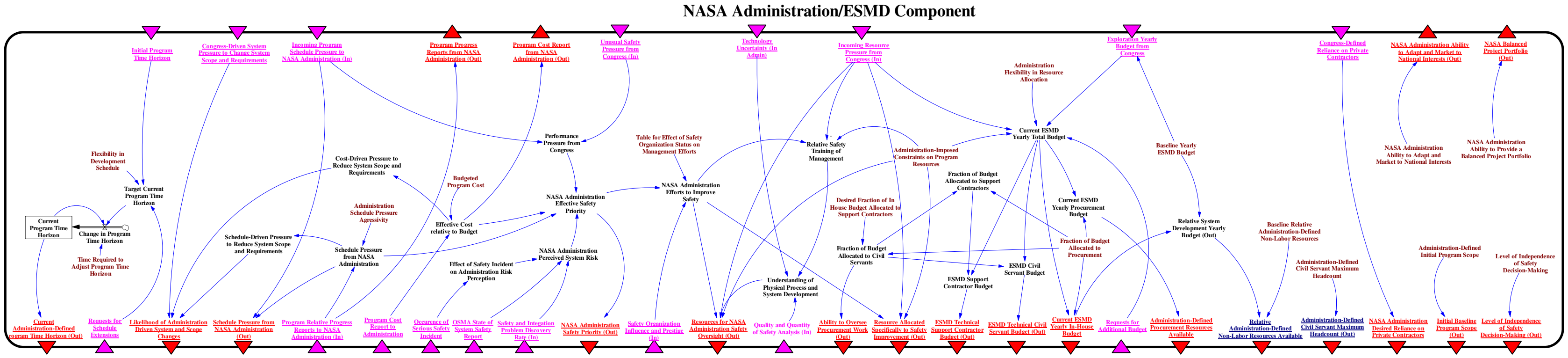

NASA Administration/ESMD Component
Initial Program Time Horizon
Congress-Driven System Pressure to Change System Scope and Requirements
Incoming Program Schedule Pressure to NASA Administration (In)
Program Progress Reports from NASA Administration (Out)
Program Cost Report from NASA Administration (Out)
Unusual Safety Pressure from Congress (In)
Technology Uncertainty (In Admin)
Incoming Resource Pressure from Congress (In)
Administration Flexibility in Resource Allocation
Exploration Yearly Budget from Congress
Congress-Defined Reliance on Private Contractors
NASA Administration Ability to Adapt and Market to National Interests (Out)
NASA Balanced Project Portfolio (Out)
Flexibility in Development Schedule
Target Current Program Time Horizon
Current Program Time Horizon
Change in Program Time Horizon
Time Required to Adjust Program Time Horizon
Cost-Driven Pressure to Reduce System Scope and Requirements
Performance Pressure from Congress
Budgeted Program Cost
Administration Schedule Pressure Agressivity
Schedule-Driven Pressure to Reduce System Scope and Requirements
Schedule Pressure from NASA Administration
Effective Cost relative to Budget
NASA Administration Effective Safety Priority
Effect of Safety Incident on Administration Risk Perception
NASA Administration Perceived System Risk
Table for Effect of Safety Organization Status on Management Efforts
NASA Administration Efforts to Improve Safety
Relative Safety Training of Management
Administration-Imposed Constraints on Program Resources
Current ESMD Yearly Total Budget
Fraction of Budget Allocated to Support Contractors
Desired Fraction of In House Budget Allocated to Support Contractors
Fraction of Budget Allocated to Civil Servants
Understanding of Physical Process and System Development
ESMD Support Contractor Budget
ESMD Civil Servant Budget
Current ESMD Yearly Procurement Budget
Fraction of Budget Allocated to Procurement
Baseline Yearly ESMD Budget
Relative System Development Yearly Budget (Out)
Baseline Relative Administration-Defined Non-Labor Resources
Administration-Defined Civil Servant Maximum Headcount
NASA Administration Ability to Adapt and Market to National Interests
NASA Administration Ability to Provide a Balanced Project Portfolio
Administration-Defined Initial Program Scope
Level of Independence of Safety Decision-Making
Current Administration-Defined rogram Time Horizon (Out)
Requests for Schedule Extensions
Likelihood of Administration Driven System and Scope Changes
Schedule Pressure from NASA Administration (Out)
Program Relative Progress Reports to NASA Administration (In)
Program Cost Report to Administration
Occurence of Serious Safety Incident
OSMA State of System Safety Report
Safety and Integation Problem Discovery Rate (In)
NASA Administration Safety Priority (Out)
Safety Organization Influence and Prestige (In)
Resources for NASA Administration Safety Oversight (Out)
Quality and Quantity of Safety Analysis (In)
Ability to Oversee Procurement Work (Out)
Resource Allocated Specifically to Safety Improvement (Out)
ESMD Technical Support Contractor Budget (Out)
ESMD Technical Civil Servant Budget (Out)
Current ESMD Yearly In-House Budget
Requests for Additional Budget
Administration-Defined Procurement Resources Available
Relative Administration-Defined Non-Labor Resources Available
Administration-Defined Civil Servant Maximum Headcount (Out)
NASA Administration Desired Reliance on Private Contractors
Initial Baseline Program Scope (Out)
Level of Independence of Safety Decision-Making (Out)

Figure 52. NASA Administration and ESMD module of the model.

NASA Administration/ESMD Module Variables:

Inputs (from above):

- Initial program time horizon
- Congress-driven pressure to change system scope and requirements
- Incoming program schedule pressure to NASA administration
- Unusual safety pressure from Congress
- Technology uncertainty
- Incoming resource pressure from Congress
- Exploration yearly budget from Congress
- Congress-defined reliance on private contractors

Inputs (from below):

- Requests for schedule extensions
- Program relative progress reports to Administration
- Program cost report to Administration
- Occurrence of serious safety incident
- OSMA state of system safety report
- Safety and integration problem discovery rate
- Safety organization influence and prestige
- Quality and quantity of safety analysis
- Requests for additional budget

Internal Variables:

- NASA Administration ability to adapt and market to national interests
- NASA Administration ability to provide a balanced portfolio
- Administration-defined initial program scope
- Level of independence of safety-decision making
- Current program time horizon
- Change in current program time horizon
- Time required to adjust Program time horizon
- Flexibility in development schedule
- Target current program time horizon
- Cost-driven pressure to reduce system scope and requirements
- Schedule-driven pressure to reduce system scope and requirements
- Administration schedule pressure aggressivity
- Schedule pressure from NASA Administration
- Budgeted program cost
- Effective cost relative to budget
- Performance pressure from Congress
- NASA administration effective safety pressure
- NASA administration perceived system risk
- Effect of safety incident on Administration risk perception
- Effect of safety organization status on management efforts
- NASA administration efforts to improve safety
- Relative safety training of management
- Understanding of physical process and system development
- Administration-imposed constraints on program resources
- Desired fraction of in-house budget allocated to contractors
- Fraction of budget allocated to civil servants
- Fraction of budget allocated to support contractors
- Administration flexibility in resource allocation
- Current ESMD yearly total budget
- ESMD support contractor budget
- ESMD civil servant budget
- Current ESMD yearly procurement budget
- Fraction of budget allocated to procurement
- Baseline yearly ESMD budget
- Relative system development yearly budget

- Baseline relative administration-defined non-labor resources
- Administration-defined civil servant maximum headcount

Outputs (to above):

- Program progress reports from NASA Administration
- Program cost report from NASA Administration
- NASA administration ability to adapt and market to national interests
- NASA balanced project portfolio

Outputs (to below):

- Current administration-defined program time horizon
- Likelihood of administration-driven system and scope changes
- Schedule pressure from NASA administration
- NASA administration safety priority
- Resources for NASA administration safety oversight
- Ability to oversee procurement work
- Resources allocated specifically to safety improvement
- ESMD technical support contractor budget
- ESMD technical civil servant budget
- Current ESMD yearly in-house budget
- Administration-defined procurement resources available
- Relative administration-defined non-labor resources available
- Administration-defined civil servant maximum headcount
- NASA administration desired reliance on private contractors
- Initial baseline program scope
- Level of independence of safety decision-making

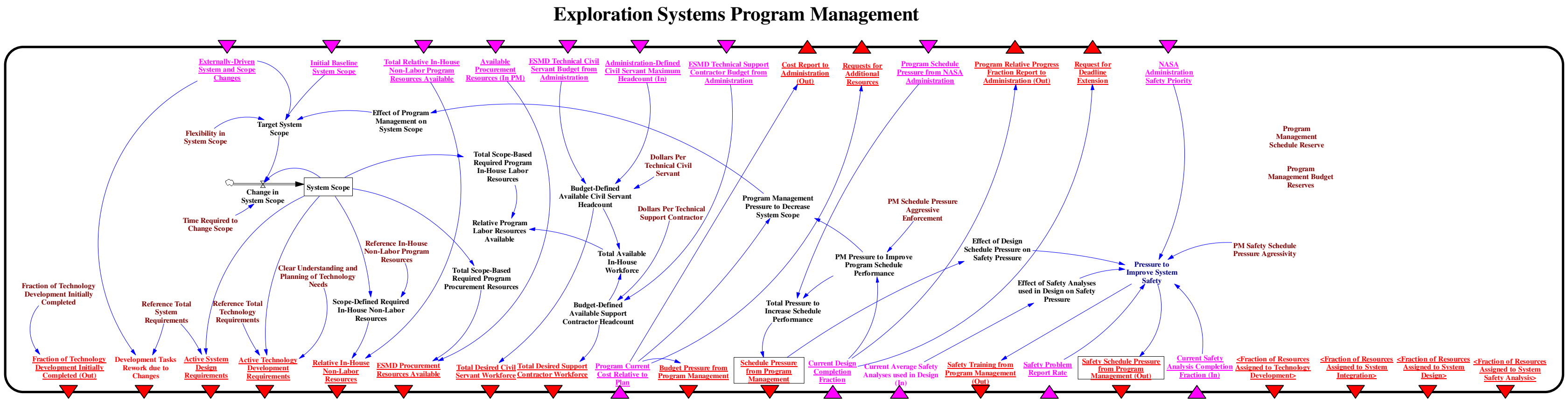

Exploration Systems Program Management
Externally-Driven System and Scope Changes
Initial Baseline System Scope
Total Relative In-House Non-Labor Program Resources Available
Available Procurement Resources (In PM)
ESMD Technical Civil Servant Budget from Administration
Administration-Defined Civil Servant Maximum Headcount (In)
ESMD Technical Support Contractor Budget from Administration
Cost Report to Administration (Out)
Requests for Additional Resources
Program Schedule Pressure from NASA Administration
Program Relative Progress Fraction Report to Administration (Out)
Request for Deadline Extension
NASA Administration Safety Priority
Effect of Program Management on System Scope
Target System Scope
Flexibility in System Scope
Program Management Schedule Reserve
Program Management Budget Reserves
Total Scope-Based Required Program In-House Labor Resources
Dollars Per Technical Civil Servant
System Scope
Change in System Scope
Budget-Defined Available Civil Servant Headcount
Program Management Pressure to Decrease System Scope
Dollars Per Technical Support Contractor
PM Schedule Pressure Aggressive Enforcement
Time Required to Change Scope
Relative Program Labor Resources Available
Reference In-House Non-Labor Program Resources
Total Available In-House Workforce
Effect of Design Schedule Pressure on Safety Pressure
PM Safety Schedule Pressure Agressivity
PM Pressure to Improve Program Schedule Performance
Pressure to Improve System Safety
Clear Understanding and Planning of Technology Needs
Total Scope-Based Required Program Procurement Resources
Effect of Safety Analyses used in Design on Safety Pressure
Fraction of Technology Development Initially Completed
Reference Total System Requirements
Reference Total Technology Requirements
Scope-Defined Required In-House Non-Labor Resources
Budget-Defined Available Support Contractor Headcount
Total Pressure to Increase Schedule Performance
Fraction of Technology Development Initially Completed (Out)
Development Tasks Rework due to Changes
Active System Design Requirements
Active Technology Development Requirements
Relative In-House Non-Labor Resources
ESMD Procurement Resources Available
Total Desired Civil Servant Workforce
Total Desired Support Contractor Workforce
Program Current Cost Relative to Plan
Budget Pressure from Program Management
Schedule Pressure from Program Management
Current Design Completion Fraction
Current Average Safety Analyses used in Design (In)
Safety Training from Program Management (Out)
Safety Problem Report Rate
Safety Schedule Pressure from Program Management (Out)
Current Safety Analysis Completion Fraction (In)
<Fraction of Resources Assigned to Technology Development>
<Fraction of Resources Assigned to System Integration>
<Fraction of Resources Assigned to System Design>
<Fraction of Resources Assigned to System Safety Analysis>

Figure 53. Exploration Program and Project Management module of the model.

Exploration Systems Program Management Module Variables:

Inputs (from above):

- Externally-driven system and scope changes
- Initial baseline system scope
- Total relative in-house non-labor program resources available
- Available program resources
- ESMD technical civil servant budget from administration
- Administration-defined civil servant maximum headcount
- ESMD technical support contractor budget from administration
- Program schedule pressure from NASA administration
- NASA administration safety priority

Inputs (from below):

- Program current cost relative to plan
- Current design completion fraction
- Current average safety analyses used in design
- Safety problem report rate
- Current safety analysis completion fraction

Internal Variables:

- Target system scope
- Flexibility in system scope
- Change in system scope
- Time required to change scope
- Effect of program management on system scope
- System scope
- Reference total technology requirements
- Fraction of technology development initially completed
- Reference total system requirements
- Clear understanding and planning of technology needs
- Reference in-house non-labor program resources
- Scope-defined required in-house non-labor resources
- Total scope-based required program procurement resources
- Total scope-based required program in-house labor resources
- Relative program labor resources available
- Budget-defined available civil servant headcount
- Total available in-house workforce
- Budget-defined available support contractor headcount
- Dollars per technical support contractor
- Dollars per technical civil servant
- Program management pressure to decrease system scope
- Total pressure to increase schedule performance
- PM pressure to improve program schedule performance
- PM schedule pressure aggressive enforcement
- Effect of design schedule pressure on safety pressure
- Effect of safety analyses used in design on safety pressure
- Pressure to improve system safety
- PM schedule pressure aggressivity
- Program management schedule reserve
- Program management budget reserves

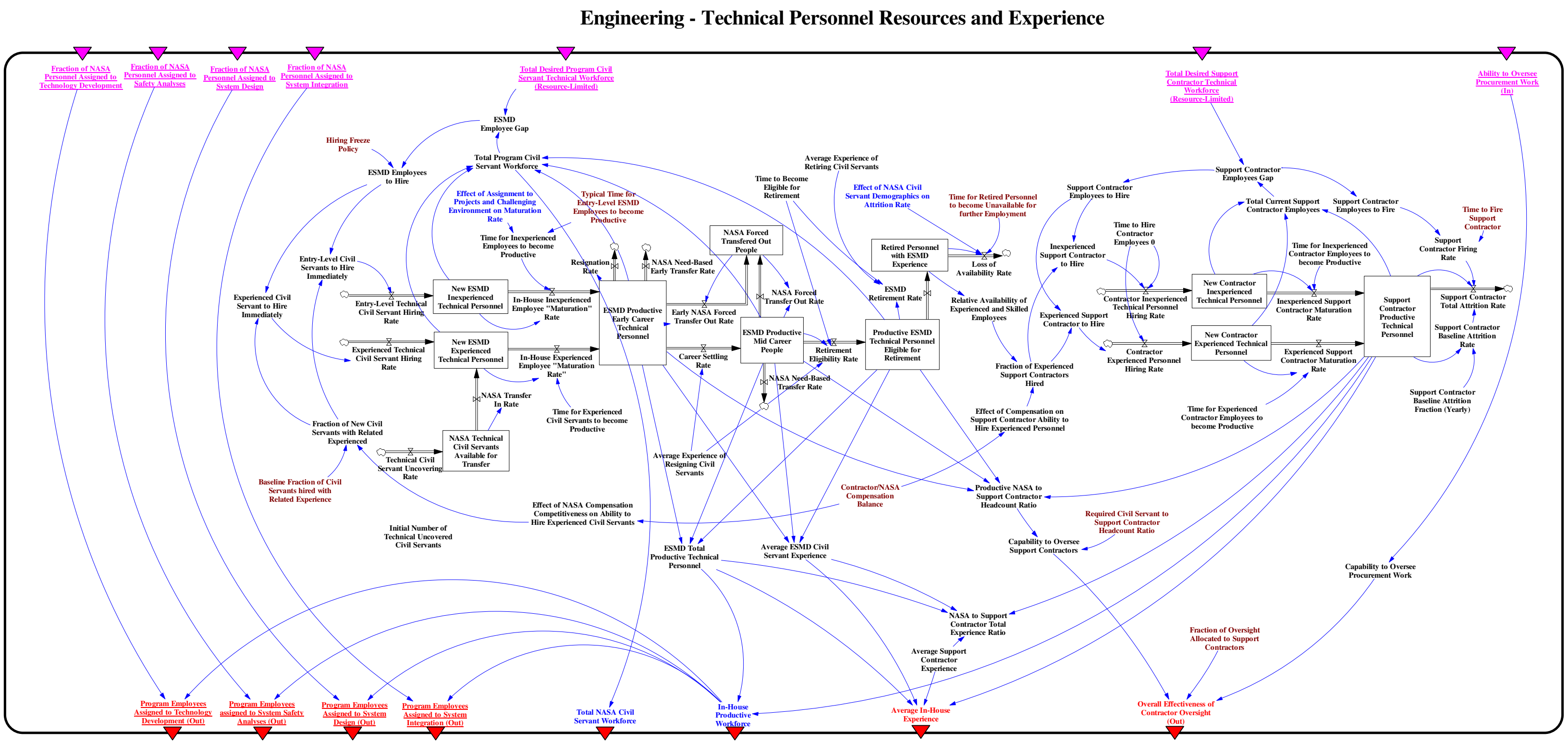
Outputs (to above):

- Cost report to administration
- Requests for additional resources
- Program relative progress fraction report to administration
- Request for deadline extension

Outputs (to below):

- Fraction of resources assigned to technology development
- Fraction of resources assigned to system integration
- Fraction of resources assigned to system design

- Fraction of resources assigned to system safety
- Fraction of technology development initially completed
- Development tasks rework due to changes
- Active system design requirements
- Active technology development requirements
- Relative in-house non-labor resources
- ESMD procurement resources available
- Total desired civil servant workforce
- Total desired support contractor workforce
- Budget pressure from program management
- Schedule pressure from program management
- Safety training from program management
- Safety schedule pressure from program management


Engineering - Technical Personnel Resources and Experience

Fraction of NASA Personnel Assigned to Technology Development
Fraction of NASA Personnel Assigned to Safety Analyses
Fraction of NASA Personnel Assigned to System Design
Fraction of NASA Personnel Assigned to System Integration
Total Desired Program Civil Servant Technical Workforce (Resource-Limited)
Total Desired Support Contractor Technical Workforce (Resource-Limited)
Ability to Oversee Procurement Work (In)
ESMD Employee Gap
Hiring Freeze Policy
Total Program Civil Servant Workforce
ESMD Employees to Hire
Effect of Assignment to Projects and Challenging Environment on Maturation Rate
Typical Time for Entry-Level ESMD Employees to become Productive
Time for Inexperienced Employees to become Productive
Entry-Level Civil Servants to Hire Immediately
Experienced Civil Servant to Hire Immediately
Entry-Level Technical Civil Servant Hiring Rate
New ESMD Inexperienced Technical Personnel
In-House Inexperienced Employee "Maturation" Rate
Experienced Technical Civil Servant Hiring Rate
New ESMD Experienced Technical Personnel
In-House Experienced Employee "Maturation" Rate
Resignation Rate
NASA Need-Based Early Transfer Rate
ESMD Productive Early Career Technical Personnel
NASA Forced Transfered Out People
Early NASA Forced Transfer Out Rate
NASA Forced Transfer Out Rate
Career Settling Rate
ESMD Productive Mid Career People
NASA Need-Based Transfer Rate
Time to Become Eligible for Retirement
Average Experience of Retiring Civil Servants
Effect of NASA Civil Servant Demographics on Attrition Rate
Time for Retired Personnel to become Unavailable for further Employment
Retired Personnel with ESMD Experience
Loss of Availability Rate
ESMD Retirement Rate
Retirement Eligibility Rate
Productive ESMD Technical Personnel Eligible for Retirement
Relative Availability of Experienced and Skilled Employees
NASA Transfer In Rate
NASA Technical Civil Servants Available for Transfer
Technical Civil Servant Uncovering Rate
Time for Experienced Civil Servants to become Productive
Fraction of New Civil Servants with Related Experienced
Baseline Fraction of Civil Servants hired with Related Experience
Initial Number of Technical Uncovered Civil Servants
Effect of NASA Compensation Competitiveness on Ability to Hire Experienced Civil Servants
Average Experience of Resigning Civil Servants
Contractor/NASA Compensation Balance
ESMD Total Productive Technical Personnel
Average ESMD Civil Servant Experience
Support Contractor Employees Gap
Support Contractor Employees to Hire
Total Current Support Contractor Employees
Support Contractor Employees to Fire
Time to Fire Support Contractor
Support Contractor Firing Rate
Time to Hire Contractor Employees 0
Inexperienced Support Contractor to Hire
Time for Inexperienced Contractor Employees to become Productive
Contractor Inexperienced Technical Personnel Hiring Rate
New Contractor Inexperienced Technical Personnel
Inexperienced Support Contractor Maturation Rate
Support Contractor Productive Technical Personnel
Support Contractor Total Attrition Rate
Support Contractor Baseline Attrition Rate
Experienced Support Contractor to Hire
Contractor Experienced Personnel Hiring Rate
New Contractor Experienced Technical Personnel
Experienced Support Contractor Maturation Rate
Fraction of Experienced Support Contractors Hired
Effect of Compensation on Support Contractor Ability to Hire Experienced Personnel
Time for Experienced Contractor Employees to become Productive
Support Contractor Baseline Attrition Fraction (Yearly)
Productive NASA to Support Contractor Headcount Ratio
Required Civil Servant to Support Contractor Headcount Ratio
Capability to Oversee Support Contractors
Capability to Oversee Procurement Work
NASA to Support Contractor Total Experience Ratio
Average Support Contractor Experience
Fraction of Oversight Allocated to Support Contractors
Program Employees Assigned to Technology Development (Out)
Program Employees assigned to System Safety Analyses (Out)
Program Employees Assigned to System Design (Out)
Program Employees Assigned to System Integration (Out)
Total NASA Civil Servant Workforce
In-House Productive Workforce
Average In-House Experience
Overall Effectiveness of Contractor Oversight (Out)

Figure 54. Engineering—Technical Personnel Resources and Experience module of the model

Engineering---Technical Personnel Resources and Experience Module Variables:

Inputs (from above):

- Fraction of NASA personnel assigned to technology development
- Fraction of NASA personnel assigned to safety
- Fraction of NASA personnel assigned to system design
- Fraction of NASA personnel assigned to system integration
- Total desired program civil servant technical workforce (resource-limited)
- Total desired support contractor technical workforce (resource-limited)
- Ability to oversee procurement work

Internal Variables:

- Hiring freeze policy
- ESMD employees to hire
- Experienced civil servants to hire immediately
- Entry level civil servants to hire immediately
- Fraction of new civil servants with related experience
- Baseline fraction of civil servants hired with related experience
- Entry-level technical servant hiring rate
- Experienced technical servant hiring rate
- Technical civil servant uncovering rate
- Initial number of technical uncovered civil servants
- ESMD employees to hire
- NASA technical civil servants available for transfer
- New ESMD experienced technical personnel
- New ESMD inexperienced technical personnel
- In-house experienced maturation rate
- In-house inexperienced maturation rate
- Time for experienced civil servants to become productive
- ESMD productive early career technical personnel
- Resignation rate
- NASA need-based early transfer rate
- ESMD employee gap
- Total program civil servant workforce
- Effect of assignment to projects and challenging environment on maturation rate
- Typical time for entry-level ESMD employees to become productive
- Time for inexperienced employees to become productive
- NASA transfer in rate
- Effect of NASA compensation competitiveness on ability to hire experienced civil servants
- Contractor/NASA compensation balance
- Effect of compensation on support contractor ability to hire experienced personnel
- Average experience of resigning civil servants
- ESMD total productive technical personnel
- Average ESMD civil servant experience
- Career settling rate
- Early NASA forced transfer out rate
- NASA forced transfer out people
- NASA forced transfer out rate
- ESMD productive mid-career people
- NASA need-based transfer rate
- Time to become eligible for retirement
- Retirement eligibility rate
- Average experience of retiring civil servants
- ESMD retirement rate
- Productive ESMD technical personnel eligible for retirement
- Retired personnel with ESMD experience

- Effect of NASA civil servant demographics on attrition rate
- Time for retired personnel to become unavailable for further employment
- Loss of availability rate
- Relative availability of experienced and skilled employees
- Fraction of experienced support contractors hired
- Experienced support contractors to hire
- Inexperienced support contractors to hire
- Support contractor employees to hire
- Time to hire contractor employees
- Contractor inexperienced technical personnel hiring rate
- Contractor experienced technical personnel hiring rate
- New contractor experienced technical personnel
- New contractor inexperienced technical personnel
- Time for experienced contractor employees to become productive
- Experienced support contractor maturation rate
- Inexperienced support contractor maturation rate
- Time for inexperienced contractor employees to become productive
- Support contractors employees gap
- Total current support contractor employees
- Support contractor employees to fire
- Support contractor firing rate
- Time to fire support contractor
- Support contractor productive technical personnel
- Support contractor baseline attrition fraction (yearly)
- Support contractor baseline attrition rate
- Support contractor total attrition rate
- Productive NASA to support contractor headcount ratio
- Capability to oversee support contractors
- Required civil servant to support contractor headcount ratio
- Fraction of oversight allocated to support contractors
- Capability to oversee procurement work
- Average support contractor experience
- NASA to support contractor total experience ratio

Outputs (to below):

- Program employees assigned to technology development
- Program employees assigned to safety
- Program employees assigned to system design
- Program employees assigned to system integration
- Total NASA civil servant workforce
- In-house productive workforce
- Average in-house experience
- Overall effectiveness of contractor oversight

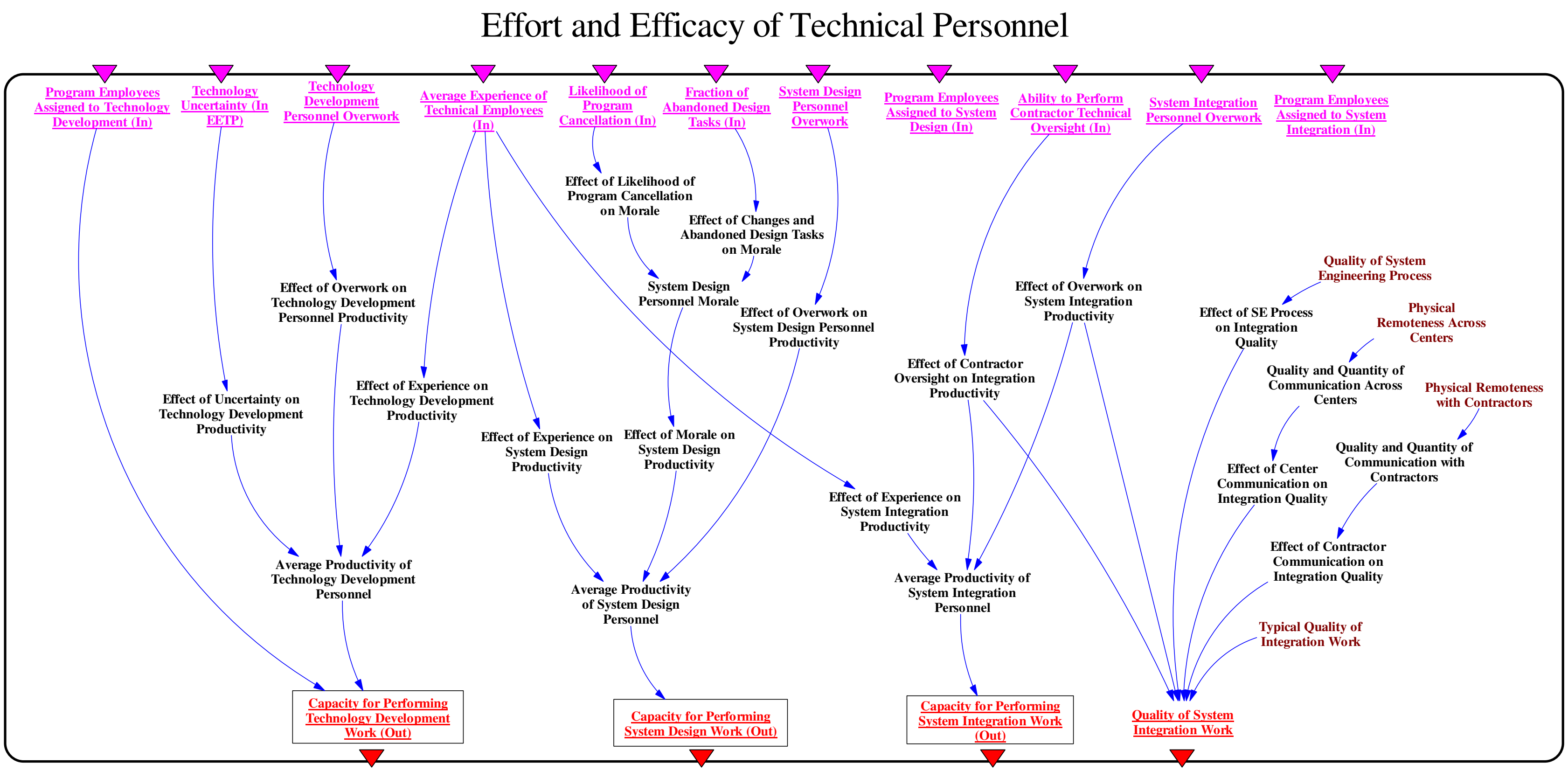

Effort and Efficacy of Technical Personnel
Program Employees Assigned to Technology Development (In)
Technology Uncertainty (In EETP)
Technology Development Personnel Overwork
Average Experience of Technical Employees (In)
Likelihood of Program Cancellation (In)
Fraction of Abandoned Design Tasks (In)
System Design Personnel Overwork
Program Employees Assigned to System Design (In)
Ability to Perform Contractor Technical Oversight (In)
System Integration Personnel Overwork
Program Employees Assigned to System Integration (In)
Effect of Likelihood of Program Cancellation on Morale
Effect of Changes and Abandoned Design Tasks on Morale
Effect of Overwork on Technology Development Personnel Productivity
System Design Personnel Morale
Effect of Overwork on System Design Personnel Productivity
Effect of Overwork on System Integration Productivity
Quality of System Engineering Process
Effect of SE Process on Integration Quality
Physical Remoteness Across Centers
Quality and Quantity of Communication Across Centers
Physical Remoteness with Contractors
Effect of Contractor Oversight on Integration Productivity
Effect of Uncertainty on Technology Development Productivity
Effect of Experience on Technology Development Productivity
Effect of Experience on System Design Productivity
Effect of Morale on System Design Productivity
Effect of Experience on System Integration Productivity
Effect of Center Communication on Integration Quality
Quality and Quantity of Communication with Contractors
Effect of Contractor Communication on Integration Quality
Average Productivity of Technology Development Personnel
Average Productivity of System Design Personnel
Average Productivity of System Integration Personnel
Typical Quality of Integration Work
Capacity for Performing Technology Development Work (Out)
Capacity for Performing System Design Work (Out)
Capacity for Performing System Integration Work (Out)
Quality of System Integration Work

Figure 55. Engineering—Effort and Efficacy of Technical Personnel module of the model.

Effort and Efficacy of Technical Personnel Module Variables:

Inputs (from above):
- Program employees assigned to technology development
- Technology uncertainty
- Technology development personnel overwork
- Average experience of technical employees
- Likelihood of program cancellation
- Fraction of abandoned design tasks
- System design personnel overwork
- Program employees assigned to system design
- Ability to perform contractor technical oversight
- System integration personnel overwork
- Program employees assigned to system integration

Internal Variables:
- Effect of uncertainty on technology development productivity
- Effect of overwork on technology personnel productivity
- Effect of experience on technology development productivity
- Average productivity of technology development productivity
- Effect of experience on system design productivity
- Effect of likelihood of program cancellation on morale
- Effect of changes and abandoned design tasks on morale
- System design personnel morale
- Effect of morale on system design productivity
- Effect of overwork on system design personnel productivity
- Average productivity of system design personnel
- Effect of experience on system integration productivity
- Effect of contractor oversight on integration productivity
- Effect of overwork on system integration productivity
- Average productivity of system integration personnel
- Quality of system engineering process
- Effect of SE process on integration quality
- Physical remoteness across centers
- Quality and quantity of communication across centers
- Effect of center communication on integration quality
- Physical remoteness with contractors
- Quality and quantity of communication with contractors
- Effect of contractor communication on integration quality
- Typical quality of integration work

Outputs (to below):
- Capacity for performing technology development work
- Capacity for performing system design work
- Capacity for performing system integration work
- Quality of system integration work

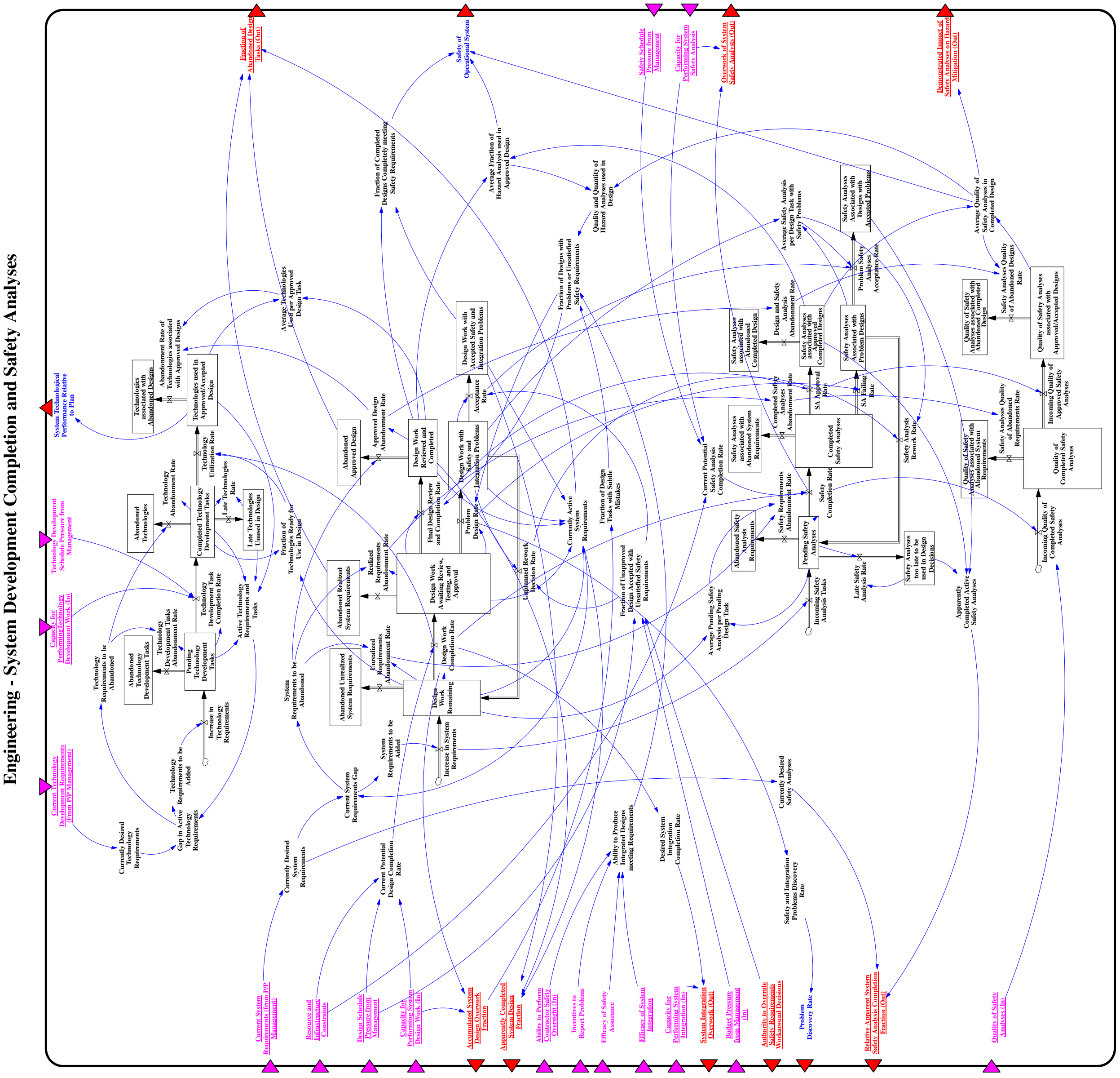

Engineering - System Development Completion and Safety Analyses
Current Technology Development Requirements (From P/P Management)
Capacity for Performing Technology Development Work (In)
Technology Development Schedule Pressure from Management
System Technological Performance Relative to Plan
Currently Desired Technology Requirements
Technology Requirements to be Abandoned
Abandoned Technology Development Tasks
Abandoned Technologies
Technologies associated with Abandoned Designs
Gap in Active Technology Requirements
Technology Requirements to be Added
Technology Development Tasks Abandonment Rate
Technology Abandonment Rate
Abandonment Rate of Technologies associated with Approved Designs
Increase in Technology Requirements
Pending Technology Development Tasks
Technology Development Task Completion Rate
Completed Technology Development Tasks
Technology Utilization Rate
Technologies used in Approved/Accepted Design
Late Technologies Rate
Active Technology Requirements and Tasks
Late Technologies Unused in Design
Fraction of Abandoned Design Tasks (Out)
Current System Requirements (from P/P Management)
Currently Desired System Requirements
System Requirements to be Abandoned
Fraction of Technologies Ready for Use in Design
Average Technologies Used per Approved Design Task
Resource and Infrastructure Constraints
Abandoned Unrealized System Requirements
Abandoned Realized System Requirements
Abandoned Approved Design
Current System Requirements Gap
Design Schedule Pressure from Management
Current Potential Design Completion Rate
Unrealized Requirements Abandonment Rate
Realized Requirements Abandonment Rate
Approved Design Abandonment Rate
Fraction of Completed Designs Completely meeting Safety Requirements
System Requirements to be Added
Capacity for Performing System Design Work (In)
Design Work Remaining
Design Work Completion Rate
Design Work Awaiting Review, Testing, and Approval
Final Design Review and Completion Rate
Design Work Reviewed and Completed
Increase in System Requirements
Problem Design Rate
Design Work with Safety and Integration Problems
Acceptance Rate
Design Work with Accepted Safety and Integration Problems
Safety of Operational System
Accumulated System Design Overwork Fraction
Average Fraction of Hazard Analysis used in Approved Design
Apparently Completed System Design Fraction
Unplanned Rework Decision Rate
Ability to Perform Contractor Safety Oversight (In)
Currently Active System Requirements
Fraction of Designs with Problems or Unsatisfied Safety Requirements
Incentives to Report Problems
Quality and Quantity of Hazard Analyses used in Design
Efficacy of Safety Assurance
Fraction of Design Tasks with Subtle Mistakes
Ability to Produce Integrated Designs meeting Requirements
Efficacy of System Integration
Fraction of Unapproved Design Accepted with Unsatisfied Safety Requirements
Safety Schedule Pressure from Management
Desired System Integration Completion Rate
Capacity for Performing System Integration (In)
Capacity for Performing System Safety Analysis
System Integration Overwork (Out)
Current Potential Safety Analysis Completion Rate
Average Pending Safety Analysis per Pending Design Task
Overwork of System Safety Analysts (Out)
Budget Pressure from Management (In)
Abandoned Safety Analysis Requirements
Safety Analyses associated with Abandoned System Requirements
Safety Analyses associated with Abandoned Completed Design
Authority to Overrule Safety Requirements Workaround Decisions
Currently Desired Safety Analyses
Safety Requirements Abandonment Rate
Completed Safety Analyses Abandonment Rate
Design and Safety Analysis Abandonment Rate
Average Safety Analysis per Design Task with Safety Problems
Safety and Integration Problems Discovery Rate
Pending Safety Analyses
Problem Discovery Rate
Incoming Safety Analysis Tasks
Safety Completion Rate
Completed Safety Analyses
SA Approval Rate
Safety Analyses associated with Approved Completed Designs
Late Safety Analysis Rate
SA Failing Rate
Safety Analyses Associated with Problem Designs
Problem Safety Analyses Acceptance Rate
Safety Analyses Associated with Designs with Accepted Problems
Relative Apparent System Safety Analysis Completion Fraction (Out)
Safety Analyses too late to be used in Design Decisions
Safety Analysis Rework Rate
Demonstrated Impact of Safety Analyses on Hazard Mitigation (Out)
Apparently Completed Active Safety Analyses
Quality of Safety Analyses associated with Abandoned System Requirements
Quality of Safety Analyses associated with Abandoned Completed Design
Average Quality of Safety Analyses in Completed Design
Safety Analyses Quality of Abandoned Requirements Rate
Safety Analyses Quality of Abandoned Designs Rate
Quality of Safety Analyses (In)
Incoming Quality of Completed Safety Analyses
Quality of Completed Safety Analyses
Incoming Quality of Approved Safety Analyses
Quality of Safety Analyses associated with Approved/Accepted Designs

Figure 56. System Development Completion and Safety Analyses module of the model.

Engineering---System Development Completion and Safety Analyses Module Variables:

Inputs:

- Current technology development requirements (from P/P management)
- Capacity for performing technology development work
- Technology development schedule pressure from management
- Safety schedule from program management
- Capacity for performing safety analyses
- Current system requirements (from P/P management)
- Resource and infrastructure constraints
- Design schedule pressure from management
- Capacity for performing system design work
- Ability to perform contractor safety oversight
- Incentives to report problems
- Efficacy of safety assurance

- Efficacy of system integration
- Capacity for performing system integration
- Budget pressure from management
- Quality of safety analyses

Internal Variables:

- Currently desired technology requirements
- Gap in active technology requirements
- Technology requirements to be added
- Increase in technology requirements
- Technology requirements to be abandoned
- Pending technology development tasks
- Technology development tasks abandonment rate
- Abandoned technology development tasks
- Technology task completion rate
- Active technology requirements and tasks
- Completed technology development tasks
- Technology abandonment rate
- Abandoned technologies
- Late technologies rate
- Late technologies unused in design
- Technology utilization rate
- Technologies used in approved/accepted design
- Abandonment rate of technologies associated with approved designs
- Technologies associated with abandoned designs
- Fraction of technologies ready for use in design
- Average technologies used per approved design task
- Currently desired system requirements
- Current potential design completion rate
- Ability to produce integrated designs meeting requirements
- Desired system integration completion rate
- Safety and integration problems discovery rate
- Currently desired safety analyses
- Current system requirements gap
- System requirements to be added
- System requirements to be abandoned
- Increase in system requirements
- Design work remaining
- Unrealized requirements abandonment rate
- Abandoned unrealized system requirements
- Design work completion work
- Design work awaiting review, testing, and approval
- Realized requirements abandonment rate
- Abandoned realized system requirements
- Final design review and completion rate
- Problem design rate
- Design work with safety and integration problems
- Unplanned rework decision rate
- Design work reviewed and completed
- Approved design abandonment rate
- Abandoned approved designs
- Acceptance rate
- Design work with accepted safety and integration problems
- Fraction of completed designs completely meeting system requirements
- Average fraction of hazard analysis used in approved design
- Quality and quantity of hazard analyses used in design
- Fraction of designs with problems or unsatisfied safety requirements
- Currently active system requirements
- Fraction of design tasks with subtle mistakes
- Fraction of unapproved design with unsatisfied safety requirements

- Average pending safety analysis per pending design task
- Incoming safety analyses tasks
- Late safety analysis rate
- Pending safety analyses
- Safety requirements abandonment rate
- Abandoned safety analysis requirements
- Safety analyses too late to be used in design decisions
- Safety completion rate
- Current potential safety analyses completion rate
- Completed safety analyses
- Completed safety analyses abandonment rate
- Safety analyses associated with abandoned system requirements
- SA approval rate
- SA failing rate
- Safety analysis rework rate
- Safety analyses associated with problem designs
- Safety analyses associated with approved completed designs
- Design and safety analysis abandonment rate
- Safety analyses associated with abandoned completed designs
- Problem safety analyses acceptance rate
- Safety analyses associated with designs with accepted problems
- Average safety analysis per design task with safety problems
- Apparently completed safety analyses
- Incoming quality of completed safety analyses
- Quality of completed safety analyses
- Safety analyses quality of abandoned requirements rate
- Quality of safety analyses associated with abandoned system requirements
- Incoming quality of approved safety analyses
- Quality of safety analyses associated with approved/accepted designs
- Safety analyses quality of abandoned designs rate
- Quality of safety analyses associated with abandoned completed design
- Average quality of safety analyses in completed design

Outputs:

- System technological performance relative to plan
- Accumulated system design overwork fraction
- Apparently completed system design fraction
- System integration overwork
- Authority to overrule safety requirements workaround decisions
- Problem discovery rate
- Relative apparent system safety analysis completion fraction
- Fraction of abandoned system design tasks
- Safety of operational system
- Overwork of system safety analysts
- Demonstrated impact of safety analyses on hazard mitigation

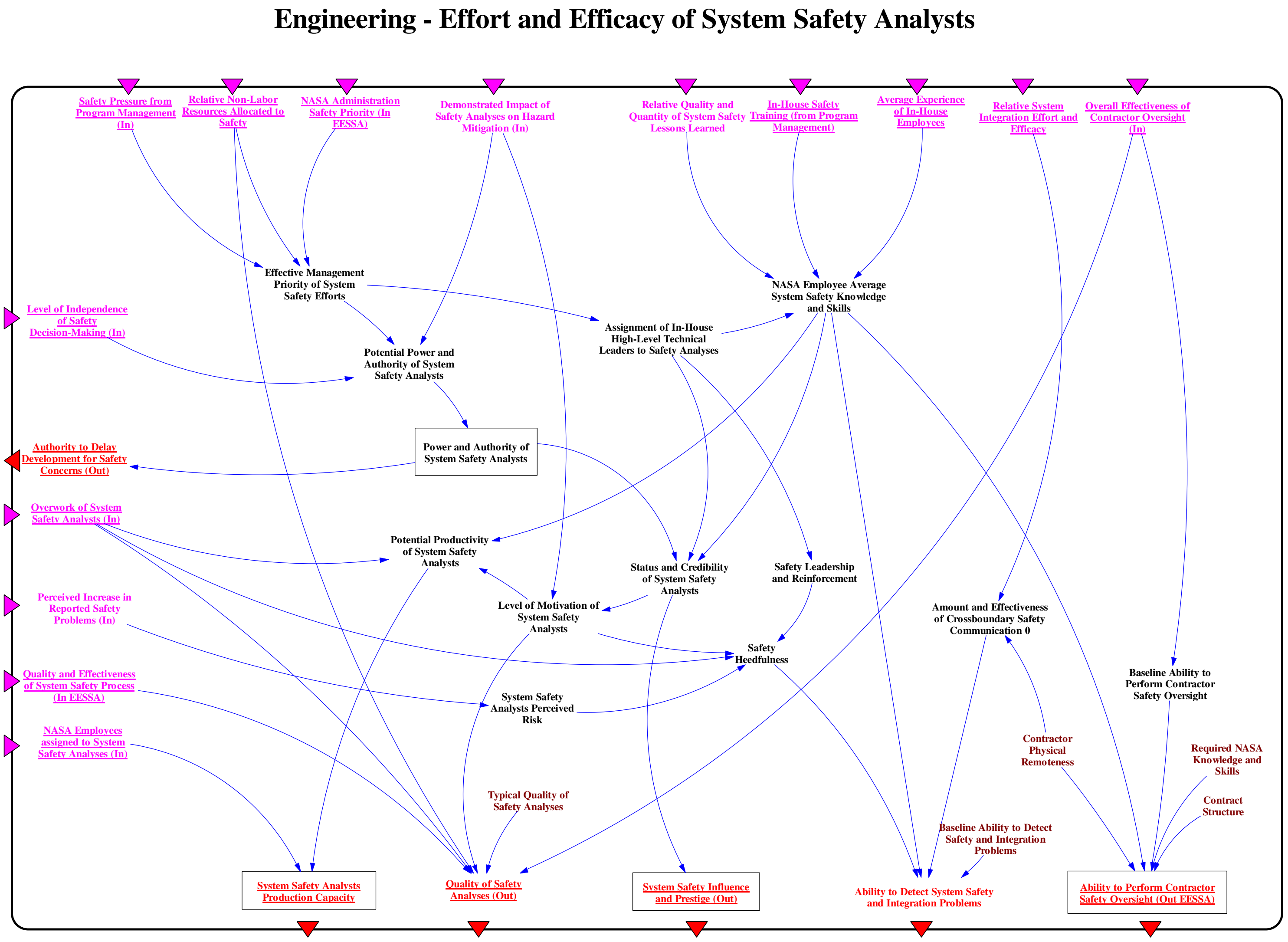

Engineering - Effort and Efficacy of System Safety Analysts
Safety Pressure from Program Management (In)
Relative Non-Labor Resources Allocated to Safety
NASA Administration Safety Priority (In EESSA)
Demonstrated Impact of Safety Analyses on Hazard Mitigation (In)
Relative Quality and Quantity of System Safety Lessons Learned
In-House Safety Training (from Program Management)
Average Experience of In-House Employees
Relative System Integration Effort and Efficacy
Overall Effectiveness of Contractor Oversight (In)
Effective Management Priority of System Safety Efforts
NASA Employee Average System Safety Knowledge and Skills
Level of Independence of Safety Decision-Making (In)
Assignment of In-House High-Level Technical Leaders to Safety Analyses
Potential Power and Authority of System Safety Analysts
Power and Authority of System Safety Analysts
Authority to Delay Development for Safety Concerns (Out)
Overwork of System Safety Analysts (In)
Potential Productivity of System Safety Analysts
Status and Credibility of System Safety Analysts
Safety Leadership and Reinforcement
Perceived Increase in Reported Safety Problems (In)
Level of Motivation of System Safety Analysts
Amount and Effectiveness of Crossboundary Safety Communication 0
Safety Heedfulness
Quality and Effectiveness of System Safety Process (In EESSA)
System Safety Analysts Perceived Risk
Baseline Ability to Perform Contractor Safety Oversight
NASA Employees assigned to System Safety Analyses (In)
Contractor Physical Remoteness
Required NASA Knowledge and Skills
Typical Quality of Safety Analyses
Contract Structure
Baseline Ability to Detect Safety and Integration Problems
System Safety Analysts Production Capacity
Quality of Safety Analyses (Out)
System Safety Influence and Prestige (Out)
Ability to Detect System Safety and Integration Problems
Ability to Perform Contractor Safety Oversight (Out EESSA)

Figure 57. Safety and Mission Assurance—Effort and Efficacy of System Safety Analysts module of the model.

Engineering--Effort and Efficacy of System Safety Analysts Module Variables:

Inputs:

- Safety pressure from program management
- Relative non-labor resources allocated to safety

- NASA administration safety priority
- Demonstrated impact of safety analyses on hazard mitigation
- Relative quality and quantity of system safety lessons learned
- In-house safety training (from Program Management)
- Average experience of in-house employees
- Relative system integration effort and efficacy
- Overall effectiveness of contractor oversight
- Level of independence of safety decision-making
- Overwork of system safety analysts
- Perceived increase in reported safety problems
- Quality and effectiveness of system safety process
- NASA employees assigned to system safety analyses

Internal Variables:

- Effective management priority of system safety efforts
- Potential power and authority of system safety analysts
- Power and authority of system safety analysts
- Assignment of in-house high-level technical leaders to safety analyses
- NASA employee average system safety knowledge and skills
- Potential productivity of system safety analysts
- Level of motivation of system safety analysts
- Status and credibility of system safety analysts
- System safety analysts perceived risk
- Typical quality of safety analyses
- Safety heedfulness
- Safety leadership and reinforcement
- Amount and effectiveness of cross-boundary safety communication
- Contractor physical remoteness
- Baseline ability to detect safety and integration problems
- Baseline ability to perform contractor safety oversight
- Required NASA knowledge and skills
- Contract structure

Outputs:

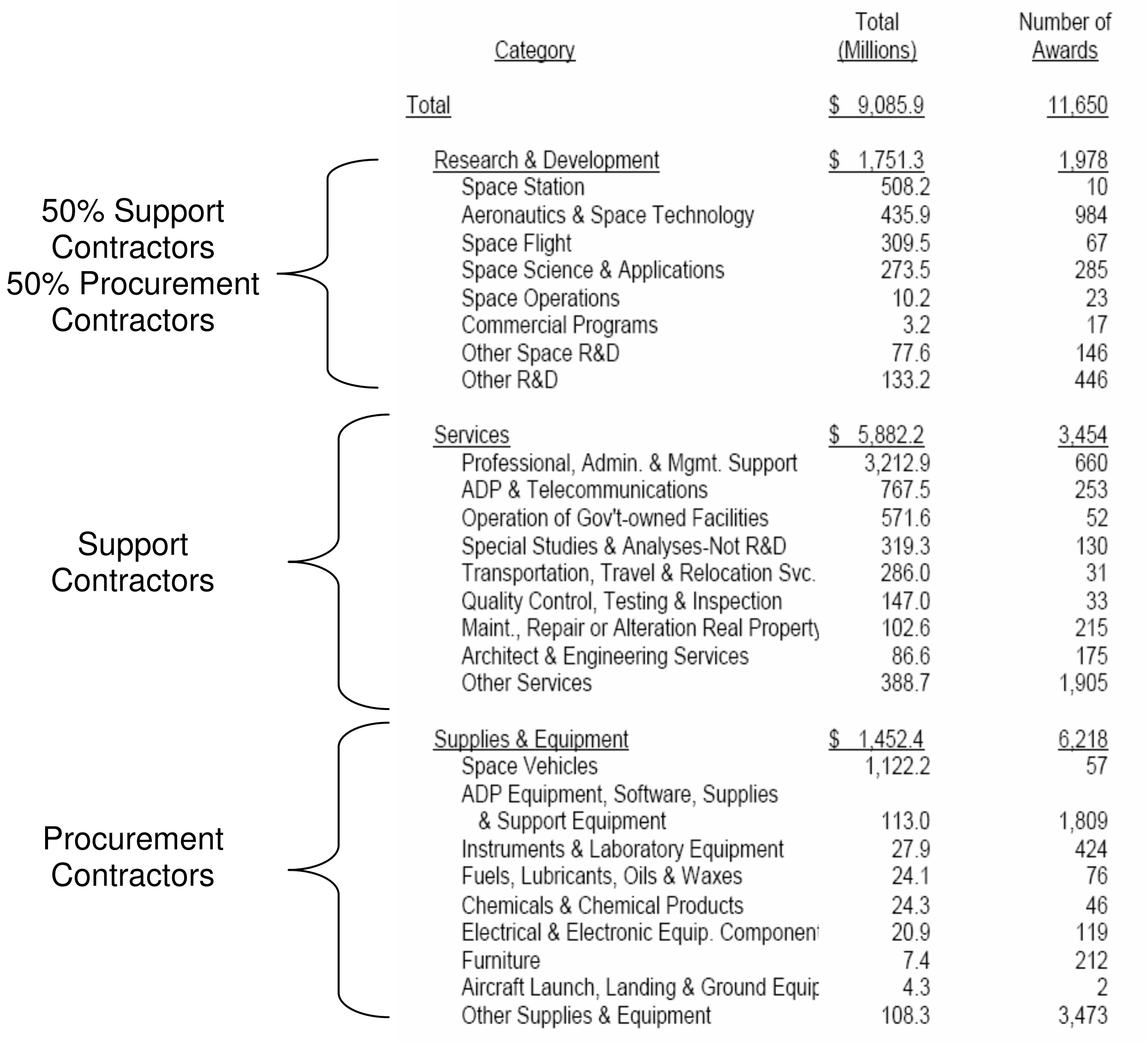
- Authority to delay development for safety concerns
- System safety analysts production capacity
- Quality of safety analyses
- System safety influence and prestige
- Ability to detect system safety and integration problems
- Ability to perform contractor safety oversight

Appendix E: Abstraction Level 4 of the Model (Conventions and Assumptions)

This Appendix contains the portion of the model conventions and assumptions following conventions and assumptions used in the model (i.e. Abstraction Level 4 of the model). The assumptions and conventions employed are as follows:

- The start date of the simulation is January 1, 2004
- The end date of the simulation is July 1, 2016
- The workforce and budget in the model is that of the entire Exploration Systems Mission Directorate
- Inflation is not accounted for in the model
- Civil servants do not get fired from ESMD, they get transferred out when there is a surplus of ESMD civil servants
- The planned initial system development time (CEV, CLV, LPRP) is 8 years
    - Only the development of the major projects at the start of the simulation are tracked
    - Projects that start up after the start of the simulation can affect the progress of the tracked projects (e.g. CaLV)
- The explicit program management schedule and budget reserves are set to zero in the baseline model. The impact of non-zero reserves is discussed further in specific scenarios
- The budget for ESMD is exogenous in the baseline model
    - There is a switch in the model for turning this assumption off
    - Between 2004 and 2011, the budget is based on a curve fit of budget request forecasts
    - Beyond 2011, the budget peaks in 2012 and decreases back to $6 Billion in order to approximate the effect of CEV/CLV ops deployment
        - Between 2010 and 2011 roughly $4 Billion will be transferred to ESMD from SOMD for Shuttle retirement, raising the ESMD budget to roughly $8.8 Billion. The assumption is that more than half of the $4 Billion ESMD received from SOMD would go back to SOMD for CEV/CLV deployment and thus the budget was rounded down to $6 Billion
- The scope of the projects tracked in the model is fixed in the baseline scenario
    - There is a switch in the model for turning this assumption off
- Whenever the term procurement is used in the context of the model, it refers to hardware/software acquired from prime contractors. It does not apply to support contractors who work on-site at the NASA centers
    - Support contractors are considered to be a part of the in-house workforce and are modeled as people
    - Prime contractors are not considered to be a part of the in-house workforce and are modeled as money that must be managed by the in-house workforce.
- The amount of reliance on contracting is fixed in the baseline model. A switch has been implemented to make this parameter endogenous and dependent on various uncertainty parameters, but it is deactivated in the baseline model.
- Roughly 42% of NASA's budget is allocated to external procurement
    - External procurement does not include funds given to on-site support contractors
    - The assumed value of 42% is derived from procurement statistics by effort for FY 2002 to FY 2004
        - The figure below shows how we broke down procurement efforts

- The values were estimated at 40%, 43%, and 44% in FY 2002, FY 2003, and FY 2004 respectively


50% Support Contractors
50% Procurement Contractors
Support Contractors
Procurement Contractors

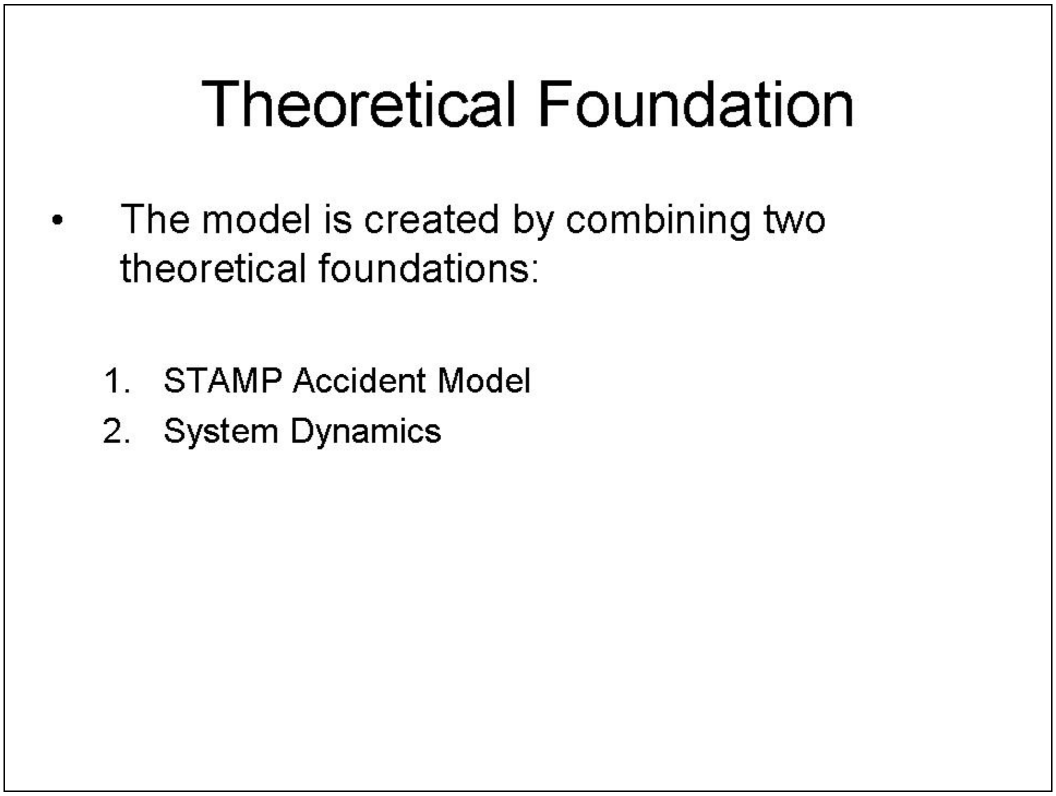
Category	Total (Millions)	Number of Awards
Total	$ 9,085.9	11,650
Research & Development	$ 1,751.3	1,978
Space Station	508.2	10
Aeronautics & Space Technology	435.9	984
Space Flight	309.5	67
Space Science & Applications	273.5	285
Space Operations	10.2	23
Commercial Programs	3.2	17
Other Space R&D	77.6	146
Other R&D	133.2	446
Services	$ 5,882.2	3,454
Professional, Admin. & Mgmt. Support	3,212.9	660
ADP & Telecommunications	767.5	253
Operation of Gov't-owned Facilities	571.6	52
Special Studies & Analyses-Not R&D	319.3	130
Transportation, Travel & Relocation Svc.	286.0	31
Quality Control, Testing & Inspection	147.0	33
Maint., Repair or Alteration Real Propert	102.6	215
Architect & Engineering Services	86.6	175
Other Services	388.7	1,905
Supplies & Equipment	$ 1,452.4	6,218
Space Vehicles	1,122.2	57
ADP Equipment, Software, Supplies & Support Equipment	113.0	1,809
Instruments & Laboratory Equipment	27.9	424
Fuels, Lubricants, Oils & Waxes	24.1	76
Chemicals & Chemical Products	24.3	46
Electrical & Electronic Equip. Componen	20.9	119
Furniture	7.4	212
Aircraft Launch, Landing & Ground Equi	4.3	2
Other Supplies & Equipment	108.3	3,473

Figure 58. Assumed Breakdown of Procurement Efforts.[97]

- Roughly 65% of the portion of the budget that does not go to external procurement goes to technical employees (both civil servants and support contractors)
  - The assumed value of 65% is estimated from workforce statistics between FY 1994 and FY 2006
    - In FY 2002 the percentage of total workforce (including support contractors) in science and engineering was 69%
    - Between FY 1994 and FY 2006 the percentage of the civil servant workforce in engineering ranged from 58.75% to 60.5% while the percentage in science ranged from 4.98% to 5.94%.

[97] The chart provided here is from a NASA Procurement Report available at: <http://ec.msfc.nasa.gov/hq/library/procreport/index.html>

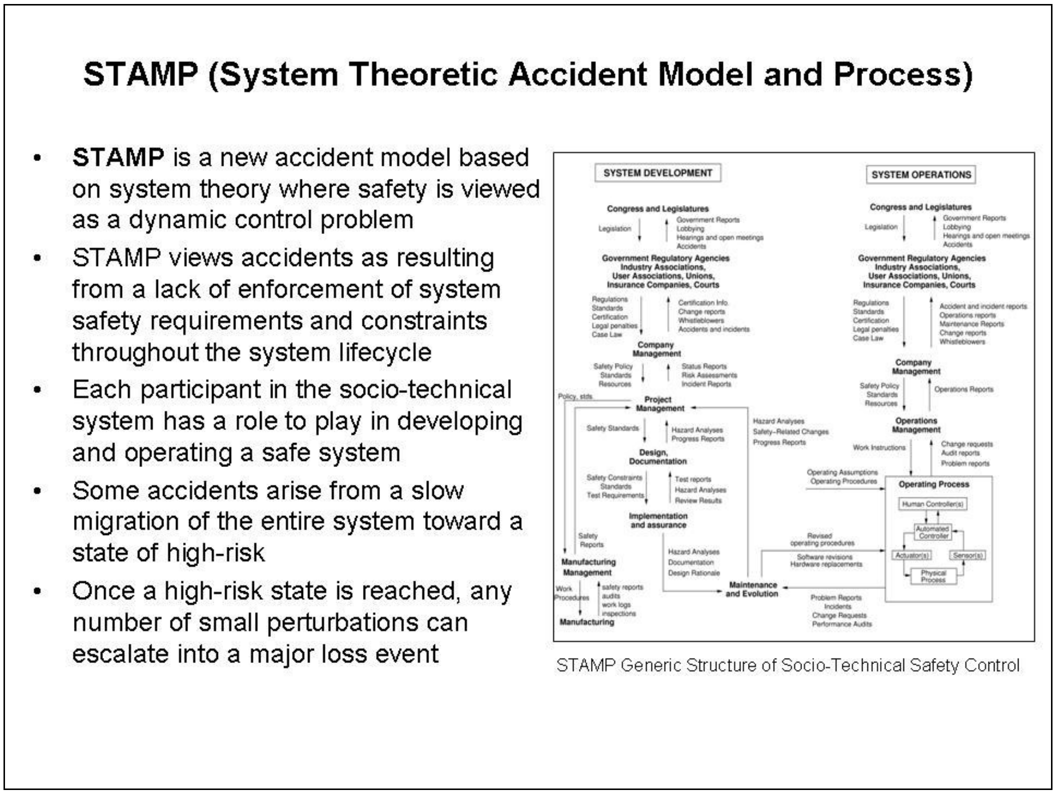
Appendix F: Interview Introduction Slides and Consent Form



Theoretical Foundation

- The model is created by combining two theoretical foundations:

1. STAMP Accident Model
2. System Dynamics



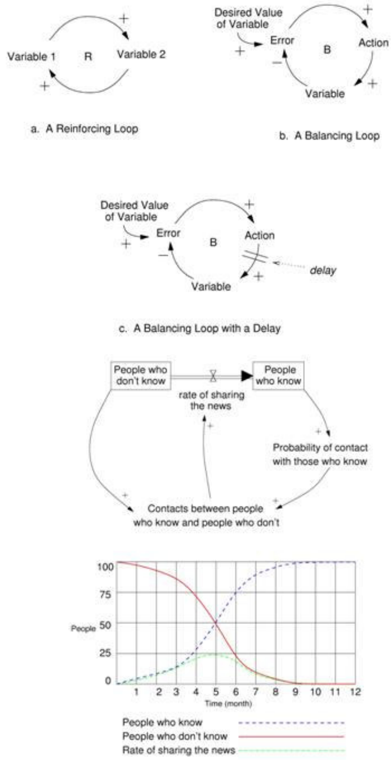
STAMP (System Theoretic Accident Model and Process)

- **STAMP** is a new accident model based on system theory where safety is viewed as a dynamic control problem
- STAMP views accidents as resulting from a lack of enforcement of system safety requirements and constraints throughout the system lifecycle
- Each participant in the socio-technical system has a role to play in developing and operating a safe system
- Some accidents arise from a slow migration of the entire system toward a state of high-risk
- Once a high-risk state is reached, any number of small perturbations can escalate into a major loss event

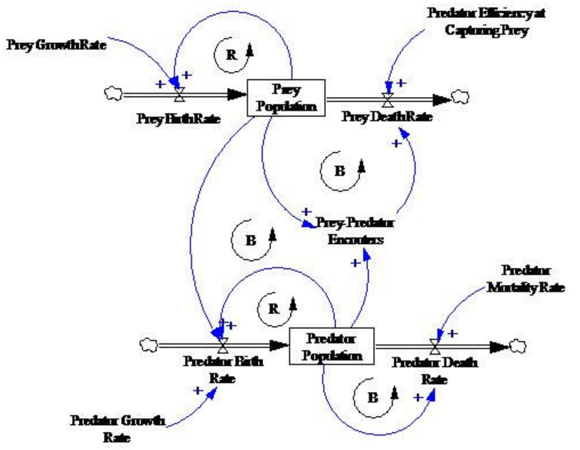
STAMP Generic Structure of Socio-Technical Safety Control

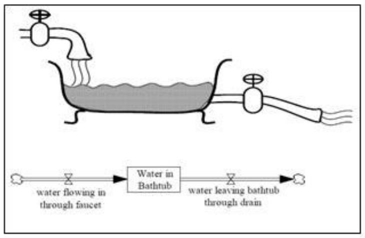
System Dynamics

- **System dynamics** is a modeling technique used to capture the dynamics of complex systems
- Augmenting STAMP with system dynamics allows us to detect and prevent the migration of complex systems toward high-risk
- System dynamics models are executable simulation models based on continuous nonlinear differential equations
- Emerging behavior patterns in a complex system are created by the interaction of a large number of feedback loops
- By analyzing this feedback loop structure, it is possible to design policies to improve system safety and remove unwanted effects.
- The building blocks of system dynamics models are stocks, flows, reinforcing loops, balancing loops, and delays.

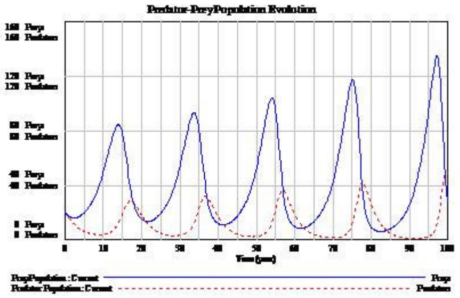


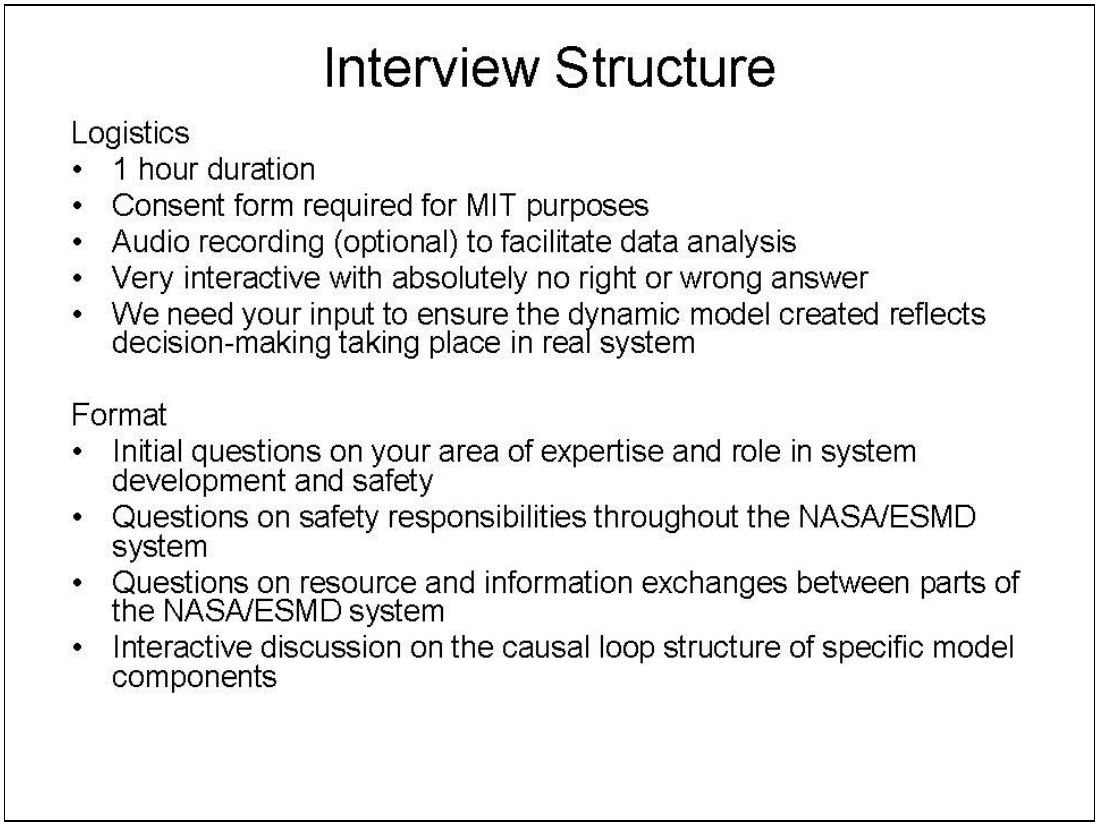
SD Example: Predator-Prey Dynamics





Water in Bathtub
water flowing in through faucet
water leaving bathtub through drain





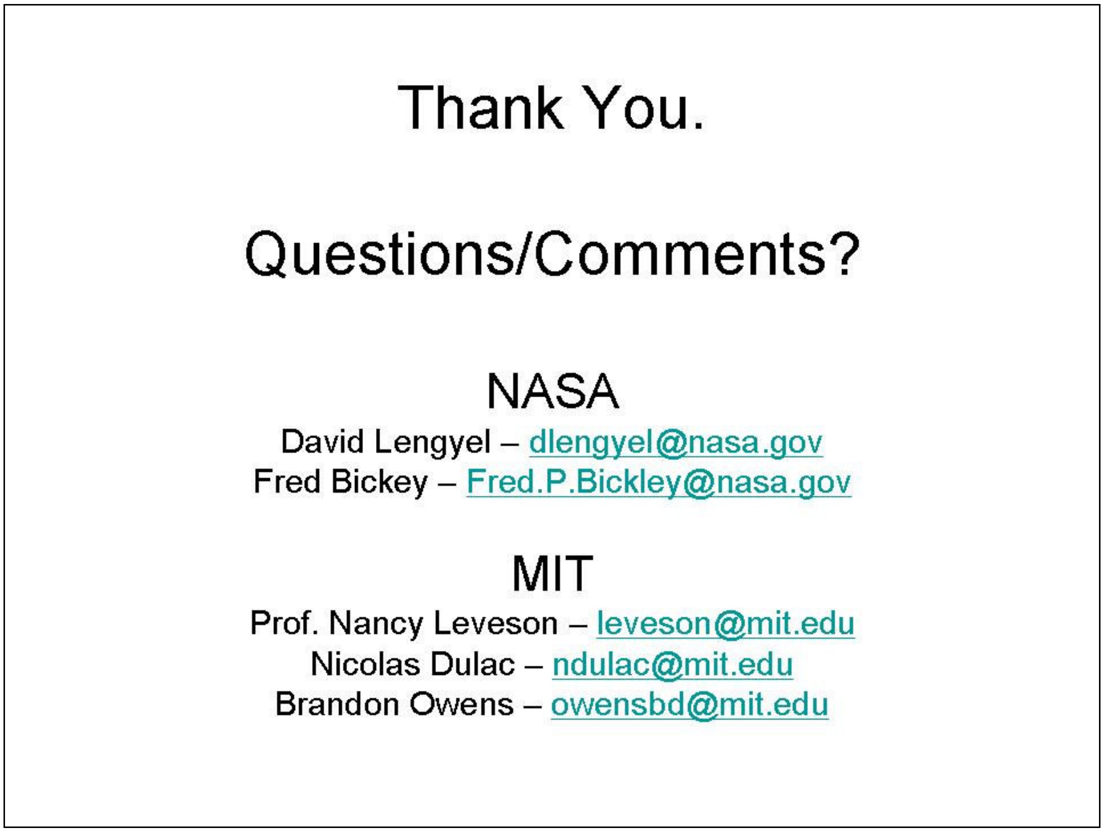
Interview Structure

Logistics

- 1 hour duration
- Consent form required for MIT purposes
- Audio recording (optional) to facilitate data analysis
- Very interactive with absolutely no right or wrong answer
- We need your input to ensure the dynamic model created reflects decision-making taking place in real system

Format

- Initial questions on your area of expertise and role in system development and safety
- Questions on safety responsibilities throughout the NASA/ESMD system
- Questions on resource and information exchanges between parts of the NASA/ESMD system
- Interactive discussion on the causal loop structure of specific model components



Thank You.

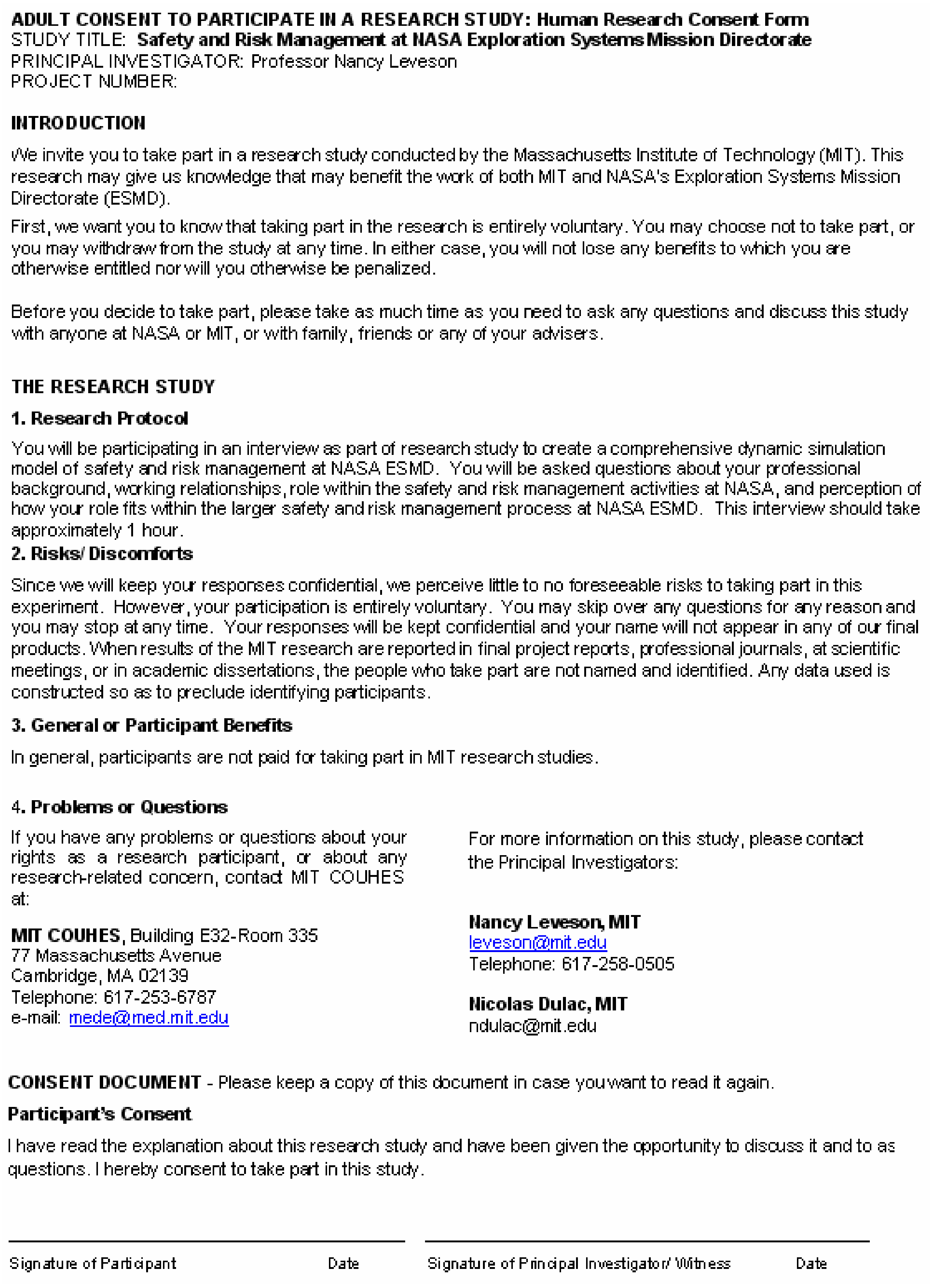
Questions/Comments?

NASA

David Lengyel – dlengyel@nasa.gov
Fred Bickey – Fred.P.Bickley@nasa.gov

MIT

Prof. Nancy Leveson – leveson@mit.edu
Nicolas Dulac – ndulac@mit.edu
Brandon Owens – owensbd@mit.edu



ADULT CONSENT TO PARTICIPATE IN A RESEARCH STUDY: Human Research Consent Form
STUDY TITLE: **Safety and Risk Management at NASA Exploration Systems Mission Directorate**
PRINCIPAL INVESTIGATOR: Professor Nancy Leveson
PROJECT NUMBER:

INTRODUCTION

We invite you to take part in a research study conducted by the Massachusetts Institute of Technology (MIT). This research may give us knowledge that may benefit the work of both MIT and NASA's Exploration Systems Mission Directorate (ESMD).

First, we want you to know that taking part in the research is entirely voluntary. You may choose not to take part, or you may withdraw from the study at any time. In either case, you will not lose any benefits to which you are otherwise entitled nor will you otherwise be penalized.

Before you decide to take part, please take as much time as you need to ask any questions and discuss this study with anyone at NASA or MIT, or with family, friends or any of your advisers.

THE RESEARCH STUDY

1. Research Protocol

You will be participating in an interview as part of research study to create a comprehensive dynamic simulation model of safety and risk management at NASA ESMD. You will be asked questions about your professional background, working relationships, role within the safety and risk management activities at NASA, and perception of how your role fits within the larger safety and risk management process at NASA ESMD. This interview should take approximately 1 hour.

2. Risks/ Discomforts

Since we will keep your responses confidential, we perceive little to no foreseeable risks to taking part in this experiment. However, your participation is entirely voluntary. You may skip over any questions for any reason and you may stop at any time. Your responses will be kept confidential and your name will not appear in any of our final products. When results of the MIT research are reported in final project reports, professional journals, at scientific meetings, or in academic dissertations, the people who take part are not named and identified. Any data used is constructed so as to preclude identifying participants.

3. General or Participant Benefits

In general, participants are not paid for taking part in MIT research studies.

4. **Problems or Questions**

If you have any problems or questions about your rights as a research participant, or about any research-related concern, contact MIT COUHES at:

MIT COUHES, Building E32-Room 335
77 Massachusetts Avenue
Cambridge, MA 02139
Telephone: 617-253-6787
e-mail: mede@med.mit.edu

For more information on this study, please contact the Principal Investigators:

Nancy Leveson, MIT
leveson@mit.edu
Telephone: 617-258-0505

Nicolas Dulac, MIT
ndulac@mit.edu

CONSENT DOCUMENT - Please keep a copy of this document in case you want to read it again.

Participant's Consent

I have read the explanation about this research study and have been given the opportunity to discuss it and to as questions. I hereby consent to take part in this study.

Signature of Participant	Date	Signature of Principal Investigator/ Witness	Date