Risk Analysis of NASA Independent Technical Authority[1]

June, 2005

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

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

Massachusetts Institute of Technology

[1] Aeronautics and Astronautic Dept.
[2] Engineering Systems Division
[3] Sloan School of Management

[1] This research was partially supported by a grant from the USRA Center for Program/Project Management Research (CPMR), which is funded by NASA APPL, and by the ITA Program within the NASA Chief Engineer's Office.

Contents

EXECUTIVE SUMMARY 4

1 INTRODUCTION 16
Defining Safety Culture 17
The STAMP Model of Accident Causation 19

2 THE PROCESS AND RESULTS 21
Preliminary Hazard Analysis 22
The ITA Hierarchical Safety Control Structure 23
Mapping Requirements to Component Responsibilities 24
Identifying the ITA Risks 26
Basic Risks 26
Coordination Risks 27
Categorizing the Risks 28
Analyzing the Risks 57
The System Dynamics Model 57
Model Validation and Analyses 63
Sensitivity Analysis 64
System Behavior Mode Analyses 66
Metrics Evaluations 69
Additional Scenario Analysis and Insights 73
Leading Indicators and Measures of Effectiveness 75

3 FINDINGS AND RECOMMENDATIONS 79

4 CONCLUSIONS AND FUTURE PLANS 86

APPENDIXES 87
A The STAMP Model of Accident Causation 87
B STAMP-Based Hazard Analysis (STPA) 92
C A Brief Introduction to System Dynamics Models 97
D Detailed Content of the Models 101
D.1 Examples from STAMP ITA Hierarchical Control Structure 112
D.2 Mapping from System Requirements and Constraints to Individual Responsibilities 112
D.3 System Dynamics Model of NASA Manned Space Program with ITA 126

Tables and Figures

Table 1: Responsibilities and Risks 29

Figure 1: Simplified Structure of ITA (March 2005) 23
Figure 2: The Nine Subsystem Models and their Interactions 58
Figure 3: ITA Model Structure 63
Figure 4a: ITA Sensitivity Analysis Trace Results 64
Figure 4b: ITA Sensitivity Analysis Density Results 65
Figure 5: ITA Sensitivity Analysis Trace Results for System Technical Risk 65
Figure 6: Behavior Mode #1 Representing a Successful ITA Program Implementation 67
Figure 7: Approach Used for Accident Generation 68
Figure 8: Behavior Mode #2 Representing an Unsuccessful ITA Program Implementation 69
Figure 9: Waiver Accumulation Pattern for Behavior Mode #2 70
Figure 10: Incidents Under Investigation—A Possible Risk Indicator 71
Figure 11: The Balancing Loop Becomes Reinforcing as the ITA Workload Keeps Increasing 71
Figure 12: Relationship Between Credibility of ITA and Technical Risk 72
Figure 13: Impact of Credibility of Participants on Success of ITA 73
Figure 14: System Risk as a Function of Increased Contracting 74
Figure 15: Effectiveness and Credibility as a Function of Increased Contracting 74
Figure 16: Availability of High-Level Technical Personnel as a Function of Increased Contracting 75
Figure A.1: General Form of a Model of Socio-Technical Safety Control 88
Figure A.2: The Safety Control Structure in the Walkerton Water Contamination Accident 90
Figure B.1: A Candidate Control Structure for the TTPS 94
Figure B.2: The Process Model for the Robot Controller using SpecTRM-RL 95
Figure B.3: Control Flaws Leading to Accidents 96
Figure C.1: The Three Basic Components of System Dynamics Models 97
Figure C.2: An Example System Dynamics and Analysis Output 99
Figure C.3: Simplified Model of the Dynamics Behind the Shuttle Columbia Loss 100

Executive Summary

Goals and Approach

To assist with the planning of a NASA assessment of the health of Independent Technical Authority (ITA), we performed a risk analysis to identify and understand the risks and vulnerabilities of this new organizational structure and to identify the metrics and measures of effectiveness that would be most effective in the planned assessment. This report describes the results of our risk analysis and presents recommendations for both metrics and measures of effectiveness and for potential improvements in the ITA process and organizational design to minimize the risks we identified.

Our risk analysis employed techniques from a new rigorous approach to technical risk management developed at MIT and based on a new theoretical foundation of accident causation called STAMP (System-Theoretic Accident Modeling and Processes). STAMP, which is based on systems theory, includes non-linear, indirect, and feedback relationships that can better handle the levels of complexity and technical innovation in today's systems than traditional causality and accident models. STAMP considers the physical, organizational, and decision-making components of systems as an integrated whole and therefore allows more complete risk and hazard analysis than formerly possible.

Instead of viewing accidents as the result of an initiating (root cause) event in a chain of events leading to a loss, accidents are conceived in STAMP as resulting from interactions among system components (both physical and social) that violate system safety constraints. Safety is treated as a *control* problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled. In the Space Shuttle Challenger loss, for example, the O-rings did not adequately control propellant gas release by sealing a tiny gap in the field joint. In the Mars Polar Lander loss, the software did not adequately control the descent speed of the spacecraft—it misinterpreted noise from a Hall effect sensor as an indication the spacecraft had reached the surface of the planet.

Accidents such as these, involving design errors, may in turn stem from inadequate control over the development process, i.e., risk is not adequately managed in the design, implementation, and manufacturing processes. Control is also imposed by the management functions in an organization—the Challenger accident involved inadequate controls in the launch-decision process, for example—and by the social and political system within which the organization exists.

The process leading up to an accident can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values. The accident or loss itself results not simply from component failure (which is treated as a symptom of the problems) but from inadequate control of safety-related constraints on the development, design, construction, and operation of the entire socio-technical system. The role of all these factors must be considered in hazard and risk analysis.

The new rigorous approach to organizational risk analysis employed in this report rests on the hypothesis that safety culture and organizational design can be modeled, formally analyzed, and engineered. Most major accidents do not result simply from a unique set of proximal, physical events but 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. In this state, some events are bound to occur that will trigger an accident. In both the Challenger and Columbia losses, organizational risk had been increasing to unacceptable levels for quite some time as behavior and decision-making evolved in response to a variety of internal and external pressures. Because risk increased slowly, nobody noticed it, i.e., the "boiled frog" phenomenon. In fact, confidence and complacency were increasing at the same time as risk due to the lack of accidents.

The challenge in preventing accidents is to establish safeguards and metrics to prevent and detect migration to a state of unacceptable risk before an accident occurs. The process of tracking leading indicators of increasing risk (the virtual "canary in the coal mine") can play an important role in

preventing accidents. Identifying these leading indicators is a particular goal of this risk analysis. We accomplish this goal using both static and dynamic models: static models of the safety control structure (organizational design) and dynamic models of behavior over time (system dynamics), including the dynamic decision-making and review processes. These models are grounded in the theory of non-linear dynamics and feedback control, but also draw on cognitive and social psychology, organization theory, economics, and other social sciences.

Underlying Assumptions about Safety Culture and Risk

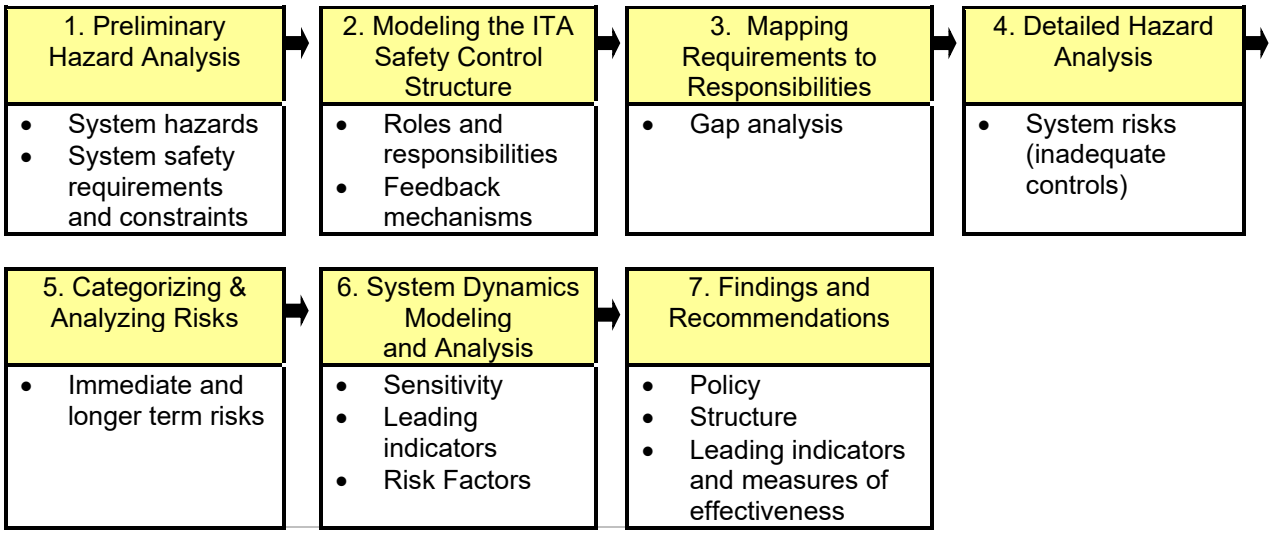
A culture is the shared set of norms and values that govern appropriate behavior. *Safety culture* is the subset of organizational culture that reflects the general attitude toward and approaches to safety and risk management. Our risk analysis and the recommendations derived from it are based on some fundamental assumptions about safety culture and risk, both general and NASA-specific:

- **The Ubiquitous Nature of Safety Culture**: Culture is embedded in and arises from the routine aspects of everyday practice as well as organizational structures and rules. 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 continuing environmental influences and pressures that tend to degrade the safety culture.
- **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. 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.

The Process

We followed a traditional system engineering and system safety engineering approach, but adapted to the task at hand (organizational risk analysis) as depicted in the following diagram:



The first step in our STAMP-based risk analysis was a preliminary hazard analysis to identify the high-level hazard(s) Independent Technical Authority was designed to control and the general requirements and constraints necessary to eliminate that 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, 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.

The next step was to create a model of the safety control structure in the NASA manned space program, augmented with Independent Technical Authority as designed. This model includes the roles and responsibilities of each organizational component with respect to safety. 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. One caveat is in order: changes are occurring so rapidly at NASA that our models, although based on the ITA implementation plan of March 2005, may require updating to match the current structure.

We next 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. Good decisions are made by the ITA, but they do not have adequate impact on system design, construction, and operation.

The hazard analysis applied each of these types of risks to the NASA organizational components and functions involved in safety-related decision-making and identified the risks (inadequate control) associated with each. The resulting list of risks is quite long (250), but most appear to be important and not easily dismissed (see Table 1 on page 29). To reduce the list to one that can be feasibly 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.

We then used our system dynamics models to identify which risks are the most important to measure and assess, i.e., which provide the best measure of the current level of organizational risk and are 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.

The analysis also pointed to structural changes and planned evolution of the safety-related decision-making structure over time that could strengthen the efforts to avoid migration to unacceptable levels of organizational risk and avoid flawed management and engineering decision-making leading to an accident.

Findings and Recommendations

Our findings and recommendations fall into the areas of monitoring ITA implementation and level of technical risk, initial buy-in, broadening participation, strengthening the role of trusted agents, enhancing communication, clarifying responsibilities, providing training, instituting assessment and continual improvement, expanding technical conscience channels and feedback, and controlling risk in a contracting environment.

1. Monitoring ITA Implementation and Level of Technical Risk

Finding 1a: It is a testament to the careful design and hard work that has gone into the ITA program implementation that we were able to create the ITA static control structure model so easily and found so few gaps in the mapping between system requirements and assigned responsibilities. We congratulate NASA on the excellent planning and implementation that has been done under severe time and resource constraints.

Finding 1b: Our modeling and analysis found that ITA has the potential to very significantly reduce risk and to sustain an acceptable risk level, countering some of the natural tendency for risk to increase over time due to complacency generated by success, aging vehicles and infrastructures, etc. However, we also found significant risk of unsuccessful implementation of ITA that should be monitored.

The initial sensitivity analysis identified two qualitatively different behavior modes: 75% of the simulation runs showed a successful ITA program implementation where risk is adequately mitigated for a relatively long period of time; the other runs identified a behavior mode with an initial rapid rise in effectiveness and then a collapse into an unsuccessful ITA program implementation where risk increases rapidly and accidents occur.

The ITA support structure is self-sustaining in both behavior modes for a short period of time if the conditions are in place for its early acceptance. This early behavior is representative of an initial excitement phase when ITA is implemented and shows great promise to reduce the level of risk of the system. This short-term reinforcing loop provides the foundation for a solid, sustainable ITA program under the right conditions.

Even in the successful scenarios, after a period of very high success, the effectiveness and credibility of the ITA slowly starts to decline, mainly due to the effects of complacency where the safety efforts start 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. However, in the successful implementations, risk is still at acceptable levels, and an extended period of nearly steady-state equilibrium ensues where risk remains at low levels.

In the unsuccessful ITA implementation scenarios, effectiveness and credibility of the ITA quickly starts to decline after the initial increase and eventually reaches unacceptable levels. Conditions arise that limit the ability of ITA to have a sustained effect on the system. Hazardous events start to occur and safety is increasingly perceived as an urgent problem. More resources are allocated to safety efforts, but at this point the Technical Authority (TA) and Technical Warrant Holders (TWHs) have lost so much credibility they are no longer able to significantly contribute to risk mitigation anymore. As a result, risk increases dramatically, the ITA personnel and safety staff become overwhelmed with safety problems and they start to approve an increasing number of waivers in order to continue flying.

As the number of problems identified increases along with their investigation requirements, corners may be cut to compensate, resulting in lower-quality investigation resolutions and corrective actions. If investigation requirements continue to increase, TWHs and Trusted Agents become saturated and simply cannot attend to each investigation in a timely manner. A bottleneck effect is created by requiring the TWHs to authorize all safety-related decisions, making things worse. Examining the factors in these unsuccessful scenarios can assist in making changes to the program to prevent them and, if that is not possible or desirable, to identify leading indicator metrics to detect rising risk while effective interventions are still possible and not overly costly in terms of resources and downtime.

Finding 1c: Results from the metrics analysis using our system dynamics model show that many model variables may provide good indications of system risk. However, many of these indicators will only show an increase in risk *after* it has happened, limiting their role in preventing accidents. For example, the number of waivers issued over time is a good indicator of increasing risk, but its effectiveness is limited by the fact that waivers start to accumulate after risk has started to increase rapidly. Other lagging indicators include the amount of resources available for safety activities; the schedule pressure, which will only be reduced when managers believe the system to be unsafe; and the perception of the risk level by management, which is primarily affected by events such as accidents and close-calls.

Finding leading indicators that can be used to monitor the system and detect increasing risk early is extremely important because of the dynamics associated with the non-linear tipping point associated with technical risk level. At this tipping point, risk increases slowly at first and then very rapidly (i.e., the reinforcing loop has a gain < 1). The system can be prevented from reaching this point, but once it is reached, multiple serious problems occur rapidly and overwhelm the problem-solving capacity of ITA. When the system reaches that state, risk starts to increase rapidly, and a great deal of effort and resources will be necessary to bring the risk down to acceptable levels.

Recommendation 1: To detect increasing and unacceptable risk levels early, the following five leading indicators (identified by our system dynamics modeling and analysis) should be tracked: (1) knowledge, skills, and quality of the TWHs and Trusted Agents; (2) ITA-directed investigation activity; (3) quality of the safety analyses; (4) quality of incident (hazardous event and anomaly) investigation; and (5) power and authority of the TA and TWHs. Specific metrics and measures of effectiveness for these leading indicators are described in Section 2.7.

2. Initial Buy-in

***Finding 2*:** The success of ITA is clearly dependent on the cooperation of the entire workforce, including project management, in providing information and accepting the authority and responsibility of the TA and TWHs. The implementers of ITA have recognized this necessity and instituted measures to enhance initial buy-in. Several of our identified leading indicators and measures of effectiveness can help to assess the success of these efforts.

Recommendation 2: Initial buy-in and acceptance of ITA should be closely monitored early in the program.

3. Broadening Participation

Finding 3: One of the important identified risks was a potential lack of broad participation of the workforce. Mechanisms are needed to allow and encourage all employees to contribute to safety-related decision-making. In particular, lack of direct engagement of line engineering in ITA (both within NASA and within the contractor organizations) may be a problem over the long run. Line engineers may feel disenfranchised, resulting in their either abdicating responsibility for safety to the warrant holders or, at the other extreme, simply bypassing the warrant holders.

Another reason for broad participation is that ITA is a potential bottleneck in accomplishing NASA's exploration goals and this problem will worsen when risk starts to increase and problems accumulate. It is important to avoid this negative reinforcing loop. Mechanisms must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making and to assume some responsibility, authority, and accountability for safety. The goal should be to prevent degradation of decision-making due to non-safety pressures but to make each person assume some responsibility and participate in the safety efforts in some way.

At the same time, NASA needs to avoid the trap existing both before Challenger and Columbia where performance pressures led to a diminution of the safety efforts. A simplified model of the dynamics involved is shown in Figure C.3 in Appendix C (page 100). One way to avoid those dynamics is to "anchor" the safety efforts through external means, i.e., Agency-wide standards and review processes that cannot be watered down by program/project managers when performance pressures build.

The CAIB report recommends establishing Independent Technical Authority, but there needs to be more than one type and level of independent authority in an organization: (1) independent technical authority *within* the program but independent from the Program Manager and his/her concerns with budget and schedule and (2) independent technical authority *outside* the programs to provide organization-wide oversight and maintenance of standards.

There are safety review panels and procedures within NASA programs, including the Shuttle program. Under various pressures, including budget and schedule constraints, however, the independent safety reviews and communication channels within the Shuttle program (such as the SSRP) degraded over time and were taken over by the Shuttle Program office and standards were weakened. At the same time, there was no effective external authority to prevent this drift toward high risk. ITA was designed to provide these external controls and oversight, but it should augment and not substitute for technical authority within line engineering.

Recommendation 3: Given the dysfunctional nature of the NASA safety control structure at the time of the Columbia accident and earlier, the current design of ITA is a necessary step toward the ultimate goal. We recommend, however, that a plan be developed for evolution of the safety control structure as experience and expertise grows to a design with distributed responsibility for safety-related decision-making, both internal and external to programs/projects. There will still be a need for external controls to ensure that the same dynamics existing before Challenger and Columbia do not repeat themselves. To achieve its ambitious goals for space exploration, NASA will need to evolve the organizational structure of the manned space program from one focused on operations to one focused on development and return to many of the organizational and cultural features that worked so well for Apollo. The appropriate evolutionary paths in ITA should be linked to these changes.

4. Independence of Trusted Agents

Finding 4: The results of safety analyses and information provided by non-ITA system components are the foundation for all TA and TWH safety-related decision-making. If the Trusted Agents do not play their role effectively, both in passing information to the TWHs and in performing important safety functions, the system falls apart. While TWHs are shielded in the design of the ITA from programmatic budget and schedule pressures through independent management chains and budgets, Trusted Agents are

not. They have dual responsibility for working both on the project and on TWH assignments, which can lead to obvious conflicts. Good information is key to good decision-making. Having that information produced by employees not under the ITA umbrella reduces the independence of ITA. In addition to conflicts of interest, increases in Trusted Agent workload due either to project and/or TWH assignments or other programmatic pressures can reduce their sensitivity to safety problems.

The TWHs are formally assigned responsibility, accountability, and authority through their warrants, and they are reminded of the role they play and their responsibilities by weekly telecons and periodic workshops, but there appears to be no similar formal structure for Trusted Agents to more completely engage them in their role. The closest position to the Trusted Agent in other government agencies, outside of the Navy, is the FAA DER (Designated Engineering Representative). Because type certification of an aircraft would be an impossible task for FAA employees alone, DERs are used to perform the type certification functions for the FAA.

Recommendation 4a: Consider establishing a more formal role for Trusted Agents and ways to enhance their responsibility and sense of loyalty to ITA. Examine the way the same goals are accomplished by other agencies, such as the FAA DER, to provide guidance in designing the NASA approach. The Trusted Agent concept may be the foundation on which an internal technical authority is established in the future.

Recommendation 4b: The term "Trusted Agent" has some unfortunate connotations in that it implies that others are untrustworthy. The use of another term such as "warrant representatives" or "warrant designees" should be considered.

5. Enhancing Communication and Coordination

Finding 5: As noted, the entire structure depends on communication of information upward to ITA decision-makers. Monitoring the communication channels to assess their effectiveness will be important. We have developed and experimentally used tools for social interaction analysis that assist with this type of monitoring. For projects with extensive outside contracting, the potential communication gaps are especially critical and difficult to maneuver given contractor concerns about proprietary information and designs. The proprietary information issues will need to be sorted out at the contractual level, but the necessary safety oversight by NASA requires in-depth NASA reviews and access to design information. The FAA DER concept, which is essentially the use of Trusted Agents at contractors, is one potential solution. But implementing such a concept effectively takes a great deal of effort and careful program design.

Beyond the contractor issues, communication channels can be blocked or dysfunctional at any point in the chain of feedback and information passing around the safety control structure. In large military programs, system safety working groups or committees have proved to be extremely effective in coordinating safety efforts.[2] The concept is similar to NASA's use of boards and panels at various organizational levels, with a few important differences—safety working groups operate more informally and with fewer constraints.

Recommendation 5a: Establish channels and contractual procedures to ensure that TWHs can obtain the information they need from contractors. Consider implementing some form of the "safety working group" concept, adapted to the unique NASA needs and culture.

Recommendation 5b: Monitor communication flow and the information being passed to ITA via Trusted Agents and contractors. Identify misalignments and gaps in the process using tools for interaction analysis on organizational networks.

[2] Nancy G. Leveson. *Safeware*, Addison-Wesley, 1995.

6. Clarifying Responsibilities

Several findings relate to the need to better clarify responsibilities. Some important responsibilities are not well defined, are assigned to the wrong group, are not assigned to anyone, or are assigned to more than one group without specifying how the overlapping activities will be coordinated.

Finding 6a: A critical success factor for any system safety effort is good safety analyses. In fact, our system dynamics modeling found that the quality of the safety analyses and safety information provided to the decision makers was the most important factor in the effectiveness of ITA. Responsibility for system hazard analysis (which NASA sometimes calls integrated hazard analysis) and communication channels for hazard information to and among contractors and NASA line engineers are not clearly defined. While TWHs are responsible for ensuring hazard and other safety analyses are used, ambiguity exists about who will actually be performing them. Currently this responsibility lies with Safety and Mission Assurance (SMA), but that has not worked well.

Safety engineering needs to be done by engineering, not by mission assurance, whose major responsibilities should be assuring quality in everything NASA does and in compliance checking, but not actually performing the design engineering functions. When SMA is both performing engineering functions and assuring the quality of those functions, the independence of the assurance organization is compromised. At the least, if SMA is controlling the hazard analysis and auditing process, communication delays may cause the analyses to be too late (as they are often today) to impact the most important design decisions. At the worst, it may lead to disconnects that seriously threaten the quality of the system safety engineering efforts. In our experience, the most effective projects have the discipline experts for system safety engineering analyses located in the system engineering organization.

It is important to note that the types of safety analyses and the information contained in them will differ if they are being used for design or for assurance (assessment). There is no reason both need to be done by one group. An unfortunate result of the current situation is that often only assurance analyses are performed and the information needed to fully support design decisions is not produced.

System safety is historically and logically a part of system engineering. A mistake was made 17 years ago when safety engineering was moved to an assurance organization at NASA. It is time to rectify that mistake. A recent NRC report concluded that NASA's human spaceflight systems engineering capability has eroded significantly as a result of declining engineering and development work, which has been replaced by operational responsibilities.[3] This NRC report assigns system safety as a responsibility for a renewed system engineering and integration capability at NASA and concludes that strengthening the state of systems engineering is critical to the long-term success of Project Constellation.

Finding 6b: In addition to producing system hazard analyses, responsibility has to be defined for ensuring that adequate resources are applied to system safety engineering; that hazard analyses are elaborated (refined and extended) and updated as the design evolves and test experience is acquired; that hazard logs are maintained and used as operational experience is gained; and that all anomalies are evaluated for their hazard potential. Again, currently many of these responsibilities are assigned to SMA, but with this process moving to engineering—which is where it should be—clear responsibilities for these functions need to be specified.

Finding 6c: While the Discipline Technical Warrant Holders own and approve the standards, it still seems to be true that SMA is writing engineering standards. As the system safety engineering responsibilities are moving to design engineering, so should the responsibility for producing the standards that are used in hazard analyses and in engineering design. SMA should be responsible for assurance standards, not technical design and engineering process standards.

[3] Donald C. Fraser (Chair). Report of the Committee on Systems Integration for Project Constellation, National Research Council, September 21, 2004.

Finding 6d: The March ITA implementation plan says that SMA will recommend a SR&QA plan for the project. The ITA will set requirements and approve appropriate parts of the plan. This design raises the potential for serious coordination and communication problems. It might make more sense for SMA to create a plan for the safety (and reliability and mission) *assurance* parts of the plan while Engineering creates the safety *engineering* parts. If this is what is intended, then everything is fine, but it deviates from what has been done in the past. We have concerns that, as a result, there will be confusion about who is responsible for what and some functions might never be accomplished or, alternatively, conflicting decisions may be made by the two groups, resulting in unintended conflicts and side effects.

Recommendation 6: System safety responsibilities need to be untangled and cleanly divided between the engineering and assurance organizations, assigning the system safety engineering responsibilities to SE&I and other appropriate engineering organizations and the assurance activities to SMA. The SE&I responsibilities should include creating project system safety design standards such as the Human Rating Requirements, performing the system safety hazard analyses used in design, and updating and maintaining these analyses during testing and operations. SMA should create the assurance standards and perform the assurance analyses.

7. Training

Finding 7a: As with other parts of system engineering, as noted in the NRC report on systems integration for Project Constellation, capabilities in system safety engineering (apart from operations) have eroded in the human spaceflight program. There is widespread confusion about the difference between reliability and safety and the substitution of reliability engineering for system safety engineering.

While the discipline technical warrant holders (DTWHs) are responsible for the state of expertise in their discipline throughout the Agency (and this would include the responsibility of the System Safety DTWH for ensuring engineers are trained in performing hazard analyses), we could not find in the ITA implementation plans documentation of who will be responsible to see that engineers and managers are trained to use the results of hazard analysis in their decision-making. While most engineers at NASA know how to use bottom-up component reliability analyses such as FMEA/CIL, they are not as familiar with system hazard analyses and their use.

Training is also needed in general system safety concepts and should include study of lessons learned from past accidents and serious incidents. Lessons learned are not necessarily communicated and absorbed by putting them in a database. The Navy submarine program, for example, requires engineers to participate in a system safety training session each year. At that time, the tapes of the last moments of the crew during the Thresher loss are played and the causes and lessons to be learned from that major tragedy are reviewed. The CAIB report noted the need for such training at NASA. The use of simulation and facilitated ways of playing with models, such as our system dynamics model of the NASA Manned Space Program safety culture at the time of the Columbia accident, along with models of typical safety culture problems, can provide powerful hands-on learning experiences.

Finding 7b: Our system dynamics models show that effective "root cause" analysis (perhaps better labeled as systemic or causal factors analysis) and the identification and handling of systemic factors rather than simply symptoms are important in maintaining acceptable risk.

Recommendation 7: Survey current system safety engineering knowledge in NASA line engineering organizations and plan appropriate training for engineers and managers. This training should include training in state-of-the-art system safety engineering techniques (including causal factor analysis), the use of the results from safety analyses in engineering design and management decision-making, and the study of past accidents and serious incidents, perhaps using hands-on facilitated learning techniques with executable models.

8. Assessment and Continual Improvement

Finding 8: Although clearly assessment of how well the ITA is working is part of the plan—this risk analysis and the planned assessment are part of that process—specific organizational structures and processes for implementing a continual learning and improvement process and making adjustments to the design of the ITA itself when necessary might be a worthwhile addition to the plan. Along with incremental improvements, occasionally the whole design should be revisited and adjustments made on the basis of assessments and audits.

> ***Recommendation 8***: Establish a continual assessment process of NASA safety-related decision-making in general and ITA in particular. That process should include occasional architectural redesigns (if necessary) in additional to incremental improvement.

9. Technical Conscience and Feedback

Finding 9: The means for communicating and resolving issues of technical conscience are well defined, but there is no defined way to express concerns about the warrant holders themselves or aspects of ITA that are not working well. Appeals channels are needed for complaints and concerns involving the TA and TWHs.

> ***Recommendation 9***: Alternative channels for raising issues of technical conscience should be established that bypass the TWHs if the concerns involve the TWH or TA. In addition, the technical conscience channels and processing needs to be monitored carefully at first to assure effective reporting and handling. Hopefully, as the culture changes to one where "what-if" analysis and open expression of dissent dominate, as was common in the Apollo era, such channels will become less necessary.

10. Impact of Increased Contracting

Finding 10: In one of our system dynamics analyses, we increased the amount of contracting to determine the impact on technical risk of contracting out the engineering design functions. We found that increased contracting does not significantly change the level of risk until a "tipping point" is reached where NASA is not able to perform the integration and safety oversight that is their responsibility. After that point, risk increases rapidly. While contractors may have a relative abundance of employees with safety knowledge and skills, without a strong in-house structure to coordinate and integrate the efforts of both NASA and contractor safety activities, effective risk mitigation can be compromised.

> ***Recommendation 10***: For projects in which significant contracting is anticipated, careful study of the types and amount of oversight needed to avoid reaching the tipping point will help with NASA's planning and staffing functions. The answer may not be a simple ratio of in-house expertise to contracting levels. Instead, the type of project as well as other factors may determine appropriate expertise as well as resource needs.

Conclusions and Future Plans

The ITA program design and implementation planning represent a solid achievement by the NASA Chief Engineer's Office. We believe that ITA represents a way to make significant progress in changing the safety culture and evolving to a much stronger safety program. We hope this risk analysis will be helpful in furthering its success.

We have a small USRA research grant to further develop the formal approach we used in this risk analysis so that it can be more easily employed by managers, particularly the system dynamics modeling. We hope to be able to continue to use the NASA manned space program as a test bed for our research. We also plan to investigate how to apply the same risk analysis approach to important system qualities beyond safety and to programmatic concerns. One longer-term goal is to design a state-of-the-art risk management tool set that provides support for improved decision-making about risk both at the organizational and physical system levels. The September 2004 NRC report on the requirements for system engineering and integration for Project Constellation concludes: "The development of space systems is inherently risky. To achieve success, risk management must go far beyond corrective action prompted by incidents and accidents. All types of risk—including risk to human life—must be actively managed to achieve realistic and affordable goals."[4]

[4] Donald C. Fraser, *op. cit*.

Risk Analysis of the NASA Independent Technical Authority

1. INTRODUCTION

This report contains the results of a risk analysis of the new NASA Independent Technical Authority (ITA). The analysis was performed to support a NASA assessment of the health of ITA. The assessment is still in the planning stage, but part of the planning effort involves understanding the risks and vulnerabilities of this new organizational structure. To assist with this goal, we applied a new rigorous approach to risk analysis developed at MIT. A more traditional risk and vulnerability analysis was conducted in parallel by the NASA Independent Program Assessment Office. The results of the two different processes will, hopefully, complement each other or, at the least, provide added assurance about the completeness of the results of each.

Our approach rests on the hypothesis that safety culture can be modeled, formally analyzed, and engineered. Models of the organizational safety control structure and dynamic decision-making and review processes can potentially be used for: (1) designing and validating improvements to the risk management and safety culture; (2) evaluating and analyzing risk; (3) detecting when risk is increasing to unacceptable levels (a virtual "canary in the coal mine"); (4) evaluating the potential impact of changes and policy decisions on risk; (5) performing "root cause" (perhaps better labeled as systemic factors or causal network) analysis; and (6) determining the information each decision-maker needs to manage risk effectively and the communication requirements for coordinated decision-making across large projects.

One of the advantages of using formal models in risk analysis is that analytic tools can be used to identify the most important leading indicators of increasing system risk. In both the Challenger and Columbia losses, risk had been increasing to unacceptable levels for quite some time before the proximate events that triggered the accidents occurred. Because risk increased slowly, nobody noticed the trend, i.e., the "boiled frog" phenomenon. Leading indicators of this migration toward a state of higher risk can play an important role in preventing accidents.

System safety at NASA has, over the years, come to be very narrowly defined and frequently confused with reliability. Jerome Lederer, who created the NASA Manned Space Flight Safety Program after the Apollo Launch Pad fire, said in 1968:

> Systems safety covers the entire spectrum of risk management. It goes *beyond the hardware* and associated procedures to systems safety *engineering.* It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.[5]

In addition, while safety is sometimes narrowly defined in terms of human death and injury, we use a more inclusive definition that also considers mission loss as a safety problem and is thus applicable to all the NASA enterprises and missions.[6] The accident reports and investigations into the loss of the two Mars 98 missions and other NASA mission failures (for example, WIRE, Huygens, and the SOHO mission

[5] Jerome Lederer, "How far have we come? A look back at the leading edge of system safety eighteen years ago." *Hazard Prevention*, page 8, May/June 1986.

[6] The official NASA definition of safety (from NPR 8715.3, *NASA Safety Manual*) is "Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."

interruption) point to cultural and organizational problems very similar to those identified by the CAIB in the more visible manned space program and the need for similar cultural and organizational improvements. Although we focus on the manned space program in this report, the approach and most of the results are applicable to all NASA missions and enterprises.

We first define what we include as "safety culture" and then provide a very brief description of STAMP (System-Theoretic Accident Modeling and Processes), the new accident model upon which our risk analysis is based. STAMP, with its foundation in systems theory, includes non-linear, indirect, and feedback relationships and can better handle the levels of complexity and technical innovation in today's systems than traditional causality and accident models. A more complete description of STAMP and the new hazard analysis technique (STPA) based on it can be found in Appendix A. Then we describe the process and results of our ITA risk analysis, including the identified risks and vulnerabilities along with metrics and measures of effectiveness associated with each risk. Our analytical models allow us to evaluate the risks to determine which leading indicators will be most effective in early detection of increasing risk and therefore should be carefully monitored. We also provide some recommendations for improving the ITA program, based partly on our analysis and partly on lessons learned by other agencies in implementing similar programs.

We note one caveat: The ITA implementation is in its preliminary stages and our modeling effort therefore involves a moving target. In our models and risk analysis, we use the design as described in the implementation plan of March 2005, which may not match the design in June 2005. It should be relatively easy, however, to make the necessary changes to our models to reflect the current design and to evaluate these and future changes for their impact on technical risk (safety) in the Agency. Changes are also happening quickly at NASA in terms of shifting responsibilities. For example, we understand the Center Directors now will report directly to the Administrator rather than to Headquarters Center Executives. This type of change does not affect our risk analysis—the risks remain the same but the responsibilities the Headquarters Center Executives had with respect to the ITA will now need to be performed by the Administrator.

1.1 Defining Safety Culture

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 SMA 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* along with their underlying values and assumptions and a clearly expressed system safety vision. The vision must be shared among all the stakeholders, not just articulated by the leaders.

There are several assumptions about the NASA safety culture that underlie our ITA risk analysis:

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.

1.2 The STAMP Model of Accident Causation

Traditionally accidents are treated as resulting from an initiating (root cause) event in a chain of directly related failure events. This traditional approach, however, has limited applicability to complex systems, where interactions among components, none of which may have failed, often lead to accidents. The chain-of-events model also does not include the systemic factors in accidents such as safety culture and flawed decision-making. A new, more inclusive approach is needed.

STAMP was developed to overcome these limitations. Rather than defining accidents as resulting from component failures, accidents are viewed as the result of flawed processes involving interactions among people, societal and organizational structures, engineering activities, and physical system components. Safety is treated as a *control* problem: accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled. In the Space Shuttle Challenger loss, for example, the O-rings did not adequately control propellant gas release by sealing a tiny gap in the field joint. In the Mars Polar Lander loss, the software did not adequately control the descent speed of the spacecraft—it misinterpreted noise from a Hall effect sensor as an indication the spacecraft had reached the surface of the planet.

Accidents such as these, involving engineering design errors, may in turn stem from inadequate control over the development process, i.e., risk is not adequately managed in the design, implementation, and manufacturing processes. Control is also imposed by the management functions in an organization—the Challenger accident involved inadequate controls in the launch-decision process, for example—and by the social and political system within which the organization exists. The role of all of these factors must be considered in hazard and risk analysis.

Note that the use of the term "control" does not imply a strict military-style command and control structure. Behavior is controlled or influenced not only by direct management intervention, but also indirectly by policies, procedures, shared values, and other aspects of the organizational culture. All behavior is influenced and at least partially "controlled" by the social and organizational context in which the behavior occurs. The connotation of control systems in engineering centers on the concept of feedback and adjustment (such as in a thermostat), which is an important part of the way we use the term here. Engineering this context can be an effective way of creating and changing a safety culture.

Systems are viewed in STAMP as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system is not treated as a static design, but as a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behavior to ensure safe operation, but it must continue to operate safely as changes and adaptations occur over time. Accidents, then, are considered to result from dysfunctional interactions among the system components (including both the physical system components and the organizational and human components) that violate the system safety constraints. The process leading up to an accident can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values. The accident or loss itself results not simply from component failure (which is treated as a symptom of the problems) but from inadequate control of safety-related constraints on the development, design, construction, and operation of the socio-technical system.

While events reflect the *effects* of dysfunctional interactions and inadequate enforcement of safety constraints, the inadequate control itself is only indirectly reflected by the events—the events are the *result* of the inadequate control. The system control structure itself, therefore, must be examined to determine how unsafe events might occur and if the controls are adequate to maintain the required constraints on safe behavior.

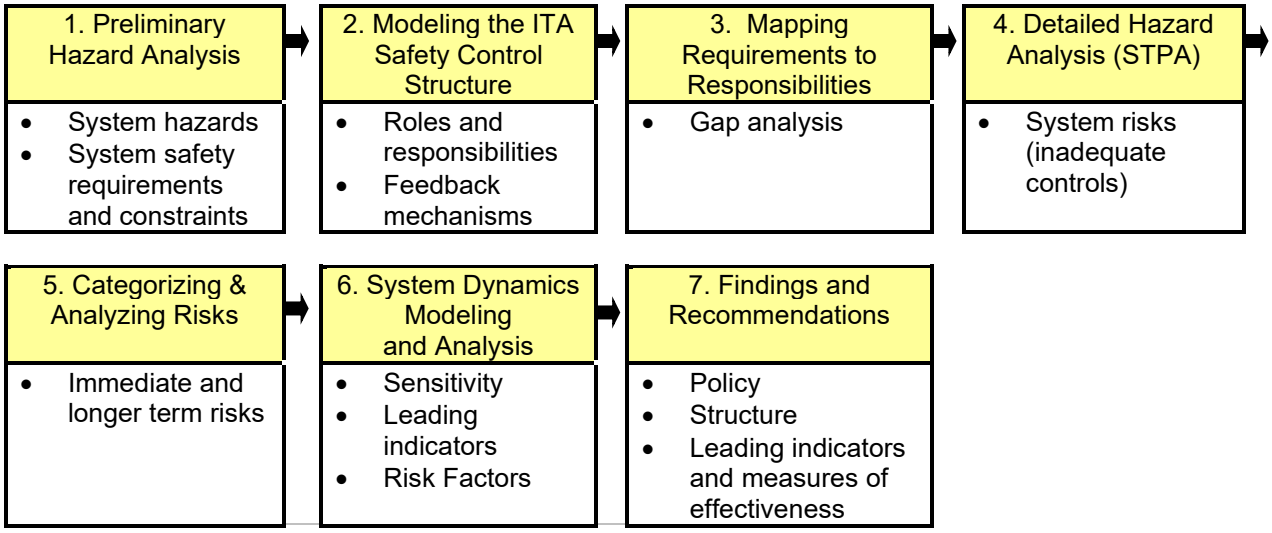
A STAMP modeling and analysis effort involves creating a model of the system safety control structure: the safety requirements and constraints that each component (both technical and organizational) is responsible for maintaining; controls and feedback channels, process models representing the view of the controlled 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 the analysis procedures defined for them can be used (1) to investigate accidents and incidents to determine the role played by the different components of the safety control structure and learn how to prevent related accidents in the future, (2) to proactively perform hazard analysis and design to reduce risk throughout the life of the system, and (3) to support a continuous risk management program where risk is monitored and controlled.

A more complete description of STAMP and the new hazard analysis technique, called STPA (STamP Analysis), used in our risk analysis can be found in Appendix A.

2. THE PROCESS AND RESULTS

There are six steps in a STAMP risk analysis:

1. Perform a high-level system hazard analysis, i.e., identify the system-level hazards to be the focus of the analysis and then the system requirements and design constraints necessary to avoid those hazards.
2. Create the STAMP hierarchical safety control structure using either the organizational design as it exists (as in this case) or creating a new design that satisfies the system requirements and constraints. This control structure will include the roles and responsibilities of each component with respect to safety.
3. Identify any gaps in the control structure that might lead to a lack of fulfillment of the system safety requirements and design constraints and places where changes or enhancements might be helpful.
4. Perform an STPA to identify the inadequate controls for each of the control structure components that could lead to the component's responsibilities not being fulfilled. These are the system risks.
5. Categorize the risks as to whether they need to be assessed immediately or whether they are longer-term risks that require monitoring over time. Identify some potential metrics or measures of effectiveness for each of the risks.
6. Create a system dynamics model of the non-linear dynamics of the system (see Appendix C for a brief introduction to system dynamics modeling) and use the models to identify the most important leading indicators of risk and perform other types of analysis.



For this modeling effort, we created a STAMP model of ITA and most of the static safety control structure in the NASA manned space program. In addition, we augmented our existing system dynamics model of the NASA Space Shuttle safety culture to include ITA. We then used these models to determine which risks were the most important and most useful in detecting increases in risk over time.

2.1 Preliminary Hazard Analysis

The first step in the process is to perform a preliminary system hazard analysis. The high-level hazard that the ITA organization is designed to prevent is:

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

Avoiding this hazard requires that NASA satisfy certain system-level requirements and constraints. These are presented below. Items underlined in square brackets represent requirements or constraints that do not appear to be reflected in the ITA implementation plan but that we feel are important to consider adding:

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, 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*

Each of these system safety requirements and constraints plays a role in controlling the system hazard (i.e., unsafe technical decision-making) and must be reflected in the overall system control structure (see Figure A.1 in Appendix A for the generic form of such a control structure). To determine whether this goal has been achieved, we need a model of the control structure.

2.2 The ITA Hierarchical Safety Control Structure

The second step in the process is to create a model of the ITA program in the form of the static ITA control structure. The basic components included are shown in Figure 1, although the structure shown is simplified. Some manned space program components not strictly part of ITA, such as line engineering and contractors, are included because they play important roles with respect to ITA functions. For each of these components, we identified the inputs and outputs, the overall role the component plays in the ITA organization, and the specific responsibilities required for that role. In a complete modeling effort, the requirements for the content of each component's process model and information about the context that could influence decision-making would also be included, but a lack of time prevented us from completing these last two parts of the model. We used the description of the responsibilities we found in the February 2005 and March 2005 ITA implementation plans, using the latter when there were differences.

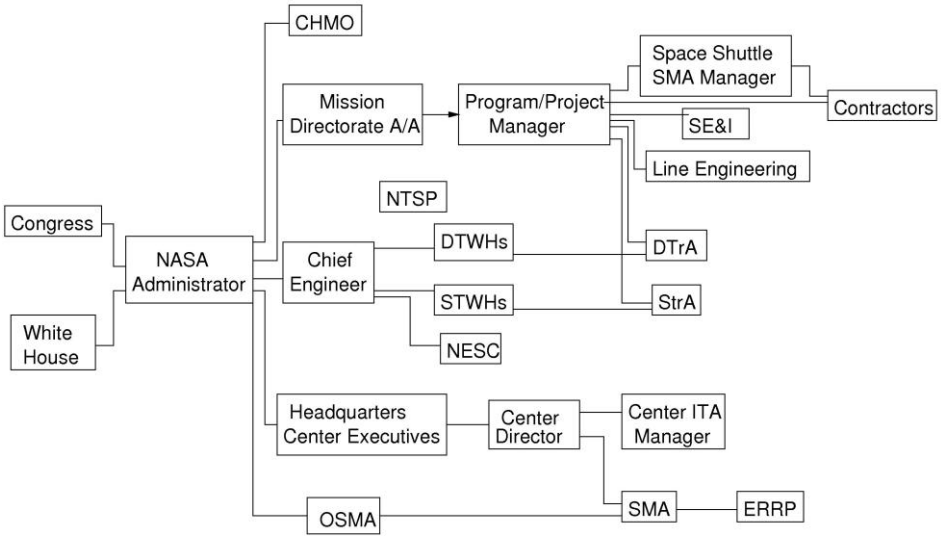


Figure 1: Simplified Structure of ITA (March 2005)

Example parts of the complete STAMP safety control structure model are contained in Appendix D.1. Only the STWH, DTWH, and Trusted Agents are included for space reasons. All the information in the parts not shown but required for the risk analysis is contained in other parts of this report.

2.3 Mapping System Requirements to Component Responsibilities

By tracing the system-level requirements and constraints identified in the preliminary hazard analysis to the specific responsibilities of each component of the ITA structure, it is possible to ensure that each safety requirement and constraint is embedded in the organizational design and to find holes or weaknesses in the design. For example, the following shows part of the mapping for system safety requirement 1a:

> *1a. 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.*

CE: Develop, monitor, and maintain technical standards and policy.

DTWHs:

- Recommend priorities for development and updating of technical standards.
- Approve all new or updated NASA Preferred Standards within their assigned discipline. (NASA Chief Engineer retains Agency approval)
- Participate in (lead) development, adoption, and maintenance of NASA Preferred Technical Standards in the warranted discipline
- Participate as members of technical standards working groups.

NTSP: Coordinate with TWHs when creating or updating standards.

OSMA:

- Develop and improve generic safety, reliability, and quality process standards and requirements, including FMEA, risk, and the hazard analysis process.
- Ensure that safety and mission assurance policies and procedures are adequate and properly documented.

Discipline Trusted Agents:

- Represent the DTWH on technical standards committees.

In the above example, the CE is responsible for developing, monitoring, and maintaining technical standards and policy. The DTWHs, NTSP, OSMA, and the Discipline Trusted Agents all play a role in implementing this CE responsibility as noted. These roles and responsibilities were developed using the ITA implementation plans of February 2005 and March 2005. Appendix D.2 contains the complete mapping.

Some specific concerns surfaced during this process, particularly about requirements not reflected in the ITA organizational structure. First, the lack of direct engagement in ITA by line engineering (both within NASA and in the contractor organizations) may be a problem over the long run. Line engineers may feel disenfranchised, resulting in their abdicating responsibility for safety to the warrant holders or, at the other extreme, simply bypassing the warrant holders. We discuss this further in the final summary

and recommendations (Section 3) along with other concerns related to the roles of the trusted agents and the contractors.

A second omission we detected is appeals channels for complaints and concerns about the ITA structure itself that may not function appropriately. All channels for expressing technical conscience go through the warrant holders, but there is no defined way to express concerns about the warrant holders themselves or aspects of ITA that are not working well.

Third, we could not find in the ITA implementation plans documentation of who will be responsible to see that engineers and managers are trained to use the results of hazard analyses in their decision-making. In general, the distributed and seemingly ill-defined responsibility for the hazard analysis process made it difficult for us to determine responsibility for ensuring that adequate resources are applied; that hazard analyses are elaborated (refined and extended) and updated as the design evolves and test experience is acquired; that hazard logs are maintained and used as experience is acquired; and that all anomalies are evaluated for their hazard potential. Currently, many of these responsibilities are assigned to SMA, but with much of this process moving to engineering (which is where it should be), clear responsibilities for these functions need to be specified. We suggest some below.

Finally, although clearly assessment of how well ITA is working is part of the plan (and the responsibility of the Chief Engineer) and this risk analysis and the planned assessment is part of that process, specific organizational structures and processes for implementing a continual learning and improvement process and making adjustments to the design of the ITA itself when necessary might be a worthwhile addition.

In order to ensure that the risk analysis (and thus the planned assessment) was complete, we added these responsibilities in the parts of the control structure that seemed to be the natural place for them. Many of these responsibilities may already be assigned and we may simply not have found them in the documentation or the place for them may not have been decided. Either way, by adding them we ensure a more complete risk analysis that incorporates the consequences of their not being fulfilled.

The most important of these additions is responsibility for system hazard analysis (which NASA sometimes calls integrated hazard analysis) and communication about hazards to and among the contractors and NASA line engineers. Theoretically, this task should be done by system engineering (SE&I), but the description of the role of SE&I in the March plan did not contain any information about such an assigned task. We added these responsibilities to SE&I as the logical place for them, and they were necessary to complete later steps of the risk analysis and generation of metrics. Alternatively, they might be the responsibility of the STWH, but this seems to overload the STWH and properly should be the responsibility of system engineering. Many of these functions would, in the defense community, be performed by the system engineering group within the prime contractor, but NASA does not employ the prime contractor concept. The added responsibilities are:

STWH:

- *Ensure communication channels are created and effective for passing information about hazards between NASA and the contractors and between multiple NASA Centers involved in the project.* Other agencies achieve this goal in different ways that might be considered by NASA. Some options are presented in Section 3.

SE&I:

- *Perform integrated hazard analyses and anomaly investigation at the system level*. Again, this seems like a natural job for SE&I. The STWH has the assigned responsibility to make sure this function is accomplished, but the plans did not say who would actually be doing the work. SMA is not the appropriate place (as discussed in Section 3), and while it might be done by discipline engineers, system interactions and dependencies can be missed as happened with the foam: Subcomponent engineers focusing on their own part of the system may correctly conclude that anomalies have no safety-related impact on their subcomponent function, but miss potential impacts on other system components.

- *Communicate system-level, safety-related requirements and constraints to and between contractors*. This is a standard system engineering function.
- *Update hazard analyses as design decisions are made and maintain hazard logs during test and operations*. Once again, this function is currently performed by SMA but properly belongs in system engineering.

We also added responsibilities for the contractors (who are not mentioned in the implementation plan) in order to make sure that each part of the required responsibilities for mitigating the system hazard (unsafe decision-making) is assigned to someone.

Contractors:

- *Produce hazard and risk analyses on contractor designs when required or using the information provided by NASA and incorporating it into their designs starting from the early design stages.*
- *Communicate information about newly identified or introduced hazard contributors in their particular components or subsystems to those building other parts of the system that may be affected*. This information might go to SE&I, which would then be responsible for its dissemination and coordination. In the Shuttle program, such communication channels currently are implemented through various boards, panels, and TIMs. The military world also uses working groups, which have some advantages. These alternatives are discussed further in Section 3.

2.4 Identifying the ITA Risks

The next step in the process is to identify the risks to be considered. We divide the risks into two types: (1) basic inadequacies in the way individual components in the control structure fulfill their responsibilities and (2) risks involved in the coordination of activities and decision-making that can lead to unintended interactions and consequences.

2.4.1 Basic Risks

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. Good decisions are made by the ITA, but do not have adequate impact on system design, construction, and operation.

Table 1 contains the complete list of specific risks related to these four high-level risks. The detailed risks were derived from the STAMP model of the ITA hierarchical safety control structure using a new type of hazard analysis called STPA. STPA works on both the technical (physical) and the organizational (social) aspects of systems. In this case, it was applied to the social and organizational aspects. A complete STPA would delve more deeply into the specific causes of the identified risks in order to further mitigate and control them, but the short time allocated for this project (essentially one month) required a higher level analysis than is otherwise possible. Further analysis will be performed experimentally for our two-year USRA research grant.

While the list looks long, many of the risks for different participants in the ITA process are closely related. The risks listed for each participant are related to his or her particular role and responsibilities and therefore those with related roles or responsibilities will have related risks. The relationships are made

clear in our tracing of the roles and control responsibilities for each of the components of the ITA STAMP hierarchical control structure model described in the previous section.

One interesting aside is that we first created a list of ITA risks using traditional brainstorming methods. Although the participants in these sessions were experts on organizational theory and risk, we were surprised when we later used the STAMP methodology at how much more comprehensive and complete the results were. We have not seen the list of ITA risks and vulnerabilities generated by the NASA IPAO, and it will be interesting to compare that list (created by experts in program risk analysis) with the one we created using our formal modeling and analysis approach.

The additional columns in the table include a categorization of each risk (explained further in Section 2.5) and information relating the risk to our system dynamics modeling and analysis (see Section 2.6). The sensitivity analysis column provides a measure of the sensitivity of the system dynamics model variables and metrics identified in the last column to variation in model parameters. The sensitivity results fall under one of three categories: Low (L), Medium (M), or High (H). In order to determine the sensitivity of specific variables, a sensitivity analysis simulation was performed that covered a range of cases including cases where the ITA is highly successful and self-sustained, and cases where the ITA quickly loses its effectiveness. A low (L) sensitivity was assigned if the maximum variation over time of the variables under study was lower than 20% of baseline values. A medium sensitivity was assigned if the maximum time variation was between 20% and 60%, and a high (H) sensitivity was assigned for variations larger than 60%. If multiple variables were evaluated at once, an average of the sensitivity results was used. To the first approximation, the sensitivity level provides information about the importance of the variable (and thus the risk associated with it) to the success of ITA.

2.4.2 Coordination Risks

Coordination risks arise when multiple groups control the same process. Two types of dysfunctional interactions may result: (1) both controllers assume the other is performing the control responsibilities and as a result nobody does or (2) controllers provide conflicting control actions that have unintended side effects.

Because ITA represents a new structure and some functions are being transferred to the TWHs from existing organizational structures (particularly SMA), *who* is responsible for *what* seems to be changing quickly and some or all of the risks included here may no longer exist, while others may have been created. In the February ITA implementation plan, the responsibility for performing many of the system safety engineering (as opposed to assurance or compliance) functions seemed to remain with SMA. The March plan, however, states that engineering has the responsibility for "the conduct of safety engineering, including hazard analyses, the incorporation of safety and reliability design standards, and the system safety and reliability processes." For the occasional in-house activities, the plan says that Engineering will build those products with process support from SMA. For contracted activities, "NASA engineering will evaluate the contractor products and the ITA will review and approve with compliance support from SMA."

This design is fraught with potential coordination problems. The same problems that exist today, with the safety engineering functions being done by mission assurance and not used by engineering, seems to be a potential effect of the new structural design if "process support" means SMA does it. Safety engineering needs to be done by engineering, not by mission assurance, whose major responsibilities should be compliance checking. In addition, there are many potential communication problems by having the analyses done by people not involved in the design decisions. At the least, delays may occur in communicating design decisions and changes that can cause the analyses (as they are today) to be too late to be useful. At the most, it may lead to disconnects that seriously threaten the quality of the system safety engineering efforts. In our experience, the most effective projects have the discipline experts for system safety engineering analyses located in the system engineering organization. Therefore, the most appropriate place again seems to be SE&I.

A second coordination risk is in the production of standards. In the plan as we understand it and as we have seen ITA being implemented, some engineering design standards are still being produced by OSMA, for example, the technical design standards for human rating. SMA should not be producing engineering standards; to have a non-engineering group producing design engineering standards makes little sense and can lead to multiple risks. As the safety engineering responsibilities, including hazard analyses, are moving to engineering, so should the responsibilities for the standards that are used in the hazard analyses. SMA should be responsible for assurance standards, not technical design and engineering standards.

The March implementation plan says that SMA will recommend a SR&QA plan for the project. ITA will set requirements and approve appropriate parts of the plan. Again, there is potential for serious coordination and communication problems. It might make more sense for SMA to create a plan for the safety (and reliability and mission) assurance parts of the plan while Engineering creates the engineering parts and ITA sets requirements for and approves both. If this is what is intended, then everything is fine, but it deviates from what has been done in the past and we have concerns that there will be confusion about who is responsible for what and some functions might never be accomplished or, alternatively, conflicting decisions are made by the two groups and unintended conflicts and side effects may result. It would be best for engineering and assurance to be cleanly divided with respect to their appropriate responsibilities.

2.5 Categorizing the Risks

The process we followed resulted in a very long list of risks. Although at first we thought that many could easily be dismissed as of less importance, we were surprised that most appear to be important. It is clear, however, that not all these risks can be assessed fully in this first planned assessment, nor need they be. To identify which risks we recommend be included, we first categorized each risk into three types:

IC: Immediate Concern: An immediate and substantial concern that should be part of the current assessment

LT: Longer-Term Concern: A substantial longer-term concern that should potentially be part of future assessments, as the risk will increase over time

SP: Standard Process: An important concern that should be addressed through inspection and standard processes rather than an extensive assessment process.

For example, it is important to assess immediately the degree of "buy-in" to the ITA program. Without such support, the ITA cannot be sustained and the risk of dangerous decision-making is very high. On the other hand, the inability to find appropriate successors to the current warrant holders is a longer-term concern that would be difficult to assess now. The performance of the current technical warrant holders will have an impact on whether the most qualified people will want the job in the future.

The list of IC (immediate concern) and LT (longer-term) risks is still long. We took each of these risks and, using our system dynamics model, analyzed which risks are the most important to measure and assess, i.e., which ones provide the most important assessment of the current level of risk and are the most likely to detect increasing risk early enough to prevent significant losses. This analysis, which is described in the next section, resulted in our list of the best leading indicators of unacceptable and increasing risk found in Section 2.7.

TABLE 1: Responsibilities and Risks

Item	Responsibility	Inadequate Control (Risk)	Cat.	Sen.	SD Variable
EXECUTIVE BRANCH					
1	Appoint the NASA administrator	Nominates administrator who does not rank safety as a high priority or who does not have the knowledge necessary to lead the Agency in safe and reliable operations.	SP		
2	Set high-level goals and vision for NASA	Imposes pressure that affects NASA decision-making, e.g., pressures to do what cannot be done safely and requires operation outside a safe envelope	LT	H	Expectations Index
3	Create a draft budget appropriation for NASA	Does not provide a realistic budget with respect to goals	SP	M	Ratio of Available Safety Resources
CONGRESS					
4	Approve Administrator nomination (appointment)	Approves an administrator who does not rank safety as a high priority or who does not have the knowledge necessary to lead the Agency in safe and reliable operations.	SP	M	External Safety Pressure Index
5	Create NASA budget allocation	Does not provide funding necessary to create and operate safely the systems funded.	SP	H	Ratio of Available Safety Resources
6	Pass legislation affecting NASA operations	Budget priorities and legislation emphasize other goals over safety.	SP	H	Ratio of Available Safety Resources
7		Imposes excessive pressure on NASA to achieve performance goals that cannot be achieved safely.	LT	M	External Performance Pressure, Expectations index
NASA ADMINISTRATOR					
8	Appoint Chief Engineer (ITA) and Chief of OSMA	Appoints a Chief Engineer who is not willing or able to lead system safety engineering efforts.	SP	L	Chief Engineer's Priority of ITA
9		Appoints a Chief Safety and Mission Assurance Officer who is not capable of leading safety assurance efforts.	SP		
10	Provide funding and authority to Chief Engineer to execute the technical authority.	Does not provide funding or leadership and power to Chief Engineer to implement ITA adequately.	LT	M	Adequacy of ITA resources
11		Tries to do more than possible to do safely with funding available. Does not make hard choices among possible goals and programs.	LT	M	Trusted Agent Workload
12	Demonstrate commitment to safety over programmatic concerns through concrete actions.	Does not through leadership and actions demonstrate a commitment to safety. Instead, sends message that safety is second to performance (e.g., launch rate)	LT	M	Launch Rate, Launch rate delays
13		Does not exhibit appropriate leadership that supports the expression of technical conscience and the independent technical authority.	LT	M	Perception of ITA Prestige, Effectiveness and Credibility of ITA

14	Provide the directives and procedural requirements that define the ITA program.	Provides conflicting authority or directives that interfere with or weaken the independent technical authority	SP		
15	Adjudicate differences between the Mission Directorate Associate Administrators and the Chief Engineer (ITA)	Adjudicates (resolves) potential conflicts raised to administrator level in favor of programmatic concerns over safety concerns. Fails to support ITA when pivotal events occur.	LT	H	Power and Authority of ITA

CHIEF HEALTH AND SAFETY OFFICER (not completed -- out of scope					
16	Develop health and medical policy				
17	Establish guidelines for health and medical practices in the Agency.				
18	Provide oversight of health care delivery.				
19	Assure professional competency Agency-wide.				
20	Review and approve research requirements and deliverables.				

CHIEF ENGINEER (ITA)					
Implementation of the ITA					
21	Delegate authority to individuals across the Agency through a system of technical warrants.	Does not delegate authority and becomes a bottleneck for necessary approvals and actions.	IC		
22	Approve selection of technical warrant holders. TWHs shall be appointed on the basis of proven credibility from demonstrated knowledge, experience, and capability. The TWH shall be the individual best able to do the job considering technical expertise, leadership, skill, and willingness to accept the accountability of the job.	Selects warrant holders who do not have adequate skills and knowledge (credibility), integrity, leadership, and networking skills ("social capital").	LT	H	Assignment of High-Level Technical Personnel and Leaders to ITA
23		Appoints an inadequate set of warrant holders (disciplines or systems are not covered).	SP	H	Assignment of High-Level Technical Personnel and Leaders to ITA
24		Interdependencies among disciplines, i.e., system issues are not handled. Some things fall through the cracks or it is assumed that someone else is handling them. Too narrow a definition of "discipline" by DTWH.	IC	M	Amount and effectiveness of Intra-ITA communication, Safety Process & Standards Effectiveness

25	Establish the Technical Warrant System consistently across the Agency.	Inadequate design and implementation of TA in parts of the Agency. In general, inconsistency is not necessarily bad; all of NASA is not the same. But problems can occur when the same, and inappropriate, processes are imposed on different (but not necessarily inferior) organizational cultures.	SP		
26	Determine and appoint new warrant areas and TWHs as appropriate and necessary to maintain the integrity of the technical authority process.	Does not make replacements to warrant holders in a timely manner.	LT		
27		Does not add new disciplines when needed.	LT		
28	Update existing NASA direction to ensure that program/project managers must comply with the decisions of the independent technical authority for matters affecting safe and reliable operations.	Direction is not updated to ensure program/project managers comply with the decisions of the ITA for matters related to safe and reliable operations.	SP		
29	Ensure that TWHs are financially independent of program budgets and independent of program authority (outside the Program Office direct chain of management).	Warrant holders are not financially independent of program budgets.	SP	L	Adequacy of ITA resources
30		Warrant holders are not independent of program authority.	LT	M	Independence Level of ITA
31	Obtain the "buy-in" and commitment (both management and engineering) throughout the Agency to the ITA program.	Management and engineers (NASA HQ and field personnel) do not "buy into" ITA and therefore do not provide information needed or execute their responsibilities in the ITA program. Delayed acceptance of ITA.	IC	H	Perception of ITA Prestige, Effectiveness and Credibility of ITA
Effectiveness of the ITA program					
32	Ensure maintenance of individual technical expertise throughout the Agency adequate to ensure safe and reliable operations.	Technical expertise is not maintained (updated) among warrant holders and the NASA workforce in general because: (1) Opportunities and directives are not provided for maintaining expertise, (2) adequate budgets and resources are not provided, (3) inadequate training is provided, (4) warrant holders are too busy executing their duties.	LT	H	Training Adequacy of TWHs, Training Adequacy of TrAs, TrAs workload
33	Establish, provide, and secure human resources, payroll funding and services, and other direct funding to support Technical Authority activities at the Centers. That budget must address the foundational and fundamental resource tools required by the TWH to form a base of knowledge and technical capability for executing technical authority.	Resources (people, funding, warrant holder information resources) provided are not adequate to do the job	IC	M	Adequacy of ITA resources

34	Develop metrics and performance measures for the effectiveness of the Technical Warrants in general.	Feedback about how the system is working is inadequate or biased because (1) metrics and performance measures are inadequate or (2) technical review/audit is not performed or is performed inadequately or too infrequently.	LT		
35	Regularly assess the credibility and performance of the individual TWHs and provide input into the individual TWH's performance appraisals.	Regular assessments of credibility and performance of TWHs are not performed.	SP		
36		Assessments of credibility and performance of TWHs are performed inadequately and technical warrant holders who are not credible or are performing below acceptable standards are not discovered.	LT		
37		Performance appraisals provided discourage participation by the best people.	LT	M	Fairness of TrA Performance Appraisal
38	Revoke the warrant of any TWH judged to be not capable of continuing to perform the responsibilities of a TWH.	Performance of technical warrant holders is not monitored and warrants revoked when necessary.	LT		
Communications With and Among Warrant Holders					
39	Establish communication channels among warrant holders	Communication channels provided are inadequate. They are not usable, they allow blockages and delays, etc.	IC	M	Amount and Effectiveness of Intra-ITA Communication
40		TWH communication is inadequate: TWHs do not provide comprehensive reports to ITA or delayed (too late or untimely); TWHs do not have adequate communication among themselves to share information and experiences.	IC	M	Amount and Effectiveness of Intra-ITA Communication
41	Consolidate TWH reports and schedule interface meetings with warrant holders.	TWH reports are not monitored and consolidated.	LT		
42		Interface meetings are not held or warrant holders do not attend.	LT		
Communication of Decisions and Lessons Learned					
43	Maintain or assure the updating of databases that archive TA decisions and lessons learned.	Database (archive) is not provided or available.	SP		
44		Database is difficult to use (information is difficult to enter correctly or time consuming and awkward).	IC	M	Normalized Quantity and Quality of Lessons Learned
45	Create and maintain communication channels for conveying decisions and lessons learned to those who need them or can use them to improve safe system design, development, and operations.	Communication channels and databases are difficult to use or information is not provided in a way that engineers and managers can use it (information is ineffectively provided).	IC	M	Normalized Quantity and Quality of Lessons Learned
46		People do not check the database or do not check it in a timely fashion.	IC		

Ownership of technical standards and system requirements (responsibility, authority, and accountability to establish, monitor, and approve technical requirements, products, and policy) and all changes, variances, and waivers to the requirements.					
47	Develop, monitor, and maintain technical standards and policy.	General technical and safety standards and requirements are not created.	LT	H	Safety Process and Standards Effectiveness
48		Inadequate standards and requirements are created.	IC	H	Safety Process and Standards Effectiveness
49		Standards degrade as changed over time due to external pressures to weaken them. Process for approving changes is flawed.	LT	H	Safety Process and Standards Effectiveness
50		Standards not changed or updated over time as the environment changes.	LT	H	Safety Process and Standards Effectiveness
51	In coordination with programs/projects, establish/approve the technical requirements and ensure they are enforced and implemented in the programs/projects (ensure design is compliant with requirements).	Project-specific technical safety requirements are not created.	SP	H	Safety Process and Standards Effectiveness
52		Project-specific technical safety requirements are not adequate to assure an acceptable level of risk.	IC	H	Safety Process and Standards Effectiveness
53		Requirements and standards are not enforced/implemented in programs/projects	IC	H	Safety Process and Standards Effectiveness
54		Requirements and standards are enforced but not adequately. (Partially enforced or procedures set up to enforce compliance but not followed or are inadequate.)	IC	H	Safety Process and Standards Effectiveness
55	Participate as a member of the SEB and approve technical content of the RFP and contractual documents.	RFP and contractual documents do not include safety requirements and design constraints or they include an inadequate set of safety requirements, design constraints, and/or deliverables.	LT		
56		Contractors and in-house developers are not provided with adequate information about system-specific, safety-related requirements and design constraints and/or high-level NASA requirements (e.g., prioritized list of system hazards to eliminate or mitigate) for safe and reliable operations.	IC		
57	Approve all changes to the initial technical requirements.	Unsafe changes to contractual requirements are approved. Does not know change is unsafe or approvals become routine.	LT		
58	Approve all variances (waivers, deviations, exceptions) to the requirements.	Unsafe (leading to unacceptable risk) variances and waivers are approved. Variances and waivers become routine. Backlog creates pressure to approve them as project milestones approach.	LT	H	Waiver Issuance rate, Outstanding waivers accumulated
59		Past waivers and variances are not reviewed frequently enough to ensure assumptions are still valid.	LT	L	Waiver resolution rate

Safety, Risk, and Trend Analysis					
60	Conduct failure, hazard, trend, and risk analyses or ensure their quality is acceptable.	Safety and reliability analyses are not done, the quality is poor, they are not done in adequate time to be used on the project, or they are available but not used in the design process.	IC	H	Quality of Safety Analyses
61		Safety personnel, TWHs, or line engineers do not have the skills or knowledge to create and/or evaluate high-quality hazard analyses.	IC	H	Knowledge and Skills of TWH and TrAs. System Safety knowledge and skills ratio value.
62		Not enough resources are provided to do an adequate job.	IC	M	System Safety Resource Ratio
63		The information available to perform the analyses is not adequate.	IC	M	Quality of Safety Analyses, Amount and Effectiveness of Intra-ITA Communication
64		Analyses are performed only at the component level and not the system level.	IC		
65		Inappropriate analysis and assessment techniques are used or appropriate techniques are used but performed inadequately.	IC	H	Quality of Safety Analyses
66	Ensure that the results of safety and risk analyses are applied early in the program design activities.	Analyses are performed too late to affect design decisions.	IC		
67		Analysis results are not communicated to those that can use them or are not communicated in a form that is usable.	IC	M	Amount and Effectiveness of Intra-ITA Communication
68		Analyses are adequate but not used early in the concept development and design processes.	LT		
69		In-line engineers and contractors do not have adequate training to use the information provided early in the concept development and design processes.	IC	L	System Safety Knowledge and Skills. Contractor Safety Experience
70	Determine what is or is not an anomalous event and perform trend analysis (or ensure it is performed) as well as root cause and hazard analyses on anomalous events.	Anomalous events are not identified.	IC	M	Fraction of Safety Incidents Reported
71		Events are identified but not traced to identified hazards.	IC		
72		Events are identified but trend analysis is not performed or is performed inadequately so that trends are not detected or not detected in time to avert an accident.	IC		
73		Events are identified but root cause analysis is not performed or is performed inadequately. Systemic causes are not identified (and eliminated or mitigated), only symptoms of the root causes are identified.	IC	H	Fraction of incidents receiving root cause fix vs. symptom fix
74	Own the FMEA/CIL and hazard analysis logging and updating systems.	Incomplete FMEA/CIL or hazard logging is done or logs are not updated as changes occur and/or new evidence is acquired.	IC	M	Quality of Safety Analyses

75	Initiate special investigations using NESC	NESC investigation requests are denied when needed because of lack of resources or wrong set of investigations is approved. Needed investigations are not done.	IC	M	TrA Workload, Adequacy of ITA resources
Independent assessment of flight (launch) readiness					
76	Use the TWH reports and other information to perform an independent assessment of launch readiness.	Assessment of launch readiness is not based on independent information or is based on incorrect or inadequate information.	IC	H	Independence Level of ITA, Quality of Safety Analyses
77		Assessment is not independent but is based totally on information provided by other supposedly independent assessors (other signers of CoFR).	IC	H	Independence Level of ITA, Quality of Safety Analyses
78	Sign the CoFR based on his/her independent assessment of launch readiness.	CoFR signed when technical issues have not been resolved adequately due to launch pressures or unknown or inadequately evaluated information.	IC	H	Independence Level of ITA, Quality of Safety Analyses, Waiver Issuance Rate
Conflict Resolution					
79	Resolve conflicts that are raised to his/her level.	Conflicts raised to ITA level are not adequately resolved, are not resolved in a timely manner, or are not resolved at the appropriate level (resolved at a lower level without adequate consideration and not communicated upward that they exist).	IC		
80		Fails to support TWHs when pivotal events occur.	IC	H	Perception of ITA Prestige, Effectiveness and Credibility of ITA
Developing a Technical Conscience throughout the engineering community					
81	Develop, assure, and maintain a technical conscience throughout the engineering community, that is, develop a culture with personal responsibility to provide safe and reliable technical products coupled with an awareness of the avenues available to raise and resolve technical concerns. [does that include contractors?]	Engineering community does not feel a personal obligation to raise technical conscience issues.	IC	H	Fear of Reporting, Organizational Tendency to Assign Blame, Employee Sensitization to Safety Problems
82		Engineering community is not aware of the channels for raising technical conscience issues.	IC		
83	Create a system in which technical conscience can and will be exercised, that is, individuals raising technical conscience issues have a means to assure their concern is addressed completely, in a timely manner, and without fear of retribution or career damage.	Channels do not exist for raising technical conscience issues.	SP	L	Effect of Corrective Actions on Incentives to Report Incidents and Participate in resolution

84		Channels exist but people do not use them due to fear of retribution or career damage, disbelief their concerns will be addressed fairly and completely, belief that concerns will be not addressed in a timely manner.	IC	H	Fear of Reporting, Organizational Tendency to Assign Blame, Employee Sensitization to Safety Problems, Effect of Corrective Actions on Incentives to Report Incidents and Participate in resolution

SYSTEM TECHNICAL WARRANT HOLDER					
Establish and maintain technical policy, technical standards, requirements, and processes for a particular system or systems					
85	Ensure program identifies and imposes appropriate technical requirements at program/project formulation to ensure safe and reliable operations.	Appropriate and necessary technical requirements for safety are not identified or are not imposed on designers or are created too late.	IC	M	Safety Process and Standards Effectiveness
86		Approves inadequate requirements, does not propose appropriate standards, does not provide for updating of standards, does not ensure projects/programs use them.	IC	M	Safety Process and Standards Effectiveness
87	Ensure inclusion of the consideration of risk, failure, and hazards in technical requirements.	Risk, failure, and hazards are not included in technical requirements.	IC	M	Safety Process and Standards Effectiveness
88	Approve the set of technical requirements and any changes to them.	Inadequate set of technical requirements is approved. Unsafe changes are made in the requirements. Does not know they are unsafe due to inadequate analyses or bow to programmatic pressures.	IC	M	Safety Process and Standards Effectiveness
89	Approve verification plans for the system(s)	Inadequate verification plans are approved. Does not know they are inadequate because of lack of knowledge or data to evaluate them or too busy to check thoroughly, etc.	IC		
90		In general, makes unsafe technical decisions because does not have adequate levels of technical expertise: does not know enough about hazard analysis, does not have adequate knowledge about particular system and issues involved in its design/operations; does not have adequate knowledge of technologies involved in the system. Do not get information from Trusted Agents or communication channels not established or are unreliable or Trusted Agents provide information. Loses objectivity because of conflicts of interest (multiple reporting chains and responsibilities). Overloaded and no time to evaluate thoroughly.	IC	H	Quality of Safety Analyses, System safety knowledge and skills ratio, System safety efforts and effectiveness, TrA skills and workload, TWH skills.

Technical Product Compliance					
91	Ensure technical requirements, specifications, and standards have been integrated into and applied in programs/projects.	Does not oversee application and integration of technical requirements, specifications, and standards in programs/projects or does this inadequately.	IC	M	Safety Process and Standards Effectiveness
92	Approve all variances.	Approves an unsafe engineering variance or waiver because of inadequate or incorrect information or because bows to pressures from programmatic concerns. Approval becomes routine. No time or information to evaluate thoroughly.	LT	H	Waiver Issuance rate, Outstanding waivers accumulated
93	Determine whether design satisfies safety-related technical requirements.	Approves a design that does not satisfy technical requirements. Inadequate evaluation or relies on S&MA or others who are also doing compliance verification (no true redundancy, potential for single point failures). S&MA does not communicate non-compliances or does not do so in a timely manner.	LT		
94	Influence decisions made about requirements and safety at all major design reviews. This can include evaluating technically acceptable alternatives and performing associated risk and value assessments.	STWH (or his trusted agents) does not act as the safety authority during technical reviews. Does not attend or does not speak up. Does not follow up on whether necessary changes are actually made. Does not receive information about inadequacies in design from Trusted Agent.	IC	M	Power and Authority of ITA, ITA influence and prestige
95	Attest by signature that the design satisfies the technical requirements.	Signs on the basis of trusting others without adequate personal investigation or on the basis of incorrect information.	IC		
Serve as primary interface between system and ITA (CE)					
96	Maintain real-time communications with the program/project to ensure timely access by the technical authority to program/project information, impending decisions, and analysis or verification results.	ITA does not get the information from the STWH about the system required for safe and reliable ITA decision-making. Communication channels are dysfunctional, STWH does not have the time and resources, STWH is overloaded with tasks, …	IC	M	Adequacy of ITA resources, amount and effectiveness of intra-ITA communication
Assist DTWH in access to data/rationale/other experts.					
97	When a technical decision requires the approval of a DTWH, assure that DTWHs have full access both to the program/project team and to pertinent technical information before a technical decision is rendered and delivered to the program/project.	Does not ensure that DTWH has the information needed to make a proper judgment.	IC	M	Amount and effectiveness of Intra-ITA communication, Safety Process & Standards Effectiveness

Production, Quality, and Use of FMEA/SIL, Trending Analysis, Hazard and Risk Analyses.					
98	Approve the technical methodologies used to develop these products.	Approves inadequate technical methodologies because of inadequate knowledge or does not keep up with changes and improvements in technology.	IC	H	STWH and TrA Knowledge and Skills, STWH and TrA Workload, Quality of Safety Analyses
99	Approve the final analysis results to be incorporated into the technical product	Approves inadequate safety and reliability engineering analyses and results because does not have skills or knowledge, does not have time or resources to evaluate properly, or approval become routine.	IC	H	TrA Knowledge and Skills, TrA Workload, Quality of Safety Analyses
100	Ensure the hazard analysis is delivered to and used by design engineers while there is still time to affect the design.	Hazard analyses are delayed beyond the point where they can affect the most critical design decisions. Hazard analyses are delivered in a timely manner but STWH does not ensure they are used in the early design stages.	IC		
101	Initiate special investigations if he/she deems further evaluation or testing is prudent for risk quantification if technical boundaries have been exceeded or if alternative technical options may be required to solve a complex issue. Can request the investigation from the project by negotiating with program/project manager and drawing on line-engineering under program/project funding or, in special cases, investigations can be funded by ITA and performed by STWH or by NESC.	Special investigations are not requested due to not believing they are needed. Resources not available.	LT	L/M	Adequacy of ITA resources, TrA workload, System Safety knowledge and Skills
Timely, day-to-day technical positions on issues pertaining to safe and reliable operations					
102	Provide input to engineering review boards, TIMs, and special technical issue topics to ensure that safety is a regular part of the design.	STWH or trusted agent does not attend or does not speak up. Does not follow up on whether inputs are implemented.	IC	M	Power and Authority of ITA, ITA influence and prestige, Skills of TWH and TrAs
103	Participate in program/project technical forums and boards to maintain cognizance of technical design and all safety-related technical issues.	Does not participate due to over-commitment of time or inadequate trusted agents to represent him/her.	IC	M	Number of Trusted Agents, TrA workload, Portion of TrA time spent on ITA activities
104	Integrate appropriate individual DTWH reviews and prepare integrated technical positions.	Information does not get passed to appropriate people.	IC		

Establishing appropriate communication channels and networks					
105	Select and train a group of Trusted Agents.	Creates an inappropriate or inadequate set of Trusted Agents. Trusted agents are not provided with adequate training, are poorly selected, or are poorly supervised (not given adequate direction and leadership). Selected Trusted Agents lack needed integrity, leadership, and networking skills ("social capital").	IC	H	Number of Trusted Agents, TrA workload, Portion of TrA time spent on ITA activities, TrA knowledge and skills
106		Does not recruit an adequate number or set of Trusted Agents and becomes overloaded so inadequately performs own responsibilities.	IC	H	Number of Trusted Agents, TrA workload, Portion of TrA time spent on ITA activities, TrA knowledge and skills
107		Cannot find appropriate Trusted Agents: The most talented people do not want to become TrAs.	LT	M	Availability of high-level technical personnel
108	Establish and maintain effective communication channels with his/her trusted agents and with in-line engineers.	Inadequate communication channels block or delay information to or from STWH	IC	M	Amount and Effectiveness of Cross-Boundary Communication, Safety Knowledge and Skills
109	Ensure communication channels are effective between NASA and contractors for passing information about hazards and between the NASA Centers involved in the program/project.	Inadequate communication channels block or delay information to or from contractors or within multi-Center programs/projects	IC	M	Amount and Effectiveness of Cross-Boundary Communication, Safety Knowledge and Skills
Succession Planning					
110	Train and mentor potential successors.	Does not groom successors.	LT		
111		Cannot find appropriate successors: The most talented people do not want to become STWHs.	LT	M	Assignment of High-Level Personnel and Leaders to ITA, Availability of high-level technical personnel
Documentation of all methodologies, actions/closures, and decisions.					
112	Sign signature page of all documents in which participate in decision-making.		SP		
113	Maintain objective quality evidence (OQE) of the decisions and information on which decisions were based.	OQE and basis for decision-making is not maintained perhaps due to overload. OQE is inadequate perhaps due to lack of accessibility to proper information, lack of understanding of what type of OQE is needed [who determines what is OQE?]	IC		
114	Provide feedback to the TA about decisions and actions.	Incorrect decisions made by TA due to lack of information	IC		

Sustaining the Agency knowledge base through communication of decisions and lessons learned.					
115	Document or ensure program/project provides documents to appropriate parties including both precedent-setting decisions (e.g., expanded technical envelopes, sensitivity data, and technical requirements) and lessons learned. This documentation shall include the circumstances surrounding the issue, technical positions (including dissenting opinions), and logic used for final decision-making.	Inadequate documentation and communication of decisions. Documentation and lessons learned not maintained or not based on objective quality evidence.	IC	M	Normalized Quantity and Quality of Lessons Learned
116	Provide input to the lessons-learned system about his/her experiences in implementing TWH responsibilities.	Incorrect or inadequate contributions to lessons-learned system due to inadequate root cause analysis or inadequate time.	IC	M	Normalized Quantity and Quality of Lessons Learned
117	Communicate decisions and lessons learned to his/her network of trusted agents and others involved in the system design, development, and operations.	Decisions and lessons learned are not communicated to STWH network of trusted agents and others who need them.	IC	M	Amount and Effectiveness of Intra-ITA communication
Assessment of launch readiness from the standpoint of safe and reliable flight and operations					
118	Integrate information provided by Trusted Agents, DTWHs, and others into an assessment of launch readiness.	STWH bases assessment of launch readiness on incorrect information, necessary information not acquired, or trusts assessment of others without adequate filtering and validation.	IC	H	Amount and Effectiveness of Intra-ITA communication, Quality of Safety Analyses, ITA Level of independence
119	Sign the CoFR to attest to system flight readiness.	Signs CoFR without adequate and independent assessment of flight readiness. Conforms to programmatic pressures.	IC	H	Quality of Safety Analyses, ITA Level of Independence, Fraction of Launches Delayed for safety reasons
Budget and Resource Requirements Definition					
120	Identify the resources necessary to support all required warrant holder activities, providing budget input and establishing working agreements.	Requests inadequate resources.	IC	M	TWH ability to obtain and manage adequate resources, Effectiveness and Credibility of ITA (proxy)
Maintaining Competence					
121	Maintain their level of technical expertise in technologies and specialties of their warranted system(s) and also currency in program efforts that affect the application of technical requirements.	Does not maintain adequate level of technical expertise or on details of warranted system design.	LT	M	Knowledge and Skills of Trusted Agents, Training Adequacy of TrAs

Leading the technical conscience for the warranted system(s)					
122	Identify technical conscience issues.	Does not identify own technical conscience issues.	LT	M	Effect of Proactive ITA efforts
123	Listen to technical personnel raising issues.	Does not respond appropriately to expressions of technical conscience reported to him or her. Responds but not in a timely manner.	IC	M	Likelihood of Reporting and participating in incident investigation, Fraction of incidents receiving corrective action
124	Act proactively to identify and implement solutions	Does not act to identify and implement solutions or delays occur in doing so.	IC	M	Effect of Proactive ITA Efforts on Risk
125	Provide feedback on the disposition of the concern to the person who reported it in the first place as well as to the Chief Engineer (ITA).	Does not provide feedback to person raising the issue.	IC	M	Fraction of incidents receiving corrective action
126	Raise unresolved technical conscience issues to the Chief Engineer.	Unresolved issues are not raised to levels above but resolution is inadequate.	IC		

DISCIPLINE TECHNICAL WARRANT HOLDER					
Interface to Specialized Technical Knowledge within the Agency					
127	Select and train a group of Trusted Agents to assist in fulfilling the technical warrant holder responsibilities. These trusted agents will be consulting experts across the Agency with knowledge in the area of interest and unique knowledge and skills in the discipline and sub-discipline areas.	Creates an inappropriate or inadequate set of Trusted Agents: Trusted Agents not provided with adequate training, poorly selected, poorly supervised (not given adequate direction and leadership). Selected Trusted Agents lack needed integrity, leadership, and networking skills ("social capital").	IC	M	Knowledge and Skills of Trusted Agents, Training Adequacy of TrAs
128		Does not recruit enough Trusted Agents or wrong set. Tries to do it all himself/herself and becomes overloaded so inadequately performs responsibilities.	IC	M	Trusted Agents Workload, Average Number of TrAs per TWH
129	Establish and maintain effective communication channels and networks with trusted agents and with in-line engineers.	Does not create or maintain effective communication channels to get information needed for good decision-making. Distance from Center/Program may limit influence and complicate communication.	IC	H	Amount and effectiveness of Intra-ITA communication
Assistance to STWHs in carrying out their responsibilities.					
130	Provide discipline expertise and a fresh set of eyes in assisting STWH in approving or disapproving all variances to technical requirements within the scope of the warrant.	Provides inadequate or incorrect information to STWH or provides it too late to be useful.	IC	H	Amount and effectiveness of Intra-ITA communication, Knowledge and Skills of Trusted Agents, Trusted Agents Workload
131	Provide assessment of technical issues as required.	Does not provide required technical positions, technical positions provided are unsafe or are too	IC	H	Amount and effectiveness of Intra-ITA

		late to be useful. Cannot get necessary insight into contracted work or work at other Centers.			communication, Knowledge and Skills of Trusted Agents, Trusted Agents Workload, Quality of SMA products and Analyses
132	In support of a STWH, evaluate a program/project's design and analysis methodologies, processes, and tools to ensure the program/project achieves the desired goals for safe and reliable operations.	Inadequate methodologies, processes, and tools are approved and used.	IC	M	Safety Process & Standards Effectiveness, ITA Credibility and Effectiveness (proxy)
133	Assist STWHs in evaluating requirements, implementation, variances and waiver requests involving the warranted technical discipline.	Recommends approving an unsafe engineering variance or waiver due to inadequate or incorrect information or pressures related to programmatic concerns.	IC	M	Quality of SMA products and Analyses, Quality of Incident Investigation, Fraction of corrective actions rejected at safety review, Waiver issuance rate
134	Document all methodologies, actions/closures, and decisions made.	Inadequate documentation perhaps due to lack of time or resources.	IC	M	Normalized Quality and Quantity of lessons learned
135	Maintain OQE to support decisions and recommendations.	Does not maintain OQE, perhaps due to overload, inaccessibility to information needed, or lack of understanding of what is OQE.	IC		
136		OQE is inadequate, perhaps due to lack of accessibility to proper information or lack of understanding of what type of OQE is needed.	IC		
137		In general, inadequate technical decisions made because does not have adequate knowledge of discipline-related issues: do not get information from Trusted Agents or get incorrect information; communication channels not established or not reliable; does not have adequate levels of technical expertise (does not know enough about hazard analyses and other safety-related products and processes) or does not have adequate or up-to-date (state-of-the-art) knowledge about discipline). Loses objectivity because of conflicts of interest (multiple reporting chains and responsibilities)). Cannot get adequate insight into contracted work or work at other Centers.	IC	H	Quality of Safety Analyses, System safety knowledge and skills ratio, System safety efforts and effectiveness, TrA skills and workload, TWH skills.
138	Identify the resources necessary to support all required warrant holder activities, providing budget input and establishing working agreements	Requests inadequate resources.	IC	M	TWH Ability to Obtain and Manage Adequate Resources
Ownership of technical specifications and standards for warranted discipline (including system safety standards)					
139	Recommend priorities for development and updating of technical standards.	Inadequate standards are not updated or needed standards are not produced. Incorrect prioritization of needs for new or updated standards.	IC	M	Safety Process & Standards Effectiveness

140	Participate as members of technical standards working groups.	Ineffective membership on technical standard working groups. Does not attend or does not speak up.	IC	M	Safety Process & Standards Effectiveness, Trusted Agents Workload
141	Approve all new or updated NASA Preferred Standards within their assigned discipline.	Approves inadequate standards.	IC	M	Safety Process & Standards Effectiveness, Knowledge and Skills of Trusted Agents, Trusted Agents Workload
142	Participate in (lead) development, adoption, and maintenance of NASA Preferred Technical Standards in the warranted discipline.	Standards not available or inadequate standards used.	LT	M	Safety Process and Standard Effectiveness, Trusted Agent Workload
143	Evaluate and disposition any variance to an owned NASA Preferred Standard.	Recommends approving unsafe engineering variance or waiver: inadequate or incorrect information or bows to programmatic pressures.	IC	M	Quality of SMA products and analyses, Fraction of corrective actions rejected by safety panel, Waiver Issuance Rate
Sustaining the Agency Knowledge Base in the Warranted Discipline					
144	Ensure that decisions and lessons learned are documented and communicated to other technical warrant holders and to his/her network of trusted agents and others involved in the technical discipline within the Agency and its contractors. This documentation shall include the circumstances surrounding the issue, technical positions (including dissenting positions), and logic used for final decision-making.	Does not ensure lessons learned are captured and communicated to those needing them.	IC	H	Normalized Quality and Quantity of lessons learned
Sustaining the General Health of the Warranted Discipline Throughout the Agency					
145	Monitor the general health of their warranted discipline throughout the Agency and provide recommendations for improvement (tools, techniques, and personnel) to the Engineering Management Board, the Chief Engineer, and other Agency and Center organizations that can improve the health of the warranted discipline.	Does not ensure Agency technical expertise is at an appropriate level because of inadequate information about state of knowledge in Agency, inadequate knowledge about state-of-the-art. Difficulty in finding out everything going on, especially at other Centers.	IC	M	Training Adequacy of TWHs, Training Adequacy of Trusted Agents, Amount and Effectiveness of Communication within TWH-TrA community
146	Ensure technical personnel supporting programs/projects are using adequate tools, equipment, and techniques that meet current expectations for the discipline and for the end products.	Does not ensure using adequate tools and techniques because does not know what is available, inaccurate information about what is actually being used by personnel (including contractors), does not have adequate information about state-of-the-art tools, equipment, and techniques. Cultural mismatches. Do not have knowledge of all projects or what is happening at contractors.	IC	M	Training Adequacy of TWHs, Training Adequacy of Trusted Agents, Amount and Effectiveness of Communication within TWH-TrA community, Safety Process and Standards Effectiveness

147	Communicate best practices for his/her warranted discipline throughout the Agency.	Does not communicate best practices or does not use effective communication channels.	IC	M	Amount and Effectiveness of Communication within TWH-TrA community, Safety Process and Standards Effectiveness
Succession Planning					
148	Train and mentor potential successors.	Does not groom successor.	LT		
149		Cannot find appropriate successors: The most talented people do not want to become DTWHs.	LT	M	Availability of High-Level Technical Personnel, Perception of ITA Influence and Prestige
Leading the technical conscience for the warranted discipline					
150	Identify technical conscience issues.	Does not identify own technical conscience issues.	IC		
151	Listen to technical personnel raising issues.	Does not respond appropriately to expressions of technical conscience reported to him or her. Responds but not in a timely manner.	IC	M	Fraction of Incidents Receiving Corrective Actions, Effect of Actions on Incentives to Report Incidents and Actively Participate in Investigations
152	Act proactively to identify and implement solutions	Does not act to identify and implement solutions or delays in doing so.	IC	H	Proactive ITA Risk Mitigation Efforts
153	Provide feedback on the disposition of the concern to the person who reported it in the first place as well as to the Chief Engineer (ITA).	Does not provide feedback to person raising the issue.	IC	M	Fraction of Incidents Receiving Corrective Actions, Effect of Actions on Incentives to Report Incidents and Actively Participate in Investigations
154	Raise unresolved technical conscience issues to the Chief Engineer.	Unresolved issues are not raised to levels above but resolution is inadequate or inappropriately terminated.	IC	M	Rate of Discarded Incidents, Rate of Incidents Leading to no Future Action
Budget and Resource Requirements Definition					
155	Identify the resources necessary to support all required warrant holder activities, providing budget input and establishing working agreements.	Requests inadequate resources.	IC	H	Adequacy of ITA resources, TWH ability to obtain and manage resources

TRUSTED AGENTS					
Screening Functions					
156	Evaluate all changes and variances and perform all functions requested by STWH or DTWH	Does not provide adequate screening of changes and variances for STWH because not adequately competent or informed: (a) selection process becomes politicized or the most talented people do not want to become Trusted Agents (e.g., negative impact on career); (b) skills erode over time due to lack of training or updating (i.e., not technically qualified); (c) lack knowledge of a particular program/project; (d) lack access to safety information (hazard and risk analyses) when needed.	IC	M	Knowledge and Skills of TWHs, Knowledge and Skills of Trusted Agents, Adequacy of Training, Quality of Safety Analyses
157		Does not provide timely information (provides it too late or provides outdated information).	IC		
158		Screens out information that should have been passed to TWH.	IC		
159		Resolves conflicts in work responsibilities between TWH and program/project manager in favor of program/project manager because: (a) funding is not independent, (b) conflicts of interest and feels more loyalty to program/project manager, (c) under pressure due to career prospects or performance appraisals, (d) places performance over safety, (e) inadequate understanding or evaluation of risk (complacency).	IC	M	Level of Independence, Fairness of Performance Approvals, Expectations Index, Quality of Safety Analyses
Conducting Daily Business for STWH					
160	Represent the STWH on boards, forums, and in requirements and design reviews.	Does not provide adequate representation. Does not attend, does not speak up, does not pass information up to TWH.	IC	M	Fraction of Corrective Actions rejected at safety review
161	Represent the DTWH on technical standards committees	Does not provide adequate representation. Does not attend, does not speak up, does not pass information up to TWH.	IC	M	Safety Process and Standards Effectiveness
Providing Information to TWHs					
162	Provide information to the TWHs about a specific project.	Communication channels between TWHs and Trusted Agents are dysfunctional (blockages, delays, distortions).	IC	M	Amount and Effectiveness of TWH-TrA communication
163		Accepts risks without communicating them to Technical Authority because does not understand the safety-critical nature of the decision.	IC	H	Knowledge and Skills of Trusted Agents, Quality of Safety Analyses, Fraction of Incidents requiring Investigation

IN-LINE ENGINEERS					
164	Provide unbiased technical positions to the warrant holders, SMA, Trusted Agents, and programs/projects	Provides biased or inadequate support or information because: (a) inadequate expertise in discipline, perhaps not updated over time; (b) conflicting loyalties and pressures from program/project managers.	IC	H	System Safety Knowledge and Skills, Quality of Safety Analyses
165		Accepts risks at own level without getting TWH involved (e.g., misclassification and mishandling of in-flight anomalies).	IC	M	Employee Sensitization to Safety Problem, Incentives to Report Problems and Participate in Investigations
166		Does not provide timely technical input to warrant holders (perhaps due to inadequate problem-reporting requirements or blocks or delays in reporting channels.)	IC		
167		Abdicates responsibility for safety to TWH.	IC	H	Quality of Safety Analyses
168		Resolves conflicts in work responsibilities between safety and program/project manager in favor of program/project manager because: (a) abdication of responsibility for safety to TWH (feels disenfranchised or assumes someone else is taking care of it) (b) conflicts of interest and feels more loyalty to program/project manager, (c) under pressure due to career prospects or performance appraisals, (d) places performance over safety due to inadequate understanding or evaluation of actual risk (complacency).	IC	H	Schedule Pressure, Quality of Safety Analyses, Risk Perception, System Safety Knowledge and Skills
169		Does not "buy into" ITA program.	IC	H	Effectiveness and Credibility of ITA, Influence and Prestige of ITA
170		Does not respect STWH or DTWH.	IC	H	Assignment of High-Level Technical Personnel and Leaders to ITA, Knowledge and Skills of TWHs, Power & Authority of ITA

171	Conduct system safety engineering, including incorporation of safety and reliability design standards, system safety and reliability analyses, and incorporation of the analysis results into the system or component design, development, and operation. For in-house activities, perform hazard and risk analysis, system safety design, FMEA, and identification of critical items. For contracted activities, evaluate the contractor-produced analyses and incorporation of results into contractor products.	Inadequate system safety engineering activities due to lack of knowledge or training.	IC	H	System Safety Efforts and Efficacy, Quality of Safety Analyses, Ability to perform Contractor Oversight, System Safety Knowledge and Skills
172	Act as the technical conscience of the Agency.	Does not exercise technical conscience or waits too long to report because: (a) under pressure from program/project manager and fear career impacts, (b) inadequate channels for expressing technical conscience, (c) does not know about reporting channels or afraid to exercise them.	IC	M	Organization Tendency to Assign Blame, Effectiveness and Credibility of ITA, Schedule Pressure, Expectations Index, Risk Perception

CHIEF SAFETY AND MISSION ASSURANCE OFFICER (OSMA)					
Leadership, policy direction, functional oversight, and coordination of assurance activities across the Agency					
173	Develop and improve generic safety, reliability, and quality process standards and requirements, including FMEA, risk, and hazard analysis process.	Does not provide adequate standards and guidelines.	IC	M	Safety Process and Standards Effectiveness
174	Selection, relief, and performance evaluation of all Center SMA Directors, lead S&MA managers for major programs, and Director of IV&V Center.	Inadequate selection, relief, and performance evaluation. Evaluation omits weaknesses, perhaps due to not knowing about them.	IC		
175	Provide oversight of the role of Center Directors in safety and provide a formal performance evaluation for each Center Director.	Inadequate oversight and evaluation.	IC		
176	Oversee the S&MA organizations at the Centers and IV&V Facility	Inadequate oversight of operations at S&MA at Centers.	IC		
177	Provide appropriate budgets, standards, and guidelines to Center S&MA personnel.	Does not provide appropriate budgets, standards and guidelines to Center S&MA personnel.	IC	H	System Safety Resource Adequacy, Safety Process and Standard Effectiveness
178	Ensure that safety and mission assurance policies and procedures are adequate and properly documented.	Safety and mission assurance policies and procedures are inadequate or improperly documented.	IC	M	Safety Process and Standards Effectiveness

Assurance of Safety and Reliability on Programs/Projects					
179	Audit adequacy of system safety engineering on projects and line engineering organizations.	As technology changes, does not update procedures and processes.	LT	M	Safety Process and Standards Effectiveness, System Safety Knowledge and Skills
180		Inadequate personnel in terms of number and skills (not adequately trained or training is not updated as technology changes).	IC	M	Number of NASA SMA employees, System Safety Knowledge and Skills
181	Oversee the conduct of reviews and obtaining of OQE to provide assurance that programs/projects have complied with all requirements, standards, directives, policies, and procedures.	Reviews are not performed and/or adequate OQE is not obtained or they are performed inadequately or too late to be effective.	IC		
182	Decide the level of SMA support for the programs/projects	Does not provide adequate resources or appropriate leadership or directions to Center S&MA	IC	M	System Safety Resources, Relative Priority of Safety Program
183	Conduct trend analysis, problem tracking, and provide input to lessons learned system.	Inadequate trend analysis, problem tracking, and documentation of lessons learned perhaps due to lack of skilled personnel, lack of resources, poor or inadequate standards and processes.	IC	M	Quantity and Quality of Lessons Learned, Safety Process and Standard Effectiveness
184	Suspend any operation or program activity that presents an unacceptable risk to personnel, property, or mission success and provide guidance for corrective action.	Does not intervene when program or project presents an unacceptable risk to personnel, property, or mission success perhaps because does not understand risk or submit to performance pressures.	IC	H	Perceived Priority of Performance, Perceived Risk
185		Intervenes but guidance for corrective action is inadequate or not provided in a timely manner.	IC		
186	Conduct launch readiness reviews and sign CoFR	Signs CoFR without adequate OQE and analyses	IC		
Incident/Accident Investigation					
187	Conduct or oversee root cause analysis and accident/incident investigations.	Root cause analysis and accident/incident analysis is superficial or flawed. Accident/incident reports and communication of lessons learned are inadequate.	IC	M	Quantity and Quality of Lessons Learned, Fraction of incident investigations leading to systemic factor fixes
188		Maybe leave out some of these roles that do not impact ITA but include potential coordination problems. Both assuming other is doing compliance checking adequately and do not obtain independent confirmation. Provide conflicting oversight and procedures.	IC	M	Safety Process and Standard Effectiveness

CENTER SAFETY AND MISSION ASSURANCE (S&MA)					
189	Conduct reviews and obtain OQE to provide assurance that programs/projects have complied with all requirements, standards, directives, policies, and procedures.	Inadequate reviews and OQE, perhaps due to inadequate resources or expertise.	N/A	M	Fraction of Corrective Actions rejected at safety review
190	Perform compliance verification assuring that the as-built hardware and software meet the design and that manufacturing adheres to specified processes.	Compliance verification not performed or performed inadequately.	N/A		
191	Perform quality (reliability and safety) assessments	Assessments not performed or performed inadequately.	N/A	M	Quality of Safety Analyses and S&MA products
192	Participate in design and readiness reviews and operations teams (e.g., MMT)	Does not participate or do not speak up.	N/A	M	Fraction of Corrective Actions rejected at Review
193	Intervene in any activity under its purview (readiness review, design review, operation) necessary to avoid an unnecessary safety risk.	Does not intervene when appropriate.	N/A	M	Fraction of Corrective Actions rejected at Review
194	Decide how much effort is to be applied to specific programs/projects	Inadequate effort applied to specific programs/projects.	N/A		
195	Recommend a Safety, Reliability, and Quality Assurance plan for each project.	Recommends an inadequate plan.	N/A		
196	Develop an Annual Operating Agreement that calls out all S&MA activities at the Center, industrial and program support, and independent assessment.	AOA is incomplete or inadequate in some way.	N/A		
197	Chair the Level 3 ERRPs at each Space Operations Center.	ERRPs have inadequate leadership.	N/A		

LEAD ERRP MANAGER AND ERRP PANELS					
198	Level 2 panels oversee and resolve integrated hazards, forwarding them to the SICB (System Integration Configuration Board) and to the ITA and Program Manager for approval.	Panels captured over time by Program Managers.	LT	H	Budget and Schedule Pressure, System Safety Resources
199	Level 3 panels conduct formal safety reviews of accepted and controlled hazards.	Reviews not performed or performed inadequately.	LT	M	Fraction of Incidents Investigated (or going through safety review), Fraction of Corrective Actions Rejected at safety Review

200	Level 3 panels assure compliance with technical requirements, accuracy, and currency of all supporting test data, hazard analysis, and controls and assure that hazards are properly classified [this is the third group to do compliance checking]	Panel captured by program/project managers. Others doing compliance checking assume it is being done here. (Coordination issues).	LT	M	Safety Process and Standard Effectiveness, Amount and Effectiveness of Cross-Boundary Communication

SPACE SHUTTLE PROGRAM S&MA MANAGER					
201	Assure compliance with requirements in the system safety engineering, reliability engineering, and quality engineering activities of the prime contractors as well as the technical support personnel from the various Centers.	Compliance not assured or assured inadequately.	LT		
202	Integrate the safety, reliability, and quality engineering activities performed by all Space Operations Centers for the various projects and program elements located at those Centers and provide them with program guidance for appropriate support and prioritization of tasks for the program.	Guidance and information not supplied and/or activities not integrated.	IC	M	Safety Process and Standard Effectiveness, System Safety Knowledge and Skills, Amount and Effectiveness of Cross-Boundary Communication

PROGRAM/PROJECT MANAGER					
203	Ensure that a full understanding of ITA is communicated through the program/project team.	Does not ensure a full understanding of ITA is communicated throughout the team and responsibilities for interfacing are not assigned or not communicated adequately.	IC	M	Amount and Effectiveness of Cross-Boundary Communication, Safety Process and Standard Effectiveness
204	Working with ITA, ensure that documentation, including the CoFR, is updated to reflect the required TA signature blocks.	Documentation is not updated to reflect required TA signature blocks.	SP	M	Safety Process and Standard Effectiveness
205	Acquire STWH's agreement before applying technical standards and requirements or altering them.	Decisions made affecting safety are not communicated to ITA perhaps because does not "buy into" ITA program or does not respect TWHs.	IC	M	Effectiveness and Credibility of ITA, ITA Influence and Prestige, Amount and Effectiveness of Cross Boundary Communication
206		Applies or alters technical standards without appropriate engagement from STWH and DTWHs.	IC		

207	In event of a disagreement with TWH, explores alternatives that would allow achieving mutual agreement and, if cannot, raises issue up chain of command.	Interacts inappropriately with TWH or does not raise issues of disagreement up chain of command.	IC	M	Fraction of Corrective Actions rejected at Safety Review, Fraction of Launches delayed for Safety Reasons
208	Obtain TWH agreement on technical decisions affecting safe and reliable operations prior to the Program or Project's application of technical standards and requirements and any alternation thereof.	Does not incorporate ITA fully in technical decision making perhaps because does not "buy into" ITA program or does not respect TWHs.	IC	M	Effectiveness and Credibility of ITA, ITA Influence and Prestige, Amount and Effectiveness of Cross Boundary Communication
209	Provide the TWH with complete and timely access to program technical data, reviews, analyses, etc.	Does not comply with warrant holder requests and controls.	IC	H	Influence and Prestige of ITA, Knowledge and Skills of TWHs, Power and Authority of ITA
210		Does not allow (limits) complete and timely access to program technical data, reviews, analyses, etc. to technical warrant holders.	IC	M	Quality of Safety Analyses, Amount and Effectiveness of Cross Boundary Communication
211	Support Trusted Agents and others and provide access to aspects of the project (reviews, etc.) necessary to perform their duties.	Penalizes employees for raising safety issues or handling safety concerns in performance appraisals or impose other career impacts.	IC	H	Organization Tendency to Assign Blame, Fear of Reporting Incidents and Problems
212	Ensure safety has priority over programmatic concerns among those who report to him (line engineering, Shuttle SMA Manager, etc.).	Places safety second and pressures those reporting to him/her to do the same. Inaccurate understanding of current risk (complacency and overconfidence).	IC	H	Perception of Risk, Performance Pressure, Expectations Index, Perceived Priority of Safety
213		Abdicates responsibility for safety to Chief Engineer and Technical authority; does not adhere to safe engineering practices.	IC	M	Quality of Safety Analyses, Amount and Effectiveness of Cross Boundary Communication

CENTER DIRECTOR					
Practice of Technical Conscience at the Center					
214	Develop a technical conscience at the Center that includes accountability for sound technical decisions and the ability to raise engineering issues and concerns affecting the safe and reliable operations that cannot be resolved through programs or projects at the Center, to the Agency Technical Warrant Holders.	Channels for expressing technical concerns are not established or are dysfunctional.	IC	L	Amount and Effectiveness of Cross Boundary Communication

Preservation of ITA financial and managerial independence at the Center					
215	Ensure that TWHs do not report through a program management chain of command when exercising TA as delegated by CE.	Compromises managerial independence of TWHs	IC	L	Effective Level of Independence of ITA
216	Structure and execute Center financial system to ensure effective execution of TWH responsibilities and preserve TWH independence from program/project funding (Ensure that financial and personnel resources are aligned with ITA).	Financial system at the Centers is inadequate to support TWH responsibilities.	IC	M	Adequacy of ITA/CE resources, Ability of TWH to obtain and manage resources
217		Financial system at the Centers does not preserve TWH independence from program/project funding.	IC		
218	Ensure that internal activities and organizations, such as operations and engineering, are aligned to support the independent exercise of TA by the STWHs.	STWHs are hindered in their exercise of technical authority by blockages and administrative hurdles.	IC	H	Effectiveness and Credibility of ITA, ITA Power and Authority
219	Ensure the TWHs do not have a supervisory reporting chain to Program and Project Management.	Reporting chain allowed that violates independence.	IC	L	Effective Level of Independence of ITA
Support of ITA Activities at the Center					
220	Ensure each technical competency/discipline represented at the Center has a working agreement with Agency DTWH for that technical discipline.	Inadequate working agreements limits exercise of TA and limits connectivity to technical disciplines across the Agency.	IC	L	Amount and Effectiveness of Intra-ITA communication and Coordination
221		Lack of coordination of ITA activities at Centers and between Centers because: communication channels not established, communication channels not known by those who need to use them, or communication channels are dysfunctional (lengthy and involve delays, easily blocked, too many nodes, etc.)	IC	L	Amount and Effectiveness of Intra-ITA communication and Coordination
222	Ensure the Center S&MA works closely with TA to resolve technical issues uncovered by S&MA independent verification and compliance assessments and assurance reviews.	Allows dysfunctional interactions between TWHs and Center S&MA.	IC	L	Amount and Effectiveness of Cross-Boundary Communication, Safety process and Standards and Effectiveness
223	Ensure workforce competencies support TWHS succession planning.	Does not ensure appropriate successors to TWHs are available at the Center.	LT		

Support of Safety Activities at the Center					
224	Intervene in any activity under his/her purview (readiness review, design review, operation) necessary to avoid an unnecessary safety risk. Includes suspending activity and providing guidance for corrective action.	Does not intervene when necessary because of inadequate resolution of conflicting goals or lack of knowledge or understanding of the risk.	IC	H	Perception of Risk, Schedule Pressure, Performance Pressure, Expectations Index
225		Intervenes but guidance for corrective action is inadequate or not provided in a timely manner.	IC	M	System Safety Knowledge and Skills
226	Set up safety and mission assurance "directed" service pools to allow S&MA labor to be applied to programs and projects in the areas and at the levels deemed necessary by the S&MA Directors and their institutional chain of authority.	Adequate resources not assigned to S&MA to support necessary activities.	IC	H	System Safety Resource Adequacy, Perceived Priority of Safety

CENTER ITA MANAGER					
Administrative support for TWHs					
227	Coordinate resources with Line Engineering Directors or their representatives.	Lack of coordination of ITA activities at Centers and between Centers because: communication channels not established, communication channels not know by those who need to use them, or communication channels are dysfunctional (lengthy and involve delays, easily blocked, too many nodes, etc.)	IC	L	Amount and Effectiveness of Intra-ITA communication, Effectiveness of TrA communication and sense of ownership
228	Communicate with other NASA Center's ITA personnel, NESC, OCE, to coordinate activities and resources.	Communication channels are dysfunctional (lengthy and involve delays, easily blocked, too many nodes, etc.)	IC	L	Amount and Effectiveness of Intra-ITA communication, Amount and Effectiveness of Cross-Boundary Communication
229	Assist in defining and obtaining resource and funding requirements with OCE, Office of Chief Financial Officer, NESC, or a program/project.	Inadequate funds available for ITA activities	IC	M	ITA/CE resource adequacy

NASA ENGINEERING AND SAFETY CENTER (NESC)					
230	Perform in-depth technical reviews, assessments, and analyses of high-risk projects.	Performs inadequate studies or reviews of technical issues: incorrect reports and studies (says safe when not or says not safe when it is); untimely reports (correct but too late to be useful); not provided with enough resources (or provided with wrong resources) to support needs of TA (studies cannot be done or can only be done superficially).	IC	M	ITA/CE resource Adequacy, System Safety resource Adequacy, Quality of Safety Analyses, Fraction of Corrective Actions Rejected at Safety Review
231	Provide in-depth system engineering analyses.	Inadequate analyses.	IC	H	Safety Process and Standard Effectiveness, Quality of Safety Analyses
232	Facilitate or lead selected mishap investigations.	Inadequate investigations	IC	H	Quality of Incident Investigation
233	Support programs or institutions in resolving Agency's high-risk technical issues.	Inadequate support provided.	IC		
234	Provide application of NASA-wide expertise in support of technical authority.	Inadequate support provided.	IC	M	Amount and Effectiveness of Cross- Boundary Communication, Quantity and Quality of Lessons Learned

HEADQUARTERS CENTER EXECUTIVES					
235	Ensure the associated Center Director aligns that Center's organization and processes to support and maintain the independence of the TA and advises the TA of any issues at their assigned Center affecting safe and reliable operations and the successful execution of ITA.	Inadequate leadership and oversight of Center Director due to inadequate resolution of conflicting goals (programmatic concerns given priority over safety)	LT	M	Performance Pressure, Perceived Priority of Safety, Perception of Risk
236	For their Centers, develop and execute a plan to monitor the conduct of the ITA and the expression and resolution of technical conscience.	Inadequate reporting from Center Director and no plan or inadequate one to monitor conduct of TA leads to inaccurate mental model of operation of ITA at their Center. Do not know about existing problems so cannot intervene when necessary.	IC		
237	Provide oversight of operation of safety and mission assurance and directed service pools for S&MA at their centers.	Inadequate reporting and monitoring of S&MA leads to inaccurate mental model of operation of S&MA and adequacy of directed service pool resources for S&MA at their Centers in turn leads to lack of oversight and intervention when necessary and inadequate resources provided.	LT		

MISSION DIRECTORATE ASSOCIATE ADMINISTRATORS					
238	Provide leadership and be accountable for all engineering and technical work done by their Mission Directorate, Centers, and affiliated activities.	Abdicates responsibility for safety to CE. Does not adhere to safe engineering practices.	LT	M	System Safety Knowledge and Skills
239		Inadequate monitoring and feedback about state of (operation of) ITA in programs/projects leads to lack of intervention when problems arise.	LT		
240	Ensure financial and personnel resources are aligned with ITA.	Financial and personnel resources are not aligned with ITA. Does not provide adequate resources (does not understand resources required or resolves conflicts on the side of programmatic concerns) or does not ensure resources are used appropriately.	IC	M	CE/ITA resource adequacy, Trusted Agent Workload, Ability of TWHs to obtain and manage resources
241	Ensure appropriate financial and engineering infrastructure to support TWHs	Does not provide infrastructure and leadership to assure ITA is effective in their programs/projects.	IC	M	Assignment of High-Level Technical Personnel and Leaders to ITA, Amount and Effectiveness of Cross-Boundary Communication
242	Notify ITA when in the concept phase of a program/project.	Does not notify ITA early enough about a program/project to get the proper contractual requirements and interfaces in place necessary for effective application of ITA.	LT		
243	Address executive-level issues and interfaces with TA to resolve differences not reconciled at the interface between a warrant holder and a program/project manager.	Differences do not get reconciled or inordinate delays occur, causing delays in programs/projects, programmatic concerns take precedence over critical safety issues.	IC		

NASA TECHNICAL STANDARDS PROGRAM					
244	Coordinate with TWHs to identify membership on Technical Standards Working Groups to create new standards, review standards produced by external groups for adoption and interpretation, update/annotate standards to incorporate experience and lessons learned, and ensure adequate review of standards by Centers, programs, and Mission Directorates.	Inadequate standards are adopted, inadequate standards are not replaced, long delay in updating standards, standards do not receive an adequate review, standards are not updated/annotated to incorporate experience and lessons learned.	LT	H	Safety Process and Standards Effectiveness, Effectiveness and Credibility of ITA

SYSTEM ENGINEERING AND INTEGRATION OFFICE					
245	Perform integrated hazard analyses and anomaly investigation at the system level.	System-level hazards are not adequately considered or handled.	IC	M	Amount and Effectiveness of Cross-Boundary Communication, System Safety Knowledge and Skills, Ability to perform Safety oversight and integration of contractor work
246	Update hazard analyses as design decisions are made and maintain hazard logs during test and operations.	Hazard analyses become out of date and therefore of limited use or even harmful.	IC	H	Quality of Safety Analyses and SMA products, System Safety Knowledge and Skills, Quantity and Quality of Lessons Learned
247	Communicate system-level, safety-related requirements and constraints to and between contractors	Contractors do not get the information necessary to build and operate systems with acceptable risk. Do not know about hazards in other system components that could affect the design of their own component. Not provided with safety-related requirements and design constraints or provided with an inadequate set.	IC	M	Safety Process and Standards Effectiveness, System Safety Knowledge and Skills, Amount and Effectiveness of Cross-Boundary Communication, Ability to perform Safety Oversight of contactor work

CONTRACTORS					
248	Produce hazard and risk analyses when required and using the information from the analyses in their designs starting from the early design stages.	Inadequate analyses and unsafe designs produced due to lack of knowledge of system safety (analysis and design), inadequate internal communication or reviews, or lack of direction from NASA.	IC	M	Contractor System Safety Knowledge and Skills, Amount and Effectiveness of Cross-Boundary Communication, Ability to perform Safety oversight and integration of contractor work
249		Inadequate communication of safety-related analysis and design information internally among those designing and developing the system.	IC	M	Amount and Effectiveness of Cross-Boundary Communication, Safety Process and Standard Effectiveness
250	Communicate information about hazards in their components or subsystems to those building other parts of the system that may be affected (or to NASA SE&I).	Inadequate problem reporting because channels do not exist or are inadequate.	IC	H	Number of Problem Reports, Fraction of Problem reports being Investigated

2.6 Analyzing the Risks

The analyses used the system dynamics model of the Space Shuttle safety culture we had created previously. While other components of the manned space program are not directly included, such as the ISS, the cultural aspects are very similar and the results should apply broadly.

The model is described in the next section and then the results are presented. We recommend that readers unfamiliar with system dynamics first read the short tutorial in Appendix C.

2.6.1 The System Dynamics Model

For Phase 1 of our USRA grant (Sept. 2004 to February 2005), we created a system dynamics model of the NASA Space Shuttle safety culture. This model can be used to understand the factors in the Shuttle safety culture that contributed to the Columbia loss. We had originally planned to also create a model of the static control structure as it existed at the time of the Columbia accident, but we found it was impossible to understand the complex system safety management and control relationships and roles within the program at that time. We were not surprised this problem occurred: The CAIB report noted the Manned Space Flight program has "confused lines of authority, responsibility, and accountability in a manner that almost defies explanation." Leveson came to a similar conclusion while trying to understand the control structure in her role on the NASA Aerospace Safety Advisory Panel (ASAP) and on various other NASA advisory committees. In our Phase 1 research, therefore, we decided that the control structure (before the ITA) was too much of a mess to provide a useful model for analysis and instead focused most of our modeling efforts on the behavioral dynamics of the NASA Shuttle safety culture, which we believed we were able to model accurately. It is a testament to the careful design and hard work that has gone into the ITA program implementation that we were able to create the ITA static control structure model so easily in the second phase of this research.

For the risk analysis, we took our existing NASA Shuttle program system dynamics model and altered it to reflect the addition of ITA. The original model was constructed using both Leveson's personal long-term association with NASA as well as interviews with current and former employees, books on NASA's safety culture (such as McCurdy[7]), books on the Challenger and Columbia accidents, NASA mishap reports (CAIB[8], Mars Polar Lander[9], Mars Climate Orbiter[10], WIRE[11], SOHO[12], Huygens[13], etc.), other NASA reports on the manned space program (SIAT[14] 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 recently at NASA.

One of the significant challenges associated with modeling a socio-technical system as complex as the Shuttle program is creating a model that captures the critical intricacies of the real-life system, but is not so complex that it cannot be readily understood. To be accepted and therefore useful to decision makers, a model must have the confidence of the users and that confidence will be limited if the users cannot understand what has been modeled. We addressed this problem by breaking the overall system model into nine logical subsystem models, each of an intellectually manageable size and complexity. The subsystem models can be built and tested independently.

---

[7] Howard McCurdy, *Inside NASA: High Technology and Organizational Change in the U.S. Space Program*, Johns Hopkins University Press, 1994.
[8] Harold Gehman (Chair), Columbia Accident Investigation Report, August 2000.
[9] Tom Young (Chair), Mars Program Independent Investigation Board Report, NASA, 14 March 2000
[10] A. Stephenson (Chair), Mars Climate Orbiter Mishap Investigation Board Report, NASA 10 Nov. 1999
[11] D.R Branscome (Chair), WIRE Mishap Investigation Board Report, NASA, 8 June 1999
[12] NASA/ESA Investigation Board, SOHO Mission Interruption, NASA, 31 August 1998.
[13] D.C.R. Link, Report of the Huygens Communications System Inquiry Board, NASA, December 2000.
[14] Harry McDonald, Shuttle Independent Assessment Team (SIAT) Report, February 2000.

Figure 2 shows the nine model components along with the interactions among them. They are

- Risk
- System Safety Resource Allocation
- System Safety Knowledge, Skills, and Staffing
- Shuttle Aging and Maintenance
- Launch Rate
- System Safety Efforts and Efficacy
- Incident Learning and Corrective Action
- Perceived Success by Management
- Independent Technical Authority

Each of these subsystem models is described briefly below, including both the outputs of the model and the factors used to determine the results. The models themselves can be found in Appendix D.3. Sections 2.6.3 through 2.6.6 present the results of our analysis using the models.

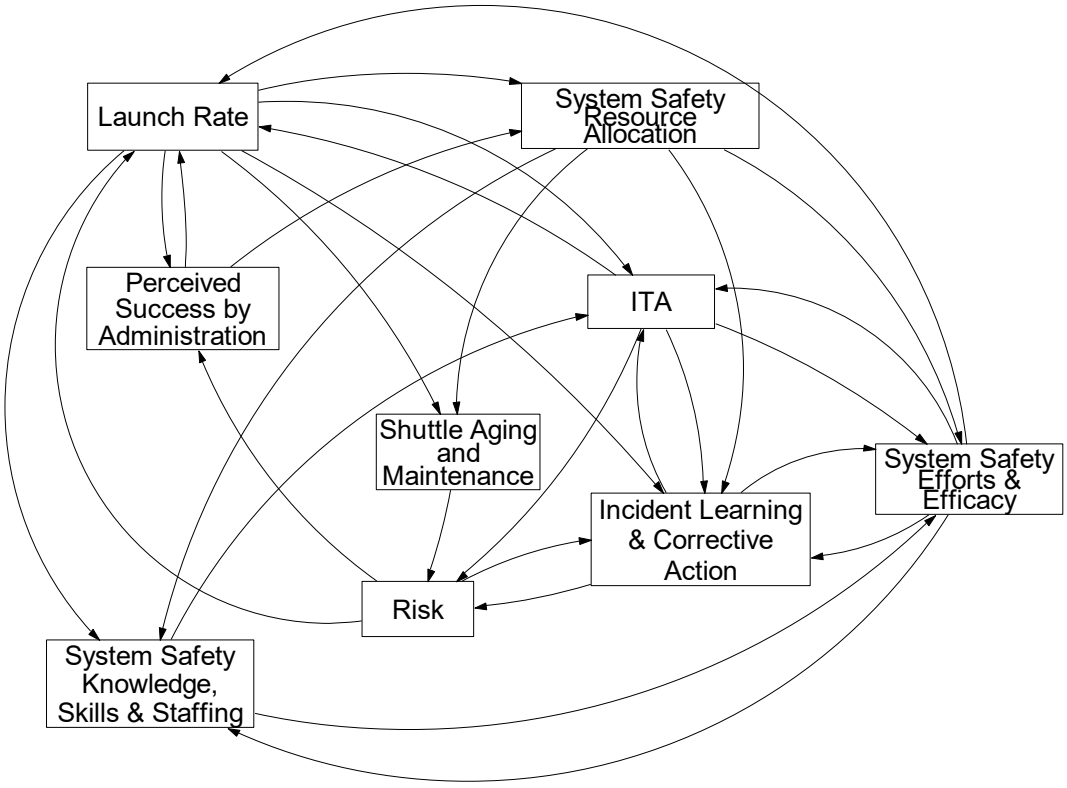


Figure 2. The Nine Subsystem Models and their Interactions

Risk: The purpose of the technical risk model is to determine the level of occurrence of problems and anomalies, as well as the interval between serious incidents (hazardous events) and accidents. The assumption behind the risk formulation is that once the system has reached a state of high risk, it is highly vulnerable to small deviations that can cascade into major accidents. The primary factors affecting the

technical risk of the system are the effective age of the Shuttle, the quantity and quality of inspections aimed at uncovering and correcting safety problems, and the proactive hazard analysis and mitigation efforts used to continually improve the safety of the system. Another factor affecting risk is the response of the program to anomalies and hazardous events (and, of course, mishaps or accidents).

The response to anomalies, hazardous events, and mishaps can either address the symptoms of the underlying problem or the root causes of the problems. Corrective actions that address the symptoms of a problem have insignificant effect on the technical risk and merely allow the system to continue operating while the underlying problems remain unresolved. On the other hand, corrective actions that address the root cause of a problem have a significant and lasting positive effect on reducing the system technical risk.

System Safety Resource Allocation: The purpose of the resource allocation model is to determine the level of resources allocated to system safety. To do this, we model the factors determining the portion of NASA's budget devoted to system safety. The critical factors here are the priority of the safety programs relative to other competing priorities such as launch performance and NASA safety history. The model assumes that if performance expectations are high or schedule pressure is tight, safety funding will decrease, particularly if NASA has had past safe operations. To prevent this decline, effective controls must be designed and implemented.

System Safety Knowledge, Skills, and Staffing: The purpose of this subsystem model is to determine both the overall level of system safety knowledge and skill in the organization and to determine if NASA has enough employees with sufficient system safety skills to be able to oversee contractor safety activities. These two parameters greatly influence the *System Safety Effort and Efficacy* subsystem model.

In order to determine these key parameters, the model tracks four basic quantities: the number of NASA employees working in system safety, the number of contractor system safety employees, the aggregate experience of the NASA employees, and the aggregate experience of the system safety contractors such as those working for United Space Alliance (USA) and other major Shuttle contractors.

The staffing numbers rise and fall based on the hiring, firing, attrition, and transfer rates of the employees and contractors. These rates are determined by several factors, including the amount of safety funding allocated, the portion of work to be contracted out, the age of NASA employees, and the stability of funding.

The amount of experience of the NASA and contractor system safety engineers relates to the new staff hiring rate and the quality of that staff. If positions related to safety and the ITA are viewed as prestigious and influential, it will be easier to attract and maintain quality employees who will bring more experience and learn faster than lower quality staff. The learning rate of the staff is also determined by training, performance feedback, and workload.

Shuttle Aging and Maintenance: The age of the Shuttle and the amount of maintenance, refurbishments, and safety upgrades affects the technical risk of the system and the number of problems, anomalies and hazardous events. The effective Shuttle age is mainly influenced by the launch rate. A higher launch rate will accelerate the aging of the Shuttle unless extensive maintenance and refurbishment are performed. The amount of maintenance depends on the resources available for maintenance at any given time. As the system ages, more maintenance may be required; if the resources devoted to maintenance are not adjusted accordingly, accelerated aging will occur.

The original design of the system also affects the maintenance requirements. Many compromises were made during the initial phase of the Shuttle design, trading off lower development costs for higher operations costs. Our model includes an exogenous variable that accounts for the original level of design for maintainability. By varying this parameter, it is possible to investigate scenarios where maintainability would have been a high priority from the beginning of the Shuttle design.

While launch rate and maintenance affect the rate of Shuttle aging, refurbishment and upgrades *decrease* the effective aging by providing complete replacements and upgrade of Shuttle systems such as

avionics, fuel systems, and structural components. The amount of upgrades and refurbishment depends on the resources available, as well as on the perception of the remaining life of the system. Upgrades and refurbishment will most likely be delayed or canceled when there is high uncertainty about the remaining operating life. Uncertainty will be higher as the system approaches or exceeds its original design lifetime, especially if there is no clear vision and plan about the future of the manned space program.

Launch Rate: The Launch Rate subsystem model is at the core of the integrated model. Launch rate affects many parts of the model, such as the perception of the level of success achieved by the Shuttle program. A high, sustained launch rate without accidents contributes to the perception that the program is safe, eventually eroding the priority of system safety efforts. A high launch rate also accelerates system aging and creates schedule pressure, which hinders the ability of engineers to perform thorough problem investigation and to implement effective corrective actions that address the root cause of the problems rather than just the symptoms.

The launch rate in the model is largely determined by three factors:

1. Expectations of high-level management: Launch expectations will be higher if the program has been successful in the recent past. The expectations are reinforced through a "Pushing the Limits" phenomenon where administrators expect ever more from a successful program, without necessarily providing the resources required to increase launch rate.
2. Schedule pressure from the backlog of flights scheduled: This backlog is affected by the launch commitments, which depend on factors such as ISS commitments, servicing (e.g., Hubble) and re-supply requirements, and other scientific mission constraints. The timing associated with various missions in the launch backlog may require mission reshuffling, which increases schedule pressure even more.
3. Launch delays caused by unanticipated safety problems: The number of launch delays depends on the technical risk, on the ability of system safety and ITA personnel to uncover problems requiring launch delays, and on the power and authority of the ITA and safety personnel to be responsible for delaying/approving launches.

System Safety Efforts and Efficacy: This subsystem model captures the effectiveness of system safety at identifying, tracking, and performing the analyses necessary to mitigate system hazards. The success of these activities will affect the number of problems and anomalies identified, as well as the quality and thoroughness of the resulting investigations and corrective actions. In the model, a combination of reactive problem investigation and proactive hazard mitigation efforts leads to effective safety-related decision-making that reduces the technical risk associated with the operation of the Shuttle. While effective system safety and ITA-related activities will improve safety over the long run, they may also result in a decreased launch rate over the short term by delaying launches when serious safety problems are identified.

The efficacy of the system safety activities depends on various factors. Some of these factors are defined outside this part of the overall model, such as the availability of resources to be allocated to safety and the availability and effectiveness of safety processes and standards, which is mainly affected by the activities of ITA personnel. Others depend on characteristics of the system safety staff, such as their number, knowledge, experience, skills, motivation, and commitment. These characteristics also affect the ability of NASA to oversee and integrate the safety efforts of contractors, which is one dimension of system safety and ITA effectiveness. The quantity and quality of lessons learned and the ability of the organization to absorb and use these lessons is also a key component of system safety effectiveness.

Incident Learning and Corrective Action: The objective of this subsystem model is to capture the dynamics associated with the handling and resolution of safety-related problems, anomalies and hazardous events. It is one of the most complex of our models, reflecting the complexity of the cognitive and behavioral processes involved in identifying, reporting, investigating, and resolving safety issues. Once integrated into the combined model, the amount and quality of learning achieved through the

investigation and resolution of safety problems impacts the effectiveness of system safety efforts and the quality of resulting corrective actions, which in turn has a significant effect on the technical risk of the system.

The structure of this model revolves around the processing of incidents or hazardous events, from their initial identification to their eventual resolution. The number of safety-related incidents is a function of the technical risk. Some safety-related problems will be reported while others will be left unreported. The fraction of safety problems reported depends on the effectiveness of the reporting process, the employee sensitization to safety problems and the possible fear of reporting if the organization discourages it, perhaps due to the impact on schedule. Problem reporting will increase if employees see that their concerns are considered and acted upon, that is, if they have previous experience that reporting problems led to positive actions. The number of reported problems also varies as a function of the perceived safety of the system by engineers and technical workers. A problem-reporting positive feedback loop creates more reporting as the perceived risk increases, which is influenced by the number of problems reported and addressed. Numerous studies have shown that the risk perceived by engineers and technical workers is different from high-level management perception of risk. In our model, high-level management and engineers use different cues to evaluate risk and safety, which results in very different assessments.

A fraction of the problems and anomalies reported are investigated in the model. This fraction varies based on the resources available, the overall number of anomalies being investigated at any time, and the thoroughness of the investigation process. The period of time the investigation lasts will also depend on these same variables.

Once a safety-related problem or anomaly has been investigated, five outcomes are possible: (1) no action is taken to resolve the problem, (2) a corrective action is taken that only addresses the symptoms of the problem, (3) a corrective action is performed that addresses the systemic factors that led to the problem, (4) the problem is deemed not to be a safety-of-flight issue and impractical to solve given budget and schedule constraints, resulting in a waiver issuance, or (5) the proposed corrective action is rejected, which results in further investigation until a more satisfactory solution is proposed. Many factors are used to determine which of these five possible outcomes results, including the resources available, the schedule pressure, the quality of the investigation process, the investigation and resolution process and reviews, and the effectiveness of system safety decision-making. As the organization goes through this ongoing process of problem identification, investigation, and resolution, some lessons are learned, which may be of variable quality depending on the investigation process and thoroughness. In our model, if the safety personnel and decision-makers have the capability and resources to extract and internalize high-quality lessons from the investigation process, their overall ability to identify and resolve problems and to do effective hazard mitigation will be enhanced.

Perceived Success by Management: The purpose of this subsystem model is to capture the dynamics behind the success of the Shuttle program as perceived by high-level management and NASA administration. The success perceived by high-level management is a major component of the "Pushing the Limit" reinforcing loop, where much will be expected from a highly successful program, creating even higher expectations and performance pressure. High perceived success also creates the impression that the system is inherently safe and can be considered operational, thus reducing the priority of safety, which affects resource allocation and the system safety and ITA status. Two main factors contribute to the perception of success: the accumulation of successful launches positively influences the perceived success while the occurrence of serious incidents (hazardous events) and accidents has a strong negative influence.

Independent Technical Authority: A new subsystem model was created to capture the effect of ITA implementation on the dynamics of the system (Figure 3). From a system-level perspective, the credibility and effectiveness of ITA directly affects *Launch Rate*, *System Safety Efforts and Efficacy*, and the way *Incident Learning and Corrective Actions* are performed, including the strength of the safety program and

the handling of requirements waivers. In the other direction, the *Credibility and Effectiveness of ITA* is directly affected by the availability of employees with high levels of *System Safety Knowledge and Skills*.

Technical Warrant Holders (TWHs) are supposed to be unaffected by schedule pressure. Trusted Agents, however, still have obligations to the project manager, so schedule pressure and *Launch Rate* may still affect their work. The effectiveness of ITA personnel is highly dependent on the quality, thoroughness and timely availability of safety analysis performed by safety experts and, therefore, it is directly affected by the *System Safety Efforts and Efficacy* model. The number of open incident investigations and waiver resolutions, captured in the *Incident Learning and Corrective Actions* model, may also affect the workload and effectiveness of the ITA designees. Finally, as the "guardian" of NASA's technical conscience, ITA promotes the raising of safety issues and concerns that can result in proactive changes in the system that will decrease system *Risk*.

Figure 3 provides an overview of the internal feedback structure of the ITA model. The internal dynamics of this model are highly reinforcing. Four internal reinforcing loops create these dynamics: Attractiveness of being a TWH, TWH Resources and Training, Ability to Attract Knowledgeable Trusted Agents, and Trusted Agent Training Adequacy. If the external influences from other parts of the overall model were removed, the *Effectiveness and Credibility of the ITA* would either grow rapidly (if left unbounded) or would collapse. The reinforcing polarity depends on the gain of each loop at every instant in time. A highly effective and credible ITA will have high Influence and Prestige, resulting in a great ability to attract highly skilled and well-respected technical leaders, ensuring the TWHs have enough power and authority to perform their functions. In addition, an effective and credible ITA will be able to obtain and manage the resources necessary for their functioning and to ensure that TWHs and Trusted Agents are provided with the resources and training necessary to remain highly knowledgeable and effective over time. On the flip side, these interactions can create a downward spiral that will act in the opposite direction.

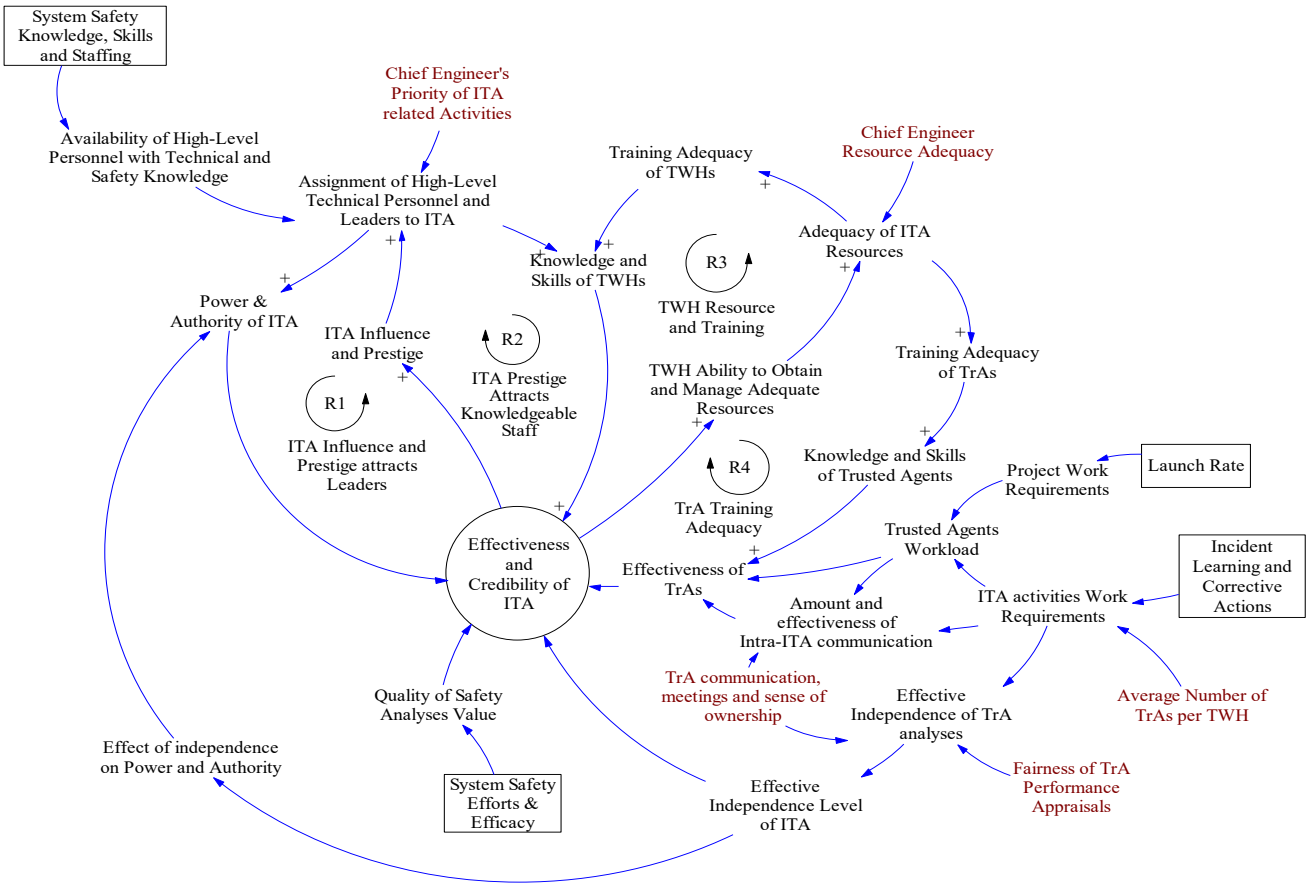


Figure 3: ITA Model Structure

2.6.2 System Dynamics Model Validation and Analyses

To validate the individual subsystem models, each was tested in isolation to ensure the behavior corresponded to our understanding of the open-loop behavior of that part of the model when critical feedback paths are removed. For example, in the absence of pressures to modify the resources allocated to safety efforts (e.g., schedule and budget pressures), the *System Safety Resource Allocation* model should output a constant level of safety resources.

After validation and comfort with the correctness of each subsystem model was achieved, they were connected to one another so important information can flow between them and emergent properties that arise from their interactions can be included in the analysis. As an example, our *Launch Rate* model uses a number of internal factors to determine the frequency at which the Shuttle can be launched. That value—the "output" of the *Launch Rate model*—is then used by many other subsystem models including the *Risk* model and the *Perceived Success by Management* models.

Once the models were tested and validated, we ran four types of analyses: (1) sensitivity analyses to investigate the impact of various ITA program parameters on the system dynamics and on risk, (2) system behavior mode analyses, (3) metrics evaluations, and (4) additional scenarios and insights. The final set of recommended leading indicators and measures of performance resulting from the analysis of the system dynamics model is presented in Section 2.7.

2.6.3 Sensitivity Analysis Results

In the open-loop test cases, the reinforcing polarity depends on initial values and on the value of exogenous parameters of the ITA model, mainly: Chief Engineer's Priority of ITA-related activities, Chief Engineer Resource Adequacy, Average number of Trusted Agents per Warrant Holder, Fairness of Trusted Agents Performance Appraisals, and Trusted Agents Communication, Meetings and Sense of Ownership. However, when the loops are closed and the ITA model is integrated within the system, many other balancing loops affect the behavior of the system and the dynamics become more complex.

In order to investigate the effect of ITA parameters on the system-level dynamics, a 200-run Monte-Carlo sensitivity analysis was performed. Random variations representing +/- 30% of the baseline ITA exogenous parameter values were used in the analysis. Figure 4a shows the results of the 200 individual traces, and Figure 4b shows the density distribution of the traces.

The initial sensitivity analysis shows that at least two qualitatively different system behavior modes can occur. The first behavior mode (behavior mode #1, Figure 4a) 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 5). More than 75% of the runs fall in that category. The second behavior mode (behavior mode #2 in Figure 4a) is representative of a rapid rise and then collapse in ITA effectiveness associated with an unsuccessful ITA program implementation. In this mode, risk increases rapidly, resulting in frequent hazardous events (serious incidents) and accidents (behavior mode #2 in Figure 5).

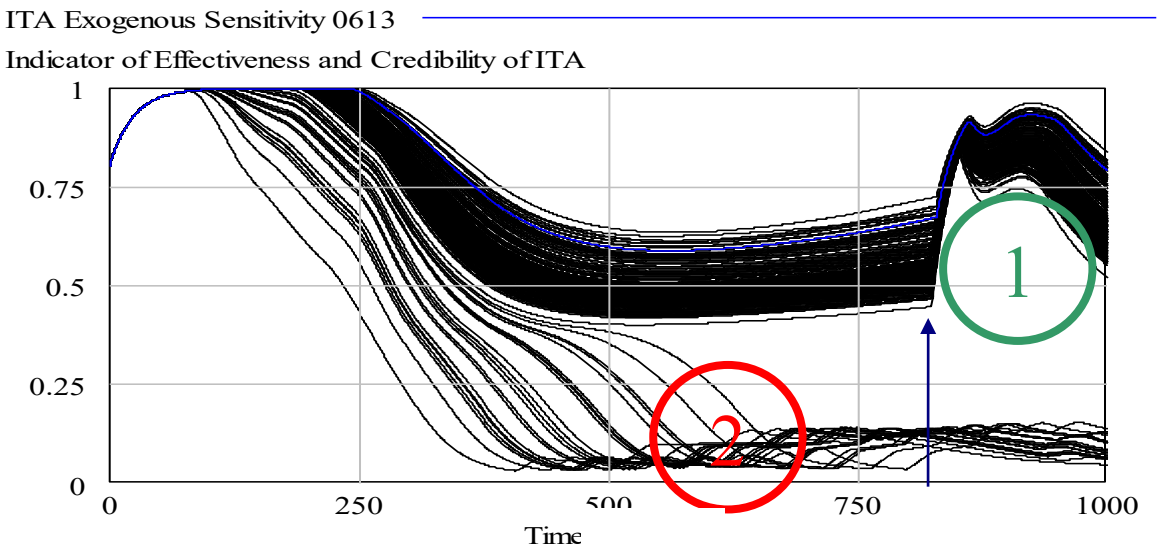


Figure 4a: ITA Sensitivity Analysis Trace Results

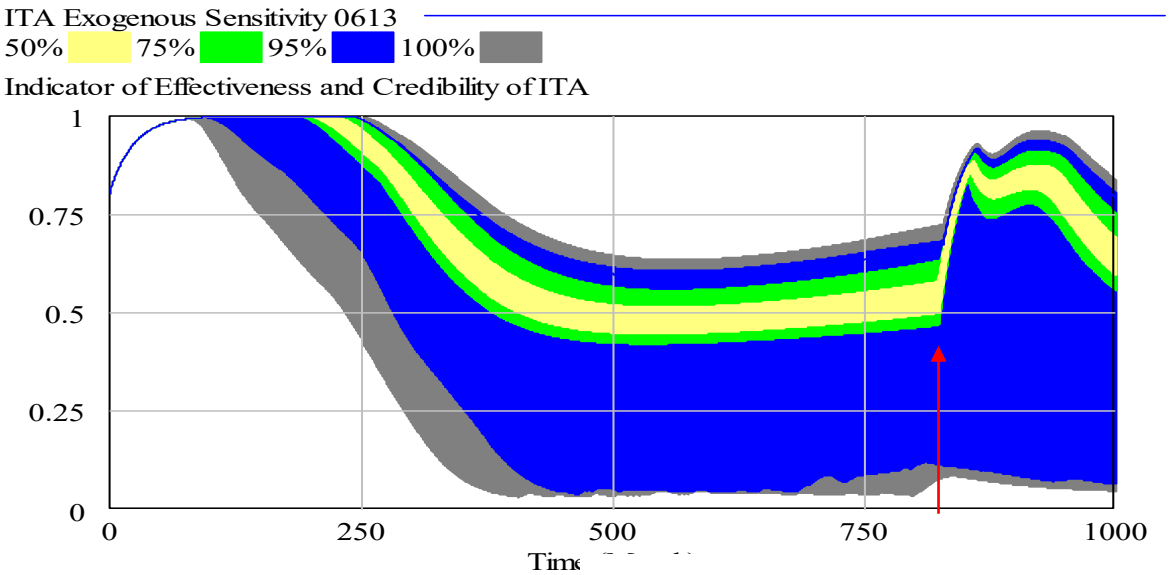


Figure 4b: ITA Sensitivity Analysis Density Results

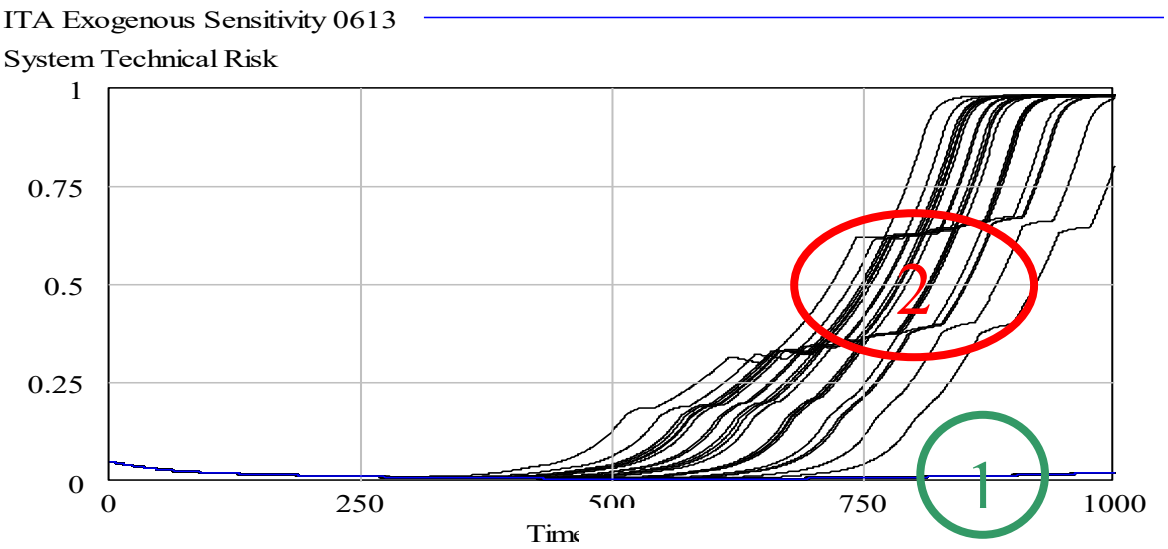


Figure 5: ITA Sensitivity Analysis Trace Results for System Technical Risk

2.6.4 System Behavior Mode Analyses

Because the results of the initial ITA sensitivity analysis showed two qualitatively different behavior modes, we performed detailed analysis of each to better understand the parameters involved. Using this information, we were able to identify some potential metrics and indicators of increasing risk as well as possible risk mitigation strategies. The ITA support structure is self-sustaining in both behavior modes for a short period of time if the conditions are in place for its early acceptance. This short-term reinforcing loop provides the foundation for a solid, sustainable ITA program implementation. The conditions under which this initial success continues or fails is important in identifying early warning metrics.

Behavior Mode #1: Successful ITA Implementation: Behavior mode 1, successful ITA program implementation, includes a short-term initial transient where all runs quickly reach the maximum *Effectiveness and Credibility of ITA*. This behavior is representative of the 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 ITA slowly starts to decline. This decline is mainly due to the effects of complacency: the quality of 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. The decrease in *Effectiveness and Credibility of ITA* is not due to intrinsic ITA program problems, but rather to a decrease in the quality of safety analysis upon which the TA and TWHs rely.

In this behavior mode, the Effectiveness and Credibility of ITA declines, then stabilizes and follows the *Quality of Safety Analyses* coming from the *System Safety Efforts and Efficacy* model. A discontinuity occurs around month 850 (denoted by the arrow on the *x*-axis of Figure 6), when a serious incident or accident shocks the system despite sustained efforts by the TA and TWHs. At this point of the system lifecycle, time-related parameters such as vehicle and infrastructure aging and deterioration create problems that are difficult to eliminate.

Figure 6 shows normalized key variables of a sample simulation representative of behavior mode #1, where the ITA program implementation is successful in providing effective risk management throughout the system lifecycle. As previously mentioned, although the *Effectiveness and Credibility of ITA* starts to decline after a while, due to eroding *System Safety Efforts and Efficacy*, ITA remains effective at mitigating risk and is able to avoid accidents for a long period of time. This behavior mode is characterized by an extended period of nearly steady-state equilibrium where risk remains at very low levels.

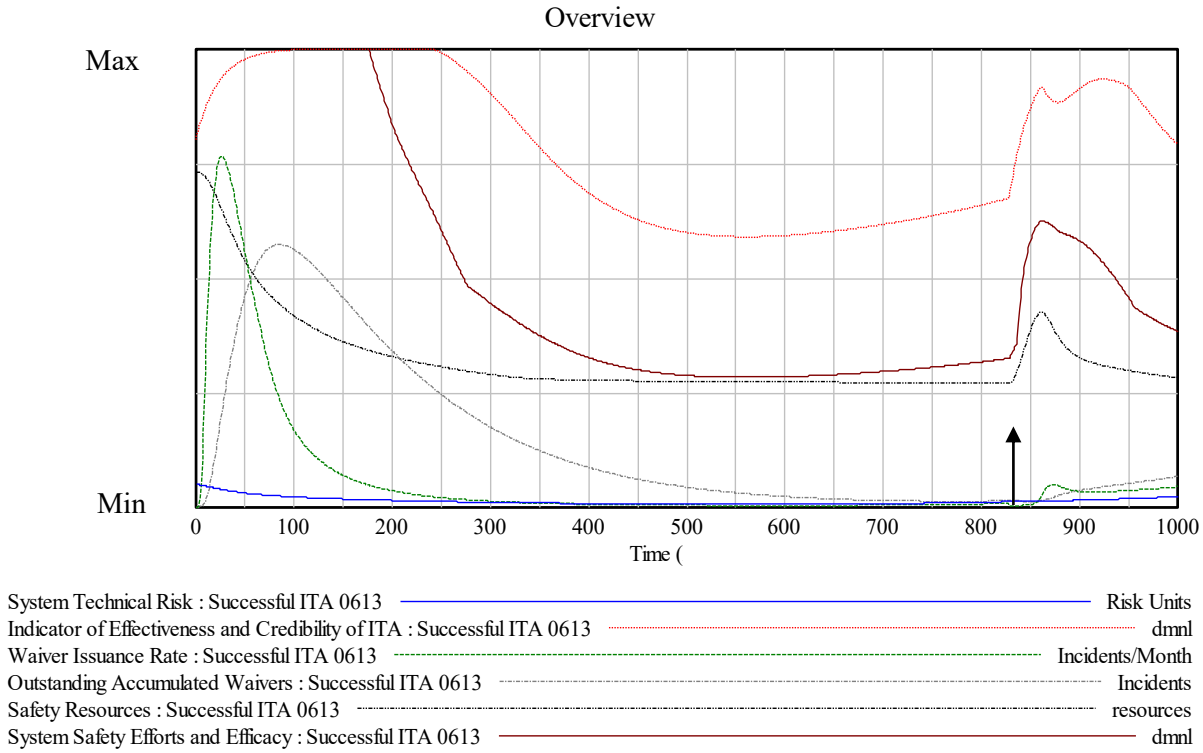


Figure 6: Behavior Mode #1 Representing a Successful ITA Program Implementation

Accidents in the model are defined as losses while incidents (hazardous events) are close calls that have a profound impact on the system, possibly requiring a pause in the launch schedule to correct the situation. In the current version of the model, the occurrence of serious incidents and accidents is deterministic. At every point in time, a value is computed to determine the *Number of Launches between Accidents*. Accidents are triggered when the number of *Consecutive Launches without Accidents* becomes equal to the *Number of Launches between Accidents* (the Accident Interval) using an accumulated probability approach. The assumption behind this computation is that for every launch, the probability of a hazardous event or incident is related to the System Technical Risk. The *Number of Launches between Accidents* is assumed to be the number of launches necessary for the accumulated probability of a hazardous event to reach 95%. At every time step, a hazardous event or accident will be triggered when the *Number of Consecutive Successful Launches* reaches the *Number of Launches between Accidents* (see Figure 7). The approach is conservative in the majority of cases, that is, it will trigger hazardous events and accidents more often when risk is increasing rapidly (when the accident interval decreases rapidly). Using a moving average of the accident interval could reduce the sensitivity to rapid changes in risk.

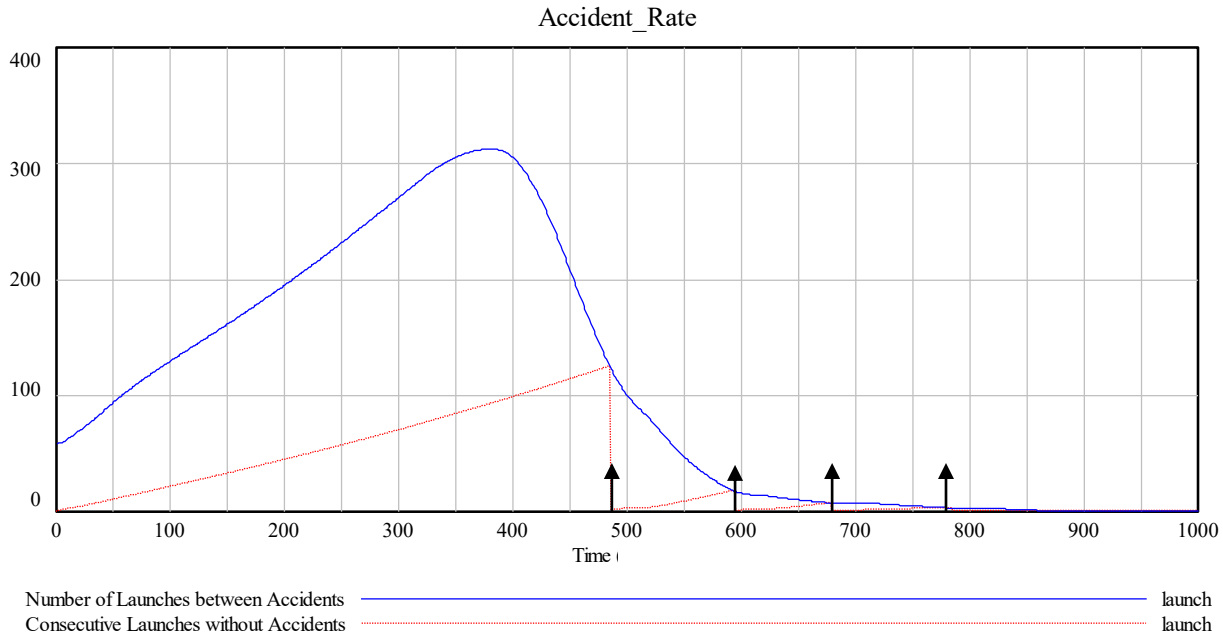


Figure 7: Approach Used for Accident Generation

Behavior Mode #2: Unsuccessful ITA Implementation: In the second behavior mode (behavior mode #2 in Figure 4a), *Effectiveness and Credibility of ITA* increases in the initial transient, then quickly starts to decline and eventually reaches bottom. This behavior mode represents cases where a combination of parameters (insufficient resources, support, staff…) creates conditions where the ITA structure is unable to have a sustained effect on the system. As ITA decline reaches a tipping point, the reinforcing loops mentioned previously act in the negative direction (they have a <1 loop gain) and the system migrates toward a high-risk state where accidents and serious incidents occur frequently (at the arrows on the *x*-axis in Figure 8).

The key normalized variables for a sample simulation run representative of the second behavior mode are shown in Figure 8. These variables are: System Technical Risk, Indicator of Effectiveness and Credibility of ITA, Waiver Issuance Rate, Outstanding Accumulated Waivers, Safety Resources, and System Safety Efforts and Efficacy. This behavior mode represents an unsuccessful implementation of the ITA program. 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, which increases *System Safety Efforts and Efficacy,* but, at this point, the TA and TWHs have lost so much credibility that they are not able to significantly contribute to risk mitigation anymore. As a result, risk increases dramatically, 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. This behavior mode includes many discontinuities created by the frequent hazardous events and accidents and provides much useful information for selection of metrics to measure the effectiveness of ITA and to provide early indication of the system migrating toward a state of increased risk.

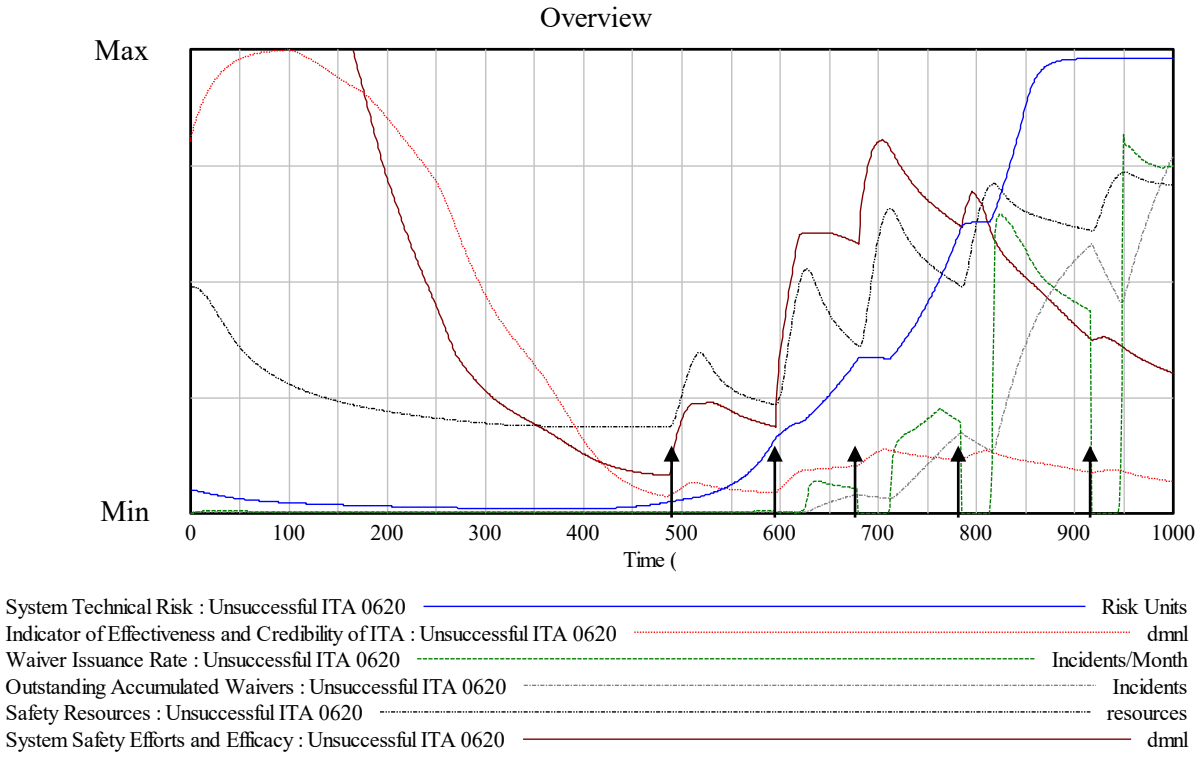


Figure 8: Behavior Mode #2 Representing an Unsuccessful ITA Program Implementation

2.6.5 Metrics Evaluations

Our models indicate that many very good indicators of increasing risk are available. However, many of these indicators become useful only after a significant risk increase has occurred, i.e., they are lagging rather than leading indicators. The requirements waiver accumulation pattern, for example, is a good indicator, but only becomes significant when risk starts to rapidly increase (Figure 9), thus casting doubt on its usefulness as an effective early warning. The use of waiver accumulation patterns as a measure of effectiveness should not be entirely discounted, however, because it is possible that the model formulation overestimates the difficulty of controlling the waiver issuance process. The model formulation assumes that waivers are only issued at the very end of an extensive problem-resolution process that includes thorough investigation of incidents and problems. Another assumption is that waivers are only issued for problems that are deemed non-safety-of-flight-related and when current resource and schedule pressures prevent their resolution. If these assumptions were relaxed, waiver accumulation would most likely start earlier in the system lifecycle.

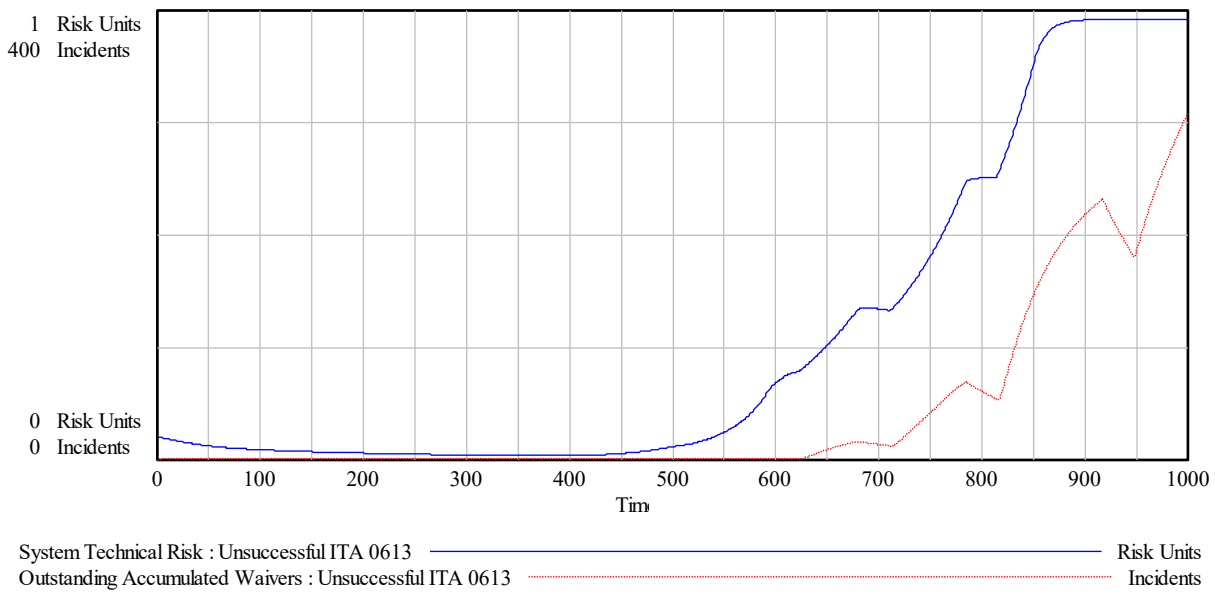


Figure 9: Waiver Accumulation Pattern for Behavior Mode #2

Alternatively, the number of incidents/problems under ITA investigation appears to be a more responsive measure of the system heading toward a state of higher risk (see Figure 10). A large number of incidents under investigation results in a high workload for trusted agents, who are already busy working on project-related tasks. Initially, the dynamics are balancing (See Figure 11), as ITA personnel are able to increase their incident investigation rate to accommodate the increased investigation requirements. As the investigation requirements become higher, corners may be cut to compensate, resulting in lower quality investigation resolutions and less effective corrective actions. If investigation requirements continue to increase, the TWHs and trusted agents become saturated and simply cannot attend to each investigation in a timely manner. A bottleneck effect is created that makes things worse through a fast acting, negative-polarity reinforcing loop (see Figure 11). This potential bottleneck points to the utility of more distributed technical decision-making (discussed further in Section 3).

Using the number of problems being worked is not without its own limitations. For a variety of reasons, the technical warrant holders may simply not be getting information about existing problems. Independent metrics (e.g., using the PRACA database) may have increased accuracy here. It is unlikely that a single metric will provide the information required—a combination of complementary metrics are almost surely going to be required.

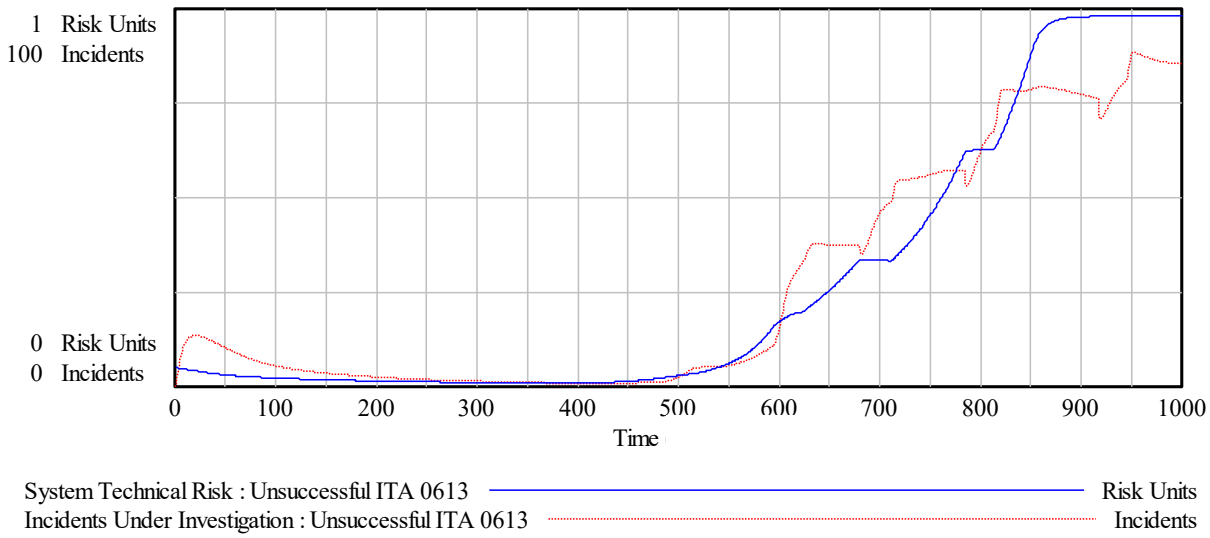


Figure 10: Incidents under Investigation—A Possible Risk Indicator

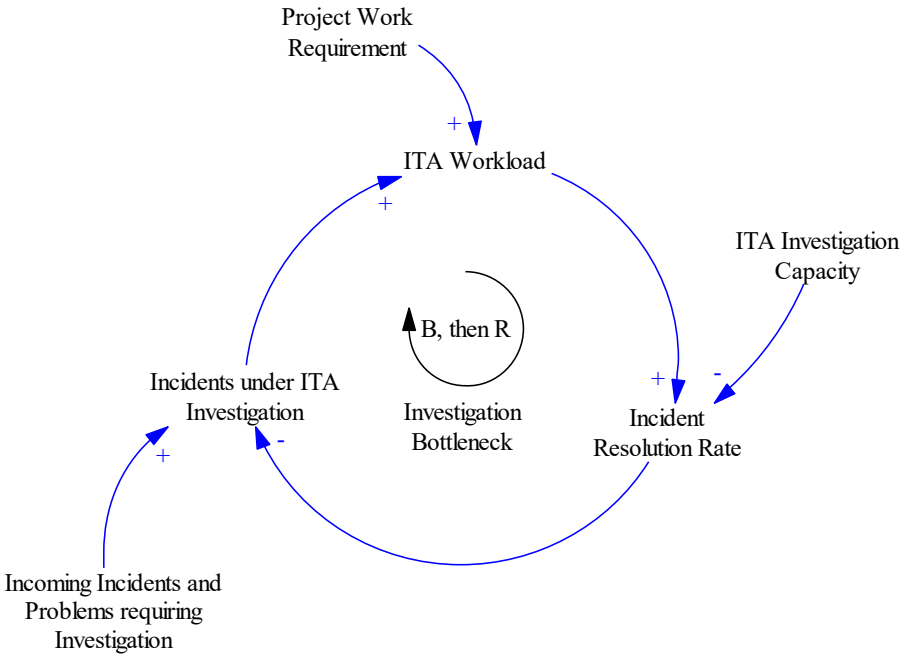


Figure 11: The Balancing Loop Becomes Reinforcing as the ITA Workload Keeps Increasing

Because of its deep structural impact on the system, the health of ITA may be the most effective early indicator of increasing risk. There is a high correlation between the *Effectiveness and Credibility of ITA* and the location of the tipping point at which risk starts to rapidly increase (see Figures 10 and 12).

However, because the *Effectiveness and Credibility of ITA* cannot be measured directly, we must seek proxy measures of ITA health.

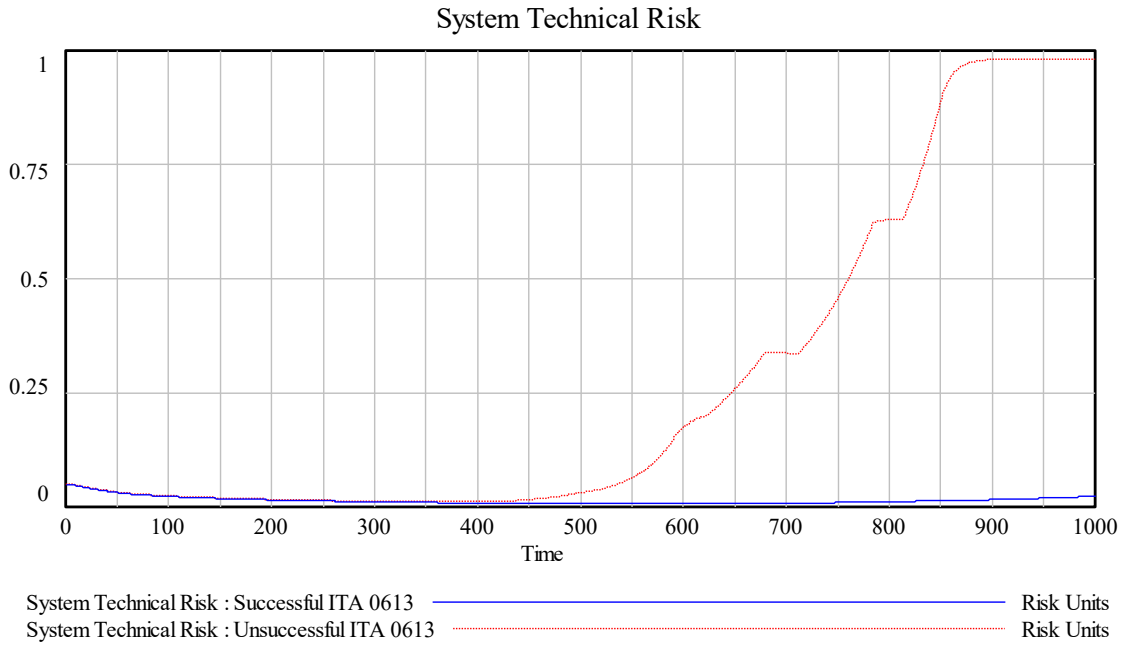


Figure 12: Relationship Between Credibility of ITA and Technical Risk

One of the most promising leading indicators of ITA health is the ability to continually recruit the "best of the best". Employees in the organization have an acute perception of which assignments are regarded as prestigious and important. As long as ITA is able to retain its influence, prestige, power and credibility, it should be able to attract the best, highly experienced technical personnel with leadership qualities. By monitoring the quality of ITA personnel (Technical Warrant Holders and Trusted Agents) over time using meaningful metrics, it should be possible to have a good indication of ITA health and to correct the situation before risk starts to increase rapidly.

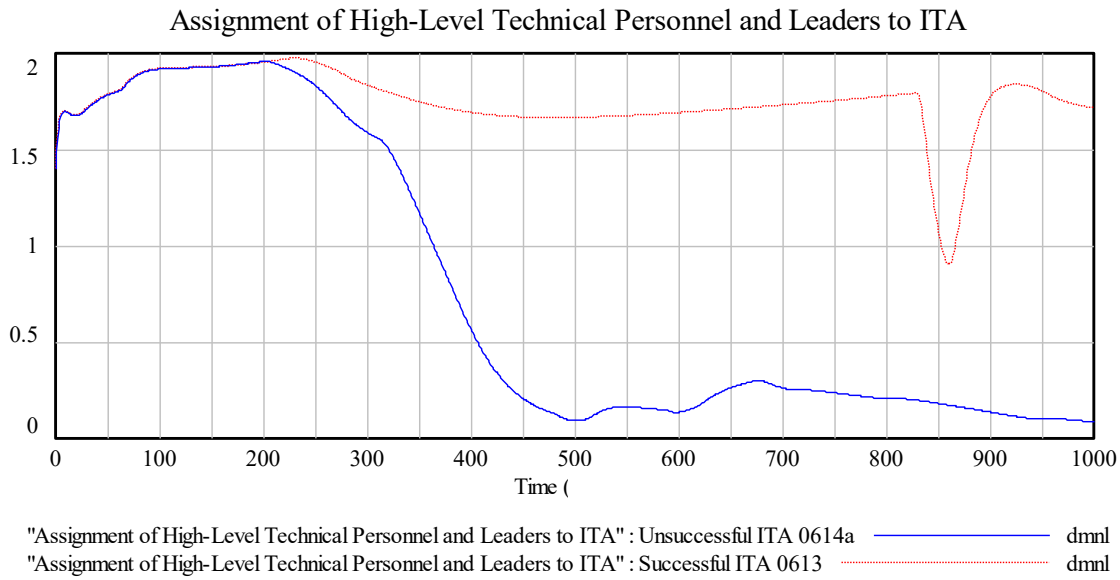


Figure 13: Impact of Credibility of Participants on Success of ITA

2.6.6 Additional Scenario Analysis and Insights

In addition to the ITA-centered analysis, scenarios were used to assess the impact of various parameters on the overall behavior of the system. One scenario evaluated the effect of contracting on system technical risk and on the ability of ITA to remain credible and effective. In order to evaluate this effect, a simulation was performed where the fraction of work contracted out was varied linearly from 4% to 96%. The results show that increased contracting does not significantly change the level of risk until a "tipping point" is reached where NASA is not able to perform the integration and safety oversight that is their responsibility. After that point, risk escalates substantially (see Figure 14).

Higher levels of contracting also affect the *Credibility and Effectiveness of the ITA* (see Figure 15). Initially, the effect is seen by the shortage of high-level technical leaders with safety knowledge that can be assigned ITA (see Figure 16). As the shortage becomes acute and the TA is unable to find high-quality people to fill ITA positions, credibility and effectiveness start to suffer, and the gain of the reinforcing loops at the core of the ITA model becomes smaller than 1, resulting in a rapid deterioration of the situation with negative ripple effects all across the system. As the situation deteriorates, the TA may have some difficulties in recruiting high-quality experienced employees, while contractors will have a relative abundance of high-level experienced employees whose safety knowledge and skills could prove very useful. However, without a strong in-house structure to coordinate and integrate the efforts of both NASA and contractor safety activities, effective risk mitigation may be compromised.

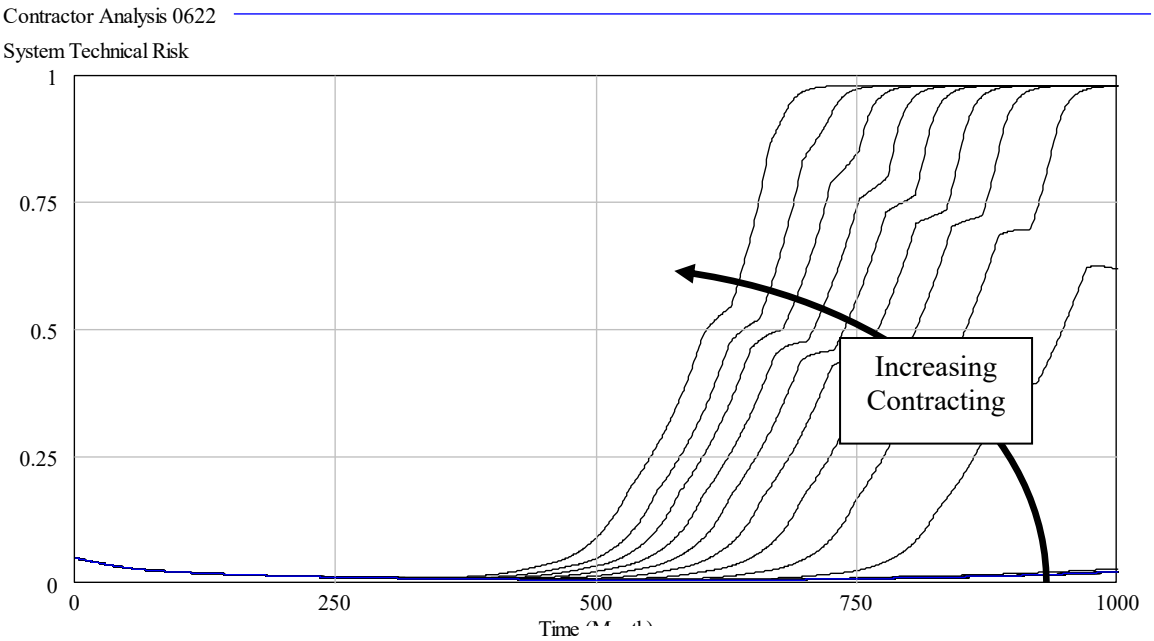


Figure 14: System Risk as a Function of Increased Contracting

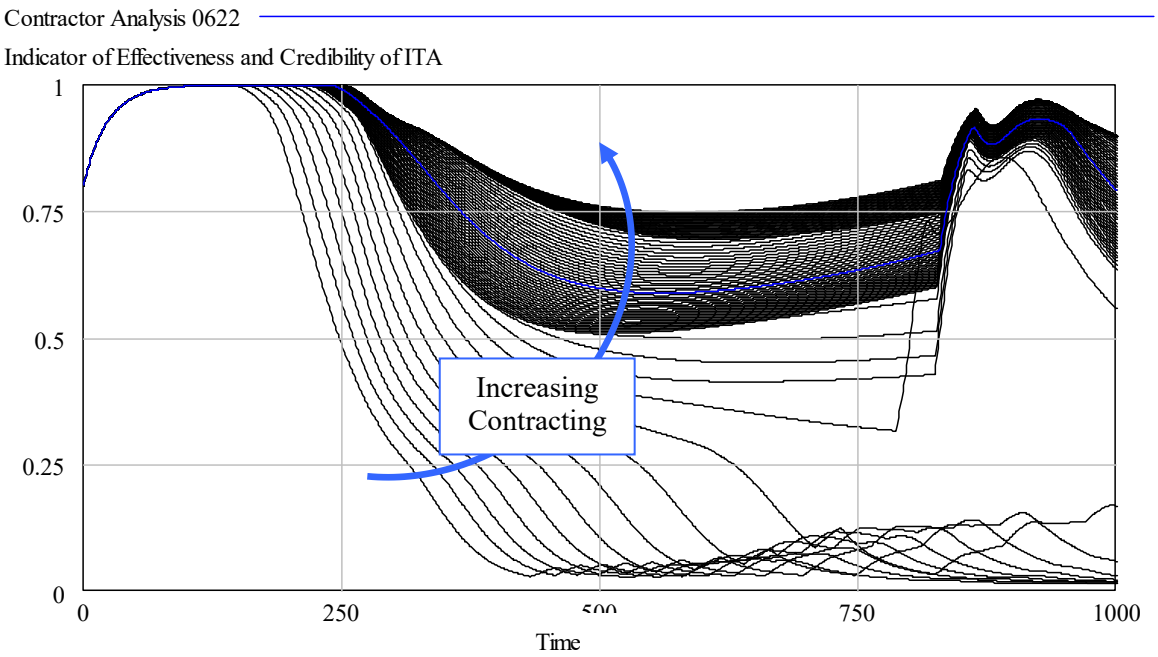


Figure 15: ITA Effectiveness and Credibility as a Function of Increased Contracting

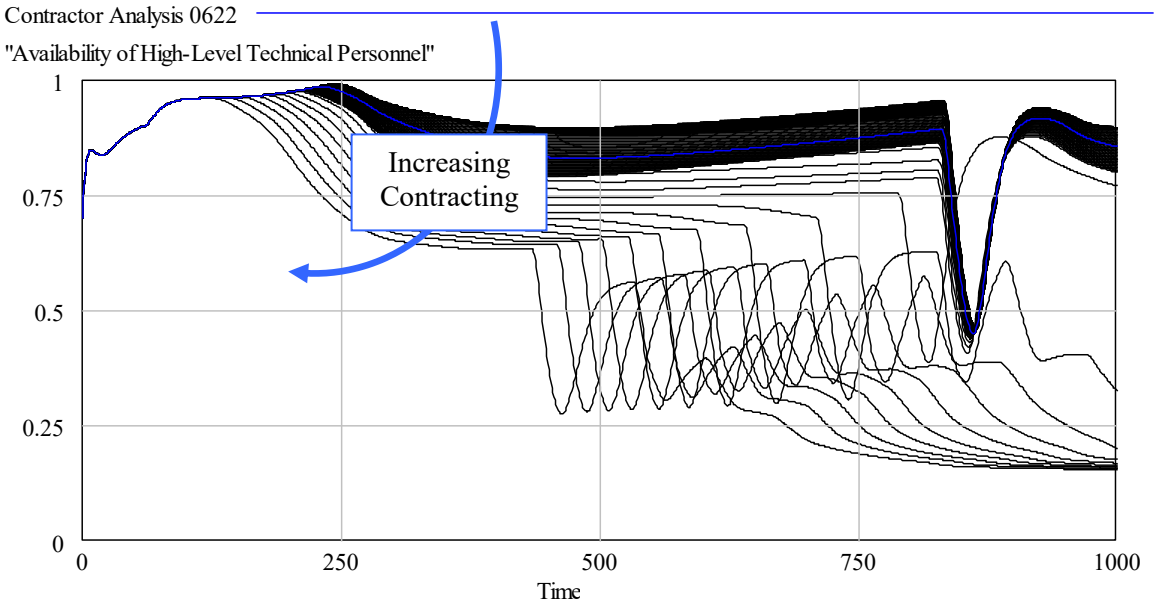


Figure 16: Availability of High-Level Technical Personnel as a Function of Increased Contracting

Additional insights and concerns supported by the modeling involve the role of the Trusted Agents. The Technical Warrant Holders are shielded in the design of ITA from programmatic budget and schedule pressures through independent management chains and budget sources. However, Trusted Agents are not shielded from these pressures because they have dual responsibility for working both on the project and TWH assignments. An increase in Trusted Agent workload due to project and/or TWH assignments or to other programmatic pressures may reduce their sensitivity to safety problems. Having the safety analyses and other components of ITA produced by sources not under the ITA program umbrella reduces the supposed independence of ITA. The results of analyses and information provided by non-ITA components are the foundation for TA and TWH safety-related decision-making. Inadequate safety analyses and information can seriously undermine the ability of ITA to provide effective risk mitigation. The acceptance and support of the entire workforce is therefore critical. We discuss possible strategies related to this requirement in Section 3.

2.7 Leading Indicators and Measures of Effectiveness

The system dynamics modeling and analysis indicate that five general categories of leading indicators and measures of effectiveness will be the most effective in assessing ITA implementation and detecting when risk is rising.

Knowledge, Skills, and Quality of TWHs and Trusted Agents: TWHs and trusted agents must have the knowledge and skills necessary to understand, appreciate, and question the safety analyses performed. In addition to having enough time and resources to actively participate in ITA-led investigations and activities, they must also have the knowledge and skills necessary to identify safety problems and provide an independent technical assessment of the problem resolution process. Because of the large scope of responsibility of each TWH, this factor can only be achieved if both TWHs and Trusted Agents are selected among the most experienced, respected and technically knowledgeable employees. The system

dynamics model analysis shows this is very likely to be the case at first, so it may not be an immediate concern. However, depending on the perceived success and prestige of the ITA process over time, it may be more difficult to recruit ITA representatives from the top engineers. Analysis shows that the ability to attract the very best may be one of the most important early indicators of reduced ITA health and of risk increase. Important measures of this property include:

- *Average Experience of TWHs and Trusted Agents*
- *Technical Knowledge of TWHs and Trusted Agents*
- *System Safety Knowledge of TWHs and Trusted Agents*
- *Communication Skills of TWHs and Trusted Agents*
- *Reputation of TWHs and Trusted Agents*
- *Social Network of TWHs and Trusted Agents within the NASA and contractor community*
- *Difficulty in recruiting replacements for TWHs and Trusted Agents*
- *Amount of training provided to TWHs and Trusted Agents*

ITA-Directed Investigation Activity:
Number of Incidents under ITA-directed investigation: Monitoring the number of incidents under ITA-directed investigations is an effective way to detect trends toward increasing risk. A potential problem with this indicator is that it depends on whether problems and anomalies are reported to the TWHs and therefore may be misleading. A low number of problems under investigation may indicate that risk mitigation activities are very effective or, alternatively, that problems are not being reported or acted upon by ITA. Therefore the metric alone is not enough to detect increasing risk but needs to be combined with other metrics.

- *Fraction of Problem Reports under ITA-Directed Investigation***:** In order to ensure that TWHs are aware of safety-related problems that may be worthy of further investigation, the number of problem reports filed by line engineers (perhaps from PRACA or similar databases) needs to be compared with the number of investigations performed under ITA funding. If the number of ITA-directed investigations decreases significantly faster than the number of problem reports filed, it may indicate that either the independent technical assessment process is becoming complacent, is overloaded, or is being bypassed by line engineering.
- *Number of Unresolved or Unhandled Problems:* The complement to the first two metrics is the number of problems reported that were left unresolved or unhandled. A large number of reported problems that are not acted upon indicate that the technical safety process defined by ITA and TWHs is ineffective and may result in rapid risk increases. Moreover, a large number of unresolved or unhandled problems undermines the reputation and credibility of the ITA and discourages employees from reporting problems and raising concerns.

Quality of Safety Analyses: Model analysis shows that the effectiveness of TWHs and trusted agents is highly dependent upon the quality of safety analyses. TWHs and trusted agents rely on this information to make informed safety-related decisions. Occasional independent audits can assess this quality. Other metrics are:

- *Knowledge and Skills of System Safety Staff*: The experience, knowledge and skills of the system safety staff can provide a good indication into the quality of safety analyses performed. This factor can be measured through the average experience, system safety knowledge, and training of the system safety staff.
- *Resources for Safety Analyses*: The resources available for safety analyses also determine the quality of the end product upon which ITA and TWH decision-making relies. Model analysis show that these resources can be relatively easily diverted, especially when the program is perceived to be successful and when resource and schedule pressures are intense.

- *Availability of Lessons Learned:* The availability of an easily accessible and comprehensive repository of lessons learned can also enhance the quality of safety analyses by allowing analysts to benefit from previous experience.

Quality of Incident Investigation: Another method of monitoring the effectiveness of the independent technical assessment process is to measure the quality of ITA-led investigations. It is not possible to measure investigation quality of safety-related problems directly, but various intermediate metrics can be used to build a reasonably accurate assessment.

- *Involvement of TWHs and Trusted Agents*: The amount of time spent by TWHs and Trusted agents on each investigation, as well as the number of System and Discipline Trusted Agents involved can provide a good indication of the amount of effort being applied
- *Trusted Agent Investigation Resources and Workload*: Ensuring that Trusted Agent positions are filled with highly qualified technical leaders and providing them with enough resources and time to oversee and participate in each investigation into safety-related problems will ensure the independent technical assessment and problem resolution process results in effective risk mitigation actions with a lasting effect on the system. Measuring the workload of TWHs and Trusted agents can provide a first order assessment of the adequacy of resources available for ITA-directed investigations and activities.
- *Trusted Agent Independence and Work Balance*: In addition to monitoring the quality of ITA-led investigations, it is necessary to provide a balance between work done by Trusted Agents on program-related activities versus ITA-related activities. The rationale is that Trusted Agents have shared loyalties, and they may be put in a situation where program-related tasks, which are not shielded against budget and schedule pressure, will inadvertently affect their duties as ITA trusted agents. This situation is most likely to happen if Trusted Agents spend a considerably smaller amount of time on ITA-related activities, particularly if this number decreases over time. The balance and fairness of trusted agents performance, the amount of involvement in ITA-led investigations, the amount and effectiveness of communication and team-building meetings and activities within the TA-TWH-Trusted Agent community are metrics that can be used to ensure that trusted agents will have the independence necessary to make quality assessments of safety-related problems.
- *Systemic Factor Fixes vs. Symptom Removal:* The problem resolution process can address systems factors and thus have a significant and lasting impact on risk mitigation or to band-aid solutions that allow the system to continue operating but without much effect on risk. Independent audits can assess how well systemic factors are being identified and addressed.

Power and Authority of TA and TWHs: Many characteristics are required to obtain a strong independent technical assessment process. Recruiting the best and ensuring that they have the resources and time necessary to perform their function is fundamental. However, the best independent technical assessments will not be useful if TWHs do not have the effective power and authority required to have an affect on critical safety-related decision-making. Consequently, it is also necessary to monitor the effective power and authority of ITA representatives.

- *Number of Safety Issues raised to the ITA/Program level*: Tracking the number of safety issues raised to the Chief Engineer and Program Manager level is a first order indicator of the TWHs exercising the authority delegated to them by the ITA.
- *Fraction of rulings/decisions in favor of TWHs*: The fraction of decisions or rulings in favor of TWHs' recommendations is a good indicator of the power, authority, and credibility of ITA.
- *Number of Launches delayed by the ITA*: Another, more extreme, method of monitoring ITA power and authority is to track the number of launches delayed by the ITA because of safety reasons. While everything should be put in place to ensure ITA-related activities and investigations are performed in a timely manner and do not overly affect launch schedules, there

will be situations where TWHs will have to recommend launch delays. This situation should occur periodically. If it never happens, then the effective authority of the ITA should be carefully examined. Model analysis does not show very large variations in the fraction of launches delayed because of safety reasons as a function of the ITA effectiveness. This is because the formulation for the number of launches delayed combines three necessary conditions for having a large number of delays: (1) Risk must be high, (2) The independent technical assessment process must be effective, and (3) The ITA must have high power and authority. In most situations, when conditions 2 and 3 are fulfilled, condition 1 is not, and vice-versa. While the analysis shows that a highly effective ITA process consistently results in more launch delays, the model variables are too aggregate to predict significant differences. A more careful investigation of the reasons and context of launch delays is required to assess the effective level of power and authority of the ITA.

3 FINDINGS AND RECOMMENDATIONS

The application of new formal modeling and analysis techniques to the NASA manned space program organizational safety control structure allowed us to rigorously identify a large number of risks and vulnerabilities of the new ITA program. We then analyzed many of these risks using our system dynamics models. This section presents the key findings from our analysis and the recommended metrics and measures of effectiveness for the assessment of ITA and for use in a continual risk management program to detect when technical risk is increasing to unacceptable levels.

Our findings and recommendations fall into the areas of monitoring ITA implementation and level of technical risk, initial buy-in, broadening participation, strengthening the role of trusted agents, enhancing communication, clarifying responsibilities, providing training, instituting assessment and continual improvement, expanding technical conscience channels and feedback, and controlling risk in a contracting environment.

Monitoring ITA Implementation and Level of Technical Risk

Finding 1a: It is a testament to the careful design and hard work that has gone into the ITA program implementation that we were able to create the ITA static control structure model so easily and found so few gaps in the mapping between system requirements and assigned responsibilities. We congratulate NASA on the excellent planning and implementation that has been done under severe time and resource constraints.

Finding 1b: Our modeling and analysis found that ITA has the potential to very significantly reduce risk and to sustain an acceptable risk level, countering some of the natural tendency for risk to increase over time due to complacency generated by success, aging vehicles and infrastructures, etc. However, we also found significant risk of unsuccessful implementation of ITA that should be monitored.

The initial sensitivity analysis identified two qualitatively different behavior modes: 75% of the simulation runs showed a successful ITA program implementation where risk is adequately mitigated for a relatively long period of time; the other runs identified a behavior mode with an initial rapid rise in effectiveness and then a collapse into an unsuccessful ITA program implementation where risk increases rapidly and accidents occur.

The ITA support structure is self-sustaining in both behavior modes for a short period of time if the conditions are in place for its early acceptance. This early behavior is representative of an initial excitement phase where ITA is implemented and shows great promise to reduce the level of risk of the system. This short-term reinforcing loop provides the foundation for a solid, sustainable ITA program implementation under the right conditions.

Even in the successful scenarios, after a period of very high success, the effectiveness and credibility of the ITA slowly starts to decline, mainly due to the effects of complacency where the safety efforts start 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. However, in the successful implementations, risk is still at acceptable levels, and an extended period of nearly steady-state equilibrium ensues where risk remains at low levels.

In the unsuccessful ITA implementation scenarios, effectiveness and credibility of the ITA quickly starts to decline after the initial increase and eventually reaches unacceptable levels. Conditions arise that limit the ability of ITA to have a sustained effect on the system. Hazardous events start to occur and safety is increasingly perceived as an urgent problem. More resources are allocated to safety efforts, but at this point the TA and TWHs have lost so much credibility they are no longer able to significantly contribute to risk mitigation anymore. As a result, risk increases dramatically, the ITA personnel and safety staff become overwhelmed with safety problems and they start to approve an increasing number of waivers in order to continue flying.

As the number of problems identified increases along with their investigation requirements, corners may be cut to compensate, resulting in lower-quality investigation resolutions and corrective actions. If investigation requirements continue to increase, TWHs and trusted agents become saturated and simply cannot attend to each investigation in a timely manner. A bottleneck effect is created by requiring the TWHs to authorize all safety-related decisions, making things worse. Examining the factors in these unsuccessful scenarios can assist in making changes to the program to prevent them and, if that is not possible or desirable, to identify leading indicator metrics to detect rising risk while effective interventions are still possible and not overly costly in terms of resources and downtime.

***Finding 1c*:** Results from the metrics analysis using our system dynamics model show that many model variables may provide good indications of system risk. However, many of these indicators will only show an increase in risk *after* it has happened, limiting their role in preventing accidents. For example, the number of waivers issued over time is a good indicator of increasing risk, but its effectiveness is limited by the fact that waivers start to accumulate after risk has started to increase rapidly. Other lagging indicators include the amount of resources available for safety activities; the schedule pressure, which will only be reduced when managers believe the system to be unsafe; and the perception of the risk level by management, which is primarily affected by events such as accidents and close-calls.

Finding leading indicators that can be used to monitor the system and detect risk increases early is extremely important because of the dynamics associated with the non-linear tipping point associated with technical risk level. At this tipping point, risk increases slowly at first and then very rapidly (i.e., the reinforcing loop has a gain < 1). The system can be prevented from reaching this point, but once it is reached, multiple serious problems occur rapidly and overwhelm the problem-solving capacity of ITA. When the system reaches that state, risk starts to increase rapidly, and a great deal of effort and resources will be necessary to bring the risk down to acceptable levels.

Recommendation 1: To detect increasing and unacceptable risk levels early, the following five leading indicators (identified by our system dynamics modeling and analysis) should be tracked: (1) knowledge, skills, and quality of the TWHs and Trusted Agents; (2) ITA-directed investigation activity; (3) quality of the safety analyses; (4) quality of incident (hazardous event and anomaly) investigation; and (5) power and authority of the TA and TWHs. Specific metrics and measures of effectiveness for these leading indicators are described in Section 2.7.

Initial Buy-in

***Finding 2*:** The success of ITA is clearly dependent on the cooperation of the entire workforce, including project management, in providing information and accepting the authority and responsibility of the TA and TWHs. The implementers of ITA have recognized this necessity and instituted measures to enhance initial buy-in. Several of our identified leading indicators and measures of effectiveness can help to assess the success of these efforts.

Recommendation 2: Initial buy-in and acceptance of ITA should be closely monitored early in the program.

Broadening Participation

Finding 3: One of the important identified risks was a potential lack of broad participation of the workforce. Mechanisms are needed to allow and encourage all employees to contribute to safety-related decision-making. In particular, lack of direct engagement of line engineering in ITA (both within NASA and within the contractor organizations) may be a problem over the long run. Line engineers may feel

disenfranchised, resulting in their either abdicating responsibility for safety to the warrant holders or, at the other extreme, simply bypassing the warrant holders.

Another reason for broad participation is that ITA is a potential bottleneck in accomplishing NASA's exploration goals and this problem will worsen when risk starts to increase and problems accumulate. It is important to avoid this negative reinforcing loop. Mechanisms must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making and to assume some responsibility, authority, and accountability for safety. The goal should be to prevent degradation of decision-making due to non-safety pressures but to make each person assume some responsibility and participate in the safety efforts in some way.

At the same time, NASA needs to avoid the trap existing both before Challenger and Columbia where performance pressures led to a diminution of the safety efforts. A simplified model of the dynamics involved is shown in Figure C.3 in Appendix C. One way to avoid those dynamics is to "anchor" the safety efforts through external means, i.e., Agency-wide standards and review processes that cannot be watered down by program/project managers when performance pressures build.

The CAIB report recommends establishing Independent Technical Authority, but there needs to be more than one type and level of independent authority in an organization: (1) independent technical authority *within* the program but independent from the Program Manager and his/her concerns with budget and schedule and (2) independent technical authority *outside* the programs to provide organization-wide oversight and maintenance of standards.

There are safety review panels and procedures within NASA programs, including the Shuttle program. Under various pressures, including budget and schedule constraints, however, the independent safety reviews and communication channels within the Shuttle program (such as the SSRP) degraded over time and were taken over by the Shuttle Program office and standards were weakened. At the same time, there was no effective external authority to prevent this drift toward high risk. ITA was designed to provide these external controls and oversight, but it should augment and not substitute for technical authority within line engineering.

Recommendation 3: Given the dysfunctional nature of the NASA safety control structure at the time of the Columbia accident and earlier, the current design of ITA is a necessary step toward the ultimate goal. We recommend, however, that a plan be developed for evolution of the safety control structure as experience and expertise grows to a design with distributed responsibility for safety-related decision-making, both internal and external to programs/projects. There will still be a need for external controls to ensure that the same dynamics existing before Challenger and Columbia do not repeat themselves. To achieve its ambitious goals for space exploration, NASA will need to evolve the organizational structure of the manned space program from one focused on operations to one focused on development and return to many of the organizational and cultural features that worked so well for Apollo. The appropriate evolutionary paths in ITA should be linked to these changes.

Independence of Trusted Agents

Finding 4: The results of safety analyses and information provided by non-ITA system components are the foundation for all TA and TWH safety-related decision-making. If the Trusted Agents do not play their role effectively, both in passing information to the TWHs and in performing important safety functions, the system falls apart. While TWHs are shielded in the design of the ITA from programmatic budget and schedule pressures through independent management chains and budgets, Trusted Agents are not. They have dual responsibility for working both on the project and on TWH assignments, which can lead to obvious conflicts. Good information is key to good decision-making. Having that information produced by employees not under the ITA umbrella reduces the independence of ITA. In addition to conflicts of interest, increases in Trusted Agent workload due either to project and/or TWH assignments or other programmatic pressures can reduce their sensitivity to safety problems.

The TWHs are formally assigned responsibility, accountability, and authority through their warrants, and they are reminded of the role they play and their responsibilities by weekly telecons and periodic workshops, but there appears to be no similar formal structure for Trusted Agents to more completely engage them in their role. The closest position to the Trusted Agent in other government agencies, outside of the Navy, is the FAA DER (Designated Engineering Representative). Because type certification of an aircraft would be an impossible task for FAA employees alone, DERs are used to perform the type certification functions for the FAA.

Recommendation 4a: Consider establishing a more formal role for Trusted Agents and ways to enhance their responsibility and sense of loyalty to ITA. Examine the way the same goals are accomplished by other agencies, such as the FAA DER, to provide guidance in designing the NASA approach. The Trusted Agent concept may be the foundation on which an internal technical authority is established in the future.

Recommendation 4b: The term "Trusted Agent" has some unfortunate connotations in that it implies that others are untrustworthy. The use of another term such as warrant representatives or warrant designees should be considered.

Enhancing Communication and Coordination

Finding 5: As noted, the entire structure depends on communication of information upward to ITA decision-makers. Monitoring the communication channels to assess their effectiveness will be important. We have developed and experimentally used tools for social interaction analysis that assist with this type of monitoring. For projects with extensive outside contracting, the potential communication gaps are especially critical and difficult to maneuver given contractor concerns about proprietary information and designs. The proprietary information issues will need to be sorted out at the contractual level, but the necessary safety oversight by NASA requires in-depth NASA reviews and access to design information. The FAA DER concept, which is essentially the use of Trusted Agents at contractors, is one potential solution. But implementing such a concept effectively takes a great deal of effort and careful program design.

Beyond the contractor issues, communication channels can be blocked or dysfunctional at any point in the chain of feedback and information passing around the safety control structure. In large military programs, system safety working groups or committees have proved to be extremely effective in coordinating safety efforts.[15] The concept is similar to NASA's use of boards and panels at various organizational levels, with a few important differences—safety working groups operate more informally and with fewer constraints.

Recommendation 5a: Establish channels and contractual procedures to ensure that TWHs can obtain the information they need from contractors. Consider implementing some form of the "safety working group" concept, adapted to the unique NASA needs and culture.

Recommendation 5b: Monitor communication flow and the information being passed to ITA via Trusted Agents and contractors. Identify misalignments and gaps in the process using tools for interaction analysis on organizational networks.

[15] Nancy G. Leveson. *Safeware*, Addison-Wesley, 1995.

Clarifying Responsibilities

Several findings relate to the need to better clarify responsibilities. Some important responsibilities are not well defined, are not assigned to anyone, or are assigned to more than one group without specifying how the overlapping activities will be coordinated.

Finding 6a: A critical success factor for any system safety effort is good safety analyses. In fact, our system dynamics modeling found that the quality of the safety analyses and safety information provided to the decision makers was the most important factor in the effectiveness of ITA. Responsibility for system hazard analysis (which NASA sometimes calls integrated hazard analysis) and communication channels for hazard information to and among contractors and NASA line engineers are not clearly defined. While TWHs are responsible for ensuring hazard and other safety analyses are used, ambiguity exists about who will actually be performing them. Currently this responsibility lies with SMA, but that has not worked well.

Safety engineering needs to be done by engineering, not by mission assurance, whose major responsibilities should be assuring quality in everything NASA does and in compliance checking, but not actually performing the design engineering functions. When SMA is both performing engineering functions and assuring the quality of those functions, the independence of the assurance organization is compromised. At the least, if SMA is controlling the hazard analysis and auditing process, communication delays may cause the analyses (as they are often today) to be too late to impact the most important design decisions. At the worst, it may lead to disconnects that seriously threaten the quality of the system safety engineering efforts. In our experience, the most effective projects have the discipline experts for system safety engineering analyses located in the system engineering organization.

It is important to note that the types of safety analyses and the information contained in them will differ if they are being used for design or for assurance (assessment). There is no reason both need to be done by one group. An unfortunate result of the current situation is that often only assurance analyses are performed and the information needed to fully support design decisions is not produced.

System safety is historically and logically a part of system engineering. A mistake was made 17 years ago when safety engineering was moved to an assurance organization at NASA. It is time to rectify that mistake. A recent NRC report concluded that NASA's human spaceflight systems engineering capability has eroded significantly as a result of declining engineering and development work, which has been replaced by operational responsibilities.[16] This NRC report assigns system safety as a responsibility for a renewed system engineering and integration capability at NASA and concludes that strengthening the state of systems engineering is critical to the long-term success of Project Constellation.

Finding 6b: In addition to producing system hazard analyses, responsibility has to be defined for ensuring that adequate resources are applied to system safety engineering; that hazard analyses are elaborated (refined and extended) and updated as the design evolves and test experience is acquired; that hazard logs are maintained and used as operational experience is gained; and that all anomalies are evaluated for their hazard potential. Again, currently many of these responsibilities are assigned to SMA, but with this process moving to engineering—which is where it should be—clear responsibilities for these functions need to be specified.

Finding 6c: While the discipline technical warrant holders own and approve the standards, it still seems to be true that SMA is writing engineering standards. As the system safety engineering responsibilities are moving to design engineering, so should the responsibility for producing the standards that are used in hazard analyses and in engineering design. SMA should be responsible for assurance standards, not technical design and engineering process standards.

[16] Donald C. Fraser (Chair). Report of the Committee on Systems Integration for Project Constellation, National Research Council, September 21, 2004.

Finding 6d: The March ITA implementation plan says that SMA will recommend a SR&QA plan for the project. The ITA will set requirements and approve appropriate parts of the plan. This design raises the potential for serious coordination and communication problems. It might make more sense for SMA to create a plan for the safety (and reliability and mission) *assurance* parts of the plan while Engineering creates the safety *engineering* parts. If this is what is intended, then everything is fine, but it deviates from what has been done in the past. We have concerns that, as a result, there will be confusion about who is responsible for what and some functions might never be accomplished or, alternatively, conflicting decisions may be made by the two groups, resulting in unintended conflicts and side effects.

Recommendation 6: System safety responsibilities need to be untangled and cleanly divided between the engineering and assurance organizations, assigning the system safety engineering responsibilities to SE&I and other appropriate engineering organizations and the assurance activities to SMA. The SE&I responsibilities should include creating project system safety design standards such as the Human Rating Requirements, performing the system safety hazard analyses used in design, and updating and maintaining these analyses during testing and operations. SMA should create the assurance standards and perform the assurance analyses.

Training

Finding 7a: As with other parts of system engineering, as noted in the NRC report on systems integration for Project Constellation, capabilities in system safety engineering (apart from operations) have eroded in the human spaceflight program. There is widespread confusion about the difference between reliability and safety and the substitution of reliability engineering for system safety engineering.

While the discipline technical warrant holders (DTWHs) are responsible for the state of expertise in their discipline throughout the Agency (and this would include the responsibility of the System Safety DTWH for ensuring engineers are trained in performing hazard analyses), we could not find in the ITA implementation plans documentation of who will be responsible to see that engineers and managers are trained to use the results of hazard analysis in their decision-making. While most engineers at NASA know how to use bottom-up component reliability analyses such as FMEA/CIL, they are not as familiar with system hazard analyses and their use.

Training is also needed in general system safety concepts and should include study of lessons learned from past accidents and serious incidents. Lessons learned are not necessarily communicated and absorbed by putting them in a database. The Navy submarine program, for example, requires engineers to participate in a system safety training session each year. At that time, the tapes of the last moments of the crew during the Thresher loss are played and the causes and lessons to be learned from that major tragedy are reviewed. The CAIB report noted the need for such training at NASA. The use of simulation and facilitated ways of playing with models, such as our system dynamics model of the NASA Manned Space Program safety culture at the time of the Columbia accident along with models of typical safety culture problems, can provide powerful hands-on learning experiences.

Finding 7b: Our system dynamics models show that effective "root cause" analysis (perhaps better labeled as systemic or causal factors analysis) and the identification and handling of systemic factors rather than simply symptoms are important in maintaining acceptable risk.

Recommendation 7: Survey current system safety engineering knowledge in NASA line engineering organizations and plan appropriate training for engineers and managers. This training should include training in state-of-the-art system safety engineering techniques (including causal factor analysis), the use of the results from safety analyses in engineering design and management decision making, and the study of past accidents and serious incidents, perhaps using hands-on facilitated learning techniques with executable models.

Assessment and Continual Improvement

Finding 8: Although clearly assessment of how well the ITA is working is part of the plan—this risk analysis and the planned assessment are part of that process—specific organizational structures and processes for implementing a continual learning and improvement process and making adjustments to the design of the ITA itself when necessary might be a worthwhile addition to the plan. Along with incremental improvements, occasionally the whole design should be revisited and adjustments made on the basis of assessments and audits.

> ***Recommendation 8***: Establish a continual assessment process of NASA safety-related decision-making in general and ITA in particular. That process should include occasional architectural redesigns (if necessary) in additional to incremental improvement.

Technical Conscience and Feedback

Finding 9: The means for communicating and resolving issues of technical conscience are well defined, but there is no defined way to express concerns about the warrant holders themselves or aspects of ITA that are not working well. Appeals channels are needed for complaints and concerns involving the TA and TWHs

> ***Recommendation 9***: Alternative channels for technical conscience should be established that bypass the TWHs if the concerns involve the TWH or TA. In addition, the technical conscience channels and processing needs to be monitored carefully at first to assure effective reporting and handling. Hopefully, as the culture changes to one where "what-if" analysis and open expression of dissent dominate, which was common in the Apollo era, such channels will become less necessary.

Impact of Increased Contracting

Finding 10: In one of our system dynamics analyses, we increased the amount of contracting to determine the impact on technical risk of contracting out the engineering design functions. We found that increased contracting does not significantly change the level of risk until a "tipping point" is reached where NASA is not able to perform the integration and safety oversight that is their responsibility. After that point, risk increases rapidly. While contractors may have a relative abundance of employees with safety knowledge and skills, without a strong in-house structure to coordinate and integrate the efforts of both NASA and contractor safety activities, effective risk mitigation can be compromised.

> ***Recommendation 10***: For projects in which significant contracting is anticipated, careful study of the types and amount of oversight needed to avoid reaching the tipping point will help with NASA's planning and staffing functions. The answer may not be a simple ratio of in-house expertise to contracting levels. Instead, the type of project as well as other factors may determine appropriate expertise as well as resource needs.

4 CONCLUSIONS AND FUTURE PLANS

The ITA program design and implementation planning represent a solid achievement by the NASA Chief Engineer's Office. We believe that ITA represents a way to make significant progress in changing the safety culture and evolving to a much stronger safety program. We hope this risk analysis will be helpful in furthering its success.

We have a small USRA research grant to further develop the formal approach we used in this risk analysis so that it can be more easily employed by managers, particularly the system dynamics modeling. We hope to be able to continue to use the NASA manned space program as a test bed for our research. We also plan to investigate how to apply the same risk analysis approach to important system qualities beyond safety and to programmatic concerns. One longer-term goal is to design a state-of-the-art risk management tool set that provides support for improved decision-making about risk both at the organizational and physical system level. The September 2004 NRC report on the requirements for system engineering and integration for Project Constellation concludes: "The development of space systems is inherently risky. To achieve success, risk management must go far beyond corrective action prompted by incidents and accidents. All types of risk—including risk to human life—must be actively managed to achieve realistic and affordable goals."[17]

[17] Donald C. Fraser, *op. cit*.

Appendix A: The STAMP Model of Accident Causality

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 for devising risk metrics and performance monitoring. 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 have great value in terms of 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[18].

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 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 designing a control structure, encompassing the entire socio-technical system, that will enforce the necessary constraints on development and operations. Figure A.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 A.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.

[18] Nancy G. Leveson, A New Accident Model for Engineering Safer Systems, *Safety Science*, Vol. 42, No. 4, April 2004.

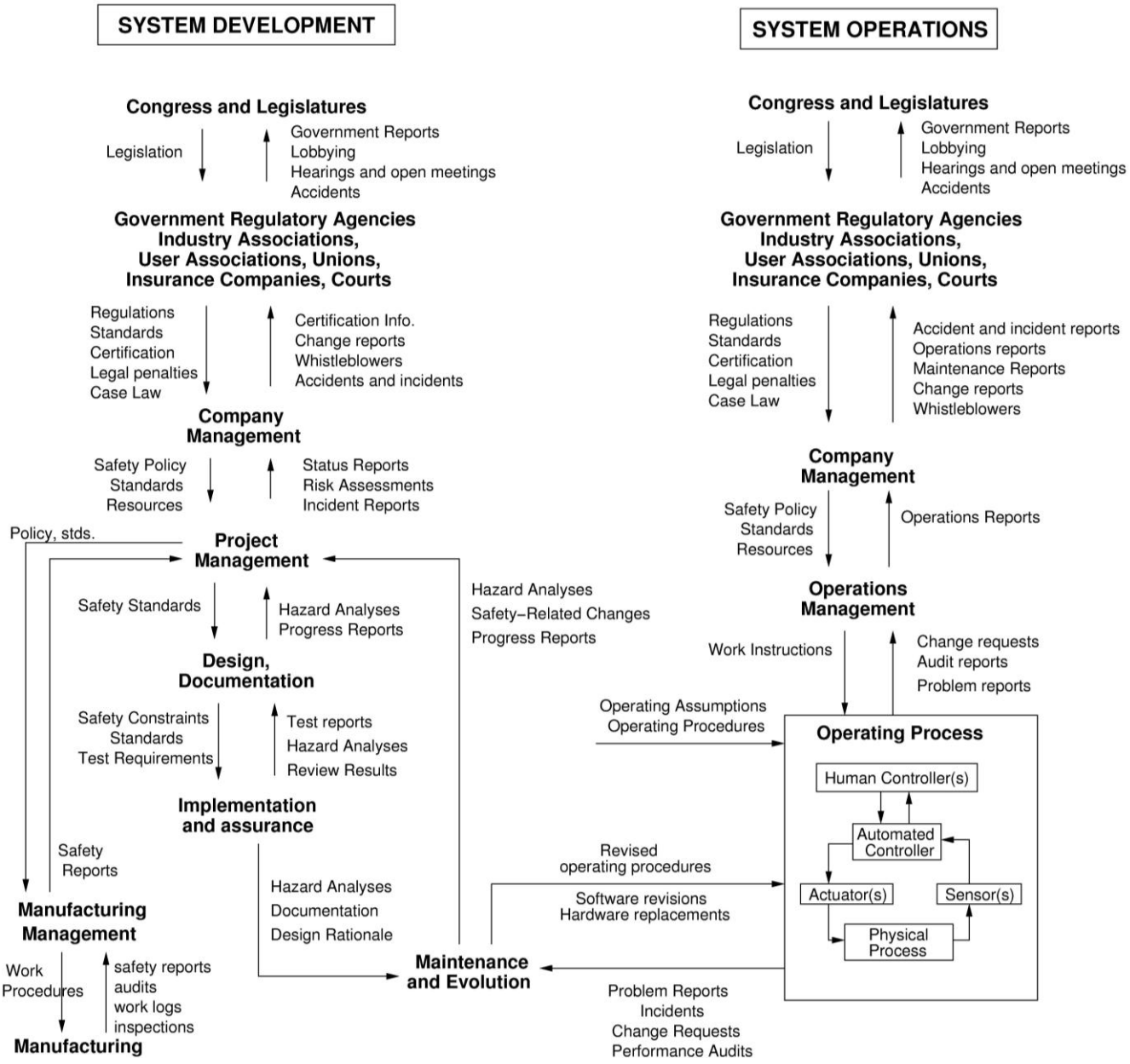


Figure A.1: General Form of a Model of Socio-Technical Safety Control

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.

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. One event may trigger the loss, but if that event had not happened, another one would have. As an example, Figure A.2 shows the changes over time that led to a water contamination accident in Canada where 2400 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. Each component of the water quality control structure played a role in the accident. The model at the top shows the control structure for water quality in Ontario Canada as designed. The figure at the bottom shows the control structure as it existed at the time of the accident. One of the important changes that contributed to the accident is 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 moving the water quality control system structure slowly 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 A.2 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. For this goal, we use system dynamics models. System dynamics models are formal and can be executed, like our other models. More information about systems dynamics models can be found in Appendix C and examples are shown (including a simple model of the Columbia accident dynamics) in Figures C.2 and C.3.

Often degradation of the control structure involves *asynchronous evolution* where one part of a system changes without the related necessary changes in other 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 gyro spin-down.

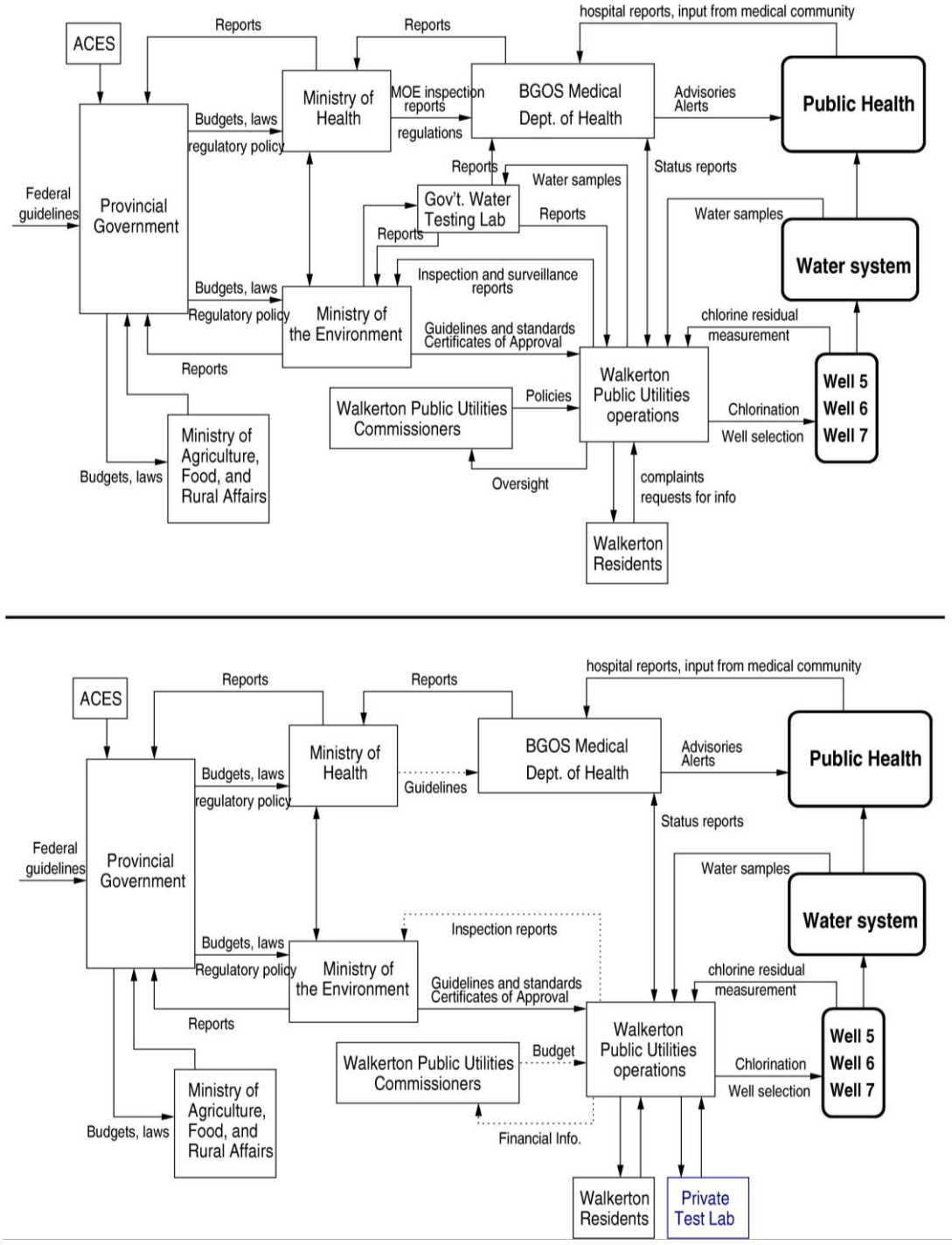
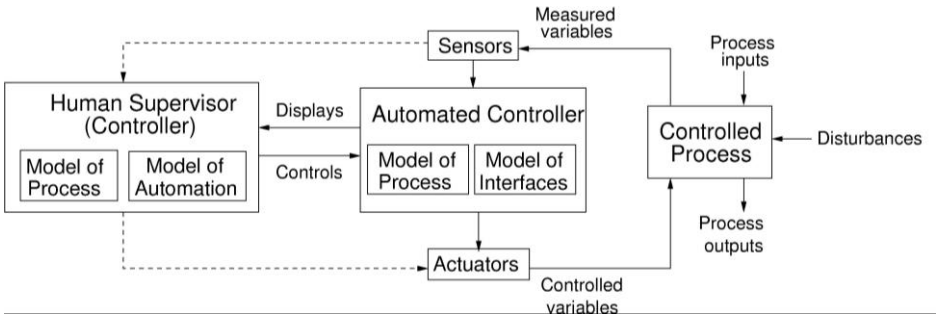


Figure A.2. The Safety Control Structure in the Walkerton Water Contamination Accident. The structure is drawn in the form commonly used for control loops. Lines going into the left of a box are control lines. Lines from or to the top or bottom of a box represent information, feedback, or a physical flow. Rectangles with sharp corners are controllers while rectangles with rounded corners represent physical processes.

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.



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 m *boundary* or *overlap* areas where two or more controllers control the same process[19] (Leplat, 1987).

A STAMP modeling and analysis effort involves creating a model of the organizational safety structure that includes the static safety control structure and safety constraints 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 and learn how to prevent related accidents in the future, to proactively perform hazard analysis and design to reduce risk throughout the life of the system, and to support a continual risk management program where risk is monitored and controlled.

[19] Jacques Leplat. 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, 1987.

Appendix B STAMP-Based Hazard Analysis (STPA)

STAMP can be used as the basis for a new approach to hazard analysis, STPA (StamP Analysis). While we first envisioned and developed this hazard analysis technique for the technical parts of the system, we have since discovered that it works equally well on the social and organizational aspects.

STPA starts at the early life cycle stages and continues through the life of the system. Its use during design can support a safety-driven design process where the hazard analysis influences and shapes the early system design decisions and then is iterated and refined as the design evolves and more information becomes available.

STPA has the same general goals as any hazard analysis: (1) identification of the system hazards and the related safety constraints necessary to ensure acceptable risk and (2) accumulation of information about how those constraints could be violated so it can be used in eliminating, reducing, and controlling hazards. Thus, the process starts with identifying the system requirements and design constraints necessary to maintain safety. In later steps, STPA assists in the top-down refinement of the safety-related system requirements and constraints into requirements and constraints on the individual system components. The overall process provides the information and documentation necessary to ensure the safety constraints are enforced in system design, development, manufacturing, and operations.

We illustrate the process of safety-driven design and the use of STPA to support it with the design of a (non-existent) Space Shuttle robotic Thermal Tile Processing System (TTPS). The TTPS will be responsible for inspecting and waterproofing the thermal protection tiles on the belly of the Shuttle. The process starts, like any design process, with identifying general environmental constraints on the system design. These environmental constraints derive from physical properties of the Orbital Processing Facility (OPF) at KSC, such as size constraints on any physical system components and the necessity of any mobile robotic components to deal with crowded work areas and for humans to be in the area.

The next step, after the high-level system requirements (functional goals such as inspection and waterproofing) and environmental conditions have been identified, is to identify hazardous conditions that could be encountered during system operation (i.e., perform a preliminary hazard analysis). A hazard is a system state or set of conditions that, together with other conditions in the environment, will lead to an accident (unacceptable loss). Hazards are not failures, but a set of conditions that may lead to a system loss. The overheating of the Space Shuttle Columbia's internal wing structure was a hazard while the accident was the loss of the seven astronauts and the Shuttle itself.

Different initial system configurations could be chosen that would introduce different hazards. For our example, the initial configuration chosen, given the identified high-level requirements and environmental constraints, consists of a robot containing a mobile base and a manipulator arm. As the concept and detailed design proceeds, information generated about hazards and design tradeoffs may lead to changes in the initial configuration. Alternatively, multiple design configurations may be considered in parallel.

The next step is to identify and prioritize the system hazards, such as contact of humans with waterproofing chemicals, fire or explosion, movement of the robot or manipulator arm causing injury to humans or damage to the orbiter, etc. Instability of the mobile robot base is used as the hazard considered in the rest of this section.

In general, safety-driven design involves first attempting to eliminate the hazard from the design and, if that is not possible or requires unacceptable tradeoffs, reducing the probability the hazard will occur, reducing the negative consequences of the hazard, and implementing contingency plans for dealing with the hazard.

As design decisions are made, an STPA-based hazard analysis is used to inform those decisions. Early in the system design process, little information is available so the hazard analysis will be very general at first and will be refined and augmented as additional information emerges from the system design activities. For example, instability of the mobile robot could lead to human injury or damage to the orbiter. A possible solution is to make the robot base so heavy that it cannot become unstable, no matter how the manipulator arm is positioned, thus eliminating the hazard. A heavy base, however, could

increase the damage caused by the base coming into contact with a human or object or make it difficult for workers to manually move the robot out of the way in an emergency situation. An alternative solution is to make the base long and wide so the moment created by the operation of the manipulator arm is compensated by the moments created by base supports that are far from the robot's center of mass. A long and wide base could remove the hazard, but may violate the environmental constraints in the facility layout (the need to maneuver through doors and in the crowded OPF). Let's say that analysis of the environmental constraints results in a maximum length for the robot of 2.5 m and a width no larger than 1.1 m. Given the required maximum extension length of the manipulator arm and the weight of the equipment that will need to be carried, a simple analysis shows that the length of the robot base is sufficient to prevent any longitudinal instability, but the width of the base is clearly not sufficient to prevent lateral instability. Other solutions might be considered such as including lateral stabilizer legs that are deployed when the manipulator arm is extended but must be retracted when the robot base moves.

At the initial stages, we identified only the general hazards, e.g., instability of the robot base, and related system design constraints, e.g., the mobile base must not be capable of falling over under worst-case operational conditions. As design decisions are proposed and analyzed, they will lead to additional refinements in the design constraints. For example, under the scenario laid out above, two new safety design constraints are identified: (1) the manipulator arm must move only when the stabilizers are fully deployed and (2) the stabilizer legs must not be retracted until the manipulator arm is fully stowed. STPA is used to further refine these constraints and to evaluate the resulting designs.

STPA starts by defining an initial hierarchical control structure for the system. A candidate structure for the mobile robot is shown in Fig. B.1. As with any part of the system design, the candidate control structure will have to be revisited when more information becomes available. In the candidate structure, a decision is made to introduce a human operator in order to supervise the robot during its operation and to perform safety-critical tasks. The STPA will identify the implications of the decision and will assist in analyzing the allocation of tasks to the various components to determine the safety tradeoffs involved.

Using the initial control structure, the next steps in STPA are to identify potentially hazardous control actions by each of the system components that could violate the safety constraints, determine the causal factors that could lead to these hazardous control actions, and prevent or control them in the system design. The process thus involves a top-down identification of scenarios in which the safety constraints could be violated so they can be used to guide design decisions. This process is similar to fault tree analysis, but provides more types of scenarios and handles design errors better.

In general, a controller can provide four different types of inadequate control:

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

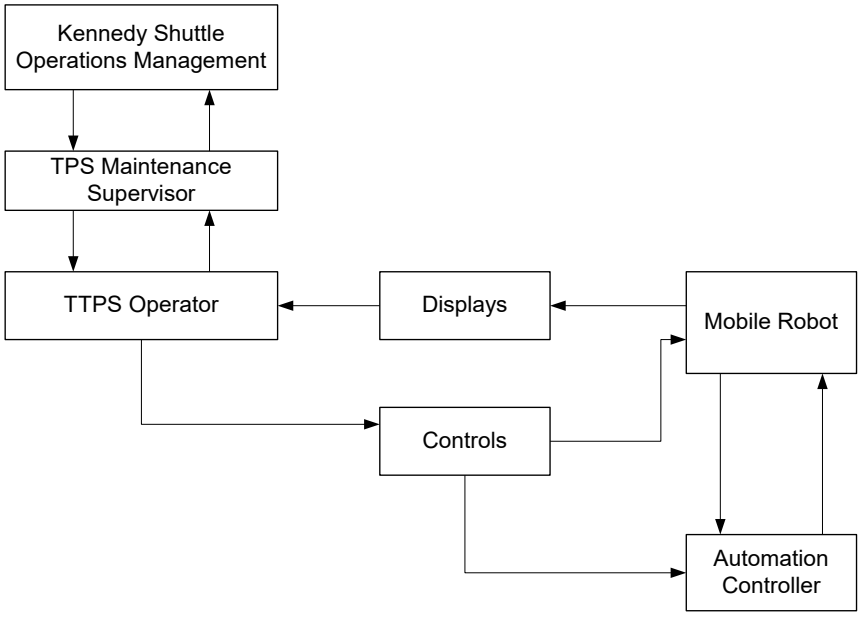


Figure B.1: A Candidate Control Structure for the TTPS

For the TTPS mobile base and the preliminary design decisions described above, the stability constraint may be violated if the component responsible for controlling the position of the stabilizer legs:

1. Does not command a deployment of the stabilizer legs when arm movements are enabled.
2. Commands a retraction of the stabilizer legs when the manipulator arm is not stowed.
3. Commands a retraction of the stabilizer legs after arm movements are enabled or commands a retraction of the stabilizer legs before the manipulator arm is stowed.
4. Stops extension of the stabilizer legs before they are fully extended.

These inadequate control actions can be restated as system safety constraints:

1. The controller must ensure the stabilizer legs are extended whenever arm movements are enabled.
2. The controller must not command a retraction of the stabilizer legs when the manipulator arm is not in a stowed position.
3. The controller must command a deployment of the stabilizer legs before arm movements are enabled; the controller must not command a retraction of the stabilizer legs before the manipulator arm is stowed.
4. The controller must not stop the leg extension until the legs are fully extended.

Similar constraints will be identified for all hazardous commands, e.g., the arm controller must not enable manipulator arm movement before the stabilizer legs are completely extended.

The above system constraints might be enforced through physical interlocks, human procedures, etc. The STPA analysis will in the next steps provide information (1) to evaluate and compare the different design choices, (2) to design fault tolerance features, and (3) to guide the test and verification procedures (or training for humans). In our research, we are using a formal behavioral system modeling language, called SpecTRM-RL, to implement a continuous simulation environment to augment the paper analyses.

To produce detailed scenarios for the violation of safety constraints, the control structure is augmented with process models. Figure B.2 shows a process model for the mobile robot containing the information available at this point in the system design. The preliminary design of the process models comes from the information necessary to assure the system safety constraints. For example, the constraint that the arm controller must not enable manipulator arm movement before the stabilizer legs are completely extended

implies that there must be some type of feedback to determine when the leg extension has been completed.

Either (1) a general controller process model can initially be constructed and the control responsibilities allocated to individual controllers (e.g., leg controllers and arm controllers) in later steps to optimize fault tolerance and communication requirements or (2) a more preliminary allocation can be proposed and then analyzed and refined. Decisions about allocation of functionality to system components are considered as the hazard analysis and system design continues.

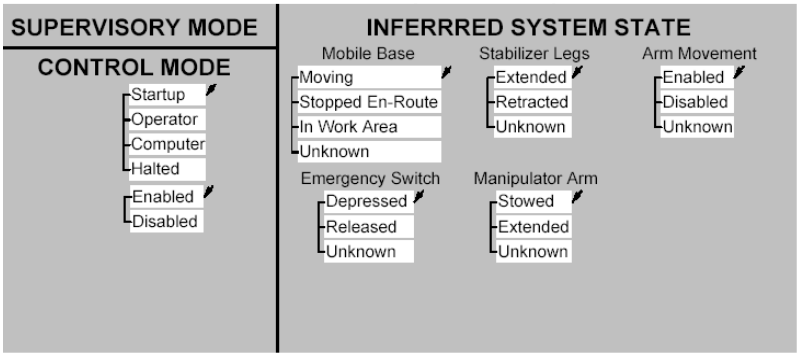


Figure B.2. The Process Model for the Robot Controller using SpecTRM-RL. As the logic is defined, it can also be specified and executed as part of a design simulation environment.

The control loop structure and process models are now used to identify ways the system could get into a hazardous state, i.e., the identified safety design constraints are violated. The process is driven by the classification of control flaws leading to hazards shown in Fig. B.3, that is, either the control actions or the execution of the control actions is inadequate. Each part of the control loop is evaluated with respect to the control flaw classification in Fig. B.3 and its potential to lead to the identified reasons for inadequate enforcement of the safety constraints.

As an example, consider how the process model of the state of the stabilizer legs could become inconsistent with the actual state. If an external object prevents the complete extension of the stabilizer legs, the robot controller (either human or automated) may assume the stabilizer legs are extended because the extension motors have been powered up (a common type of design error). Subsequent movement of the manipulator arm would then violate the identified safety constraints.

Accidents often occur during initial system startup and when restarting after a temporary shutdown. For example, the requirements for the mobile robot might specify that it must be possible to move the mobile base out of the way in case of an emergency. If the mobile robot requires an emergency shutdown while servicing the tiles, the stabilizer legs may have to be manually retracted in order to move the robot out of the way. When the robot is restarted, the controller may assume that the stabilizer legs are still extended and arm movements may be commanded that would violate the safety constraints. Such scenarios must be prohibited in the system design.

- **Inadequate control actions (enforcement of constraints)**
  - Unidentified hazards
  - Inappropriate, ineffective, or missing control actions for identified hazards
    - Design of control algorithm (process) does not enforce constraints
    - Process models inconsistent, incomplete, or incorrect (lack of linkup)
      - Flaw(s) in creation process
      - Flaws(s) in updating process (asynchronous evolution)
      - Time lags and measurement inaccuracies not accounted for
    - Inadequate coordination among controllers and decision–makers (boundary and overlap areas)
- **Inadequate Execution of Control Action**
  - Communication flaw
  - Inadequate actuator operation
  - Time lag
- **Inadequate or missing feedback**
  - Not provided in system design
  - Communication flaw
  - Time lag
  - Inadequate sensor operation (incorrect or no information provided)

Figure B.3. Control Flaws Leading to Hazards

In later stages of system development, when the logic of the controller has been specified, it can be analyzed to ensure that the identified hazardous scenarios cannot occur. The analysis results are also useful in testing and other review activities.

Additional analysis is required when humans are involved in the control loops. The analysis cannot simply consider the normative procedures because humans may not follow the specified procedures. Humans will adapt their behavior to be consistent with the reality of their work environment and informal work systems will emerge as a more efficient way of attaining the conflicting goals of task performance, schedule pressure, and resource scarcity. STPA starts from the hazard, working backward to identify the types of deviations that could lead to it and can identify the types of human behavioral deviations from procedures that can lead to hazardous system states. We use system dynamics models to assist in this process. Once these hazardous human behaviors are identified, the system design might be changed to prevent or reduce their occurrence or, if this is not possible, prevention and mitigation strategies might involve training, monitoring for safety-critical deviations, and developing operator skills at judging when, when not, and how to adapt procedures to local circumstances.

Just as operator behavior may degrade or change over time, so may other parts of the hierarchical safety control structure. An effective safety control structure at the beginning of a system lifecycle may become less effective at enforcing safety constraints as a result of asynchronous evolution of the components of the structure or eroding control mechanisms. Traditional hazard analysis techniques are static in nature, focusing on the ability of the system to avoid unsafe states given the current system design and its environment. In contrast, a STAMP-based hazard analysis assumes that systems are dynamic in nature and will evolve and adapt based on changes within the system and in its operating environment as well as economic pressures, tight schedules, and creeping expectations. A complete hazard analysis must therefore identify the possible changes to the safety control structure over time that could lead to a high-risk state. We believe system dynamics models can be useful in identifying migration of the system over time to states of elevated risk. This information can be used to prevent such changes through system design or, if not possible, generate operational metrics and auditing procedures to detect such degradation and to design controls on maintenance, system changes, and upgrade activities.

Appendix C: A Brief Introduction to System Dynamics Models

The field of system dynamics, created at MIT in the 1950s by Forrester, 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. Like the other models used in a STAMP analysis, 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[20].

System behavior in system dynamics is modeled by using feedback (causal) loops, stock 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[21]. 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.

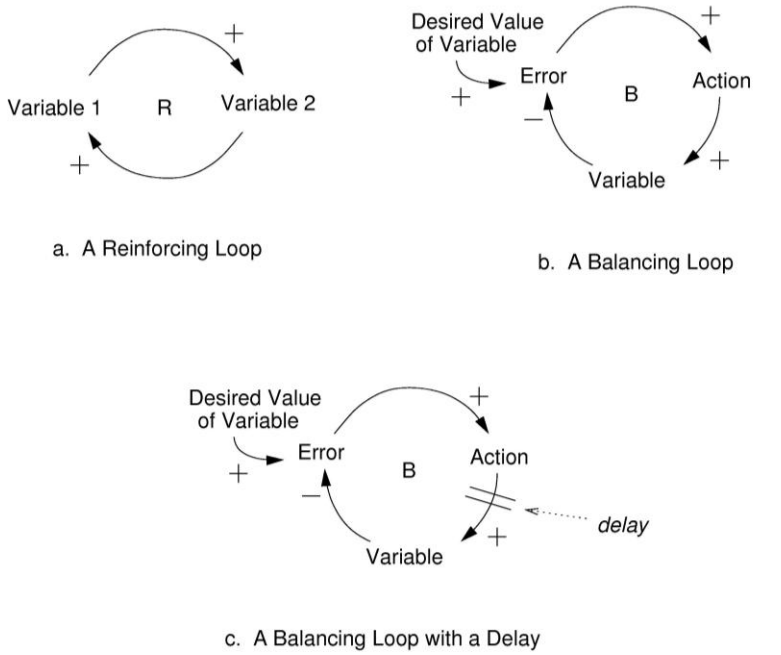


Figure C.1. The Three Basic Components of System Dynamics Models

Figure C.1a 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), which leads to an increase in variable 1 and so on. The "+" does not mean the values necessarily increase, only that variable 1 and

[20] John Sterman. *Business Dynamics: Systems Thinking and Modeling for a Complex World*, McGraw-Hill, 2000.
[21] Peter M. Senge. The Fifth Discipline: The Art and Practice of the Learning Organization, Doubleday Currency, New York, 1990.

variable 2 will change in the same direction (polarity). If variable 1 decreases, then variable 2 will decrease. A "-" indicates that the values change in opposite directions. 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 C.1b) 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. 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 C.1c. 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 C.2 is helpful in understanding the stock and flow syntax and the results of our modeling effort. 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 *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 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, i.e., 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:

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

$$People\ who\ know(0) = 1$$

$$People\ who\ don't\ know(0) = 99$$

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

$$Total\ People = People\ who\ don't\ know(t) + People\ who\ know(t)$$

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

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

The graph in Figure C.2 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.

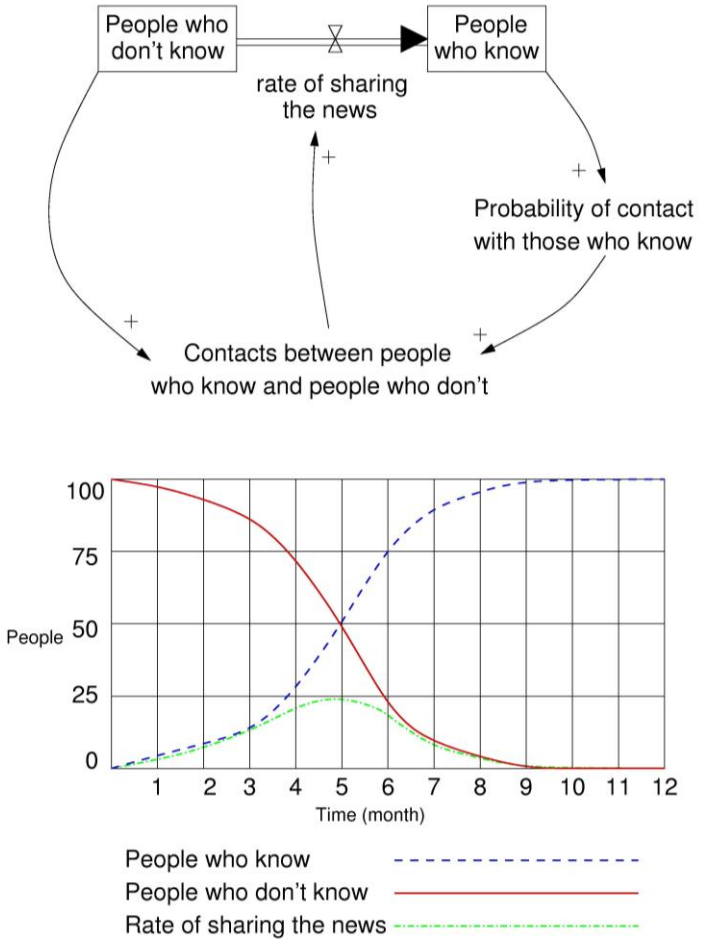


Figure C.2. An Example System Dynamics and Analysis Output

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 C.3 shows a simple systems dynamics model of the Columbia accident. This model contains just a small part of our complete model but is useful in understanding this type of model. There are three main variables in the model: safety, complacency, and success in meeting launch rate expectations.

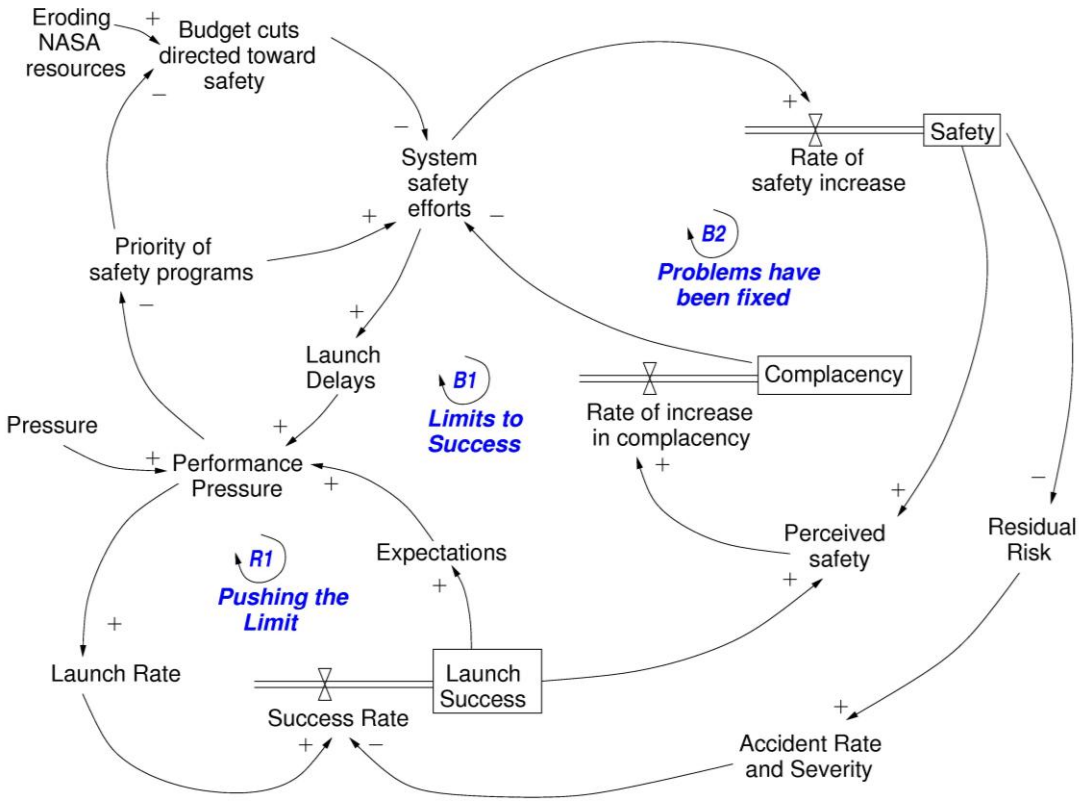


Figure C.3. Simplified Model of the Dynamics Behind the Shuttle Columbia Loss

The control loop in the lower left corner of Figure C.3, labeled R1 or *Pushing the Limit*, shows how as external pressures increased, performance pressure increased, which led to increased launch rates and thus success in meeting the launch rate expectations, which in turn led to increased expectations and increasing 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.

One thing not shown in the diagram is 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 C.3 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.

Appendix D: Detailed Content of the Models

D.1 Examples from STAMP ITA Hierarchical Control Structure

Only part of the STAMP structural model is included here for space reasons. Examples of the STWH, the DTWH, and the Trusted Agents are provided. All the information needed from the complete model for the risk analysis is included in other parts of this report and therefore is redundant here.

Inputs:

Budgets, goals, conflict resolutions, approval of implementation plan

Other Inputs:

- System design decisions (from in-line engineers and trusted agents)
- Hazard and other analyses (from S&MA)
- Information about technical disciplines and system design
- Specifications from NASA, Centers, programs, projects, other government agencies, and industry

CE

- Monthly and annual reports, meetings, reports on unresolved conflicts, reports on decisions, lessons learned, TWH implementation plan
- Report to TA of issues raised in Technical Conscience as well as final resolution. If not resolved, then add recommended path and plan of action to resolve issue.
- Requests for special investigations by NESC.

SYSTEM TECHNICAL WARRANT HOLDER (STWH)

Overall Role:

Primary ITA interface to one or more mission-related systems and representative of ITA for lower-level decision-making and actions. Ensure, as appropriate, the evaluation of technical issues and identification of risks through the use of existing engineering organizations.

Responsibilities:

1. *Establish and maintain technical policy, technical standards, requirements, and processes for a particular system or systems.*
    a. STWH shall ensure program identifies and imposes appropriate technical requirements at program/project formulation 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)
2. *Technical Product Compliance*
    a. STWH shall ensure technical requirements, specifications, and standards have been integrated into and applied in programs/projects.
    b. STWH shall approve all variances.
    c. STWH shall be responsible for determining whether design satisfies safety-related technical requirements.
    d. STWH shall influence decisions about requirements and safety at all major design reviews. This can include evaluating technically acceptable alternatives and performing associated risk and value assessments.
    e. STWH shall attest by signature that the design satisfies the technical requirements.
3. *Serve as primary interface between system and ITA (CE)*
    a. STWH shall maintain real-time communications with the program/project to ensure timely access by the technical authority to program/project information, impending decisions, and analysis or verification results [potential time lags here]
4. *Assist DTWH in access to data/rationale/other experts*.
    a. When a technical decision requires the approval of a DTWH, STWH shall assure that the DTWHs have full access both to the program/project team and to pertinent technical information before a technical decision is rendered and delivered to the program/project.

SYSTEM TECHNICAL WARRANT HOLDER (STWH) (Cont'd)

Responsibilities (cont'd)

5. *Production, quality, and use of FMEA, CIL, trending analysis, hazard, and risk analyses*
    a. STWH shall approve the technical methodologies used to develop these products.
    b. STWH shall approve the final analysis results to be incorporated into the technical product provided to the program/project.
    c. STWH shall ensure hazard analysis delivered to and used by design engineers while still time to affect design. [says "enforce concept that FMEA and hazard analysis will be used as part of the design process, not developed after the design is complete.] (*Note: Safety, risk, and hazard analyses, formerly accomplished outside the purview of engineering and after the completion of the technical product, are now included in the technical products approved by the TWHs*.)
    d. The STWH shall initiate special investigations if he/she deems further evaluation or testing is prudent for risk quantification if technical boundaries have been exceeded or if alternative technical options may be required to solve a complex issue:
        i. STWH shall request the investigation from the project by negotiating with program/project manager and drawing on in-line engineering under program/project funding.
        ii. In special cases, STWH shall perform independent investigations funded by ITA or NESC.
6. *Timely, day-to-day technical positions on issues pertaining to safe and reliable operations.*
    a. The STWH shall provide input to engineering review boards, TIMs, and special technical issue topics to ensure that safety is a regular part of design.
    b. The STWH shall participate in program/project technical forums and boards to maintain cognizance of technical design and all safety-related technical issues.
    c. The STWH shall integrate appropriate individual technical discipline warrant holder reviews and prepare integrated technical positions.
7. *Establishing appropriate communication channels and networks*
    a. The STWH shall select and train a group of Trusted Agents.
    b. The STWH shall establish and maintain effective communication channels with his or her trusted agents and with in-line engineers.
8. *Succession Planning*
    a. The STWH shall train and mentor potential successors.
9. *Documentation of all methodologies, actions/closures, and decisions*
    a. The signature of all parties participating in decision-making shall appear on documentation signature sheet
    b. The STWH shall maintain objective quality evidence (OQE) of the decisions and information on which decisions were based.
    c. The STWH shall provide feedback to ITA about decisions and actions.

(Cont'd below)

SYSTEM TECHNICAL WARRANT HOLDER (STWH) (Cont'd)

Responsibilities (cont'd)

1. *Sustaining the Agency knowledge base through communication of decisions and lessons learned*
    a. The STWH shall document or ensure program/project provides documents to appropriate parties including both precedent-setting decisions (e.g., expanded technical envelopes, sensitivity data, and technical requirements that supercede other imposed requirements) and lessons learned. This documentation shall include the circumstances surrounding the issue, technical positions (including dissenting opinions), and logic used for final decision-making.
    b. The STWH shall provide input to the lessons-learned system about his/her experiences in implementing TWH responsibilities.
    c. The STWH shall communicate decisions and lessons learned to his/her network of trusted agents and others involved in the system design, development, and operations.
2. *Assessment of launch readiness from the standpoint of safe and reliable flight and ground operations*
    a. The STWH shall integrate information provided by the Trusted Agents, DTWHs, and others into an assessment of launch readiness.
    b. The STWH shall sign the CoFR to attest to system flight readiness
12. *Budget and resource requirements definition*
    a. The STWH shall identify the resources necessary to support all required warrant holder activities, providing budget input and establishing working agreements.
13. *Maintaining competence*
    a. The STWHs shall maintain their level of technical expertise in technologies and specialties of their warranted system(s) and also currency in program efforts that affect the application of technical requirements.
14. *Leading the technical conscience for the warranted system(s)*
    a. The STWH shall identify technical conscience issues
    b. The STWH shall listen to technical personnel raising issues
    c. The STWH shall act proactively to identify and implement solutions.
    d. The STWH shall provide feedback on the disposition of the concern to the person who reported it in the first place as well as the Chief Engineer (ITA)
    e. The STWH shall raise unresolved technical conscience issues to the Chief Engineer (ITA).

Environmental and Behavior-Shaping Factors (Context):

Must be respected and have influence. Performance pressures, career (performance appraisal) pressures

(Cont'd below)

SYSTEM TECHNICAL WARRANT HOLDER (STWH) (Cont'd)

Mental Model Requirements:

1. Extensive knowledge of system [and knowledge of disciplines used in it?]
    a. Understand system design in sufficient detail and have current knowledge of technical work going on in the program to make sound, responsible technical decisions.
    b. In-depth comprehension of the failure scenarios and hazards.
2. Ability to perform trend analyses and risk assessments and incorporate results into a final technical product that includes a risk management plan
3. Knowledge of Agency's engineering capability
4. Understanding of risk management process and expertise (including knowledge of uses and limitations) of tools such as FTA, PRA, FMEA/CIL and hazard analysis techniques.

Coordination and Communication Requirements:

Interacts with program/project manager to establish working relationships with Boards, to establish the review process, and to formalize the signature methodology and appropriate documentation.

Controls:

Approval of hazard and risk analyses, signature on design reviews and CoFR, approval of hazard and risk analysis methodologies and definition. Approval of technical content of RFP including contractual documentation requirements, approval of verification plans, approval of variances, requests to program/project managers for special investigations.

Potential Inadequate Control Actions:

1. Does not ensure safety analyses built into design (does not get information to developers at appropriate times);
2. Approves inadequate safety and reliability engineering products (FMEA/CILs, hazard analyses, etc.)
3. Inadequate interaction and communication among system and discipline warrant holders.
4. Makes unsafe technical decisions due to inadequate knowledge of issues in program/project/design decisions.
    a. Do not get information and feedback from Trusted Agents
    b. Communication channels not established or unreliable
5. Makes unsafe technical decisions because does not have adequate levels of technical expertise.
    c. Does not know enough about hazard analyses
    d. Does not have adequate knowledge about system
    e. Does not have adequate knowledge of technologies involved in system
6. Does not ensure technical standards and requirements are adequate
    f. Approves inadequate standards
    g. Does not propose appropriate standards
    h. Does not provide for updating of standards
    i. Does not ensure projects/programs use them
7. Does not act as the safety authority during technical reviews
8. Documentation and lessons learned not maintained or not based on objective quality evidence.

(Cont'd)

SYSTEM TECHNICAL WARRANT HOLDER (STWH) (Cont'd)

Potential Inadequate Control Actions (Cont'd):

10. Incorrect documentation and lessons learned maintained (e.g., inadequate root cause analysis)
11. Accepts technical products that do not conform with technical policy, standards, and requirements
12. Approves unsafe engineering variance or waiver
    a. Inadequate or incorrect information
    b. Bows to pressures from programmatic concerns
13. Accepts and uses inadequate hazard analysis, risk assessments, and trend analysis. Approves inadequate technical methodologies to develop these products.
14. Does not ensure that hazard analyses are used in the early P/P design stages
15. Creates an inappropriate or inadequate set of Trusted Agents
    a. Trusted agents are not provided with adequate training
    b. Poorly selected
    c. Poorly supervised (not given adequate direction and leadership)
16. Does not ensure lessons learned captured and communicated to those needing them
17. Inadequate communication among TWHs (system and discipline), both too much (information overload) and too little.
18. Does not provide required technical positions, technical positions provided are unsafe or are too late (too delayed) to be useful.
19. Does not respond appropriately to expressions of technical conscience reported to him or her. Responds but not in a timely manner.
20. Requests inadequate resources
21. Does not have adequate access to data/rationale/other experts.
22. Blocks communication of info up chain to ITA
23. Does not provide for succession and training of possible replacements.

Feedback:

1. Information from trusted agents (what get?)
2. Information from network of engineers in matrix organizations, in-line safety, and mission assurance personnel, and in-line engineering experts
3. Program technical data, reviews, evaluations, analyses, tests, and process evaluations
4. Requests for changes and variances from requirements.
5. System design decisions from the program/project and/or contractor.
6. Variance reports (from Program/Project Manager)
7. Completed system engineering reviews of variances, including approval of all new or updated hazards, risk, and reliability analyses and disposition (to Program/Project manager [and also ITA?])

STrA

Reference Channel:

- Feedback on disposition of reported technical concern.
- Requests for information.
- Assignments for trusted agents.
- Approval for changes and variances to requirements. (Disposition of variances from established technical requirements)
- Documents, written assessment of technical decisions and requirements, including risk and value considerations. Integrated technical positions of individual technical discipline TWH reviews.
- Forwards variance reports to appropriate discipline warrant holders

Other Inputs:

- New developments in their technical disciplines
- Specifications from NASA, Centers, programs, projects, other government agencies, and industry
- Variance reports (from System Technical Warrant Holders)

CE

- Monthly and annual reports, meetings, reports on unresolved conflicts, reports on decisions, lessons learned, TWH implementation plan.
- Report to TA of issues raised in Technical Conscience as well as final resolution. If not resolved, then add recommended path and plan of action to resolve issue.

DISCIPLINE TECHNICAL WARRANT HOLDER (DTWH)

Overall Role:

Authority for a particular technical discipline as applied to all warranted missions within the Agency. Interface and assistance for ITA and STWH with technical disciplines.

Responsibilities:

1. *Interface to specialized technical knowledge within the Agency*
    a. The DTWH shall select and train a group of Trusted Agents to assist in fulfilling technical warrant holder responsibilities. These trusted agents will be consulting experts across the Agency with knowledge in the area of interest and unique knowledge and skills in the discipline and sub discipline areas.
    b. The DTWH shall establish and maintain effective communication channels and networks with trusted agents and with in-line engineers.
2. *Assistance to STWHs in carrying out their responsibilities*
    a. The DTWH shall provide discipline expertise and a fresh set of eyes in assisting STWH in approving or disapproving all variances to technical requirements within the scope of the warrant.
    b. The DTWH shall provide assessment of technical issues as required.
    c. In support of a STWH, the DTWH shall evaluate a program/project's design and analysis methodologies, processes, and tools to ensure program/project achieves desired goals for safe and reliable operations.
    d. The DTWH shall assist STWHs in evaluating requirements, implementation, variances and waiver requests involving the warranted technical discipline.
        i. The DTWH shall document all methodologies, actions/closures, and decisions made.
        ii. The DTWH shall maintain OQE to support decisions and recommendations.
3. *Ownership of technical specifications and standards for warranted discipline. (System Safety Warrant Holder shall own the system safety standards.)*
    a. The DTWH shall recommend priorities for development and updating of technical standards.
    b. The DTWH shall participate as members of technical standards working groups.
    c. The DTWH shall approve all new or updated NASA Preferred Standards within their assigned discipline. (NASA Chief Engineer retains Agency approval)
    d. The DTWH shall participate in (lead) development, adoption, and maintenance of NASA Preferred Technical Standards in the warranted discipline
    e. The DTWH shall evaluate and disposition any variance to an owned NASA Preferred Standard

(Cont'd below)

DISCIPLINE TECHNICAL WARRANT HOLDER (DTWH) (Cont'd)

Responsibilities: (Cont'd)

4. *Sustaining the Agency knowledge base in the warranted discipline*
    a. The DTWH shall ensure that decisions and lessons learned are documented and communicated to other technical warrant holders and to his/her network of trusted agents and others involved in the technical discipline within the Agency and its contractors. This documentation shall include the circumstances surrounding the issue, technical positions (including dissenting opinions), and logic used for final decision-making.
    b. The DTWH shall provide input to the lessons-learned system about his/her experiences in implementing TWH responsibilities.
5. *Sustaining the general health of the warranted discipline throughout the Agency*
    a. The DTWH shall monitor the general health of their warranted discipline throughout the Agency and provide recommendations for improvement (tools, techniques, and personnel) to the engineering Management Board, the Chief Engineer, and other Agency and Center organizations that can improve the health of the warranted discipline.
    b. The DTWH shall ensure technical personnel supporting programs/projects are using adequate tools, equipment, and techniques that meet current expectations for the discipline and for the end products.
    c. The DTWH shall communicate best practices for their warranted discipline throughout the Agency
6. *Succession Planning*
    a. The DTWH shall train and mentor potential successors.
7. *Leading the technical conscience for the warranted discipline*
    a. The DTWH shall identify technical issues
    b. The DTWH shall listen to technical personnel raising issues
    c. The DTWH shall act proactively to identify and implement solutions.
    d. The DTWH shall provide feedback on the disposition of the concern to the person who reported it in the first place as well as to the Chief Engineer (ITA) [says "employee" but what about contractors or others like me?]
    e. The DTWH shall raise unresolved technical conscience issues to the Chief Engineer (ITA).
8. *Budget and resource requirements definition*.
    a. The DTWH shall identify the resources necessary to support all required warrant holder activities, providing budget input and establishing working agreements.

Environmental and Behavior-Shaping Factors (Context):

Performance pressures, career pressures

Mental Model Requirements:

1. Must be cognizant of health of discipline throughout the Agency
2. Must have and maintain expertise in warranted discipline

(Cont'd)

DISCIPLINE TECHNICAL WARRANT HOLDER (DTWH) (Cont'd)

Coordination and Communication Requirements:

1. Primary responsibility to STWH and programs/projects is as a subject matter expert. Has a team of DTrA's, line engineers, or safety and mission assurance personnel to assist in fulfilling TA responsibilities.
2. Center Directors required by NPR to establish working agreements with each Agency DTWH where the discipline resides at their center. DTWHs can use these agreements to communicate across the discipline throughout the agency as well as to provide resources for work to be accomplished. The agreements will provide communication between the STWHs at each Center to the DTWH through the local discipline experts in accordance with these working agreements.
3. When performing TA responsibilities, the DTWH reports only to the NCE.
4. All requests for program/project-provided information are to be directed through the STWH since this position is the primary point of contact for the program/project. If an STWH has not been assigned for a given program/project, then the Chief Engineer or lead systems engineer of the program/project should be the point of entry for the DTWH.

Controls:

Technical standards approval, agreement with Center Directors.

Potential Inadequate Control Actions or Feedback:

1. Inadequate interaction and communication among WHs.
2. Makes Inadequate technical decisions because does not have adequate knowledge of discipline-related issues
    a. Do not get information and feedback from Trusted Agents
    b. Communication channels not established or unreliable
3. Makes inadequate technical decisions because does not have adequate levels of technical expertise.
    a. Does not know enough about hazard analyses and other safety-related products and processes.
    b. Does not have adequate or up-to-date (state-of-the-art) knowledge about discipline.
4. Does not ensure technical standards and requirements for discipline are adequate
    a. Approves inadequate standards
    b. Does not propose appropriate standards
    c. Does not provide for updating of standards
    d. Does not ensure projects/programs use them
5. Does not act as the safety authority during technical reviews (e.g., does not speak up, does not attend)
6. Documentation and lessons learned not maintained
7. Does not ensure Agency technical expertise is at an appropriate level
    a. Has inadequate knowledge about state of technical expertise in agency
    b. Does not provide for training and updating of skills when technology changes
8. Accepts technical products that do not conform with technical policy, standards, and requirements
9. Recommends approving unsafe engineering variance or waiver
    a. Inadequate or incorrect information
    b. Bows to pressures from programmatic concerns

(Cont'd)

DISCIPLINE TECHNICAL WARRANT HOLDER (DTWH) (Cont'd)

Potential Inadequate Control Actions or Feedback: (Cont'd)

10. Accepts and uses inadequate hazard analysis, risk assessments, and trend analysis. Approves inadequate technical methodologies to develop these products.
11. Does not ensure that hazard analyses results are applied within his or her discipline or ensure applied early enough to have an impact on design decisions.
12. Creates an inappropriate or inadequate set of Trusted Agents
    a. Trusted agents are not provided with adequate training
    b. Poorly selected
    c. Poorly supervised (not given adequate direction and leadership)
13. Does not ensure lessons learned are captured and communicated to those needing them
14. Inadequate communication among TWHs (system and discipline)
15. Does not provide required technical positions, technical positions provided are unsafe or are too late (too delayed) to be useful.
16. Does not respond appropriately to expressions of technical conscience reported to him or her. Responds but not in a timely manner.
17. Requests inadequate resources
18. Does not have adequate access to data/rationale/other experts.
19. Blocks (or delays) in communication of info up chain to ITA (or downward)
20. Does not provide for succession and training of potential replacements.

Feedback:

a. Information from trusted agents
b. Information from network of engineers in matrix organizations, in-line safety, and mission assurance personnel, and in-line engineering experts
c. Program technical data, reviews, evaluations, analyses, tests, and process evaluations
d. Analyses of variance acceptability and implications on safety and reliability along with interface considerations with rest of system or vehicle. Recommendation for approval or denial of variance.
e. Information about state of discipline in Agency

Reference channel: (DTrA)

- Feedback on disposition of reported technical concern.
- Requests for information.
- Information about best practices.
- Assignments for trusted agents.
- Variance reports to Trusted Agents.
- Recommendations on approval or denial of variances to STWHs including basis for recommendation and any risk assessment.
- Requests for special studies and analyses by NESC.

Other Inputs:
Requests for information and special analyses from System and Discipline Technical Warrant Holders.

STWH, DTWH & PPM
Reports, hazard analyses, Board and Panel activity reports, technical inputs to warrant holder decision-making, reports on acceptability of potential variances and implications for safety and reliability along with interface considerations with the larger system or vehicle.

TRUSTED AGENTS (DTrA, STrA)

Overall Role:

Provide technical support to ITA (both STWH and DTWH) and perform many of tasks necessary to implement the ITA.

Responsibilities:

1. Perform a screening function
    a. The Trusted Agents shall evaluate all changes and variances and perform all functions requested by STWH or DTWH.
2. Conduct daily business for STWH
    a. The System Trusted Agents shall represent the STWH on boards, forums, and in requirements and design reviews.
    b. The Discipline Trusted Agents shall represent the DTWH on technical standards committees.
3. Provide information to TWHs
    a. The Trusted Agents shall provide information to the TWHs about a specific project.

Environmental and Behavior-Shaping Factors (Context):

- While performing an ITA task, must be funded independently from program/project
- Do not hold warrants and do not have signature authority on decisions affecting safety or reliable operations
- Performance appraisals by program/project managers.

Mental Model Requirements:

- Need to be technically qualified and understand program/project. (Working knowledge of programs/projects at a particular Center or unique skills/knowledge at the sub discipline level.)
- Need to understand when a risk needs to be communicated upward and not accepted at their level.

Controls:

Represent the TWH on Boards and Panels.

Potential Inadequate Control Actions:

1. Trusted Agents do not provide adequate screening of changes and variances for STWH
    a. TrAs are not adequately competent or informed
        - Selection process becomes politicized
        - Skills erode over time due to lack of training or updating (i.e., not technically qualified)
        - Lack knowledge of a particular program/project
        - Lack access to safety information (e.g., hazard analyses and risk analyses) when needed
    b. Do not provide timely information
2. Screens information that should have been passed up to technical warrant holder.
4. Resolves conflicts in work responsibilities between TWH and program/project manager in favor of program/project manager. Funding is not independent or conflicts of interest. Feel more loyalty to P/P manager.
    a. Under pressure due to career prospects or performance appraisals
5. Communication channels between TWHs and Trusted Agents are dysfunctional
6. Accept risks without communicating them to Technical Authority

D.2 Mapping from System Requirements and Constraints to Individual Responsibilities

1. ***Safety considerations must be first and foremost in technical decision-making.***

1a. 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.

CE: Develop, monitor, and maintain technical standards and policy.

DTWHs:

- Recommend priorities for development and updating of technical standards.
- Approve all new or updated NASA Preferred Standards within their assigned discipline. (NASA Chief Engineer retains Agency approval)
- Participate in (lead) development, adoption, and maintenance of NASA Preferred Technical Standards in the warranted discipline
- Participate as members of technical standards working groups.

NTSP: Coordinate with TWHs when creating or updating standards.

OSMA:

- Develop and improve generic safety, reliability, and quality process standards and requirements, including FMEA, risk, and the hazard analysis process.
- Ensure that safety and mission assurance policies and procedures are adequate and properly documented.

Discipline Trusted Agents:

- Represent the DTWH on technical standards committees.

CE: In coordination with the Programs/Projects, establish/approve the technical requirements and ensure they are enforced and implemented in the programs/projects (ensure design is compliant with requirements)

STWH:

- Ensure program identifies and imposes appropriate technical requirements at program/project formulation to ensure safe and reliable operations.
- Ensure inclusion of the consideration of risk, failure, and hazards in technical requirements.
- Approve the set of technical requirements and any changes to them.
- Approve verification plans for the system(s).
- Ensure technical requirements, specifications, and standards have been integrated into and applied in programs/projects.
- Be responsible for determining whether design satisfies safety-related technical requirements.
- Influence decisions about requirements and safety at all major design reviews. This can include evaluating technically acceptable alternatives and performing associated risk and value assessments.
- Attest by signature that the design satisfies the technical requirements.

DTWH: In support of a STWH, evaluate a program/project's design and analysis methodologies, processes, and tools to ensure program/project achieves desired goals for safe and reliable operations.

OSMA: Oversee the conduct of reviews and obtaining of OQE to provide assurance that programs/projects have complied with all requirements, standards, directives, policies, and procedures.

S&MA:

- Conduct reviews and obtain OQE to provide assurance that programs/projects have complied with all requirements, standards, directives, policies, and procedures.
- Perform compliance verification assuring that the as-built hardware and software meet the design and that manufacturing adheres to specified processes.

Center Director:

- Ensure the Center S&MA works closely with TA to resolve technical issues uncovered by S&MA independent verification and compliance assessments and assurance reviews.

Program/Project Manager:

- Acquire STWH's agreement before applying technical standards and requirements or altering them.
- Obtain TWH agreement on technical decisions affecting safe and reliable operations prior to the Program or Projects' application of technical standards and requirements and any alteration thereof. Decisions on whether safe and reliable operations are affected or the item affects the establishment of or complies with the technical requirements shall be under the purview of the TWH.

Trusted Agents:

- Represent the STWH on boards, forums, and in requirements and design reviews.
- Provide information to the TWHs about a specific project.

In-line engineers: Provide unbiased technical positions to the warrant holders, S&MA, trusted agents, and programs/projects.

CE: Participate as a member of the SEB and approve technical content of the RFP and contractual documents

Mission-Directors: Notify the ITA when in the concept phase of a program/project.

CE: Approve all variances (waivers, deviations, exceptions) to the requirements and all changes to the initial technical requirements.

STWH: Approve all variances.

DTWH:

- Provide discipline expertise and a fresh set of eyes in assisting STWH in approving or disapproving all variances to technical requirements within the scope of the warrant.

- Evaluate and disposition any variance to an owned NASA Preferred Standard

Trusted Agents: Evaluate all changes and variances and perform all functions required by the STWH or DTWH

1b. Safety-related technical decision-making must be independent from programmatic considerations, including cost and schedule.

1b.1 Technical warrant holders must be outside of the program office direct chain of management.

CE: Ensure that TWHs are independent of program authority.

Headquarters-Center-Executives: Ensure the associated Center Director aligns that Center's organization and processes to support and maintain the independence of the TA and advises the TA of any issues at their assigned Center affecting safe and reliable operations and the successful execution of the ITA.

Center-Director:

- Ensure that TWHs do not report through a management chain of command when exercising TA as delegated by CE.
- Ensure that internal activities and organizations, such as operations, and engineering, are aligned to support the independent exercise of TA by the STWHs.
- Ensure that Technical Warrant Holders do not have a supervisory reporting chain to Program and Project Management.

1b.2 The TWHs must be paid from a separate budget account for execution of independent technical authority. That budget must be adequate to support the activities and foundational and fundamental resource tools required by the TWH to form a base of knowledge and technical capability for executing technical authority.

CE: Ensure that TWHs are financially independent of program budgets and independent of program authority.

Center-Director: Structure and execute Center financial system to ensure effective execution of WH responsibilities and preserve WH's independence from program/project funding (Ensure that financial and personnel resources are aligned with ITA).

Center ITA Manager: Assist in defining and obtaining resource and funding requirements with OCE, Office of Chief Financial Officer (OCFO), NESC, or a program/project.

Mission Directors:

- Ensure financial and personnel resources are aligned with ITA.
- Ensure appropriate financial and engineering infrastructure to support TWHs.

CE: Establish, provide, and secure human resources, payroll funding and services, and other direct funding to support Technical Authority activities at the Centers.

STWH: Identify the resources necessary to support all required ITA activities, providing budget input and establishing working agreements.

DTWH: Identify the resources necessary to support all required ITA activities, providing budget input and establishing working agreements.

1c. Safety-related decision-making must be based on correct, complete, and up-to-date information.

CE: Use TWA reports and other information to perform an independent assessment of launch readiness.

STWH: Integrate information provided by the Trusted Agents, DTWHs, and others into an assessment of launch readiness.

OSMA: Conduct launch readiness reviews.

CE: Sign the CoFR (provide independent assessment of flight readiness) based on his or her independent assessment of launch readiness.

STWH: Sign the CoFR to attest to system flight readiness

Program/Project Mgr: Working with ITA, ensure that documentation, including the CoFR, is updated to reflect the required TA signature blocks.

OSMA: Sign the CoFR.

The Program Manager must not limit access to program or project information by the TWH—the TWH and his/her trusted agents shall be given complete and timely access to program technical data, reviews, analyses, etc.

CE: Maintain or assure the updating of the databases that archive ITA decisions and lessons learned.

STWH:

- Provide input to the lessons learned system about his/her experiences in implementing TWH responsibilities.
- Maintain objective quality evidence (OQE) of the decisions and information on which decisions were based.
- Provide feedback to the ITA about decisions and actions.

DTWH:

- Provide input to the lessons-learned system about his/her experiences in implementing TWH responsibilities.

CE: Create and maintain communication channels for conveying decisions and lessons learned to those who need them or can use them to improve safe system design, development, and operations.

STWH:

- Document or ensure program/project provides documents to appropriate parties including both precedent-setting decisions (e.g., expanded technical envelopes, sensitivity data, and technical requirements that supercede other imposed requirements) and lessons learned. This documentation shall include the circumstances surrounding the issue, technical positions (including dissenting opinions), and logic used for final decision-making.
- Communicate decisions and lessons learned to his/her network of trusted agents and others involved in the system design, development, and operations.

DTWH:

- Ensure that decisions and lessons learned are documented and communicated to other technical warrant holders and to his/her network of trusted agents and to others involved in the technical discipline with the Agency and its contractors.

CE: Establish communication channels among warrant holders.

STWH: Maintain real-time communications with the program/project to ensure timely access by the technical authority to program/project information, impending decisions, and analysis or verification results.

DTWH: Establish and maintain effective communication channels and networks with trusted agents and with in-line engineers.

Trusted Agents: Provide information to the TWHs about a specific project.

In-line engineers: Provide unbiased technical positions to the warrant holders, S&MA, trusted agents, and programs/projects.

CE: Consolidate TWH reports and schedule interface meetings with the warrant holders.

OSMA: Conduct or oversee the conduct of incident/accident investigation (root cause analysis).

1d. Decision-making must include transparent and explicit consideration of both safety and programmatic concerns.

Office of Chief Engineer: Update existing NASA direction to ensure that program/project managers must comply with the decisions of the independent technical authority for matters affecting safe and reliable operations.

CE: Obtain "buy-in" and commitment (both management and engineering) throughout the Agency to the ITA program.

CE: Resolve conflicts that are raised to his/her level.

Program/Project Mgr: In event of a disagreement with TWH, explore alternatives that would allow achieving mutual agreement and, if cannot, shall raise issue up chain of command.

Mission Director: Address executive-level issues and interfaces with the ITA to resolve differences not reconciled at the interface between a warrant holder and a program/project manager.

OSMA: Suspend any operation or program activity that presents an unacceptable risk to personnel, property, or mission success and provide guidance for corrective action.

S&MA

- Perform reliability and safety assessments.
- Intervene in any activity under its purview (readiness review, design review, operation) necessary to avoid an unnecessary safety risk.

1e. The Agency must provide for effective assessment and improvement in safety-related decision making.

CE: Develop metrics and performance measures for the effectiveness of the Technical Warrants.

Headquarters Center Executive: For their Center, develop and execute a plan to monitor the conduct of the ITA.

2. Safety-related technical decision-making must be done by eminently qualified experts [with broad engagement of the full workforce.]

2a. Technical authority must be credible (executed using credible personnel, technical requirements, and decision-making tools).

CE: Approve selection of technical warrant holders. TWHs shall be appointed on the basis of proven credibility from demonstrated knowledge, experience, and capability. The TWH shall be the individual best able to do the job considering technical expertise, leadership, skill, and willingness to accept the accountability of the job.

CE: Determine and appoint new warrant areas and TWHs as appropriate to maintain integrity of the technical authority process.

STWH. Train and mentor potential successors.

DTWH. Train and mentor potential successors.

Center-Director: Ensure workforce competencies support TWH succession planning.

CE: Ensure maintenance of individual technical expertise throughout the Agency adequate to ensure safe and reliable systems.

STWH: Maintain their level of technical expertise in technologies and specialties of their warranted system(s) and also currency in program efforts that affect the application of technical requirements.

DTWH:

- Monitor the general health of their warranted discipline throughout the Agency and provide recommendations for improvement (tools, techniques, and personnel) to the Engineering Management Board, the Chief Engineer, and other Agency and Center organizations that can improve the health of the warranted discipline.
- Communicate best practices for their warranted discipline throughout the Agency
- Ensure technical personnel supporting programs/projects are using adequate tools, equipment, and techniques that meet current expectations for the discipline and for the end products.

CE: Regularly assess the credibility and performance of the individual TWHs and provide input into the individual TWH's performance appraisal.

CE: Revoke the warrant of any TWH judged to be not capable of continuing to perform the responsibilities of a TWH.

2b. Technical authority must be clear and unambiguous regarding the authority, responsibility, and accountability of participants. (Warrants must have defined scope, authority, responsibility, and accountability.)

CE: Delegate authority to individuals across the Agency through a system of technical warrants

STWH:

- Select and train a group of Trusted Agents
- Establish and maintain effective communication channels and networks with his or her trusted agents and with in-line engineers.

DTWH:

- Select and train a group of Trusted Agents to assist in fulfilling technical warrant holder responsibilities. These trusted agents will be consulting experts across the Agency with knowledge in the area of interest and unique knowledge and skills in the discipline and sub-discipline areas.
- Establish and maintain effective communication channels with his or her trusted agents and with in-line engineers.

Program/Project Mgr: Ensure that a full understanding of ITA is communicated through the program/project team

Center Director: Ensure each technical competency/discipline represented at the Center has a working agreement with the Agency DTWH for that technical discipline. (Agreement provides avenue for ultimate exercise of TA and provides connectivity to technical disciplines across the Agency.)

Center ITA Manager: Act in an administrative capacity for ITA matters supporting the warrant holders:

(a) Coordinate resources with Line Engineering Directors or their representatives
(b) Communicate with other NASA Center's ITA personnel, NESC, OCE, to coordinate activities and resources

CE: Establish the Technical Warrant System consistently across the Agency.

2c. All technical decisions within the scope of the warrant as determined by the TWH and before being issued by the program must have the technical approval of the TWH for that area.

STWH:

- Provide input to engineering review boards, TIMs, and special technical issue topics to ensure that safety is a regular part of design.
- Participate in program/project technical forums and boards to maintain cognizance of technical issues and all safety-related issues.
- Integrate appropriate individual technical discipline warrant holder reviews and prepare integrated technical positions on safety-related issues.
- When a technical decision requires the approval of a DTWH, assure that the DTWHs have full access both to the program/project team and to pertinent technical information before a technical decision is rendered and delivered to the program/project.

DTWH:

- Provide assessment of technical issues as required.
- Assist STWHs in evaluating requirements, implementation, variances and waiver requests involving the warranted technical discipline.
  - Document all methodologies, actions/closures, and decisions made.
  - Maintain OQE to support decisions and recommendations.

2d. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making.

We could find no specific parts of the implementation plan that addressed this requirement

3. Safety analyses must be available and used starting in the early acquisition, requirements development, and design processes.

3a. High-quality system hazard analyses must be created.

CE: Owns the FMEA /CIL and hazard analysis and updating systems

STWH: Approve the technical methodologies used to develop FMEA/CIL, trending analysis, hazard, and risk analyses.

CE: Determine what is or is not an anomalous event and perform trend analysis (or ensure it is performed) as well as root cause and hazard analyses on them.

CE: Conduct failure, hazard, and risk analyses or ensure their quality is acceptable. (Note: Safety, risk, and hazard analyses, formerly accomplished outside the purview of engineering and after the completion of the technical product, are now included in the technical products approved by the TWHs.)

In-line engineers: Conduct system safety engineering, including incorporation of safety and reliability design standards, system safety and reliability analyses, and incorporation of the analysis results into the system or component design, development, and operation.

- For in-house activities, perform hazard and risk analysis, system safety design, failure modes and effects analysis, and identification of critical items for in-house activities.
- For contracted activities, evaluate the contractor produced analyses and incorporation of results into contractor products.

STWH:

- Approve final safety and reliability engineering analyses to be incorporated into the technical product provided to the program/project.
- Initiate special investigations if he/she deems further evaluation or testing is prudent for risk quantification if technical boundaries have been exceeded or if alternative technical options may be required to solve a complex issue

(i.) Request the investigation from the project by negotiating with program/project manager and drawing on in-line engineering under program/project funding.
(ii.) In special cases, perform independent investigations funded by ITA or NESC.

System Engineering and Integration:

It seems like SE&I should have some role here to ensure that system hazards are handled correctly, but we could not find it in the implementation plan.

OSMA

- Audit adequacy of system safety engineering on projects and line engineering organizations.
- Conduct trend analysis, problem tracking, and maintain a lessons-learned system

CE: Initiate special investigations using NESC.

NESC: Provide independent review of technical issues. Acts as a resource for ITA and for technical warrant holders.

CE: Determine what is or is not an anomalous event and perform trend analysis (or ensure it is performed) as well as root cause and hazard analyses on them.

3b. Personnel must have the capability to produce high-quality safety analyses.

CE: Ensure maintenance of individual technical expertise throughout the Agency adequate to ensure safe and reliable systems.

STWH: Maintain their level of technical expertise in technologies and specialties of their warranted system(s) and also currency in program efforts that affect the application of technical requirements.

DTWH:

- Monitor the general health of their warranted discipline throughout the Agency and provide recommendations for improvement (tools, techniques, and personnel) to the Engineering Management Board, the Chief Engineer, and other Agency and Center organizations that can improve the health of the warranted discipline.
- Communicate best practices for their warranted discipline throughout the Agency
- Ensure technical personnel supporting programs/projects are using adequate tools, equipment, and techniques that meet current expectations for the discipline and for the end products.

3c. Engineers and managers must be trained to use the results of hazard analyses in their decision-making.

We could find nothing in the implementation plan where this requirement is addressed. It is important as currently misunderstanding of hazard analysis and the difference between safety and reliability are a problem for most managers and many engineers. The Discipline Technical

Warrant Holder for System Safety has the responsibility for assessing and maintaining expertise among the engineers but not among the managers.

3d. Adequate resources must be applied to the hazard analysis process.

We could find no specific parts of the implementation plan that addressed this requirement. In fact, the distributed and poorly defined responsibility for the hazard analysis process may lead to coordination problems where adequate resources are not applied.

3e. Hazard analyses 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).

CE: Ensure that results of safety and risk analyses are applied early in the program design activities.

STWH: Ensure hazard analyses are delivered to and used by design engineers while still time to affect design. Enforce concept that FMEA and hazard analysis will be used as part of the design process, not developed after the design is complete.

System Engineering and Integration:

SE&I should be involved here, but we could not find a clear explanation of their role and responsibilities.

Contractors:

The role and responsibilities of contractors is not clearly explained.

3f. Hazard analyses must be elaborated (refined and extended) and updated as the design evolves and test experience is acquired.

Who is responsible for this requirement? It should not be OSMA as the hazard analyses and logs should be maintained by the line-engineers who are creating the hazard analyses (see above).

3g. During operations, hazard logs must be maintained and used as experience is acquired. All in-flight anomalies must be evaluated for their hazard potential.

Who is responsible for this requirement? It should not be OSMA as the hazard analyses and logs should be maintained by the line-engineers who are creating the hazard analyses (see above).

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.

CE: Develop, assure, and maintain a technical conscience throughout the engineering community (i.e., develop a culture with personal responsibility to provide safe and reliable technical products coupled with an awareness of the avenues available to raise and resolve technical concerns

CE: Create a system in which technical conscience can and will be exercised, i.e., individuals raising technical conscience issues have a means to assure their concern is addressed completely, in a timely manner, and without fear of retribution or damage to their career.

CE: Ensure that technical conscience communication channels remain functional and that blockages and delays do not ensure, e.g., ensure there is no more than two layers between the individual raising the concern and the ultimate technical authority with the responsibility to resolve it.

STWH: Lead the technical conscience for the warranted system(s).

- Identify technical issues
- Listen to technical personnel raising issues
- Act proactively to identify and implement solutions.
- Provide feedback on the disposition of the concern to the person who reported it in the first place.
- Raise unresolved technical conscience issues to the Chief Engineer (ITA).

DTWH: Lead the technical conscience for the warranted discipline

- Identify technical issues
- Listen to technical personnel raising issues
- Act proactively to identify and implement solutions.
- Provide feedback on the disposition of the concern to the person who reported it in the first place
- Raise unresolved technical conscience issues to the Chief Engineer (ITA).

Center-Director: Develop a technical conscience at the Center that includes accountability for sound technical decisions and the ability to raise engineering issues and concerns affecting the safe and reliable operations that cannot be resolved through programs or projects at the Center, to the Agency Technical Warrant Holders.

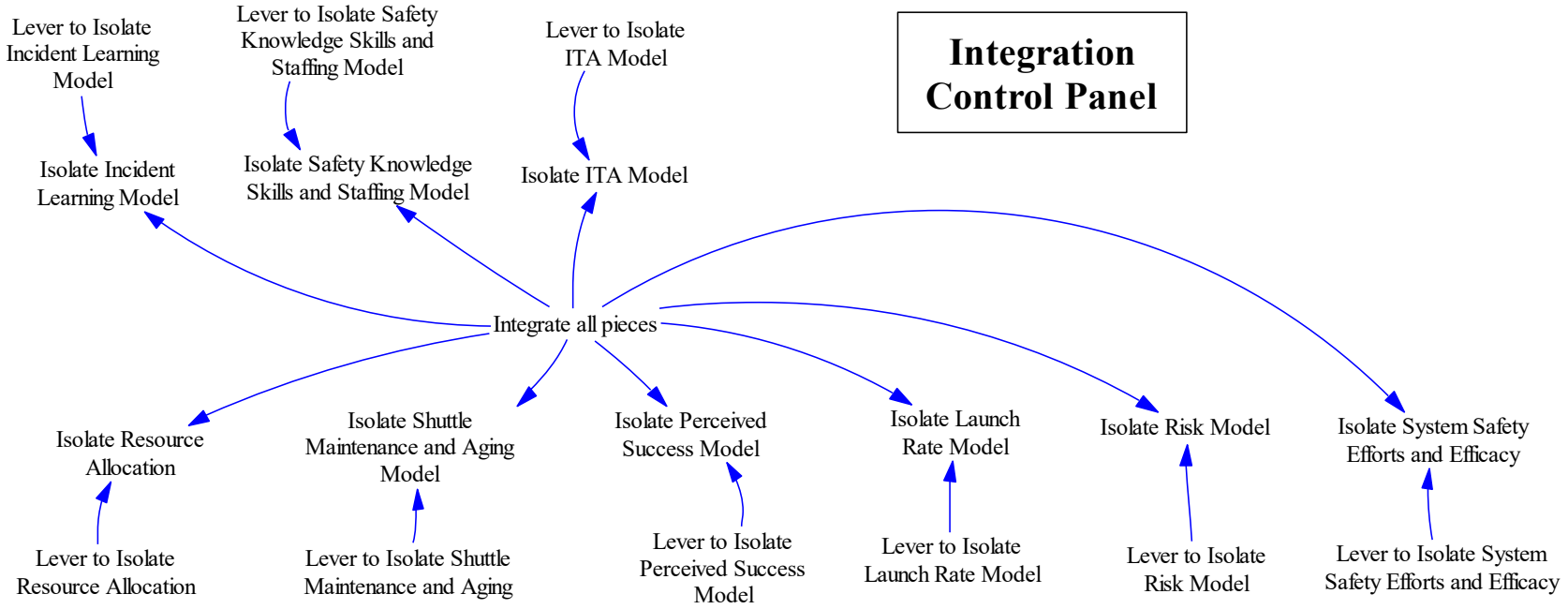
In-line engineers: Act as the technical conscience of the Agency.

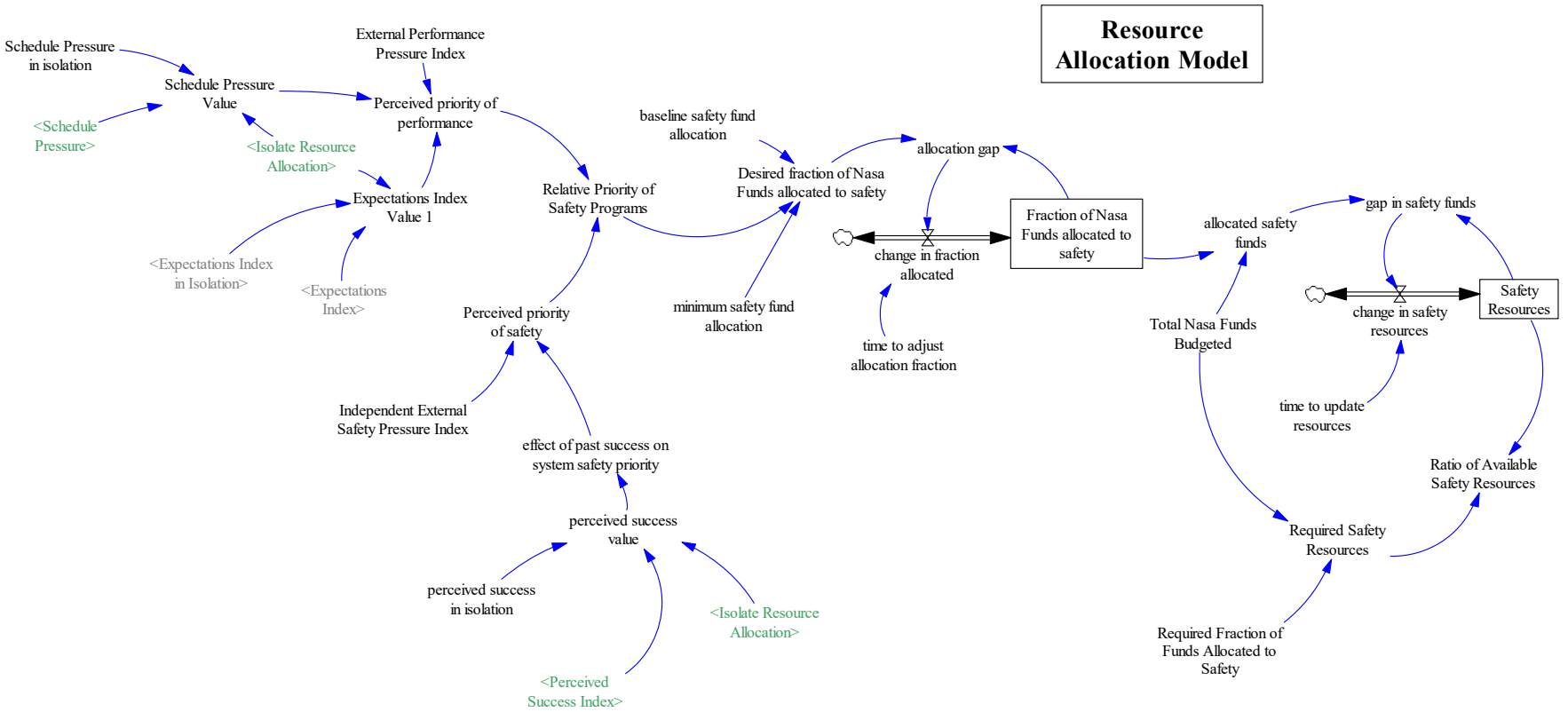
Contractors: Do contractors have the ability to raise issues of technical conscience?

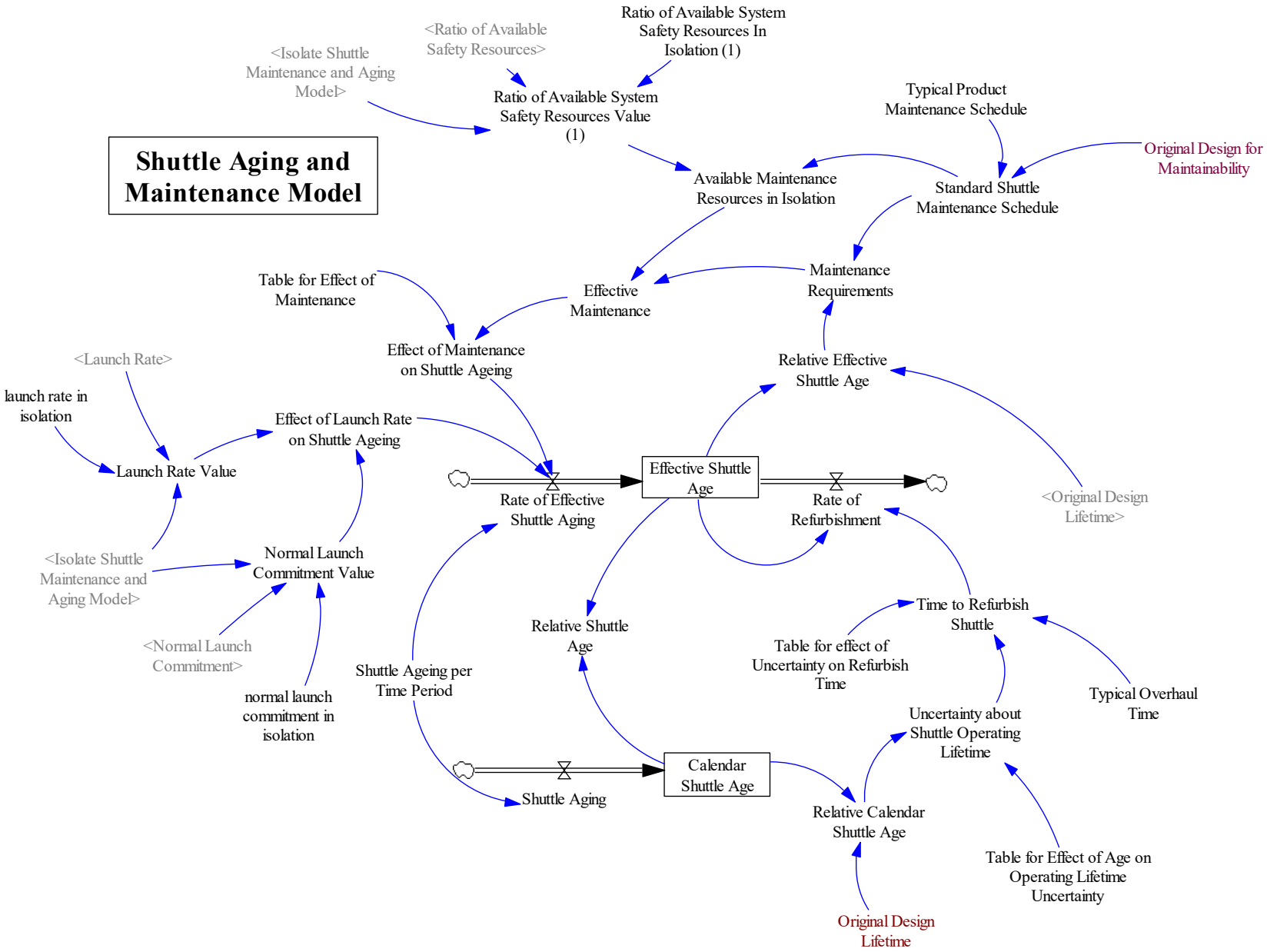
4a. Appeals channels must be established to surface complaints and concerns about aspects of the technical authority structure that are not functioning appropriately.

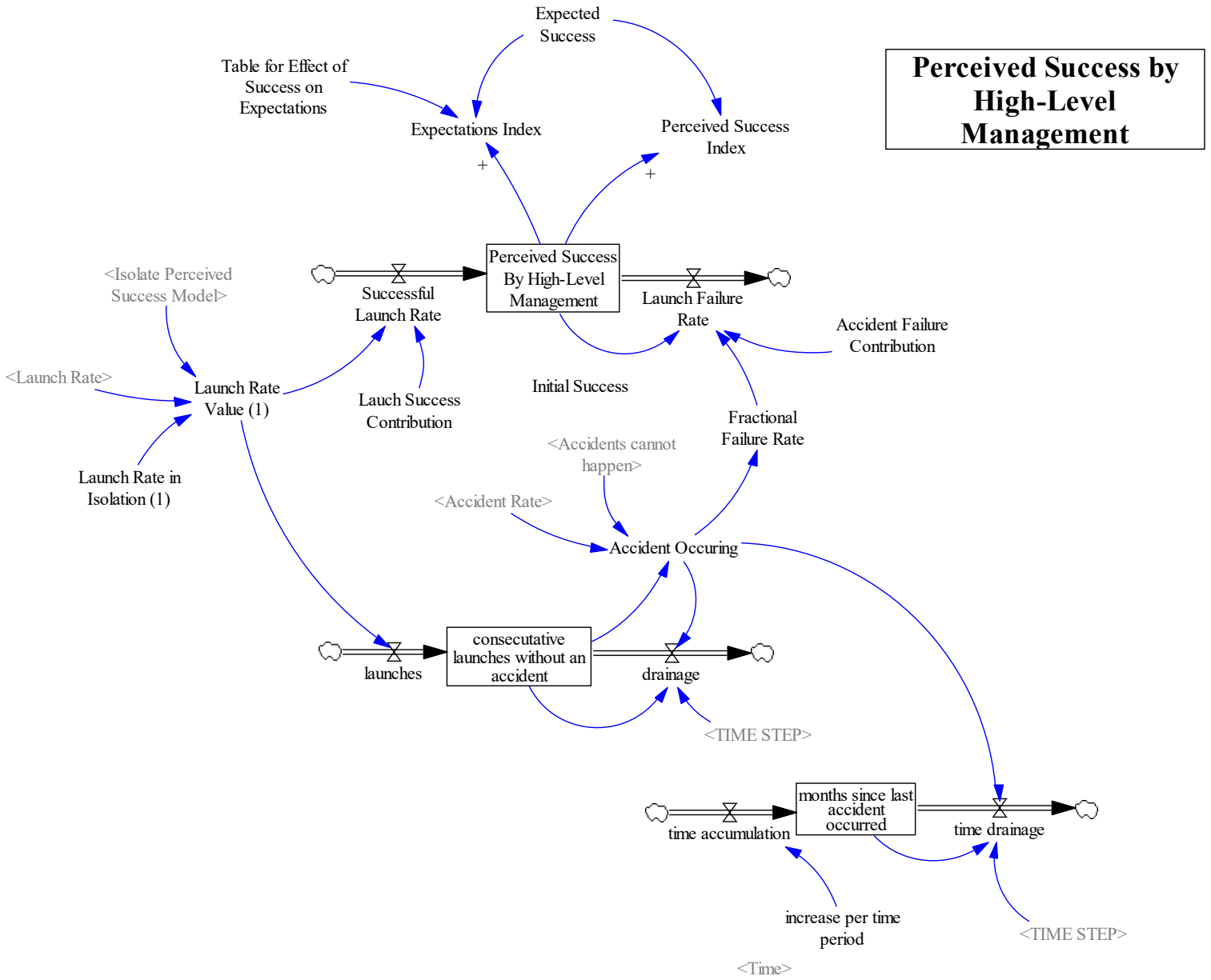
We could find no channel or procedure for raising technical conscience concerns about the operation of the technical warrant holders themselves, as they seem to be the route for expressing concerns.

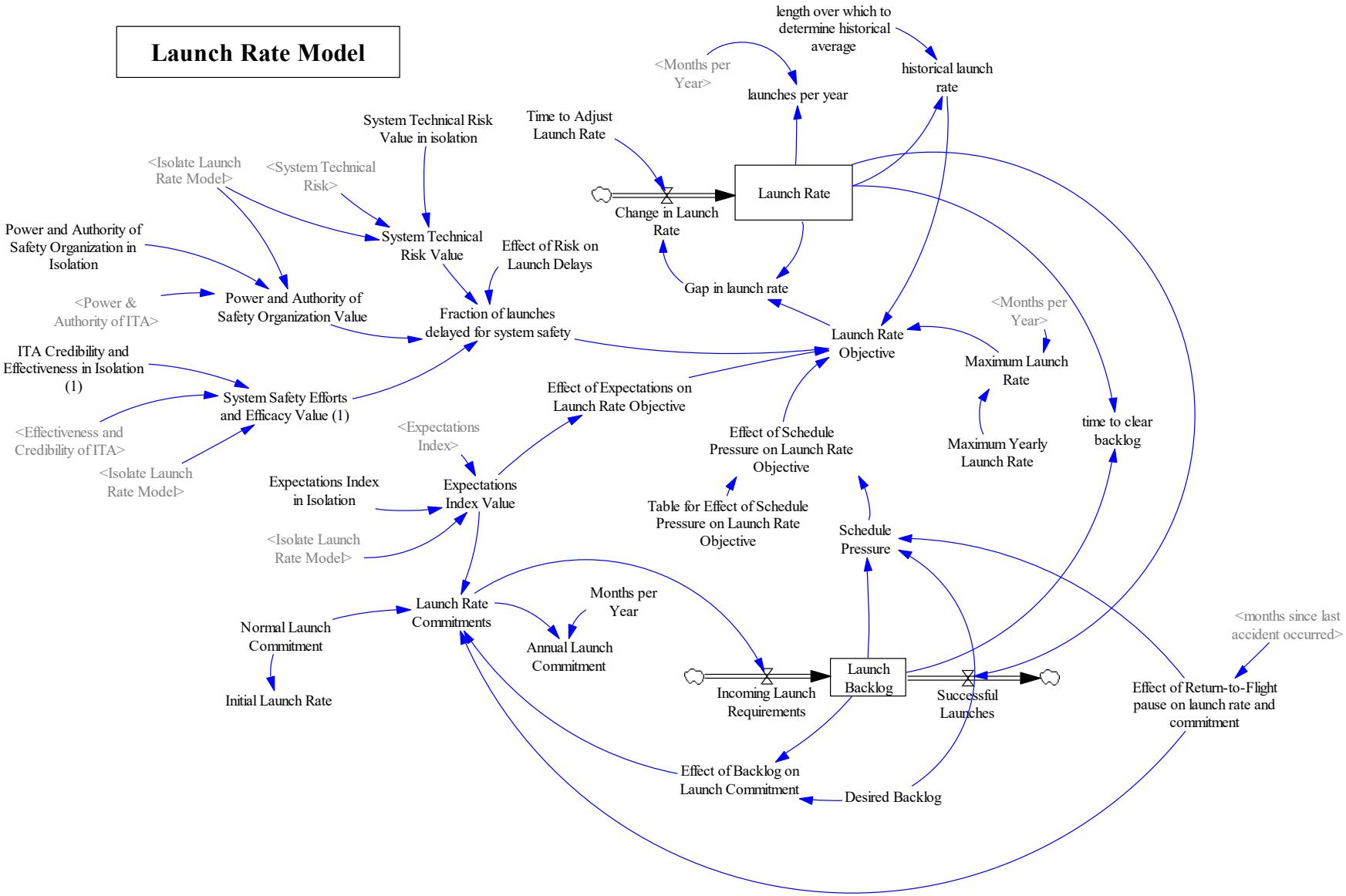
D.3 System Dynamics Model of NASA Manned Space Program with ITA

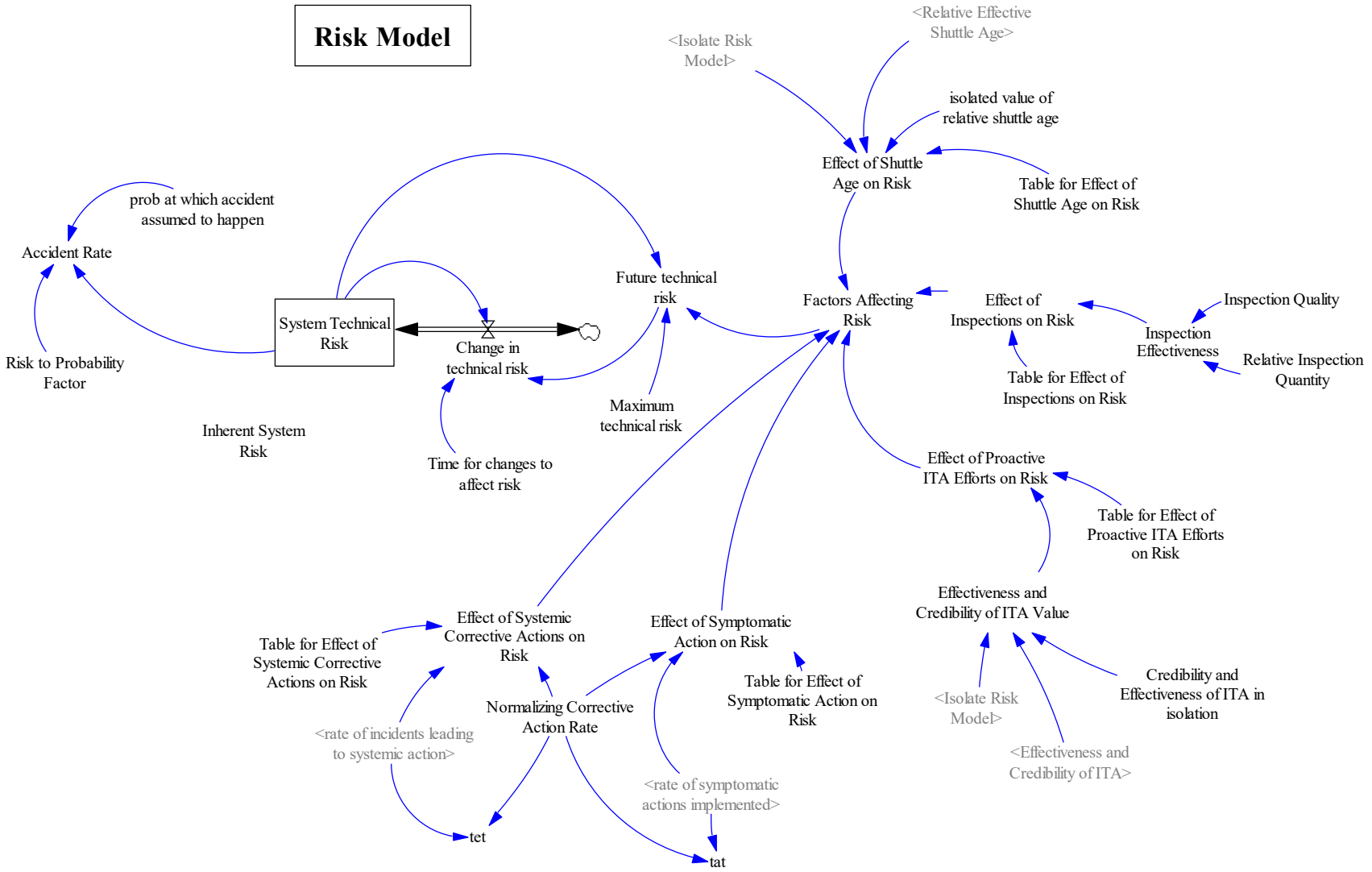

Integration Control Panel
Lever to Isolate Incident Learning Model
Lever to Isolate Safety Knowledge Skills and Staffing Model
Lever to Isolate ITA Model
Isolate Incident Learning Model
Isolate Safety Knowledge Skills and Staffing Model
Isolate ITA Model
Integrate all pieces
Isolate Resource Allocation
Isolate Shuttle Maintenance and Aging Model
Isolate Perceived Success Model
Isolate Launch Rate Model
Isolate Risk Model
Isolate System Safety Efforts and Efficacy
Lever to Isolate Resource Allocation
Lever to Isolate Shuttle Maintenance and Aging
Lever to Isolate Perceived Success Model
Lever to Isolate Launch Rate Model
Lever to Isolate Risk Model
Lever to Isolate System Safety Efforts and Efficacy

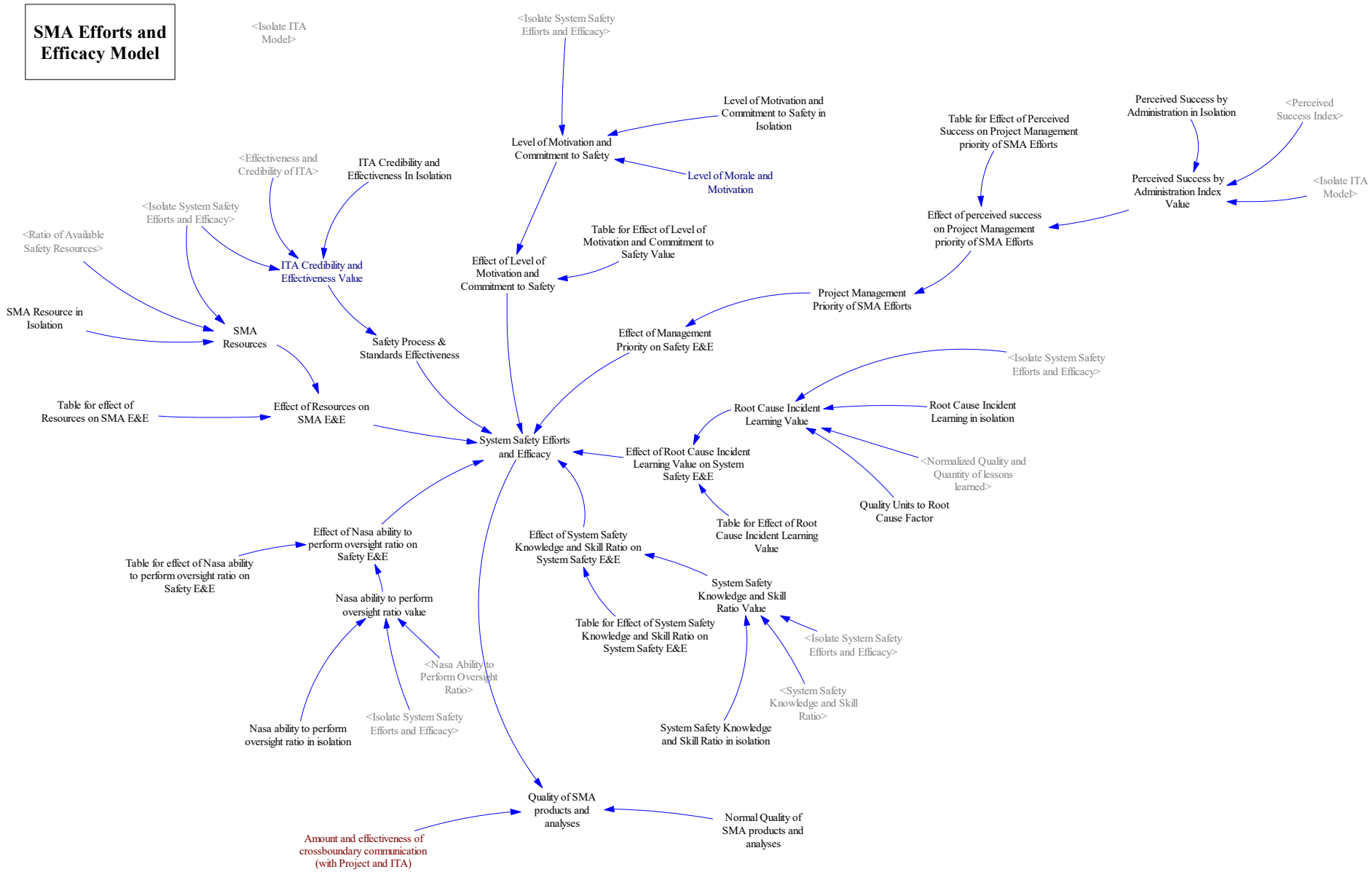

Resource Allocation Model
Schedule Pressure in isolation
Schedule Pressure Value
<Schedule Pressure>
<Isolate Resource Allocation>
External Performance Pressure Index
Perceived priority of performance
Expectations Index Value 1
<Expectations Index in Isolation>
<Expectations Index>
Relative Priority of Safety Programs
baseline safety fund allocation
Desired fraction of Nasa Funds allocated to safety
allocation gap
change in fraction allocated
Fraction of Nasa Funds allocated to safety
time to adjust allocation fraction
minimum safety fund allocation
Perceived priority of safety
Independent External Safety Pressure Index
effect of past success on system safety priority
perceived success value
perceived success in isolation
<Isolate Resource Allocation>
<Perceived Success Index>
allocated safety funds
Total Nasa Funds Budgeted
gap in safety funds
change in safety resources
Safety Resources
time to update resources
Ratio of Available Safety Resources
Required Safety Resources
Required Fraction of Funds Allocated to Safety


Shuttle Aging and Maintenance Model
<Isolate Shuttle Maintenance and Aging Model>
<Ratio of Available Safety Resources>
Ratio of Available System Safety Resources In Isolation (1)
Ratio of Available System Safety Resources Value (1)
Typical Product Maintenance Schedule
Original Design for Maintainability
Available Maintenance Resources in Isolation
Standard Shuttle Maintenance Schedule
Table for Effect of Maintenance
Effective Maintenance
Maintenance Requirements
Effect of Maintenance on Shuttle Ageing
Relative Effective Shuttle Age
<Launch Rate>
launch rate in isolation
Effect of Launch Rate on Shuttle Ageing
Launch Rate Value
Effective Shuttle Age
Rate of Effective Shuttle Aging
Rate of Refurbishment
<Original Design Lifetime>
<Isolate Shuttle Maintenance and Aging Model>
Normal Launch Commitment Value
Relative Shuttle Age
Time to Refurbish Shuttle
<Normal Launch Commitment>
normal launch commitment in isolation
Shuttle Ageing per Time Period
Table for effect of Uncertainty on Refurbish Time
Typical Overhaul Time
Uncertainty about Shuttle Operating Lifetime
Calendar Shuttle Age
Shuttle Aging
Relative Calendar Shuttle Age
Table for Effect of Age on Operating Lifetime Uncertainty
Original Design Lifetime

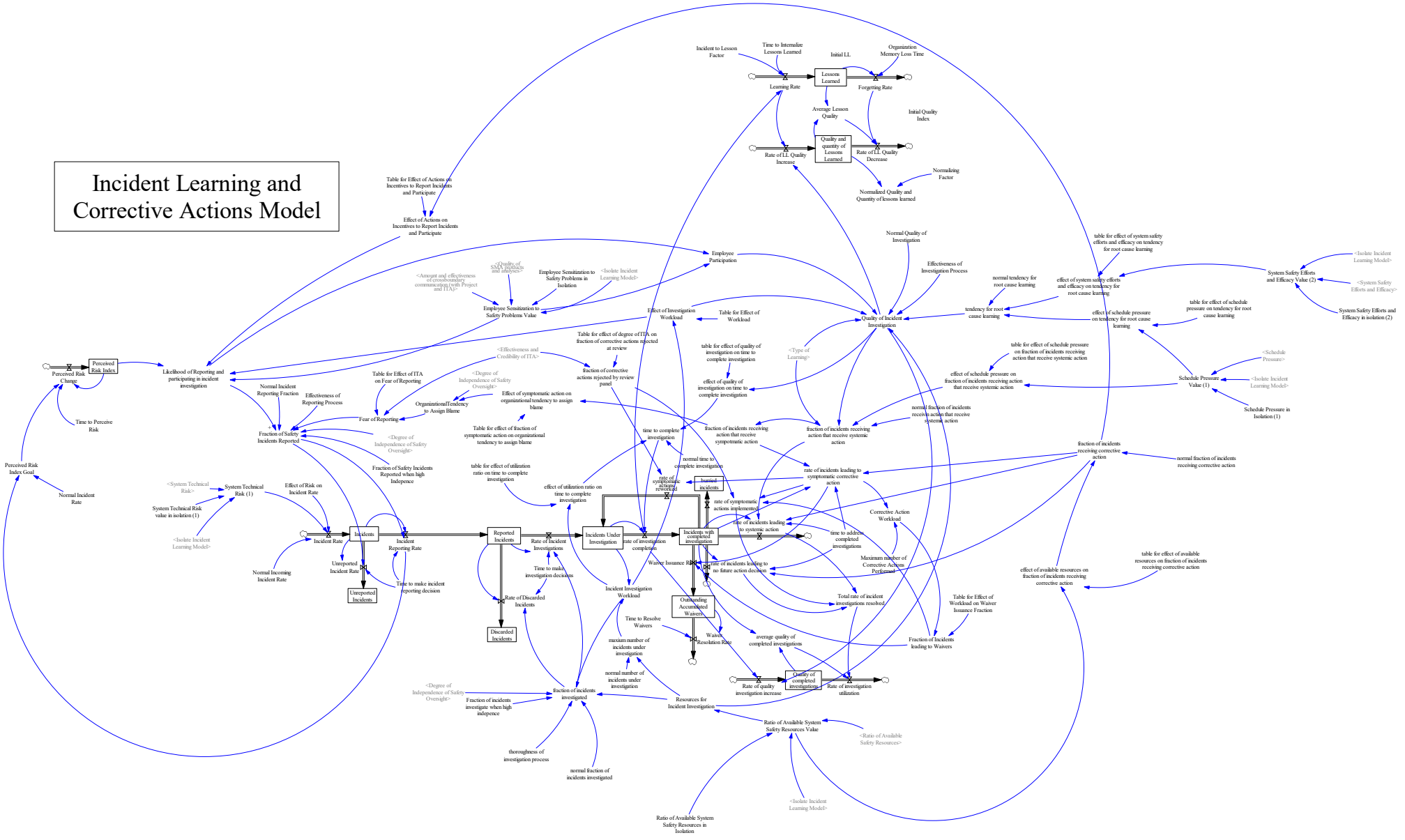

Perceived Success by High-Level Management
Expected Success
Table for Effect of Success on Expectations
Expectations Index
Perceived Success Index
+
+
Perceived Success By High-Level Management
<Isolate Perceived Success Model>
Successful Launch Rate
Launch Failure Rate
Accident Failure Contribution
<Launch Rate>
Launch Rate Value (1)
Lauch Success Contribution
Initial Success
Fractional Failure Rate
<Accidents cannot happen>
Launch Rate in Isolation (1)
<Accident Rate>
Accident Occuring
consecutative launches without an accident
launches
drainage
<TIME STEP>
months since last accident occurred
time accumulation
time drainage
increase per time period
<TIME STEP>
<Time>

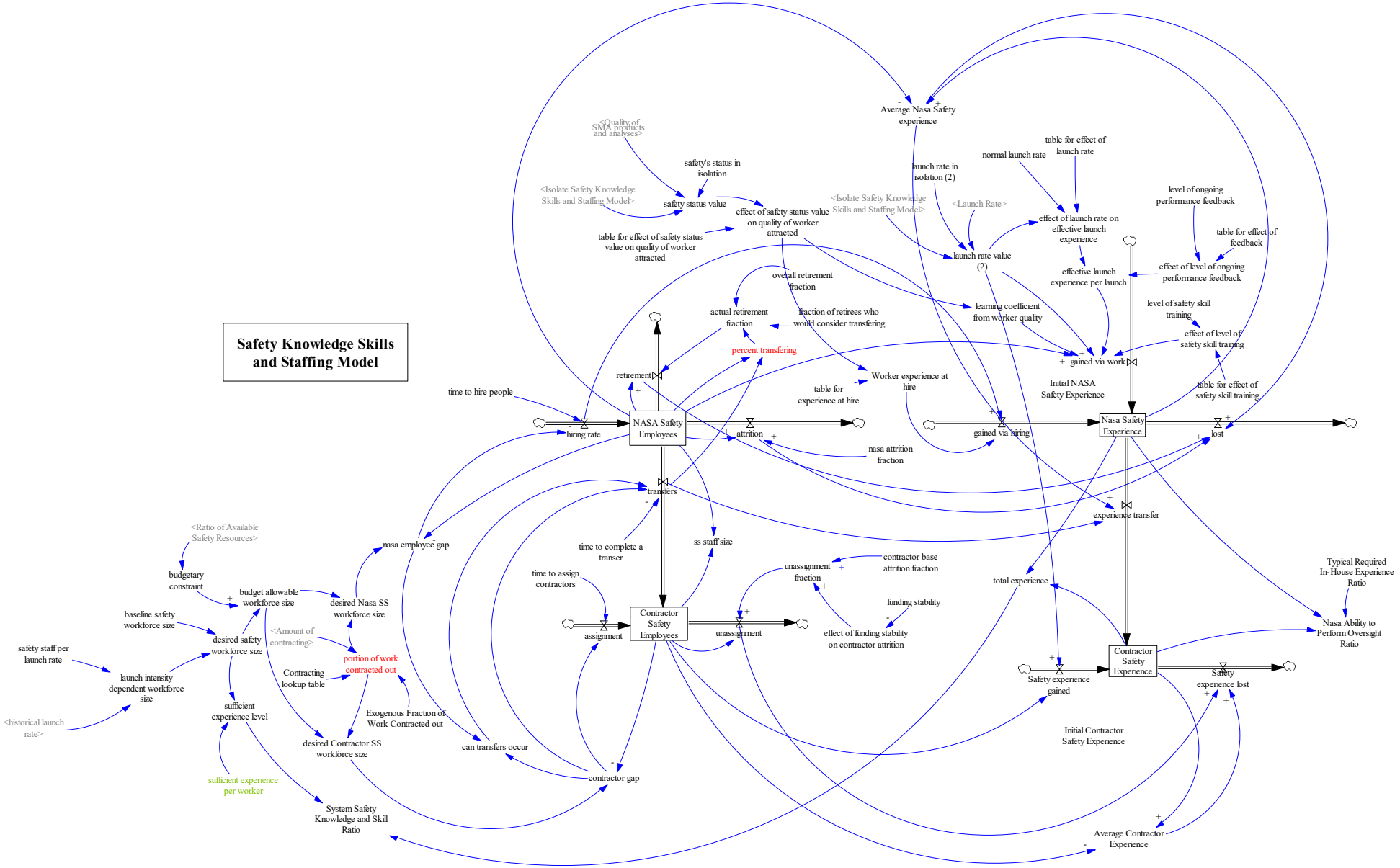

Launch Rate Model
length over which to determine historical average
<Months per Year>
launches per year
historical launch rate
System Technical Risk Value in isolation
Time to Adjust Launch Rate
<Isolate Launch Rate Model>
<System Technical Risk>
Launch Rate
Change in Launch Rate
Power and Authority of Safety Organization in Isolation
System Technical Risk Value
Effect of Risk on Launch Delays
Gap in launch rate
<Power & Authority of ITA>
Power and Authority of Safety Organization Value
Fraction of launches delayed for system safety
Launch Rate Objective
<Months per Year>
Maximum Launch Rate
ITA Credibility and Effectiveness in Isolation (1)
System Safety Efforts and Efficacy Value (1)
Effect of Expectations on Launch Rate Objective
time to clear backlog
<Effectiveness and Credibility of ITA>
<Isolate Launch Rate Model>
<Expectations Index>
Effect of Schedule Pressure on Launch Rate Objective
Maximum Yearly Launch Rate
Expectations Index in Isolation
Expectations Index Value
Table for Effect of Schedule Pressure on Launch Rate Objective
Schedule Pressure
<Isolate Launch Rate Model>
Launch Rate Commitments
Months per Year
Normal Launch Commitment
Annual Launch Commitment
<months since last accident occurred>
Launch Backlog
Incoming Launch Requirements
Successful Launches
Effect of Return-to-Flight pause on launch rate and commitment
Initial Launch Rate
Effect of Backlog on Launch Commitment
Desired Backlog

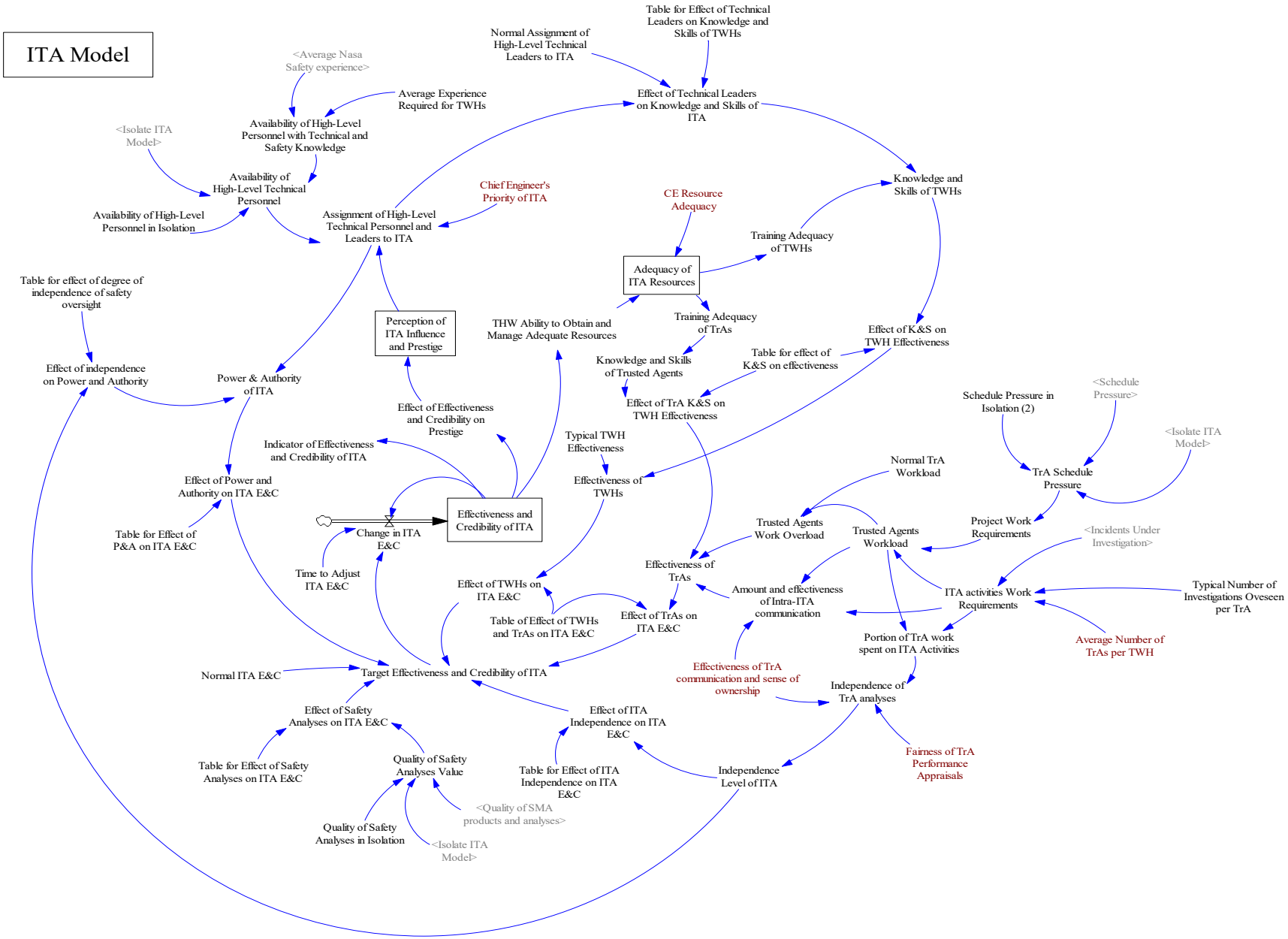

Risk Model
<Isolate Risk Model>
<Relative Effective Shuttle Age>
isolated value of relative shuttle age
Effect of Shuttle Age on Risk
Table for Effect of Shuttle Age on Risk
prob at which accident assumed to happen
Accident Rate
Risk to Probability Factor
System Technical Risk
Change in technical risk
Future technical risk
Factors Affecting Risk
Effect of Inspections on Risk
Inspection Quality
Inspection Effectiveness
Relative Inspection Quantity
Table for Effect of Inspections on Risk
Inherent System Risk
Time for changes to affect risk
Maximum technical risk
Effect of Proactive ITA Efforts on Risk
Table for Effect of Proactive ITA Efforts on Risk
Effectiveness and Credibility of ITA Value
Credibility and Effectiveness of ITA in isolation
<Isolate Risk Model>
<Effectiveness and Credibility of ITA>
Effect of Systemic Corrective Actions on Risk
Table for Effect of Systemic Corrective Actions on Risk
Effect of Symptomatic Action on Risk
Table for Effect of Symptomatic Action on Risk
Normalizing Corrective Action Rate
<rate of incidents leading to systemic action>
<rate of symptomatic actions implemented>
tet
tat


SMA Efforts and Efficacy Model
<Isolate ITA Model>
<Isolate System Safety Efforts and Efficacy>
Level of Motivation and Commitment to Safety in Isolation
Level of Motivation and Commitment to Safety
Level of Morale and Motivation
Table for Effect of Perceived Success on Project Management priority of SMA Efforts
Perceived Success by Administration in Isolation
<Perceived Success Index>
Perceived Success by Administration Index Value
<Isolate ITA Model>
Effect of perceived success on Project Management priority of SMA Efforts
<Effectiveness and Credibility of ITA>
ITA Credibility and Effectiveness In Isolation
<Isolate System Safety Efforts and Efficacy>
<Ratio of Available Safety Resources>
ITA Credibility and Effectiveness Value
Table for Effect of Level of Motivation and Commitment to Safety Value
Effect of Level of Motivation and Commitment to Safety
Project Management Priority of SMA Efforts
SMA Resource in Isolation
SMA Resources
Safety Process & Standards Effectiveness
Effect of Management Priority on Safety E&E
<Isolate System Safety Efforts and Efficacy>
Table for effect of Resources on SMA E&E
Effect of Resources on SMA E&E
Root Cause Incident Learning Value
Root Cause Incident Learning in isolation
System Safety Efforts and Efficacy
Effect of Root Cause Incident Learning Value on System Safety E&E
<Normalized Quality and Quantity of lessons learned>
Quality Units to Root Cause Factor
Table for Effect of Root Cause Incident Learning Value
Effect of Nasa ability to perform oversight ratio on Safety E&E
Effect of System Safety Knowledge and Skill Ratio on System Safety E&E
Table for effect of Nasa ability to perform oversight ratio on Safety E&E
System Safety Knowledge and Skill Ratio Value
Nasa ability to perform oversight ratio value
Table for Effect of System Safety Knowledge and Skill Ratio on System Safety E&E
<Isolate System Safety Efforts and Efficacy>
<Nasa Ability to Perform Oversight Ratio>
<System Safety Knowledge and Skill Ratio>
Nasa ability to perform oversight ratio in isolation
<Isolate System Safety Efforts and Efficacy>
System Safety Knowledge and Skill Ratio in isolation
Quality of SMA products and analyses
Amount and effectiveness of crossboundary communication (with Project and ITA)
Normal Quality of SMA products and analyses

Incident Learning and Corrective Actions Model




Safety Knowledge Skills and Staffing Model
Average Nasa Safety experience
<Quality of SMA products and analyses>
safety's status in isolation
<Isolate Safety Knowledge Skills and Staffing Model>
safety status value
effect of safety status value on quality of worker attracted
table for effect of safety status value on quality of worker attracted
launch rate in isolation (2)
normal launch rate
table for effect of launch rate
<Isolate Safety Knowledge Skills and Staffing Model>
<Launch Rate>
effect of launch rate on effective launch experience
launch rate value (2)
level of ongoing performance feedback
table for effect of feedback
effective launch experience per launch
effect of level of ongoing performance feedback
overall retirement fraction
actual retirement fraction
fraction of retirees who would consider transfering
learning coefficient from worker quality
level of safety skill training
effect of level of safety skill training
percent transfering
gained via work
retirement
Worker experience at hire
table for experience at hire
Initial NASA Safety Experience
table for effect of safety skill training
time to hire people
hiring rate
NASA Safety Employees
attrition
gained via hiring
Nasa Safety Experience
lost
nasa attrition fraction
transfers
experience transfer
<Ratio of Available Safety Resources>
budgetary constraint
budget allowable workforce size
desired Nasa SS workforce size
nasa employee gap
time to complete a transer
ss staff size
time to assign contractors
assignment
Contractor Safety Employees
unassignment
unassignment fraction
contractor base attrition fraction
funding stability
effect of funding stability on contractor attrition
total experience
Typical Required In-House Experience Ratio
Nasa Ability to Perform Oversight Ratio
baseline safety workforce size
desired safety workforce size
<Amount of contracting>
portion of work contracted out
safety staff per launch rate
launch intensity dependent workforce size
Contracting lookup table
Exogenous Fraction of Work Contracted out
Contractor Safety Experience
Safety experience gained
Safety experience lost
<historical launch rate>
sufficient experience level
desired Contractor SS workforce size
can transfers occur
Initial Contractor Safety Experience
sufficient experience per worker
contractor gap
System Safety Knowledge and Skill Ratio
Average Contractor Experience


ITA Model
<Average Nasa Safety experience>
Average Experience Required for TWHs
Availability of High-Level Personnel with Technical and Safety Knowledge
<Isolate ITA Model>
Availability of High-Level Technical Personnel
Availability of High-Level Personnel in Isolation
Normal Assignment of High-Level Technical Leaders to ITA
Table for Effect of Technical Leaders on Knowledge and Skills of TWHs
Effect of Technical Leaders on Knowledge and Skills of ITA
Knowledge and Skills of TWHs
Chief Engineer's Priority of ITA
Assignment of High-Level Technical Personnel and Leaders to ITA
CE Resource Adequacy
Adequacy of ITA Resources
Training Adequacy of TWHs
Training Adequacy of TrAs
Table for effect of degree of independence of safety oversight
Perception of ITA Influence and Prestige
THW Ability to Obtain and Manage Adequate Resources
Effect of K&S on TWH Effectiveness
Knowledge and Skills of Trusted Agents
Table for effect of K&S on effectiveness
Effect of TrA K&S on TWH Effectiveness
Effect of independence on Power and Authority
Power & Authority of ITA
Effect of Effectiveness and Credibility on Prestige
Indicator of Effectiveness and Credibility of ITA
Typical TWH Effectiveness
Effectiveness of TWHs
Schedule Pressure in Isolation (2)
<Schedule Pressure>
<Isolate ITA Model>
TrA Schedule Pressure
Normal TrA Workload
Effect of Power and Authority on ITA E&C
Effectiveness and Credibility of ITA
Table for Effect of P&A on ITA E&C
Change in ITA E&C
Time to Adjust ITA E&C
Trusted Agents Work Overload
Trusted Agents Workload
Project Work Requirements
<Incidents Under Investigation>
Effectiveness of TrAs
Amount and effectiveness of Intra-ITA communication
ITA activities Work Requirements
Typical Number of Investigations Oveseen per TrA
Effect of TWHs on ITA E&C
Table of Effect of TWHs and TrAs on ITA E&C
Effect of TrAs on ITA E&C
Portion of TrA work spent on ITA Activities
Average Number of TrAs per TWH
Normal ITA E&C
Target Effectiveness and Credibility of ITA
Effectiveness of TrA communication and sense of ownership
Independence of TrA analyses
Effect of Safety Analyses on ITA E&C
Effect of ITA Independence on ITA E&C
Table for Effect of Safety Analyses on ITA E&C
Quality of Safety Analyses Value
Table for Effect of ITA Independence on ITA E&C
Independence Level of ITA
Fairness of TrA Performance Appraisals
<Quality of SMA products and analyses>
Quality of Safety Analyses in Isolation
<Isolate ITA Model>