INEEL/EXT-03-00661

Real-Time Risk and Fault Management in the Mission Evaluation Room for the International Space Station

W. R. Nelson
S. D. Novack

May 2003

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-03-00661

Real-Time Risk and Fault Management in the Mission Evaluation Room for the International Space Station

William R. Nelson
Steven D. Novack

May 2003

Idaho National Engineering and Environmental Laboratory

Idaho Falls, Idaho 83415

This work was sponsored by the
National Aeronautics and Space Administration
Under U.S. Department of Energy
Idaho Operations Office
Contract DE-AC07-99ID13727

ABSTRACT

Effective anomaly resolution in the Mission Evaluation Room (MER) of the International Space Station (ISS) requires consideration of risk in the process of identifying faults and developing corrective actions. Risk models such as fault trees from the ISS Probabilistic Risk Assessment (PRA) can be used to support anomaly resolution, but the functionality required goes significantly beyond what the PRA could provide. Methods and tools are needed that can systematically guide the identification of root causes for on-orbit anomalies, and to develop effective corrective actions that address the event and its consequences without undue risk to the crew or the mission. In addition, an overall information management framework is needed so that risk can be systematically incorporated in the process, and effectively communicated across all the disciplines and levels of management within the space station program. The commercial nuclear power industry developed such a decision making framework, known as the critical safety function approach, to guide emergency response following the accident at Three Mile Island in 1979.

This report identifies new methods, tools, and decision processes that can be used to enhance anomaly resolution in the ISS Mission Evaluation Room. Current anomaly resolution processes were reviewed to identify requirements for effective real-time risk and fault management. Experience gained in other domains, especially the commercial nuclear power industry, was reviewed to identify applicable methods and tools. Recommendations were developed for next-generation tools to support MER anomaly resolution, and a plan for implementing the recommendations was formulated. The foundation of the proposed toolset will be a “Mission Success Framework” designed to integrate and guide the anomaly resolution process, and to facilitate consistent communication across disciplines while focusing on the overriding importance of mission success.

CONTENTS

FIGURES

Real-Time Risk and Fault Management in the Mission Evaluation Room for the International Space Station

SUMMARY

The recent loss of the space shuttle Columbia and her crew has highlighted the critical importance of risk and fault management for manned space missions. It is possible that for this event nothing could have been done once the vehicle was launched to prevent this tragedy. We will not know this until the investigation has clearly identified the cause of the accident.

For many on-orbit events however, effective tools to assess anomalies and identify and evaluate alternative corrective actions are absolutely essential. It is impossible to pre-analyze all possible events that could occur, or to train for recovery from each of them. No matter how rigorous the pre-analysis, there will always be a residual set of events and recovery actions left unaccounted for. In some cases the ability to analyze events as they occur on-orbit could mean the difference between life and death, or between success and failure of a mission.

Various tools have been developed to model and quantify the risks associated with human space flight. These are used primarily in the pre-launch phase, as aids to assess the overall risks of a particular vehicle or mission. When sufficient details are included in the risk models, they can be used to support design decisions, and to guide the development of contingency procedures for off-normal or emergency situations.

However, the application of such tools in real-time (i.e. in time to develop effective corrective actions for an ongoing anomaly) is a much more difficult proposition. Risk models developed pre-launch tend to represent a few envelope-defining scenarios, rather than the full spectrum of events that could occur in-flight. They typically model an assumed vehicle design that is "frozen in time," and are very difficult to update for the continually evolving states of a vehicle on-orbit. The models most commonly used for risk assessment are failure oriented fault trees, which are better suited to identifying the causes of faults rather than identifying and evaluating possible corrective actions for an incident in progress. For these reasons it will be necessary to modify and supplement currently available models and tools for effective use in real time for on-orbit anomalies.

The commercial nuclear industry was forced to take a hard look at the prevailing real-time risk and fault management paradigm following the 1979 accident at the Three Mile Island (TMI) nuclear power plant (NPP) in Pennsylvania. Prior to TMI, large risk models had been developed to support Probabilistic Risk Assessment (PRA) for quantifying the risks of nuclear power plant operations, and to compare those risks to more familiar risks such as cigarette smoking and commercial air travel. Emergency procedures for nuclear power plants were organized around the response to certain pre-analyzed "design basis accidents" (DBAs). Selecting a response for an ongoing event depended on an accurate classification of the origin of the specific event in progress. Risk models were rarely used as effective tools to support detailed design or operational decisions, and they were not available at all for real-time use in the case of an actual accident such as the one at TMI.

Post-accident investigations of Three Mile Island focused on the inadequacy of information in the control room for assessment of the event and selection of corrective actions. More effective use of various kinds of decision making tools including risk models was suggested as one way to address this serious shortcoming in real-time risk and fault management in nuclear power plants. Following TMI

focused research programs were organized around the world to explore different approaches for the management of real-time anomalies in nuclear power plants.

One of the most significant outcomes of the Three Mile Island accident was the development of a new philosophy of operations that focused on mission success rather the prevailing event-oriented approach that focused on identification and treatment of specific event scenarios. This new paradigm was referred to as the Critical Safety Function approach, and was based on success-oriented logic models rather than the failure models that were the logical foundation of the event-based approach. When both success and failure approaches were combined in the new Emergency Procedure Guidelines for nuclear power plants, the result was a robust approach for real-time risk and fault management. Although such an approach has been implemented in various forms in the procedures of nuclear power plants in the United States since TMI, implementation of computer-based systems to support emergency response has been much more limited. This is partly due to the conservative regulatory stance taken by the U.S. Nuclear Regulatory Commission (NRC), which wanted to ensure that the introduction of computer-based tools did not introduce new hazards into reactor operations. Thus the effectiveness of these tools has not yet been fully demonstrated in U.S. nuclear power plants. Implementation of computer-based tools in operating facilities has been more aggressive in other countries such as France, Germany, and Japan. Even so, the full potential of these tools remains unproven, because of the challenges of integrating computerized decision aids with human decision-making capabilities. The strengths of both human and computer must be effectively combined for successful performance of the overall problem solving process. This would be very difficult in the time-pressured but localized decision environment of the nuclear power plant control room. The distributed nature of real-time fault and risk management decisions for space operations will present different but equally significant challenges.

We believe that the effective integration of success-based models such as Critical Safety Functions with fault-based models such as fault trees, and their implementation in a computer-based form, has the potential to enhance real-time risk and fault management for space vehicles such as the Space Shuttle and the International Space Station (ISS). This report explores the possible application of these risk-based tools for use in the Mission Evaluation Room (MER) for the International Space Station. An integrated approach called the Mission Success Framework for real-time risk and fault management in the MER is described, as well as preliminary steps needed to develop and implement tools based on this approach.

BACKGROUND

NASA tasked the Idaho National Engineering and Environmental Laboratory (INEEL) to evaluate anomaly resolution activities and processes within the ISS Mission Evaluation Room, and to develop recommendations and initial steps to implement software-based support for real-time risk and fault management in the MER.

The Safety and Mission Assurance/Program Risk Branch of the International Space Station Program Office envisions three phases for implementing risk analysis capabilities for ISS:

1. Probabilistic Risk Assessment (PRA) for performing trade studies and sensitivity analyses for different ISS increments.
2. A fault tree tool for performing fault isolation and failure analysis for ISS operations.
3. The Risk Monitor, an integrated risk analysis tool for real-time monitoring.

Phase 1 of this sequence is already being implemented in the form of PRAs that have been performed for various increments of ISS assembly. Phase 2 has begun with the initial development of the Galileo fault tree tool for use in fault isolation and failure analysis in the ISS Mission Evaluation Room.

However, the application of Galileo to these tasks is only beginning at the present time, and much remains to be done before Galileo can serve as a full-featured tool for fault isolation and failure analysis. Phase 3, the development of the ISS Risk Monitor, has not yet begun.

One major objective of this project is to identify the remaining steps required to achieve Phase 2 of the planned risk assessment program, i.e. what additional functionality must be added to Galileo to comprise a full capability for fault isolation and failure analysis for the MER.

Another major objective of this project is to identify the high-level functions of the Phase 3 Risk Monitor, and to identify the initial steps for moving from the Phase 2 Galileo tool currently available to the fully integrated Risk Monitor.

PROJECT ORGANIZATION

Document review

The first task of this project was to review the documents that govern real-time risk and fault management in the ISS Mission Evaluation Room. This review focused on the following documents:

- Safety and Mission Assurance/Program Risk Mission Evaluation Room Console Operations Handbook for the International Space Station Program, SSP 50437 Revision C, August 2002.
- On-Orbit Anomaly Resolution Process Work Instruction, MGT-OA-019, Baseline, May 7, 2002.
- ISS System Problem Resolution Team (SPRT) Work Instruction, MGT-OA-018 Basic, February 2002.
- Probabilistic Risk Assessment of the International Space Station Phase III – Stage 12A.1 Configuration, Futron Corporation, June 2001.
- International Space Station Familiarization, Mission Operations Directorate Space Flight Training Division, TD9702, Revision B, CPN-1, October 18, 2001.
- System specific training manuals from the Space Flight Training Division series listed above.

Data Collection Visits

The second phase of the project was data collection in the Mission Evaluation Room in the Mission Control Center (MCC) at the Johnson Space Center (JSC). Two data collection visits were conducted. The first occurred on June 18-20, 2002 and focused on the following:

- Discussion of project objectives and plans with personnel from the International Space Station Program Office, Safety and Mission Assurance/Program Risk.
- Tour of the Mission Evaluation Room, discussions with MER safety console operators, and demonstration of computer tools and data sources available to safety console personnel.
- Discussions with a MER Manager focusing on the anomaly resolution process.
- Attendance at a daily MER tagup meeting.
- Attendance at a Flight Investigation Team (FIT) meeting focusing on overheating of the MCOR data collection computer.
- Orientation to the PHALCON power systems console in the Multi-Purpose Support Room (MPSR).
- Orientation to the ISS Flight Control Room (FCR) including monitoring of Flight Director communications with the ISS crew.

- Discussions regarding capabilities of the Galileo fault tree tool and the underlying analysis and calculation algorithms.

The second data collection visit occurred on September 5, 2002 and focused on the following:

- Discussion with Safety and Mission Assurance/Program Risk personnel about project objectives and progress.
- Discussions with MER safety console personnel and demonstration of available data sources.
- Attendance at a daily MER tagup meeting.
- Detailed discussions with a MER console operator focusing on Galileo functionality, selection of corrective actions, and detailed discussion of ongoing carbon dioxide removal assembly (CDRA) anomaly.
- Attendance at a Flight Investigation Team meeting focusing on the CDRA anomaly.
- Discussions with a MER manager focusing on the CDRA anomaly in progress and general approach for formulating and evaluating corrective actions.

Review of Experience in Other Industries

The next phase of the project was the review of experience gained in real-time risk and fault management in other comparable domains. The most relevant experience in using risk models in accident and emergency response comes from the commercial nuclear power industry in the United States and around the world. The suitability of this experience to space operations comes from a number of factors, but there are two that are essential:

- The nuclear industry is steeped in the use of risk assessment models and methods. The risk assessment perspective, particularly quantitative methods of Probabilistic Risk Assessment, reached maturity and universal acceptance in the nuclear industry. The bulk of applications in the commercial nuclear industry however have been focused on regulatory considerations rather than real time operations.
- The nuclear industry has spent twenty-five years since the Three Mile Island accident focusing on developing effective methods for accident management, including methods that explicitly use risk models to guide decision making, as well as many other approaches.

The NASA space operations community has much to gain by learning from the experience gained in the nuclear industry. The Idaho National Engineering and Environmental Laboratory has been intimately involved in both major risk management activities listed above. In addition, we have performed a series of projects for NASA over the past ten years, seeking to adapt risk-based methods from the nuclear industry for the specific design and operational needs of commercial aviation, air traffic management, and space operations. A major goal of this project is to apply this experience to identify effective approaches for real-time risk and fault management in the ISS Mission Evaluation Room.

Experience from other domains such as offshore oil and ongoing research of the NASA Engineering for Complex Systems (ECS) program was also reviewed to identify insights applicable to ISS real-time risk and fault management.

Review Galileo Fault Tree Tool and Its Application in the Mission Evaluation Room

The Galileo fault tree tool was reviewed to identify its current capabilities to carry out fault isolation and failure analysis for ISS operations. This was accomplished through demonstrations in the MER and interviews of MER safety console operators.

Identify Requirements

Based on the information gathered above, high-level requirements were developed for real-time risk and fault management in the ISS Mission Evaluation Room.

Develop Recommendations

The final task was to develop recommendations for providing the remaining functionality for the real-time tool for fault isolation and failure analysis, and preliminary steps needed to begin the development of the Risk Monitor, the integrated risk analysis tool for real-time monitoring.

MISSION EVALUATION ROOM REAL-TIME RISK AND FAULT MANAGEMENT

Prescribed Functions for Anomaly Resolution

The functions of real-time risk and fault management in the MER are focused in the activities of Anomaly Resolution Teams (ARTs) and Flight Investigation Teams (FITs), and particularly the role of the safety console operator in these processes. The two types of teams perform essentially the same anomaly resolution functions:

- Determine the immediate and short-term impacts of the anomaly to ISS systems, hardware, software, operations, and the on-orbit crew.
- Identify immediate and short-term corrective actions to resolve and/or mitigate the on-orbit impacts associated with the anomaly.
- Identify measures for preventing or minimizing recurrence of the anomaly on-orbit.
- Identify any other actions or controls required to ensure safety and mission assurance.

(Excerpted from *On-Orbit Anomaly Resolution Process Work Instruction*, MGT-OA-019, May 7, 2002)

The ISS Safety and Mission Assurance (S&MA) MER Console (commonly called the Safety Console) is represented in the ART/FIT anomaly resolution activities by the ART/FIT Point of Contact (POC). The primary functions performed by the POC in support of anomaly resolution include the following:

- Assist the ART/FIT in isolation of the on-orbit anomaly to the correct element, system, hardware, or software.
- Identify the required fault-tolerance and determine if the on-orbit anomaly resulted in the loss of a level of fault-tolerance. If so, assess the impacts of the lost level of fault tolerance.
- Assess ISS and crew safety on a continuous basis. Identify and concur with any safety-based constraints or workaround to on-orbit operations.

- Develop an applicable failure history
- Develop fault trees, as required.
- Identify worst-case effects and associated safety hazards.
- Develop risk assessment for ART/FIT developed work-around and corrective action option(s).

(Excerpted from *Safety and Mission Assurance/Program Risk Mission Evaluation Room Console Operations Handbook for the International Space Station Program,* SSP 50437 Revision C, August 2002.)

The functions listed above for the ART/FIT and particularly the MER Safety Console in anomaly resolution are the primary focus of this study. Since the functions of the ART and FIT are essentially similar (the ART is a more rigorous process used for more serious events) discussions of the ART in this report will apply (unless otherwise stated) to the FIT as well.

The basic anomaly resolution functions listed above can be translated into generic task descriptions as follows:

1. Catalog the symptoms of the anomaly.
2. Identify immediate and potential future consequences of the anomaly.
3. Assess current defense-in-depth and vulnerabilities to further degradation of defense-in-depth.
4. If possible, identify the root cause of the anomaly and contributing factors.
5. Identify potential corrective actions and workarounds.
6. Evaluate corrective actions and workarounds based on risk to the vehicle, crew, and mission.
7. Select the most desirable corrective actions and develop procedures for implementation.
8. Monitor implementation of the corrective actions and ensure that they have the desired effects.

These are the basic tasks that are the focus of the recommendations of this report.

It should be noted from the beginning that these tasks are not primarily conducted by individuals but rather by teams; that they are not conducted in a short period but rather over a period of days; and that they are not conducted in a single location but with involvement of a widely distributed group of experts. While the primary focus of this study is the personnel of the MER Safety Console, it is also recognized that they perform their functions within the broader context of the Anomaly Resolution Team and the MER, so that methods and tools recommended in this study should be understandable (and preferably usable) by other members of the ART and the MER. In addition, the recommendations formulated through the use of these methods or tools need to be explained in terms that can be readily understood by the MER Manager, Flight Control Teams, the Flight Director, the Mission Management Team, Space Station Program Office management, and finally, (and perhaps most importantly) the ISS crew. Simply put, the models used and the resulting tools should serve as a "common language" for decision making and communication among all the affected members of the ISS team.

Observations Regarding the Current Approach to Anomaly Resolution in the MER

As described previously, two formal data collection visits were made to the Johnson Space Center to identify and characterize the current approach to anomaly resolution in the MER, focusing on the role of the S&MA personnel.

The following are some general observations regarding the current MER anomaly resolution process:

1. The front end of the anomaly resolution process is very much data-driven, requiring the gathering of information from a wide variety of sources, including on-orbit performance data, information on previous failure history for comparable systems and components, review of existing fault models, gathering of hardware design and performance data, identification of available process models, etc.
2. Discussions focusing on anomaly identification in the FIT meetings we attended seemed to range freely among potential causes without a systematic process for narrowing down to a single most likely cause. While fault trees were used to guide the discussions, there was a lot of cycling from one potential cause to another, and from fault identification to corrective actions and back again. Such free-wheeling discussions are not entirely bad as they allow for consideration of a broad range of ideas. However, it would be helpful if the discussions followed a systematic process for eliminating unlikely causes while focusing in on the most likely scenarios.
3. Discussions of the consequences of on-orbit anomalies and possible corrective actions depend on input from multiple subsystem engineers for input. This is natural, as the effects of an anomaly will be spread across multiple subsystems. However, there is not a common model that systematically identifies the consequences across multiple subsystems.
4. Identification and evaluation of possible corrective actions seems to be an ad hoc process, dependent on brainstorming among multiple systems experts to identify and evaluate the pros and cons of possible strategies. We did not observe the systematic application of a model-based process to guide the evaluation of alternative corrective actions. In addition, we did not observe a process to ensure that the full range of potential strategies is systematically identified.
5. There is not a systematic method available to evaluate fault tolerance and the consequences of "the next failure" as required by the MER S&MA Console Operations Handbook. Consequence evaluations and assessment of the effects of system interdependencies depend on the expertise of multiple subsystem engineers.
6. A method is not available to systematically evaluate the cumulative risk effects of multiple workarounds.
7. An approach is not available to exercise and consistently evaluate multiple what-if scenarios for selecting corrective actions.

Role of the Galileo Fault Tree Tool in the MER

A software tool called Galileo, under development for NASA by the University of Virginia, is used in the MER to support the anomaly resolution process. It is primarily used to support identification of the cause of the anomaly. When an Anomaly Response Team is established, a fault tree is developed and used to help identify the range of possible causes for the event. The fault tree is then discussed during the ART meetings to determine which branches represent the most likely cause of the event. The fault tree puts the possible causes for an anomaly in a logical form that allows for guided "pruning" of the tree to narrow the investigation to the most likely cause. Examination of the fault tree can also be helpful in identifying additional tests or data collection to provide additional information that can help narrow down the diagnosis.

Branches on the Galileo fault trees can be color-coded red, yellow, or green to denote the relative likelihood of specific branches, but they cannot currently be evaluated in a dynamic "what-if" sense other than to develop separate fault trees to illustrate different scenarios. The Galileo fault trees can also be quantified to help determine the most likely failure paths, but in practical application this is not as helpful as it could be because of a shortage of detailed component failure data.

Galileo can currently be used within the MER conference room to develop and evaluate a fault tree during an ongoing discussion. That is, the fault tree can be developed and displayed on the large screen as the discussion proceeds. However, development cannot currently take place in real time among multiple distributed locations because of limitations of file structure and networking hardware.

The Galileo tool represents a significant beginning for the effective use of fault trees to support anomaly identification. Its primary utility at present is to develop and display fault trees to support ART/FIT discussions regarding fault identification. At present Galileo has very limited capabilities to guide the fault identification process. To achieve this potential, necessary first steps include enhancing Galileo's utility to perform what-if analyses and to support fault identification discussions in multiple locations. In addition, a high level process for guiding the use of Galileo to focus discussion on the most likely causes of the anomaly would be very helpful.

Assessment of the Current Anomaly Resolution Process

One of the most striking things about anomaly resolution activities in the MER is that decisions and analyses are performed without a particular framework to guide the decisions or to assess the relationships among diagnoses and selected actions. Risk considerations are not directly tied to an underlying model that denotes the relationship of the current event with any others. Also, there is no explicit framework to guide identification of the side effects of the event under consideration. This requires the expertise of subsystem engineers representing the other systems that could be impacted. Moreover, complete identification of the side effects requires substantial knowledge of system interactions and interdependencies. This knowledge may or may not be possessed by the assembled group of subsystem engineers. It would be very helpful if this knowledge of system interdependencies could be captured in a logic model so it would be available for consideration in all anomaly resolution activities.

There are long range plans to tie anomaly resolution into the fault models of the ISS PRA. However, at present the PRAs are conducted for particular increments or snapshots in time, and are focused on a few specific top events. The difficulty of developing the PRA down to the component level for a sufficiently broad range of possible top events, and keeping it up to date for all the detailed workarounds that occur regularly during day-to-day operations, make it impractical to rely on the PRA as a unifying framework for anomaly resolution. In addition, the fault tree structures focus on failures that occur rather than on implementation of corrective actions, so the PRA fault models do not naturally align with the corrective action portion of anomaly resolution.

Anomaly resolution within the MER would benefit greatly by embedding it within a unifying framework so that each event could be placed in context with others. This would also have the benefit of providing a unifying language for integrating input from multiple disciplines including engineering, operations, safety, and management.

REAL-TIME RISK AND FAULT MANAGEMENT IN OTHER DOMAINS

Commercial Nuclear Power

Prior to the accident at the Three Mile Island nuclear power plant in 1979, the prevailing philosophy was that the human operators only had a small role to play in responding to accidents. Nuclear power plant anomaly operations were organized around response to certain "design base accidents" (DBAs) that were used to guide the design and licensing process. For the most part NPPs were designed so that response to DBAs was the responsibility of automated systems such as dropping the control rods ("SCRAM") for reactivity excursions and flooding by the Emergency Core Cooling System (ECCS) in the event of a Loss of Coolant Accident (LOCA). The operating crew's primary responsibility was to monitor the operation of the automated emergency system, and to intervene only if the emergency system failed to perform as expected. Once the effects of the initiating event were controlled by the automated systems, the operating crew would resume control to place the reactor systems back into the nominal state so that normal operations could resume.

The accident procedures and operating philosophy of NPPs prior to TMI were event oriented. That is, anomaly procedures and training were organized around specific events, especially the design basis accidents. The procedures included an "initiating conditions" or "diagnosis" section that informed operators of the expected symptoms of an event. Selecting a procedure to use in an accident was a matter of recognizing the current conditions and matching them to the symptoms of one of the procedures. Once a procedure was selected, operators were required to carry it out exactly as written; no deviations were allowed. If-then rules were built into the procedures to allow for expected contingencies that were pre-identified. The goal of anomaly response was to stabilize the plant in a safe state. Then, recovery procedures would be implemented to return the plant to its original state so that normal operations could resume. The use of any "workarounds" was strictly controlled within a very narrow range of acceptable operating conditions defined by the plant's NRC-approved "Technical Specifications."

In the environment described above, "anomaly identification" was performed within very narrow boundaries. It was primarily an exercise in matching the current plant state to the symptoms listed in a relatively small set of off-normal and emergency procedures. Because of the requirements for verbatim compliance with emergency procedures, there was little or no opportunity for improvisation in anomaly response.

The primary flaw in this system is that events in the real world do not neatly match the pre-defined sets that were contained in the NPP off-normal and emergency procedures. Thus, if an incident occurred that did not match the pre-analyzed symptoms, incorrect diagnosis and response was possible. This is exactly what happened at TMI. The failure of a relief valve at the top of the pressurizer should have been treated as a small break loss of coolant accident. However, the symptoms resulting from this particular event made it appear that the pressurizer was overfilled. To deal with this perceived situation the operators turned off the emergency core cooling system. Over a matter of hours the water boiled away from the fuel rods, the fuel rods overheated and failed, and the bottom of the pressure vessel was nearly breached due to excessive temperature. Failure of the pressure vessel (which would have led to a much larger release of radiation to the environment) was only narrowly averted when the crew belatedly restarted the emergency cooling systems.

When compared to on-orbit space operations, a major difference of the real-time risk and fault management process in the NPP control room is that it is carried out by a relatively small group of people. For major accidents the control room crew is supported by a small group of experts in the Technical Support Center (analogous to the ISS Mission Evaluation Room) and the engineering staff is always on call. However under most conditions the primary responsibility for anomaly resolution abides with the control room crew, guided by the off-normal and emergency procedures.

Another significant difference between real-time risk and fault management in a nuclear power plant and the ISS MER is the time element. Because a nuclear power plant is basically a dynamic thermal system, anomalies most often are characterized by changing thermodynamic and reactivity conditions in the reactor core and heat removal systems. The time available for response by the crew typically ranges from minutes to hours. This is because the thermal systems of a nuclear power plant are very tightly coupled, and a disruption in one system typically propagates very rapidly to other systems. By contrast, anomalies onboard the ISS most often originate in the performance of a single system, and major effects on critical functions such as habitability or mission success are typically not expected to occur for days or weeks, or with the occurrence of an additional component failure. While there are many linkages among ISS systems (for example, problems that affect attitude control will have consequences in electrical power production), there is much less immediate dynamic coupling than in a thermal process like a nuclear power plant.

Changes in Nuclear Power Plant Operations Following the Three Mile Island Accident

The Three Mile Island accident caused significant soul-searching at all levels of the nuclear industry, and led to fundamental changes in the way NPPs are operated, especially in the assessment of accidents or incidents in progress, and the steps taken to identify, implement, and monitor corrective actions. The official inquiry into the TMI accident[1] highlighted deficiencies in the prevailing approach to accident diagnosis and response. In particular, it highlighted problems in the way information is summarized and presented to the crew to facilitate risk management, procedures used to identify and treat accidents and incidents, and training of reactor operators to perform risk management as contrasted to normal operations.

The most significant outcome of the TMI accident was a fundamental paradigm shift in the way incidents and accidents are evaluated and treated. Prior to TMI, the emergency response paradigm was characterized by event-based diagnosis of the initiating event. In other words, real-time fault management was initiated (and was largely dependent on) an accurate assessment of the event in progress in terms of identifying the initiating event or the primary cause leading to the accident. Thus, effective treatment of an anomaly was dependent on correct identification of the initiating event. As TMI demonstrated so effectively, this approach left a significant risk of serious consequences if the event was incorrectly diagnosed, or if the symptoms could not be accurately matched to the correct anomaly response procedure.

Following the TMI accident, the paradigm for accident response in nuclear power plants shifted to a focus on controlling the effects of the accident, rather than a primary emphasis on diagnosing the initial cause. While diagnosing and correcting the initiating event may sometimes be the most effective and rapid approach to anomaly resolution, this isn't always the case. The new paradigm places primary emphasis on placing the plant in a safe state and controlling and limiting the consequences of the initiating event. (In some ways this is analogous to the use of "workarounds" for anomaly resolution for ISS. However, the tightly coupled dynamics of a nuclear power plant can make the consequences of an incorrect choice regarding the choice of a corrective action very serious, as witnessed by the TMI accident.)

The two basic approaches to implementing this new paradigm are called "function-oriented" and "symptom-based" emergency response. The function-oriented approach is based on the definition of several "critical safety functions" that are constantly monitored during normal and off-normal conditions. When a deviation in the health of one of the critical safety functions is detected, the goal is to systematically evaluated the availability of a set of pre-identified "success paths" that could be implemented to address the critical function challenges. Following the TMI accident the plants belonging to the Combustion Engineering Owner's Group implemented function-oriented emergency procedure guidelines using "resource assessment trees" to identify the critical safety functions, the parameters used to monitor their health, and possible success paths to be used in the event of a critical function challenge. The Westinghouse Owner's Group implemented another approach to function-based emergency procedures. Logic trees called "critical safety function status trees" (CSFSTs) were used to monitor key parameters for the critical safety functions. Based on the combinations of those key parameters, safety function status was rated according to its relative seriousness as "green," "yellow," or "red." Operators were guided to specific procedures for dealing with the critical function challenges based on the specific combination of parameters at a given point in time.

The symptom-based approach means that assessment of status and identification of corrective actions are explicitly based upon current symptoms observed in the plant. Rather than having simply a list of symptoms at the front of the procedure for fault diagnosis purposes, this approach includes an explicit algorithm for evaluating plant state and selecting corrective actions. The symptom-based approach could be used as the front end for either event-based or function-based approaches for anomaly resolution. That is, the symptom based logic structure could either be used to guide event identification or assessment of critical function status. Then, procedures could be selected either to correct the initiating event or to control critical function challenges.

The Babcock and Wilcox (B&W) Owner's group was the primary advocate of the symptom-based approach to anomaly resolution. Three Mile Island was a B&W plant, and one of the major errors of the TMI operators was the failure to correlate reactor temperature and pressure, which would have quickly provided evidence that the water in the reactor vessel was steam rather than liquid. For this reason the B&W emergency procedures following TMI used a symptom-based approach with a primary focus on the pressure-temperature correlation. A set of IF-THEN rules was used in conjunction with this correlation to assess the thermal conditions within the reactor vessel and to select corrective actions accordingly.

Tools for Real-Time Risk and Fault Management in the Nuclear Industry

Following the TMI accident there was a surge of activity focused on the development of tools to support real-time risk and fault management in nuclear power plant control rooms. The Kemeny Commission report had recognized the critical need to provide useful information to reactor operators during off-normal conditions and accidents, and research institutes around the world began to develop prototype systems. There was a great sense of optimism that computer technology, including advanced methods from Artificial Intelligence (AI), would provide an effective solution for the challenges presented by problem-solving in time critical, highly stressful emergency conditions.

A wide range of institutions from around the world began developing possible computer solutions to the problems highlighted by TMI. In the United States the primary activity was focused at the reactor vendors (Westinghouse, Babcock and Wilcox, Combustion Engineering, and General Electric), the Electric Power Research Institute (EPRI), the Department of Energy (DOE) national laboratories (including INEEL), and universities such as Massachusetts Institute of Technology (MIT), Georgia Institute of Technology, and the University of Tennessee. In parallel, the United States Nuclear Regulatory Commission started a major research program focused on identifying and resolving regulatory issues regarding the implementation of computer technology in nuclear power plant control rooms. In the early 1980's the NRC's research program focused on the evaluation of specific concepts for computer support in the control room, as well as the back-room Technical Support Centers that were mandated for U.S. nuclear facilities. In the mid-and late 1980's and beyond the NRC's research shifted to more generic issues such as human reliability analysis, risk impacts of digital technology, and risk informed regulation of nuclear power plants. Many of these programs continue in one form or another to the present day, providing a rich base of information regarding real-time risk and fault management in U.S. nuclear power plants. However, because the NRC is a regulatory agency without a responsibility for operations or mission success, much of the work focuses on risk assessment and regulation rather than operational risk management. As a result, the NRC's focus is very much focus on quantitative Probabilistic Risk Assessment rather than the qualitative risk management methods that are more appropriate for operational risk management, where detailed risk models and quantitative failure data may not be adequate for real-time application.

Other countries around the world with major commercial nuclear programs also aggressively researched potential applications of computer technology to nuclear power plant operations in the wake of the TMI accident. Because of differing regulatory approaches, plant designs, and operating philosophies, the systems developed in different countries often took very different approaches to the same generic problems. Some of the more prominent research efforts were conducted in France, Germany, and Japan. In addition, the OECD Halden Reactor Project in Norway conducts a focused research program on behalf of 20 member nations of the Organization for Economic Cooperation and Development. Because many of these countries have less conservative regulatory approaches than the United States, they have been more aggressive in moving computer technology from the laboratory in the control room for real-time risk and fault management functions.

Computer-based tools have been developed and tested in the nuclear industry for all phases of anomaly response. For example, early fault detection systems[2] based on comparison of plant parameters to computer simulation models have been used to detect impending anomalies before standard alarm systems are tripped. Rule-based expert systems[3] have been developed that use combinations of plant parameters to assist fault diagnosis. Critical function-based methods[4] have been used to help identify potential corrective actions and to formulate procedures based on the availability of success paths during the evolution of an event. Computer-based procedure systems[5] have been developed to assist in the implementation of corrective actions during accident conditions. Finally, integrated toolsets[6] have been developed combining many of the above capabilities to provide the full range of risk and fault management functions for anomaly resolution.

These representative systems are only a small sample of the tools that have been proposed to support real-time risk and fault management in nuclear power plants. There is a wealth of literature describing the experienced gained in development and testing of these systems that can be used to provide insights in the development of analogous systems for space operations. For example, the U.S. Nuclear Regulatory Commission has issued a series of reports[7-11] summarizing experience gained and design guidance for computer-based systems to support reactor operations. The International Atomic Energy Agency has published a report[12] summarizing experience gained worldwide in developing and implementing computerized support systems for nuclear power plants. Finally, the OECD Halden Reactor Project has published a historical overview[13] of the research conducted over the past 30 years on behalf of the member nations of the Halden Project. These documents provide numerous references to papers and reports providing details on dozens of systems that have been tested in the international nuclear community.

Offshore Oil

The approach to risk management used in the offshore oil and gas industry has been greatly influenced by the fire and explosion that occurred on the Piper Alpha platform in the North Sea on July 6, 1988. In part because the platform was laid out so that the living quarters were inaccessible to rescuers, 167 lives were lost. The resulting investigation and recommendations had a great influence on the risk management and regulation of offshore facilities, particularly in the U.K. and the North Sea [14]. For the most part, risk management has been implemented from the perspectives of design and regulation, rather than focusing on real-time anomaly response.

The Piper Alpha accident was a watershed incident for the offshore oil and gas industry in the same fashion that Three Mile Island led to fundamental changes for the worldwide nuclear industry. Piper Alpha brought home the lesson that compliance with static safety regulations is not always adequate, but rather that regulators, designers, and operators of high risk facilities need to pay attention to the processes by which systems are designed and work is planned and carried out. Piper Alpha had different effects on industry practices in the U.K. and U.S., in part due to the different proximity to the event and degree of public awareness in the two countries.

Regarding the UK, the Piper Alpha inquiry recommended the development of a Safety Case program supervised by a government ministry to demonstrate and oversee the safety of offshore facilities. Each facility would be required to develop a comprehensive safety case to demonstrate that an adequate safety management system was in place for the facility, that major hazards and risks had been identified, and that personnel could be evacuated in an emergency. The Safety Case approach has resulted in the introduction of formal risk assessment methods into the U.K. offshore industry.

In contrast to the U.K. Safety Case approach, the U.S. offshore oil and gas industry is testing the suitability of voluntary practices for controlling the safety of offshore installations. The U.S. Minerals Management Service (MMS), the government agency responsible for regulation of offshore facilities, recommended in 1991 that all facilities should develop a Safety and Environmental Management Program (SEMP). The philosophy of the SEMP is that management of hazards should be an integral part of the design, construction, maintenance, and operation of offshore facilities.

For the most part, risk and fault management in the offshore oil industry has been treated primarily by pre-analyzing accident states using qualitative or quantitative risk assessment methods, and then incorporating the resulting insights in operating guidance and procedures.

More recently however, increased attention is being given to the issues of automation or advanced computer-based operator support systems for real-time risk and fault management for offshore facilities. Many large operators, especially those in the Norwegian North Sea, are beginning to implement digital technology in the control rooms of production platforms. This will require that significant attention be given to human roles in the use of advanced computer-based risk and fault management systems.

NASA Engineering for Complex Systems Program

The NASA Engineering for Complex Systems (ECS) program is engaged in the development of tools to support management of risk in the design and operation of space and aeronautics systems. Some of the projects being conducted under the ECS program could potentially provide capabilities that can be adapted for real-time risk and fault management in the ISS Mission Evaluation Room. For example, the Mishap Initiator Identification System is being developed to provide more consistency in mishap reporting, and to provide greater depth in anomaly and failure analysis. Rather than focusing on only the failure at hand, the tool will help provide increased understanding resulting from comparison across multiple events, and more systemic understanding of the causes of failures. This tool is primarily an off-line tool to provide a searchable repository of NASA mishap reports, which then could be used to guide inquiry in the assessment of a new mishap, or to support the development of generic lessons learned across multiple events.

The Investigation Organizer is a set of tools to support mishap and anomaly investigation, and is based on the existing Science Organizer web-based collaborative infrastructure. The inquiry is guided by incorporation of models of mishap event chains, and the Management Oversight and Risk Tree (MORT) structure is used to organize information about potential contributing factors for an incident. The system helps gather information that can either support or refute a particular hypothesis regarding the cause of the event. Once again, this is primarily an off-line tool, best suited for post-mortem analysis of a failed mission such as the failure of a planetary probe.

The Model-Based Hazard Analysis project is developing tools to identify potential hazardous states during the design process, so that such hazards can be eliminated or controlled through design modifications. The tools will depend on both heuristic (relying on analyst's knowledge and experience) and model-based (relying on formal system representations and analysis methods) for identifying and mitigating potential hazards during design. The model-based approach will utilize dynamic event trees to explore potential combinations of hardware states, human actions, and physical variables to explore the relative probability of possible hazardous end states.

The SimStation project is working to develop an integrated, quick-look model of ISS behavior to assist the VIPeR (Vehicle Integration Performance) team in performing what-if analyses. The primary focus of the VIPeR team is long-term management, planning, and operation of ISS systems. SimStation will include a high-resolution functional model based on reliability block diagrams in which faults can be inserted to explore consequences. It will also have a first-order model of ISS behavior, and an integrated redundancy and risk model. Expected benefits of SimStation include the more rapid consideration of alternative corrective actions, providing focused direction to subsystem teams performing high fidelity analysis, and broader understanding of system trades across subsystem teams, especially under off-nominal conditions.

Activities focused on real-time fault and risk management for the ISS Mission Evaluation Room should include assessment of the capabilities and tools developed by the Engineering for Complex Systems program, to ensure that maximum benefit is realized from the investment of ECS.

REQUIREMENTS FOR SOFTWARE SUPPORT FOR REAL-TIME RISK AND FAULT MANAGEMENT IN THE MISSION EVALUATION ROOM

The following requirements should be addressed when developing software tools for anomaly resolution, based on our evaluation of MER anomaly resolution processes:

1. It is very important that risk tools utilized in the MER be accepted by the ISS Sustaining Engineering organization, and integrated with operations in the Flight Control Room. That is, the tools used for anomaly resolution must perform analyses and convey recommendations in ways that interface naturally with the engineering and operations functions.
2. Risk and fault management tools must be able to account for constantly evolving systems due to ISS increment construction and the cumulative effects of workarounds.
3. Initial implementation of risk and fault management tools should focus on qualitative aspects of anomaly resolution. Quantification should be introduced gradually and carefully supported with credible data to ensure acceptance by engineering and operations personnel.
4. Risk and fault management tools should be capable of clearly representing system interrelationships and the consequences of “the next failure.”
5. Risk and fault management tools should be capable of evaluating suggested corrective actions according to relevant parameters such as risk, effects on other systems, ease of implementation, etc.
6. A logic framework focusing on mission success (rather than failure) should be included to systematically assess effects of failures on mission success, and to identify and evaluate potential corrective actions.
7. The impact on the crew should be considered when evaluating potential corrective actions. For example, corrective actions should be evaluated with regards to time required for implementation, potential safety hazards, etc.
8. Tools for anomaly resolution should be embedded within procedures or higher level tools for guiding the overall process, e.g. to guide fault tree development, identify issues, focus discussion, and identify impacts on other systems.
9. One of the potential benefits for risk and fault management tools is to reduce the number of people required for real-time risk and fault management. However, measures should be taken to ensure that

all relevant information and perspectives are still included in the anomaly resolution process. A model focused on mission success could be used to ensure that all relevant issues are addressed.

10. The "workaround" paradigm for anomaly resolution will require a flexible data structure to allow ongoing analyses to be effectively plugged into the risk and fault management toolset. Configuration management will be a major concern to ensure that models always represent the current configuration of the system. Finely detailed workarounds that are performed within the confines of a single Orbital Replacement Unit (ORU) may be very difficult to adequately model, both individually and to reflect the effects of multiple workarounds.
11. Training will be required to ensure that risk and fault management tools are used accurately and effectively.
12. When possible, multiple paths of inquiry should be used to avoid potential incorrect diagnoses of initiating events. Experience from past events should be used to help determine whether the assessment is credible. Alternative methods of analysis, such as using both fault- and success-based approaches in parallel, can provide safeguards against incorrect diagnosis and selection of corrective actions. The tools should guide the collection of additional information that can confirm or disconfirm possible diagnoses.
13. Process models should be integrated with the logical processes, especially to support identification of tests that can confirm/disconfirm diagnoses.

RECOMMENDATIONS AND NEXT STEPS

The following recommendations describe a plan for utilizing computer-based support for MER anomaly resolution. They include near-term recommendations to develop the Phase 2 structured approach and common toolset for anomaly resolution, and long-term recommendations for the Phase 3 integrated Risk Monitor.

Near-Term Recommendations

Phase 2A – Fault Identification and MER Process Changes

1. Galileo updates

- Develop a diagnostic tool to guide and focus fault tree analysis for fault identification and discussion. The tool should assist in “pruning” the tree to focus on the most likely cause of the event, and to identify tests that can gather additional information if required for further pruning.
- Develop a dynamic analysis capability to manage multiple “what-if” cases to explore multiple possible diagnoses of the fault.
- Develop a distributed system to allow development and evaluation of Galileo fault tree models in remote locations.
- Archive fault trees, make them accessible for future use, and integrate them into the common risk and/or mission success framework. Master Logic Diagrams within Galileo could serve as a "meta-controller" to access and link together the fault trees for a particular analysis.
- Work with users to develop good user interfaces to enhance acceptance and usability.

2. MER process changes for anomaly resolution

- Develop a common success-oriented framework to show functional relationships, system relationships, and their contribution to mission success. This framework will serve as a common

language for communication across multiple disciplines, layers of management, and with the ISS crew.
- Identify the process changes and the software architecture required to maximize safety console effectiveness in MER anomaly resolution.
- Identify suitability of existing risk models (PRAs, reliability block diagrams, Failure Mode and Effect Analyses, etc.) for incorporating into the anomaly resolution process.
- Investigate and develop the detailed schema for expert software support for anomaly resolution.

Phase 2B – Tools for Integrated Analysis

Develop methods and prototype software tools to support anomaly resolution including the following functionality:

- Systematically assess the immediate and future (dynamic) consequences of an anomaly and possible additional failures, and to manage multiple "what-if" scenarios.
- Model and clearly illuminate the dependencies of components and systems on the "utility" support systems – power, thermal control, and data.
- Prioritize diagnostic tests to assist event identification, based on considerations of success likelihood, cost, and time.
- Guide the development and evaluation of alternative corrective actions. The identification of near-term corrective actions will be based on the "success path" concept from critical function analysis.
- Formulate rules for selection of corrective actions or workarounds based on the specific circumstances of the anomaly in progress. Once viable corrective actions are identified, they need to be systematically evaluated against the relevant criteria. The method should explicitly compare the desirability of corrective actions for the original event with potential workarounds.
- Evaluate the risk of cumulative effects of workarounds. This will require the assessment of risk in the context of what has happened previously, rather than relative to a static PRA model.
- Integrate fault and consequence models with simulation models of components and systems.
- Incorporate and evaluate crew requirements for implementing alternative corrective actions, and impacts on other crew tasks.

The basic approach for building on the Galileo fault isolation and failure analysis capability will be to develop a critical function-oriented Mission Success Framework. It will start with high level ISS program critical functions/goals, and work down to systems at the resource level. Methods for identification of alternative corrective actions using the new mission success models will be developed and incorporate information contained in fault trees, Failure Modes and Effects Analyses (FMEAs), reliability block diagrams, etc. The framework can then be used as a tool to do consequence analysis, "next failure" analysis, and to identify potential corrective actions (to confirm diagnosis and to generate workarounds).

The enhanced Galileo tool will be used to generate fault trees for fault identification and then plug them into the functional model for assessment of consequences and identification of corrective actions.

The functional models will be extended for the specific event in progress to identify information requirements for further diagnosis and to identify alternative resource options and success paths for workarounds. Mission-success based guidelines (risk, effectiveness, crew requirements, impacts on other critical functions, etc.) will be developed for selecting corrective actions.

The critical function models and fault trees will be continually “bootstrapped” to add details and follow increment buildups and workarounds. Guidelines will be established for "configuration management" to ensure that models are kept up to date for long-term use.

The Phase 2A and 2B methods and tools will be developed so that they can be applied to the space shuttle as well as the International Space Station.

Long-Term Recommendations

Phase 3A – Automated and integrated risk tools

- Develop a full-featured tool for fault isolation and corrective action selection, integrating both the failure oriented Galileo tool and the mission success tools developed in Phase 2. The ability to perform and manage multiple “what-if” scenarios will be included.
- Develop a formal “risk monitor” tool to assess risk impact of maintenance and logistics activities.

Phase 3B – Combine all the tools into a fully-integrated Mission Success Framework

All the tools developed previously will be tested in the operational environment and combined into a fully-integrated toolset for anomaly resolution. The following paragraphs describe the overall vision for the integrated Mission Success Framework.

We believe that the most effective framework for performing anomaly resolution within the MER is one that focuses on mission success. This is because mission success defines the goals of the entire space station program, helps prioritize the significance of any off-normal events, and can be used to take all considerations into account when evaluating potential corrective actions.

We believe that a Mission Success Framework patterned after the critical function approach utilized in the commercial nuclear power industry will serve as an effective guide for anomaly resolution in the ISS Mission Evaluation Room. This Mission Success Framework will form the foundation of the integrated Risk Monitor for real-time anomaly resolution in the MER.

The initial development of the Mission Success Framework should focus on the hardware systems that are used to provide the mission success critical functions. At a later stage of development broader critical functions could be added, to address programmatic issues, international partner considerations, etc.

CONCEPTUAL FEATURES OF THE MISSION SUCCESS FRAMEWORK

Functional modeling

Functional modeling methods were developed and implemented following the Three Mile Island to provide an alternative perspective for real-time fault and risk management in commercial nuclear power plants. The type of functional models most suited for real-time risk and fault management are success-oriented logic structures that show how plant resources can be configured in multiple ways to provide critical functions in normal, off-normal, and emergency conditions. During the late 1970’s INEEL implemented a functional modeling approach called response trees that were implemented in the emergency procedures of the Loss of Fluid Test (LOFT) reactor[15]. The response trees were used to guide reactor operators in evaluating critical functions during an accident, and for selecting success paths for restoring critical functions that were challenged by the event and its consequences.

Following the TMI accident, Bill Corcoran of Combustion Engineering developed the foundational principles of critical safety functions and how they could be used to support accident and emergency management in nuclear power plants[16]. Mohammed Modarres of the University of Maryland has developed methods[17] such as goal tree/success trees (GTSTs) and master plant logic diagrams (MPLDs) to model critical functions for complex systems. He has also organized an international community of researchers to explore possible applications of functional models in the nuclear industry and other domains. This group has sponsored six international workshops aimed at stimulating further development and application of these methods.

At INEEL we have developed a general structure for functional models that can be adapted and implemented in many different ways depending on the intended application. Figure 1 shows the general structure of a functional model using this framework.

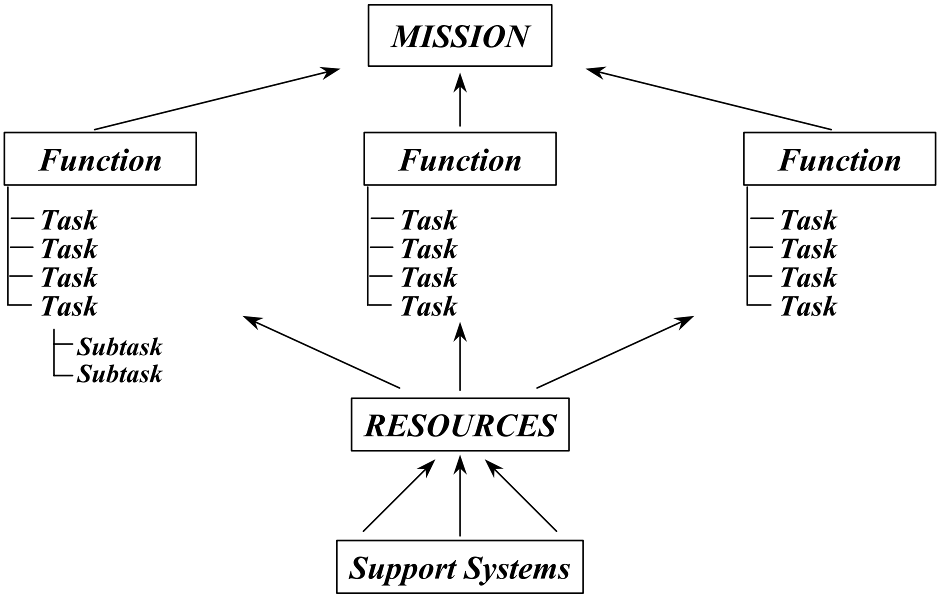

Figure 1. General structure for functional models.

As the figure shows, the functional model organizes information about the structure of a system into five different categories represented by the different levels of the tree:

- Mission – The overall purpose or overarching goal for the system. For a nuclear power plant the mission could be defined as “produce electrical power efficiently, economically, and safely.” For the ISS the mission might be described as “provide a habitable platform for supporting on-orbit scientific research.”

- Critical functions – Those functions that must be performed or maintained at all times in order to carry out the mission of the system. For risk and fault management in a nuclear power plant these are usually the plant's critical safety functions – core cooling, reactivity control, heat removal, and containment of radioactive materials.
- Tasks – Those tasks that must be performed to maintain the critical safety functions. In this context the word task is used generically. That is, a task may be performed by human action, automatically or passively through plant hardware, by software control, or any combination of human, hardware, and software.
- Resources – The resources are the hardware, software, procedures, and other resources that can be configured to perform and maintain the critical functions.
- Support systems – The support systems are those utilities that are required for the resources to operate. Example resources in a nuclear power plant are electrical power, component cooling systems, and data systems. A primary feature of support systems is that they provide the support functions to many components, so that their failure can disable numerous components. In nuclear power plants and space vehicles this vulnerability to "common cause failure" is typically addressed by provide multiple redundant support systems supplying the function to independent "trains" of components that can be used to provide the same critical function.

The arrangement of the components on the functional model shows the different ways that the resources can be configured to provide and maintain the critical functions. Each of the configurations that will provide a critical function is referred to as a success path for that critical function.

When an event or anomaly occurs, the functional model can be used to evaluate, based on the available systems and components, which success paths can be used to restore a critical function that has been lost, or to maintain a critical function that has been degraded or challenged. It can also be used to explore different strategies for restoring an unavailable critical function – e.g. whether to correct the cause by repairing or replacing failed components, or to bypass the failed components by utilizing an alternate success path. The latter case is widely used for anomaly response on the ISS, and is referred to as a workaround. Repairing a failed component can be accomplished in some cases when ground personnel can devise a repair procedure. Replacing a failed component most often requires that a replacement be manifested on a future shuttle mission, so it is usually not a near term option for restoring a challenged critical function onboard the ISS.

Functional models are also very useful for illustrating the effects of failed equipment, and to identify and evaluate possible corrective actions. The logic structure makes it easy to show what side effects the failure of any combination of components and systems will have, and what success paths will be disabled by the initial failures and their side effects. This is particularly helpful in understanding the consequences of a support system failure. By examining the model to identify the success paths that remain available following a set of failures and consequences, it is possible to evaluate and select the best course of action to follow. Basic rules can be established in advance to help guide the selection of alternative success paths for implementation. These rules can then be augmented by specific considerations for the particular situation in progress to complete the selection process.

Figures 2-6 show preliminary high-level functional models for the International Space Station. Models are shown for ISS habitability and for the electrical power and thermal control support systems. These models are for demonstration purposes only. A rigorous process including review by ISS engineering staff will be required to develop approved functional models for use in the Mission Evaluation Room.

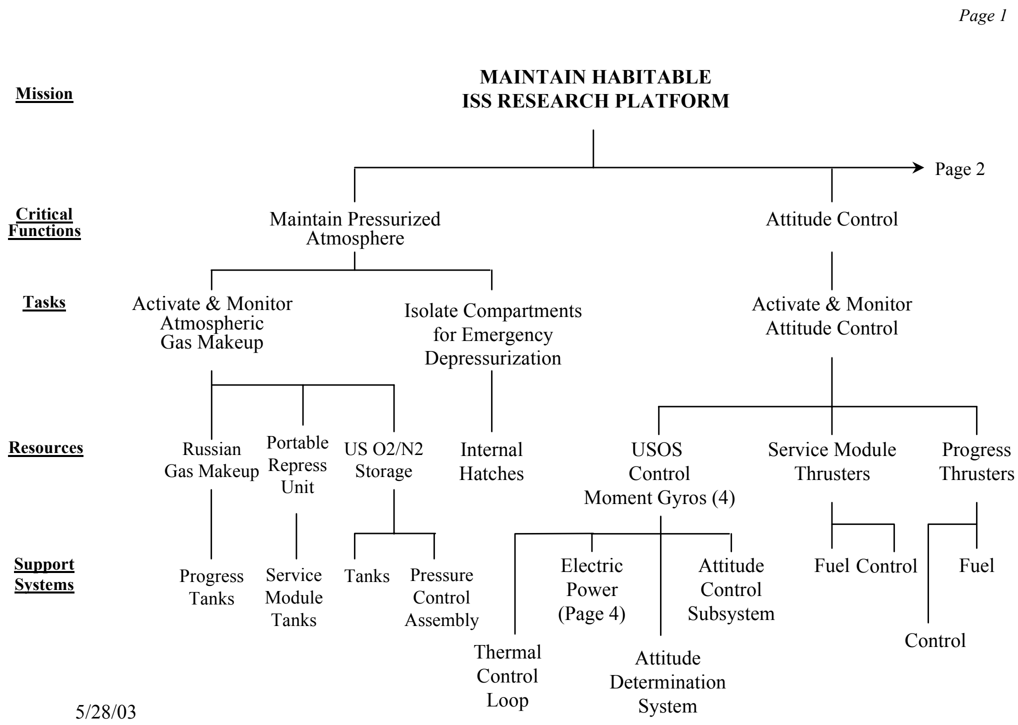
Page 1
Mission
MAINTAIN HABITABLE ISS RESEARCH PLATFORM
Page 2
Critical Functions
Maintain Pressurized Atmosphere
Attitude Control
Tasks
Activate & Monitor Atmospheric Gas Makeup
Isolate Compartments for Emergency Depressurization
Activate & Monitor Attitude Control
Resources
Russian Gas Makeup
Portable Repress Unit
US O2/N2 Storage
Internal Hatches
USOS Control Moment Gyros (4)
Service Module Thrusters
Progress Thrusters
Support Systems
Progress Tanks
Service Module Tanks
Tanks
Pressure Control Assembly
Thermal Control Loop
Electric Power (Page 4)
Attitude Determination System
Attitude Control Subsystem
Fuel
Control
Fuel
Control
5/28/03

Figure 2. Functional Model for the International Space Station.

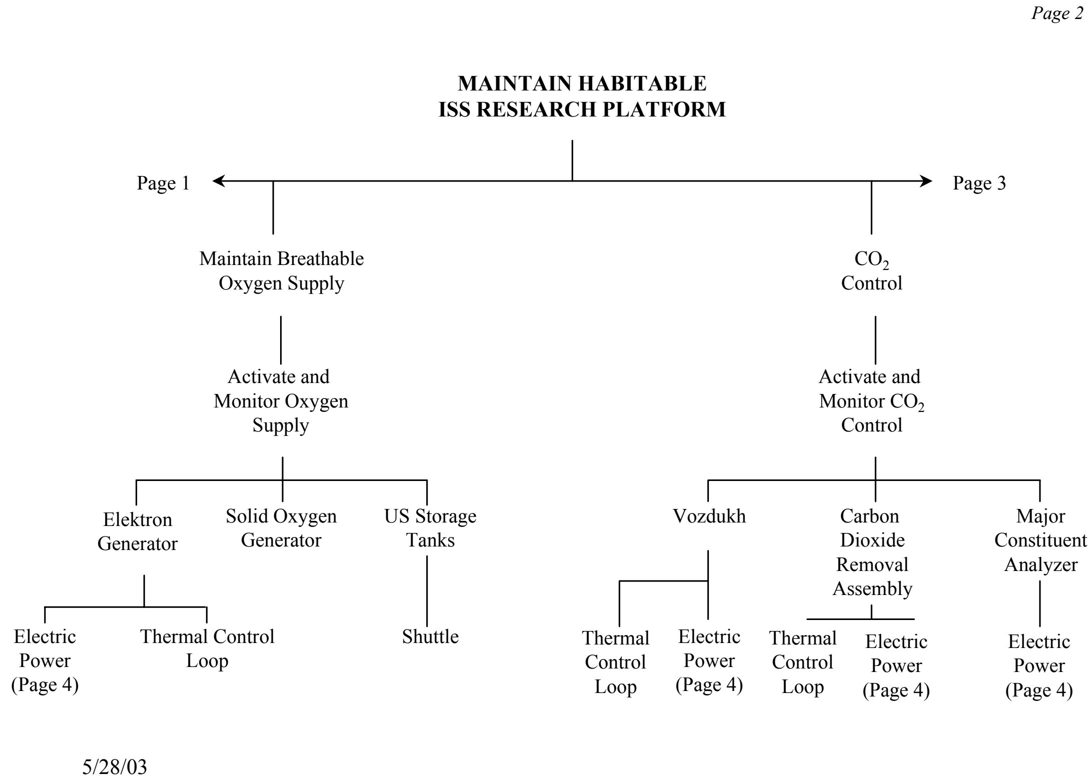

Figure 3. Functional Model for the International Space Station (cont.).

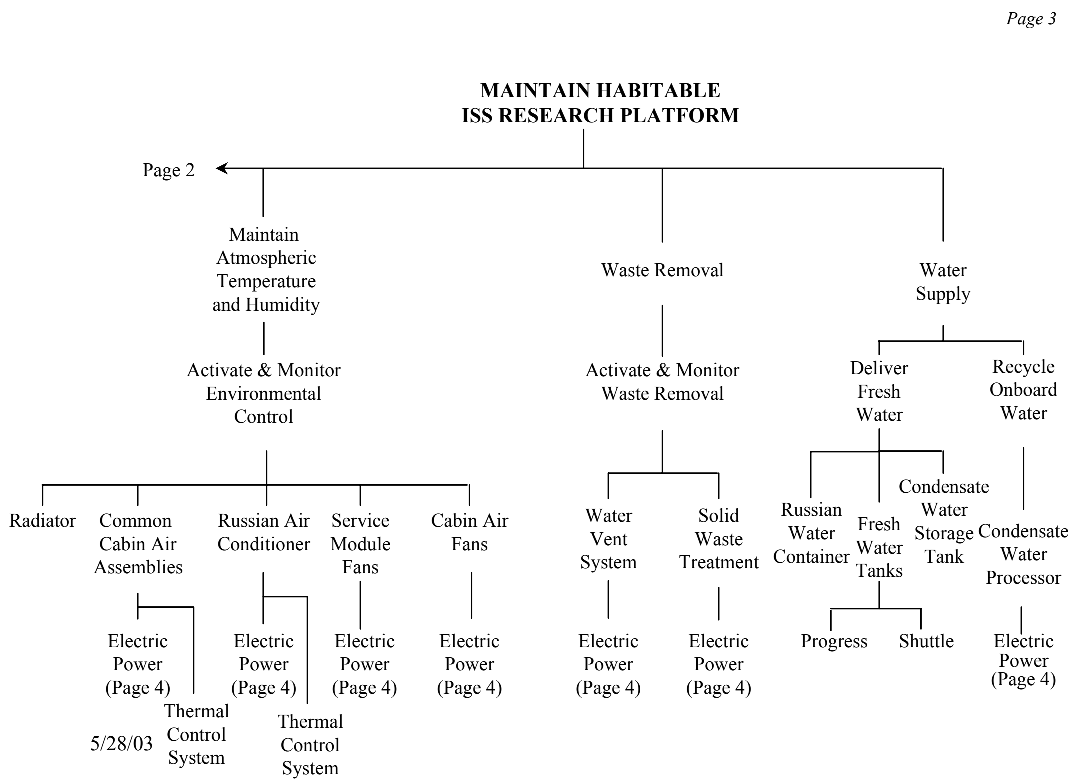

Figure 4. Functional Model for the International Space Station (cont.).

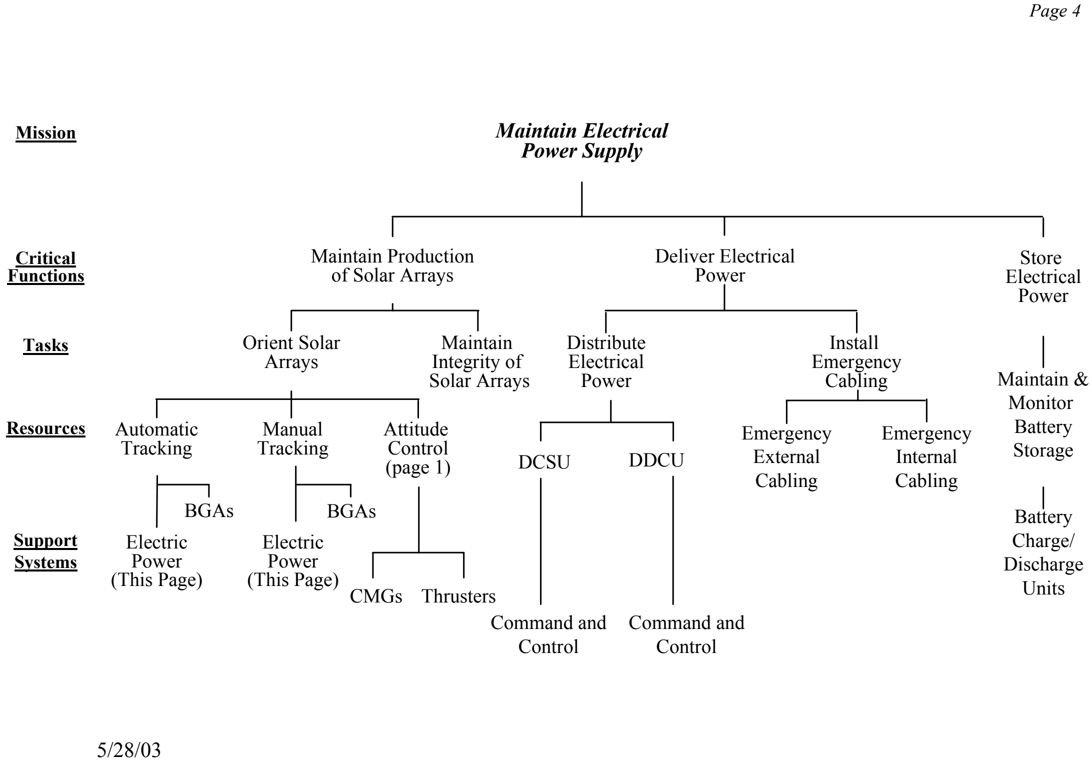
Page 4
Mission
Maintain Electrical Power Supply
Critical Functions
Maintain Production of Solar Arrays
Deliver Electrical Power
Store Electrical Power
Tasks
Orient Solar Arrays
Maintain Integrity of Solar Arrays
Distribute Electrical Power
Install Emergency Cabling
Maintain & Monitor Battery Storage
Resources
Automatic Tracking
Manual Tracking
Attitude Control (page 1)
DCSU
DDCU
Emergency External Cabling
Emergency Internal Cabling
BGAs
BGAs
Battery Charge/ Discharge Units
Support Systems
Electric Power (This Page)
Electric Power (This Page)
CMGs
Thrusters
Command and Control
Command and Control
5/28/03

Figure 5. Functional Model for the International Space Station (cont.).

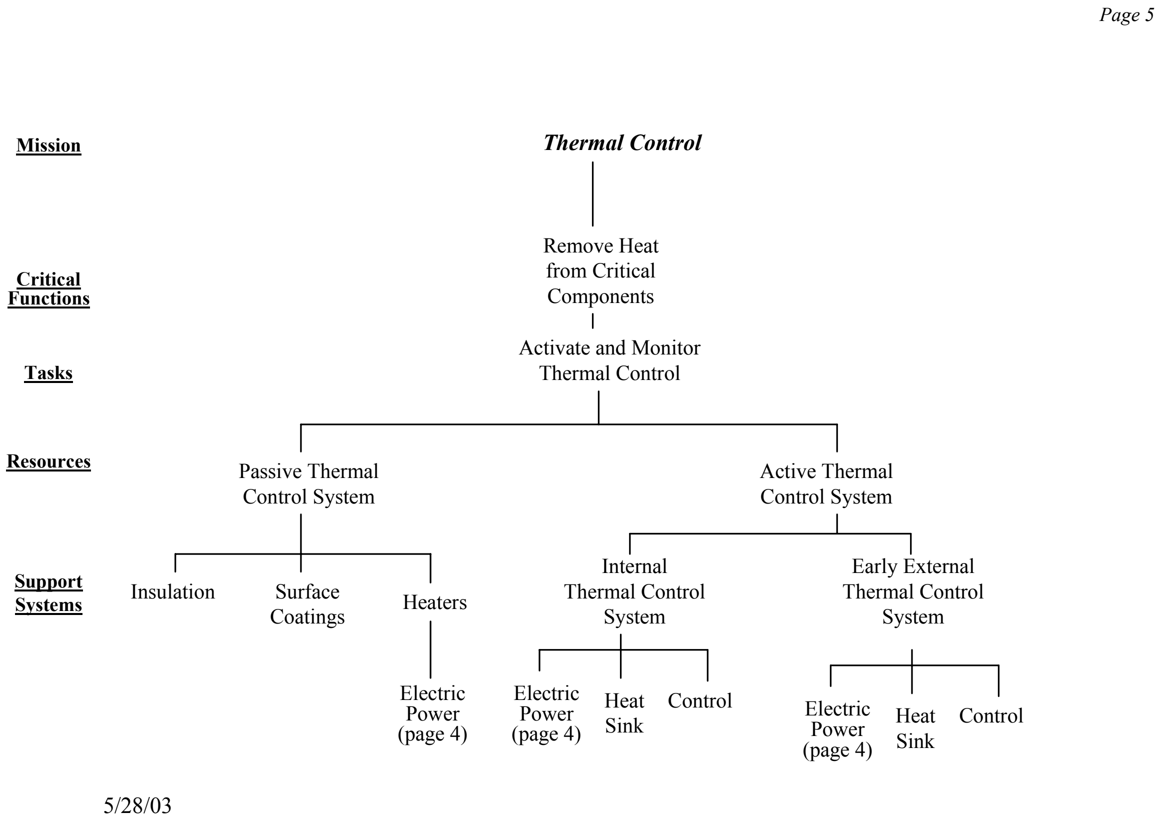

Figure 6. Functional Model for the International Space Station (cont.).

Application of the Mission Success Framework in the Mission Evaluation Room

The Mission Success Framework will be used to guide real-time risk and fault management in the ISS Mission Evaluation Room. This framework will be a functional model describing in logical and graphical form how space station tasks, resources, and support systems work together to provide the critical functions necessary for mission success. The particular form of the functional model forming the foundation of the Mission Success Framework should be chosen to suit the specific operational requirements for the space station program. Usability and understandability of the models for communication and decision making purposes should be the primary criteria for selecting the specific format to be used. Similarly, the software used to implement and exercise the Mission Success Framework should be selected based on the operational requirements of the MER, effective communication with the MPSR and FCR, and usability by all involved program personnel. It is possible that a commercial software package for developing and manipulating functional models could be adapted for the space station program. However, at the base functional models are simple Boolean structures, so it may be more efficient to adapt a general purpose risk analysis program such as Galileo or SAPHIRE to manipulate success trees as well as fault trees. Or, it might be most cost-effective to develop a software module specifically to handle the Mission Success Framework, which could then be interfaced with the fault tree package by a higher-level “meta-analysis” program.

Important considerations for the Mission Success Framework

Combining Success and Failure Models

The Mission Success Framework should be combined with the enhanced Galileo tool to provide a complete package for event identification, assessment of consequences, and identification and selection of alternative corrective actions. Conceptually, the fault trees will plug into the resource or support system levels of the functional model, illustrating the potential causes of a resource or support system failure. At this interface the fault and success models will be combined. Looking up the tree structure will provide guidance on consequence evaluation and corrective action selection, while looking down the tree to the fault tree model will provide guidance for event identification. Once a fault tree has been developed and validated it can be stored for future use in anomaly resolution for events involving failure of the same components or systems. The fault trees can be stored in a separate database and then plugged into the functional model in a modular fashion when specific events occur involving failure of the modeled component or support system. A meta-level analysis tool can be developed to guide use of the total fault/success package for performing all the major tasks of anomaly resolution.

To Quantify or Not

A very important question about the use of any kind of risk models in real-time risk and fault management is whether or not quantitative estimates of success or failure should be used. The first priority is to make sure that the logic models and procedures for using them are accurate in helping identifying event causes and corrective actions. The real goal is to identify the actual cause of the event in question, and to choose an effective corrective action. Quantification comes into play in selecting between two possible event diagnoses, or evaluating the likelihood of adverse effects when two different corrective actions are under consideration. Quantified probability estimates should be used with great caution. Currently available estimates of failure probability are not adequate for purposes of fault and risk management in real time situations. They can be effectively used for longer-term considerations of recurrence control and evaluation of options for returning ISS systems to their design state. For real time evaluations, the highest priority is to ensure that the models that guide decision making and the procedures for using them are as accurate as possible given the current understanding of risk management and vehicle configuration.

Developing the Mission Success Framework

The Mission Success Framework should be developed with participation from all stakeholders including engineering, operations, S&MA, MER managers, ISS program management, and the crew office. The foundation of the Mission Success Framework should be developed from existing information including system descriptions and risk models. One of the most important steps is for all parties to agree on the definition of the top level mission and the critical functions required to carry out the mission. Then the tasks and resources that are available for performing the critical functions will be modeled, and the interdependencies between systems and critical functions. Next, the support system dependencies are detailed, and detailed component and system details are added.

The preliminary version of the Mission Success Framework should focus on the technical systems only. It should be tested through analytical exercises and then in training exercises. Once the technical version has been validated and implemented for anomaly resolution, development of the programmatic critical functions can be initiated.

Components of the Mission Success Framework

The primary visible component of the Mission Success Framework is the functional model organized into the mission, task, resources, and support system hierarchy described above. At the component level fault trees for component failures are linked in, providing the capability to identify causes for component failures and other anomalies. However, the Mission Success Framework is supplemented by direct links (in tabular form or software structures) to the following information:

1. Detailed information about components and systems – operating limits, performance characteristics, process models, failure modes, etc.
2. Models of support system dependencies and component failure states resulting from failure of the support systems.
3. Instrumentation available for monitoring the health of the critical functions, determining the availability of success paths, monitoring the performance of success paths, and monitoring the status of components.
4. A set of static or dynamic rules for selecting success paths for implementation in response to an anomaly. Static selection rules are not dependent on system status and thus are the easiest to establish. Dynamic selection rules change according to system status and thus are much more complex to develop.

Procedure for use of the Mission Success Framework for Anomaly Resolution in the MER

The following is a generic procedure for use of the Mission Success Framework in the ISS Mission Evaluation Room.

1. Collect indications and symptoms of the anomaly, and previous data showing the precursors of the anomaly.
2. Identify components that have failed as a result of the anomaly.
3. Use the functional model to identify side effects of the failures, challenges to the critical functions, vulnerabilities to additional failures, and effects on success paths for the challenged critical functions.
4. Select and implement alternative success path(s) if required for near-term restoration of the challenged critical functions.
5. Perform a "quick-look" analysis to evaluate the tradeoffs between the extended use of alternative success paths versus detailed diagnosis for repair/replacement of failed components.
6. Develop a fault tree for the identified failures based on system design information and previous failure history.
7. Identify and assess the relative likelihood of different failure paths based on currently available information.
8. Identify additional tests that could generate additional information if needed to conclusively identify the failure path that caused the anomaly.
9. Use the functional model to evaluate the relative desirability (in terms of risks and effects on other critical functions) of alternative success paths, include options to repair/replace failed components, or workarounds based on implementation of alternative success paths.
10. Select the desired success path(s) for implementation.
11. Develop detailed procedures for implementing the selected success path(s).
12. Identify indicators and measurements that can be used to verify effectiveness of the selected success path(s).
13. Implement the selected success path(s) and monitor for effectiveness.

Benefits of the Mission Success Framework for Real-Time Risk and Fault Management in the Mission Evaluation Room

The following are some of the expected benefits from using the Mission Success Framework to support anomaly resolution in the Mission Evaluation Room:

1. The Mission Success Framework can serve as the foundation for group decisions in real-time risk and fault management. The framework will provide the common discussion focus for the anomaly resolution activities performed by individuals from many disciplines working together as a team, including the MER manager, subsystem engineers, and the S&MA POC.
2. One of the primary benefits of the Mission Success Framework is the capability to organize the information for anomaly resolution within a common framework directly tied to mission success. This helps to ensure that different disciplines and groups within the anomaly resolution process can consider the information in a consistent manner, and evaluate the implication of anomaly resolution decisions across disciplinary boundaries.
3. The Mission Success Framework allows individual pieces of information to be systematically related to the implications for mission success.
4. The Mission Success Framework provides a powerful tool for modeling system interdependencies, and the implication of those interdependencies on any number of real or hypothetical anomaly scenarios.
5. The Mission Success Framework can be combined with a systematic information requirements analysis to help identify additional tests that can be made to isolate the root cause of an anomaly. In addition, it is possible to systematically evaluate the information required to:
   - Evaluate the health of the critical function in question.
   - Evaluate the availability of alternative success paths.
   - Evaluate the most desirable success paths for implementation.
   - Implement the chosen success path.
   - Monitor the performance of the success path in maintaining or restoring the critical function.
6. The Mission Success Framework serves as a fundamental “map” of the problem solving space for anomaly resolution. Once the structure of the functional model and rules for selecting success path are established, the framework serves as an unbiased guide for systematic anomaly resolution. All anomaly resolution decisions can then be made in an unbiased way with mission success as the primary driver.
7. The function-oriented Mission Success Framework explicitly compensates for the fact that not all possible scenarios can be pre-analyzed and planned for. It provides a mission-focused means to derive corrective actions for the full range of events and combinations of events that challenge the mission-significant critical functions.
8. The Mission Success Framework provides a means to incorporate information from multiple disciplines and place it within a common framework for evaluation. In this way all disciplines and opinions can be represented and systematically considered in light of mission success.
9. Any number of “what-if” scenarios can be evaluated using the Mission Success Framework and directly compared with other alternative scenarios.
10. The Mission Success Framework provides a natural means to integrate both success- and failure-oriented risk models with physical or virtual models of the system, such as those being developed within the SimStation project of the NASA Engineering for Complex Systems program.

LONG-TERM VISION FOR INTEGRATED RISK TOOLS FOR THE ISS PROGRAM

The difficulty of envisioning an integrated tool for use by the overall ISS program is that it will have multiple objectives and be used by individuals or teams with varying skills. Therefore, a long-term vision for an integrated tool to be used by the ISS program should follow the R^3 (**R**isk Assessment, **R**isk Management, and **R**isk Communication) concept. The R^3 concept represents the evaluation of risk, the decisions associated with this information, and the clear dissemination of the evaluation and decisions to appropriate entities. This concept follows, in theory, the natural progression of a problem to its solution and incorporates the ability to involve multiple individuals. Figure 2 shows an overview of the R^3 concept.

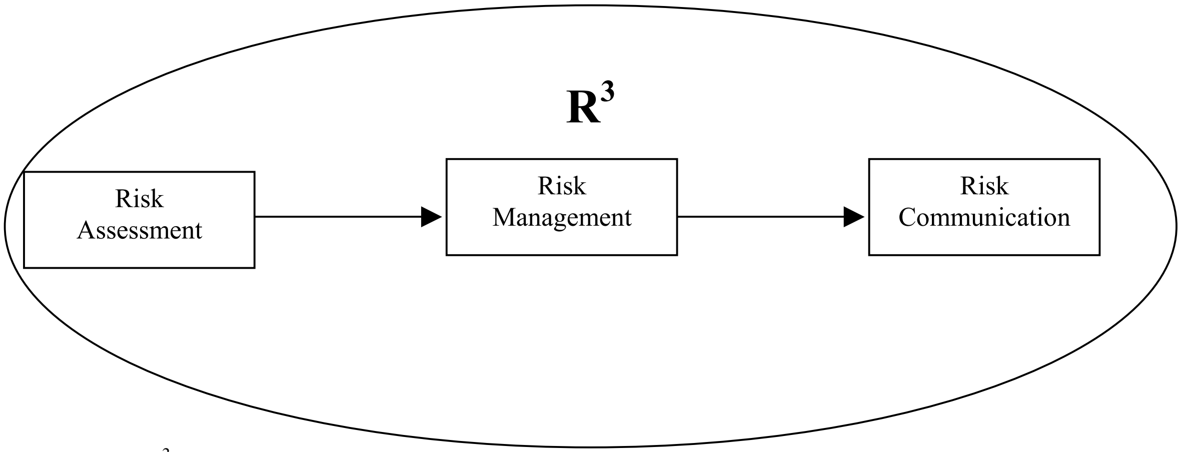

Figure 7. The R^3 concept.

The following paragraphs discuss the specific characteristics and supporting technologies of a tool that contains these concepts. Some of these technologies are available while others are in development or need to be planned to support a long-term goal for a NASA tool that can be used in operations.

Risk Assessment

The evaluation of risk is strictly designed to be an unbiased view of potential vulnerabilities and weaknesses in a system. Evaluation includes a baseline risk that establishes system concerns in a new or pristine state and relative risk to the system as it undergoes changes due to normal wear and use. Evaluation techniques should include associated hardware, software, and human interactions. Inter- and intra-dependencies should be modeled in failure space with the option of converting to success space.

Evaluation of risks should be performed in a qualitative and quantitative manner. They should include static and dynamic modeling methods. A flexible tool is needed to evaluate risks for functions, systems, subsystems, and components. Additionally, user-defined endstates can be created to combine members at the same level of this hierarchy for evaluation.

The ISS program incorporates a modular approach and therefore demands a flexible risk assessment tool interface. As modules are added to the ISS, the risk assessment is modified by definition. In addition, the existing risk assessment also undergoes modification over time as systems are changed to accomplish ISS required functions. This tool would need to accommodate new modules and join them to the modified portion of the ISS.

New risk assessment tools and new versions of current risk assessment tools will be developed in the future. The integrated tool must be able to import and export information to these new versions. This infers that a standard method of converting models into a more universal tool must be available.

Risk Management

Risk management is the process of weighing risk analysis results with other considerations to determine the best manner of reducing significant risks to an acceptable level. The management of risks is a decision making process that encompasses information gathered from the risk analysis including functional impacts, magnitude of risks, and uncertainty of results. Probably the most important aspect of risk management is the ability to direct “what if” questions for analytical resolution that weigh different solutions and their impact on system and functional success. This is often referred to as the risk-informed decision making process. Separation from the analytical process maintains unbiased analyses and allows for other considerations (e.g., public opinion, and political sensitivities) to be included in any controversial decisions.

The integrated tool will have to be able to support some automatic risk management information. Namely, based on the understanding of the risks on a function, system, subsystem, component level, or endstate level, the software will have to be aware when risks in these areas is above a determine area or is trending upwards toward an unacceptable risk level. The risk levels will be user-defined and can be set at different quantitative and qualitative levels. This information should be time based and be displayed for a variety of user-determined time frames. Uncertainty should be displayed in any projection of risk, such that it is clearly understood what the most likely and upper and lower bounds of the associated risks are to enhance management decision.

Understanding the associated risks for the current situation or a postulated scenario projects most of the immediate information to risk managers. However, as systems are modified the dynamics of a risk model may change causing less important components to suddenly become essential to a function, system, or endstate. Viewing the risks along with the important components provides a more complete view for managerial risk-informed decisions.

Risk Communication

Risk communication, in a traditional sense, encompasses risk analysis and management areas. The ability to quickly communicate results in a meaningful manner is important in both of these areas. Although displays for risk management and analysis need to be clear and communicate information to multiple individuals well, this is not the emphasis of this section. NASA and the ISS program have a unique situation that requires the ability to communicate risk analyses and the management of these risks to a set of interdisciplinary team members. This must be done quickly and minimize divergent and unfocused concepts. A tool that can quickly get to the root or close to the root of a problem will be valuable in the MER. This tool must also support communicating this information to individuals and directing conversations on the best solution for problems. We recommend tools that can support both fault and success model development and also be used as a diagnostic aid in a quantitative and qualitative manner. A functional diagram is the most effective manner in relaying this information. We suggest that a functional diagram tied to a success tree be used as a front-end for analysts, operators, and management. The prospective tool should be able to demonstrate Failure Modes and Effects information in a graphical 3D manner.

Another aspect to communication is the ability to easily communicate procedures and safety considerations via text and animations. The integrated tool should provide animations that display general maintenance and recovery information. Special corrective measures or complex installations should be available to reduce maintenance times and potential reworking.

CONCLUSIONS

Real-time risk and fault management is a critical function of the anomaly resolution process for the International Space Station Mission Evaluation Room. The ability to efficiently identify and evaluate on-orbit anomalies, and to formulate and evaluate potential corrective actions is essential for the safe operation of the International Space Station. Current anomaly resolution activities in the MER depend on the effective teamwork of a large number of subsystems engineers and risk specialists. While the current approach has been honed in the operation of NASA manned missions for more than 40 years, there is always the possibility that a critical factor can be overlooked and serious consequences result.

Computer technology may be part of the answer for more efficient and reliable anomaly resolution for space operations. Computers are already invaluable tools for collecting and distributing information about anomalies in progress, and bringing the results of past events and risk assessments to bear for resolution of the current situation. However, effective use of computer technology to directly support the analytic processes of real-time risk and fault management is just beginning.

The nuclear industry has been exploring promising approaches for real-time risk and fault management in the twenty five years since the accident at Three Mile Island. The Critical Safety Function approach has proven to be a powerful paradigm for accident management in nuclear power plants. To date this approach has primarily been applied in the form of hard copy emergency procedures. The implementation of critical function methods as computer-based tools for risk and fault management has been limited because of the difficulties of licensing software tools for performing safety-related functions in commercial NPPs. However, a wealth of research and development experience has been generated that hints at the promise of these methods for application to space operations.

This study has explored the current processes for real-time risk and fault management in the ISS Mission Evaluation Room, and developed recommendations for the use of software tools to assist these processes. Recommendations have been developed for building upon the Galileo fault tree tools to form a full-featured tool for fault isolation and failure analysis. A Mission Success Framework that combines the features of critical function modeling with the fault tree tool has been proposed to form the foundation of an integrated Risk Monitor for real-time risk and fault management in the ISS Mission Evaluation Room.

The Columbia accident has once again demonstrated the absolute necessity for effective risk management processes for manned space operations. It is our hope that organizing system and risk knowledge within a logical framework focusing on mission success may provide one of the risk management components for reducing the likelihood that such a tragedy will occur again.

REFERENCES

1. John G. Kemeny et al., *The Need for Change: The Legacy of TMI,* Report of the President's Commission on the Accident at Three Mile Island, October 1979.
2. A. Bye and E. Ness, "Early Fault Detection and On-line Diagnosis in Real-Time Environments," *Enlarged HPG Meeting on Fuel and materials Performance and Analysis and Computerised Man-Machine Communication, Bolkesjo, Norway, June 9-14, 1991.*
3. W. R. Nelson, "REACTOR: An Expert System for Diagnosis and Treatment of Nuclear Reactor Accidents," *National Conference on Artificial Intelligence, AAAI-82, Pittsburgh, PA, August 18-20, 1982.*
4. P.J. Gaudio Jr. and D.S. Jamison, *Computerized Diagnostic Aid – Success Path Monitor,* EPRI NP-5088, Electric Power Research Institute, 1987.
5. John-Einar Hulsund, Yeonsub Jung, and Svein Nilsen, *COPMA-III, Intelligent Handling of Existing Procedures,* HWR-579, OECD Halden Reactor Project, April 1999.
6. K. Haugset, Ø. Berg, N. T. Førdestrømmen, J. Kvalem, and W. R. Nelson, "ISACS-1, The Prototype of an Advanced Control Room," *IAEA International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich, West Germany, July 9-13, 1990.*
7. U.S. Nuclear Regulatory Commission, *Advanced Information Systems Design: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6633, March 2000.
8. U.S. Nuclear Regulatory Commission, *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6634, March 2000.
9. U.S. Nuclear Regulatory Commission, *Soft Controls: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6635, March 2000.
10. U.S. Nuclear Regulatory Commission, *Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6636, March 2000.
11. U.S. Nuclear Regulatory Commission, *Human Systems Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance,* NUREG/CR-6637, March 2000.
12. International Atomic Energy Agency, *Computerized support systems in nuclear power plants,* IAEA-TECDOC-912, October 1996.
13. Fridtjov ∅wre, "Historical Overview, Current Status, and Future Trends in Human-Computer Interfaces for Process Control," *Nuclear Technology,* Vol. 141, No. 1, January 2003.
14. W. Cullen, *The Public Inquiry into the Piper Alpha Disaster,* London: HMSO, November 1990.
15. W. R. Nelson, *Response Trees and Expert Systems for Nuclear Reactor Operations,* NUREG/CR-3631, February, 1984.
16. W.R. Corcoran et al., "Nuclear Power Plant Safety Functions," *Nuclear Safety,* March/April 1981.
17. M. Modarres, "Functional Modeling of Complex Systems Using a GTST-MPLD Framework," *Proceedings of the International Workshop on Functional Modeling of Complex Technical Systems,* Ispra, Italy, May 12-14, 1993.