IMPROVING PERFORMANCE OF THE SYSTEM SAFETY FUNCTION AT MARSHALL SPACE FLIGHT CENTER

Ed Kiessling, NASA Marshall Space Flight Center,
Donald D. Tippett, The University of Alabama in Huntsville,
and Herb Shivers, NASA Marshall Space Flight Center

Abstract
The *Columbia* Accident Investigation Board (CAIB) determined that organizational and management issues were significant contributors to the loss of Space Shuttle *Columbia*. In addition, the CAIB observed similarities between the organizational and management climate that preceded the *Challenger* accident and the climate that preceded the *Columbia* accident. To prevent recurrence of adverse organizational and management climates, effective implementation of the system safety function is suggested. Attributes of an effective system safety program are presented. The Marshall Space Flight Center (MSFC) system safety program is analyzed using the attributes. Conclusions and recommendations for improving the MSFC system safety program are offered in this case study.

Objective
In August 2003, the CAIB released its report on the causes of the loss of the Space Shuttle *Columbia* during reentry into the Earth's atmosphere on February 1, 2003. In addition to the expected discussion of the physical causes, the CAIB report devoted an entire chapter to discussion of a number of organization-based shortcomings that contributed to the loss of *Columbia*. The CAIB report also described similarities between organizational/cultural conditions manifest at the time of the *Columbia* accident and those prevalent at the time of the Space Shuttle *Challenger* accident in 1986.

The CAIB stated that some of the Rogers Commission recommendations regarding *Challenger* were not in place at the time of the *Columbia* accident some 17 years later. MSFC provided project management and sustaining engineering for the propulsion elements associated with each Space Shuttle mission. The objective of this paper is to review the elements and attributes of a generic system safety program, assess implementation of the system safety function at MSFC (as a case study), and provide recommendations that may prove helpful in preventing future accidents. This paper also seeks to share the NASA/MSFC experience with other enterprises in the hope that they may benefit from the lessons provided by NASA's experience.

This paper is written in the context of NASA as it existed at the time of the loss of *Columbia* and does not consider changes that NASA is developing and implementing in response to the CAIB report. This paper presents the analysis, conclusions, and recommendations of the authors, but does not constitute an official NASA position.

Introduction
Over the course of nearly 22 years, NASA's Space Shuttle program has conducted 113 missions. Two missions ended in catastrophic failure with the loss of a total of 14 astronauts and the Shuttles *Columbia* and *Challenger*. The total financial impact of the *Challenger* accident has been estimated at $12 billion. The total financial impact of the *Columbia* accident has not yet been determined. Space Shuttle flights were suspended for 32 months following the loss of *Challenger*. Current schedules project that at least 25 months will elapse from the date of *Columbia's* loss until Shuttle flights resume.

The two accident investigations readily determined the specific hardware failures responsible for each accident. Both investigations (the Rogers Commission for *Challenger* and CAIB for *Columbia*) also identified organization and management shortcomings that contributed to the accidents. The CAIB noted a number of similarities among the organization and management shortcomings associated with the accidents. Consequently, the CAIB became concerned that some of the organization and management shortcomings may be systemic throughout NASA. NASA intends to prevent a recurrence of this situation and robust implementation of system safety across the Agency is suggested as a means for achieving that objective.

This paper first provides the results of a literature search that identified the generic attributes of a comprehensive system safety program, and then provides validation of those attributes through benchmarking four organizations that are models of excellence in safety. The implementation of the system safety function at MSFC is then analyzed against the necessary attributes, conclusions drawn, and recommendations provided. The MSFC Safety and Mission Assurance (S&MA) Office reviewed this

paper and noted that several of the recommendations have been independently undertaken by the Agency or MSFC. This is considered further validation of the attributes selected as necessary for an effective system safety program.

Literature Review

Definitions. Safety is freedom from accidents (loss events) (Leveson, 2002). System safety is the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle (Air Force Safety Agency, 2000). The definition makes the point that risk can be optimized, reduced, or driven to an acceptable level but cannot be eliminated universally. It also acknowledges that system effectiveness, cost, and schedule considerations are necessary elements in the determination of acceptable mishap risk.

Purpose and Principles of System Safety. System safety employs system theory and system engineering to prevent foreseeable accidents and to minimize the result of unforeseeable accidents. Accidents involve losses in general and include human death and injury, damage and destruction of property, loss of mission, and environmental harm. When potential losses are considered sufficiently serious to warrant expenditure of time, effort, and resources for prevention, a system safety program is appropriate.

The primary concern of system safety is management of hazards. "A hazard is a condition that can cause injury or death, damage to equipment or property, or environmental harm" (Roland and Moriarty, 1990). Thus, hazards are sources of risk of loss. System safety provides for identification, evaluation, elimination, and control of hazards via analysis, design, and management procedures that provide a planned, disciplined, and systematic approach to preventing or reducing the consequences of accidents throughout the life cycle of a system. System safety emphasizes early identification and classification of hazards so corrective action can be taken to eliminate/mitigate hazards before final design decisions are made. Human, organizational, legal, and certification issues are included in the scope of system safety (Leveson, 1995).

Attributes of an Effective System Safety Program. The Federal Aviation Administration (FAA) identifies four attributes of an effective system safety program as planned approach to accomplish tasks, qualified people, authority to implement tasks, and appropriate funding (FAA, 2000).

The Department of Defense (DoD) articulates the attributes of an effective system safety program, as follows:

–Management is always aware of mishap risk.

–Hazards are identified, assessed, tracked, and monitored. Associated mishap risks are eliminated or controlled throughout the system life cycle.

–Actions taken to eliminate or reduce mishap risk are identified and archived for tracking and lessons learned purposes.

–Historical hazard and mishap data, including lessons learned from other systems, are considered and used.

–Safety requirements are designed into the system in a timely and cost-effective manner.

–System users are kept abreast of the safety of the system and are included in the safety decision process.

Leveson identifies flaws in the safety culture, ineffective organization structure, and ineffective technical activities as the generic root causes of accidents (Leveson, 1995). Lack of independence of safety personnel, limited communication channels and information flow, and information deficiencies are elements of these root causes (Leveson, 1995).

System safety engineers have found that the degree of safety achieved depends directly on the emphasis received in the organization (Leveson, 1995). The preceding information from the FAA, the DoD, and Leveson suggests that an effective system safety program should possess a sincere commitment from management, a strong safety culture, a safety organization with authority and independence, open communication, qualified safety personnel, clearly defined roles and policy, effective processes and tools, and sufficient resources to function effectively.

Management Commitment. This is the most important attribute of an effective system safety program (Bahr, 1997 and Leveson, 1995). Each manager must sincerely believe that safety truly does come first and must consistently and unwaveringly demonstrate that belief *through action*. Verbal and written statements of commitment alone are not sufficient. A manager's commitment must be continuously demonstrated through decisions and actions involving planning, designing for, and conducting hazardous operations themselves, but also through issues such as providing sufficient safety resources, maintaining and communicating effective safety processes, and training and educating employees. The presence of a strong management commitment plays an important role in assuring all the other attributes of an effective system safety program are effectively implemented on an ongoing basis (Leveson, 1995).

Safety Culture. An organization has a healthy safety culture when all employees, both management and workers, sincerely believe that safety is the top priority and consistently demonstrate that belief through actions and decisions. A healthy safety culture helps an organization exercise continuous vigilance, keeps safety first, and maintains sound safety decision-making processes at all levels. As with management commitment, actions that demonstrate commitment to system safety are the best indications of a healthy safety culture. Uninhibited yet responsible exercise of 'stop work authority' by any employee is an indicator of a healthy safety culture. Employee willingness to openly report, without fear of retribution, process errors with cost, schedule, and safety consequences is another positive indicator.

Independent Safety Organization. An independent safety organization must have the ability and authority to speak openly and with effect, and must have sufficient technical resources to effectively penetrate issues and provide credible positions with solid supporting rationale and evidence. An independent safety organization must have sufficient stature in the organization to be able to promptly communicate issues and concerns to the relevant decision authority in order to assure the proper focus on safety. To be truly independent, an independent safety organization should be funded by a neutral element of the organization structure rather than by the supported program or project office.

Effective communication. Decision makers require timely knowledge of safety issues to make informed decisions or positively influence the decisions of others. An all-inclusive communication process helps minimize the chance that any organizational element, such as an independent safety office, is isolated from the project's information flow and associated decision process. In large organizations, effective communication of safety information is sometimes accomplished through the use of safety working groups.

Qualified Personnel. This attribute addresses the education, training, and experience requirements not only for employees performing specialized system safety tasks but also all other employees throughout the program/project organization. System safety specialists must be knowledgeable of the information systems, analytical tools, and verification and validation processes necessary to conduct a system safety program. Competence in the applicable project technical disciplines may also be important. Depending on the technical complexity of the project, training a project technical expert on the relevant system safety tools and processes may be more economical than training a system safety specialist on the technical discipline.

In addition to the education, training, and experience necessary to perform assigned technical functions, project employees need some familiarity with system safety. Project employees may not need to know how to perform a hazard analysis but do need to know how to exercise stop work authority, how to present concerns and dissenting opinions, and how to report mishaps and errors with potential safety consequences. To promote a healthy safety culture, employees should also have an appreciation of the value of the system safety program

Independent system safety organization managers are often required to have a current professional engineer's license as well as certification as a Certified Safety Professional (CSP) (Leveson, 1995). The Air Force Space and Missile Division requires all contractor system safety managers to hold a B. S. degree in engineering or an applied science, have registration as a professional engineer (PE) or CSP, and have at least 4 year's experience as a system safety engineer covering at least three of six Air Force-defined system safety functional categories (Leveson, 1995).

System Safety Roles, Processes and Tools. Well-defined system safety roles and processes supported by effective tools must be employed throughout the system life cycle to avoid accidents and enable the identification, analysis, and disposition of hazards. Disposition of hazards involves elimination, mitigation, or acceptance of the hazards.

A system safety program plan (SSPP) specifies the processes and tools to be employed on a project and addresses the roles, responsibilities, and authorities of organizations included in the project. The plan should contain a safety policy statement that defines the role of safety in relation to other project goals and assigns authority. The plan addresses all phases of the project life cycle.

The SSPP specifies standards that will be used. Standards specify a minimum level of practice but can also limit flexibility. Typically, the SSPP addresses the degree of tailoring that will be allowed and provides for oversight of the tailoring process.

The SSPP addresses methodologies for identifying hazards. Hazard analysis and fault tree analysis have been the primary analytical tools for the system safety discipline (Bahr, 1997) and have traditionally been applied to investigating hardware failures (Leveson, 2002). The results of the analyses are used in studies that determine whether or not the hazard will be accepted, eliminated, or mitigated. Throughout the design, development, and testing phases, periodic

reviews are essential to validate the continued relevance of the analysis. A configuration management process for tracking, reviewing, and verifying the controls is required. For the operational phase, a performance audit process is customarily employed to assure that controls continue to be properly implemented.

Mishap and problem reporting databases provide a means of capturing and processing accident and failure information that can then be added to the lessons learned file. Furthermore, trend analysis of these databases and selected system performance parameters can be useful in identifying problems that are growing more frequent and severe with the passage of time.

Finally, a visible and efficient process for eliciting and resolving dissenting opinions concerning safety in design and management must also be established. This process can be performed by a safety working group, if one is created, or through the established review and decision processes employed by the program or project office.

Resources. Personnel and material resources are essential to collect information, perform the necessary analyses, conduct trade studies to determine which controls will be implemented, administer tracking and status systems, and conduct reviews and audits. If sufficient resources are not allocated for the safety function, the healthy safety culture will likely erode.

Based on the preceding discussion, the criteria presented in Exhibit 1 constitute the attributes of an effective system safety program.

Exhibit 1. Effective System Safety Program Attributes.

Management Commitment
Safety Culture
Independent Safety Organization
Communication
Qualified/Educated Personnel
Well-Defined Roles/Processes/Tools including:
– Use of Technical Standards
– Capture/Use of Lessons Learned
– Audits and Reviews
– Stop Work Authority
Sufficient Resources

Validation of System Safety Program Attributes. The CAIB compared NASA safety practices to those of three organizations (The Aerospace Corporation, Naval Reactors program, and the Navy's SUBSAFE program) that operate risky technologies and have achieved or nearly achieved accident-free performance (Gehman et al., 2003). In October 2003, representatives from each of these organizations and a Dupont Corporation representative delivered prepared statements to the House Science Committee regarding the practices responsible for their safety success. The authors reviewed the relevant information in the CAIB report (Gehman et al., 2003) and the four statements presented to the House Science Committee (Bowman, 2003; Grubbe, 2003; Johnson, 2003; Sullivan, 2003) to determine the extent to which the effective system safety program attributes presented in Exhibit 1 paralleled the practices identified by the five organizations. Exhibit 2 summarizes the results of the comparison.

Dupont, which began as a manufacturer of black powder, has over 200 years experience in the production of a variety of chemical products via extremely hazardous processes. Dupont has established the reputation of a world-class leader in safety and provides safety consultant services internationally to a variety of corporations and government agencies. Dupont's practices completely parallel the Exhibit 1 attributes.

The Aerospace Corporation is a private not-for-profit corporation that operates a federally funded research and development center for the DoD. A major component of The Aerospace Corporation's mission is to reduce the risk of launch failure of DoD space missions, and it has been successful as evidenced by a 2.9% probability of failure on DoD expendable launches in comparison to 14.6% for commercial launches. The Aerospace Corporation emphasizes the education and experience level of its staff as a major element of its success. Average years of experience are approximately 25 with 74% holding advanced degrees and 29% holding Ph.D.s. The Aerospace Corporation's practices parallel all of the Exhibit 1 attributes except Management Commitment and Safety Culture. This is most likely a consequence of the perspective of The Aerospace Corporation as an assurance organization. Unlike Dupont and the Naval Reactors program, The Aerospace Corporation only reviews and evaluates, but does not operate, high-risk systems. Technical excellence provided by The Aerospace Corporation enables the safe performance record achieved by DoD expendable vehicles and their payloads.

The Naval Reactors program administers all aspects of the Navy's nuclear propulsion program from initial research through disposal of retired systems. The effectiveness of the Naval Reactors program is indicated by the fact that the U.S. Navy has never lost a submarine due to nuclear propulsion system malfunction. The Naval Reactors practices parallel all of the Exhibit 1 attributes except the Independent Safety Organization. The Naval Reactors program elected to "mainstream" safety. Mainstreaming safety

means integrating safety into all line and staff organizations in lieu of maintaining an independent safety organization. The Naval Reactors program has been successful with this approach by establishing a strong safety culture combined with strong management commitment (Bowman, 2003).

The Navy's SUBSAFE program administers a certification process that focuses on the design, material, fabrication, and testing of submarines to assure watertight integrity and recovery capability for all U.S. Navy submarines. SUBSAFE is specifically focused on this assigned mission and does not address other issues such as fire safety, weapons system safety, or nuclear reactor safety. SUBSAFE has been an active program since 1963 and no SUBSAFE-certified submarine has been lost during that period. SUBSAFE program safety practices parallel all of the Exhibit 1 attributes.

Each of the four organizations either operates, evaluates, or certifies high-risk systems with potentially catastrophic accident scenarios and thus has some common ground with the NASA Space Shuttle. The close agreement of the safety practices of the four organizations with the effective system safety program attributes presented in Exhibit 2 validate the effective system safety attributes presented in Exhibit 1 so the attributes will be used as the criteria for analyzing the NASA MSFC system safety program in the following section.

Analysis

MSFC is one of NASA's nine major field Centers and performs engineering and scientific development functions in the fields of space propulsion (Earth-to-orbit as well as in space), space transportation (crewed and non-crewed) vehicles, microgravity research, and optics manufacturing technology. The Center employs ~2600 civil servants and ~3000 contractors. MSFC's major accomplishments include development of the Mercury-Redstone vehicle that carried America's first astronauts into space, the Saturn rockets that launched the Apollo vehicles that carried humans to the Moon and placed *Skylab* in orbit, the Hubble Telescope, the Chandra X-Ray Observatory, and the Space Shuttle propulsion system.

Project offices for the four Space Shuttle propulsion elements—Space Shuttle Main Engine, External Tank, redesigned Solid Rocket Motor, and Solid Rocket Booster—reside at MSFC. NASA policy assigns each project manager the ultimate responsibility for project safety. The MSFC S&MA Office assists the project managers with their safety responsibility.

The system safety function is implemented through a hazard analysis process. Another safety process is the investigation of mishaps, which makes extensive use of fault tree analysis. Each project prepares a safety plan and tailors the contents of that plan to implement an effective, yet affordable, system safety program. MSFC S&MA participates in the milestone technical reviews established by the project. In the case of projects destined to fly on the Space Shuttle or *International Space Station*, MSFC S&MA administers a Payload Safety Review Board that is staffed by experts from both the MSFC Engineering Directorate and the MSFC SM&A Office.

MSFC S&MA performs three system safety roles. They serve as an expert safety consultant when assisting programs and projects establish safety plans and formulate safety requirements. They act as an in-line engineering resource by conducting hazard analyses, fault tree analyses, etc. for program and project offices. Finally, S&MA performs a review/oversight role by participating in program or project milestone reviews or conducting safety audits.

Exhibit 2. Comparison of Organization Practices with Effective System Safety Program Attributes.

Attribute	Dupont	The Aerospace Corporation	Navy Reactors	SUBSAFE
Management Commitment	X		X	X
Safety Culture	X		X	X
Independent Safety Organization	X	X		X
Communication	X	X	X	X
Qualified/Educated Personnel	X	X	X	X
Well-Defined Roles, Processes and Tools Including:	X	X	X	X
– Use of Technical Standards	X	X	X	X
– Capture/Use of Lessons Learned	X	X	X	X
– Audits and Reviews	X	X	X	X
– Stop Work Authority	X	X	X	X
Sufficient Resources	X	X	X	X

In the following paragraphs, the attributes of an excellent system safety (Exhibit 1) are used to evaluate the MSFC system safety program and identify improvement opportunities. Exhibit 3 summarizes organizational issues identified as common to both the *Challenger* and *Columbia* accidents.

Management Commitment. The CAIB states that its, "investigation revealed that in most cases, the Human Space Flight Program is extremely aggressive in reducing threats to safety" (Gehman et al., 2003). This suggests an overall positive safety performance for managers and employees alike. However, the CAIB also observed that NASA's ambitious goals during the lean budget years preceding the *Columbia* accident provided insufficient resources for S&MA functions. In 1999, MSFC began a focused effort to raise and maintain safety consciousness and practice. The implementation was very successful for occupational and industrial safety. The CAIB acknowledges that NASA has excellent occupational and industrial safety programs. For system safety, the CAIB noted "the Board witnessed a consistent lack of concern about the debris strike on *Columbia*" (Gehman et al., 2003). With regard to Failure Modes and Effects Analysis/Critical Items List retention rationale, the CAIB also noted that "the retention rationales appear biased toward proving that the design is 'safe' sometimes ignoring significant evidence to the contrary" (Gehman et al., 2003).

Deficiencies in other attributes of an effective system safety program may be an indication that management commitment is suboptimum. The preceding discussion and the data presented in Exhibit 3 suggest insufficient safety resources, inadequate analysis and information processing procedures, communication shortcomings, and dependent safety organizations all contributed to diminished performance of the Space Shuttle system safety function. For MSFC, the issue may be that project, engineering, and S&MA personnel focused on solving the technical hardware problems of the day, but did not provide sufficient emphasis for assuring that their processes were fully integrated and executed to the necessary standard. This would explain why the hazard analysis and documentation process and the failure mode and effects analysis (FMEA) process exhibited the shortcomings identified by the CAIB.

Safety Culture. The CAIB determined that the Space Shuttle program and the associated safety organizations constituted "a broken safety culture" (Gehman et al., 2003). One significant indication of this condition reported by the CAIB was the silence of safety personnel during the events leading up to the loss of *Columbia*. The CAIB also noted "Shuttle Program management made erroneous assumptions about the robustness of a system based upon prior successes rather than dependable engineering data or rigorous

Exhibit 3. Common findings from *Challenger* and *Columbia* Investigations.

Challenger (Rogers et al., 1986)	*Columbia* (Gehman et al., 2003)	Perceived Issues
"Reductions in safety, reliability, and quality assurance work force at Marshall and NASA HQ have seriously limited capability in those vital functions." "As the flight rate increased, the Marshall safety, reliability, and quality work force was decreasing which adversely effected mission safety."	"Throughout its history, NASA has consistently struggled to achieve viable safety programs to the constraints and vagaries of changing budgets. Yet, according to multiple high level independent reviews, NASA's safety system has fallen short of the mark."	Insufficient staff (mainly as a consequence of funding limitations).
"Organizational structures at Kennedy and Marshall have placed safety, reliability, and quality assurance offices under the supervision of the very organizations and activities whose efforts they are to check."	"Safety and Mission Assurance organizations supporting the Shuttle program are largely dependent upon the Program for funding, which hampers their status as independent advisors."	Lack of independence driven by funding practice.
"Problem reporting requirements are not concise and fail to get critical information to the proper levels of management."	"NASA information databases such as the Problem Reporting and Corrective Action System are marginally effective decision tools."	Poor presentation and communication of critical information across organization boundaries.
"Little or no trend analysis was performed on O-ring erosion and blow-by problems."	"The Space Shuttle has a wealth of data tucked away in multiple databases without a convenient way to integrate and use the data for management, engineering, or safety decisions."	Ineffective use or failure to use available information for safety analyses.

testing" (Gehman et al., 2003). Acceptance of such logic is uncharacteristic of an organization with a healthy safety culture. Given MSFC's responsibility for managing the four major propulsion elements of the Space Shuttle, the CAIB observations give cause for reassessing the health of the MSFC safety culture.

The CAIB and senior NASA management agree that strengthening an organization's safety culture takes time—probably years. Consequently, the results of the recent Assessment and Plan for Organizational Culture Change at NASA (BST, 2004) may be the best available measure of the strength of the safety culture at MSFC. MSFC employees placed the MSFC "safety climate" in the 88th percentile, "approaching others about safety" ranked in the 98th percentile, and "upward communication about safety" scored in the 73rd percentile (BST, 2004). This suggests an overall very positive employee attitude toward safety; however, upward communication of safety issues requires attention. MSFC's scores also reflect a very positive teaming environment as evidenced by a teamwork score in the 93rd percentile and a work group relations score in the 94th percentile. It may be that employees, like management, focus on resolving the pressing hardware issues while unintentionally underemphasizing the effort necessary for keeping processes and supporting information systems current, effective, and disciplined.

Independent Safety Organization. The CAIB reported that the Space Shuttle "operational and system safety program is flawed by its dependence on the Shuttle program... the safety apparatus is not currently capable of fulfilling its mission... An independent safety structure would provide the Shuttle program a more effective operational safety process" (Gehman et al., 2003). The MSFC S&MA Office is funded by the programs and projects that it supports. Consequently, MSFC S&MA is limited by the amount of resources a given program or project is willing to fund and hence in the amount of service that can be provided to that program or project. The CAIB also observed that NASA "could not obtain budget increases during the 1990s" and did not "adjust its ambitions to this new state of affairs" (Gehman et al., 2003). The CAIB noted that S&MA organizations had not received adequate funding in recent years. Furthermore, there is a natural human tendency to agree with the judgements of one's benefactor. Thus, MSFC S&MA employees may be predisposed to be more understanding and less critical of the programs and projects supported.

MSFC S&MA does not possess in-depth technical expertise in the aerospace engineering subdisciplines. The CAIB observed that "structure and process place Shuttle safety programs in the unenviable position of having to choose between rubber-stamping engineering analyses, technical efforts, and Shuttle program decisions, or trying to carry the day during a committee meeting in which the other side almost always has more information and analytic capability" (Gehman et al., 2003). When MSFC S&MA attempts to establish a technical position on a complex engineering issue, the MSFC Engineering Directorate must provide assistance. However, the Engineering Directorate is a primary source of engineering expertise for the program and project offices. Consequently, MSFC S&MA seeks assistance in preparing an independent assessment from the same organization that worked with the program and project offices (and their contractors) to develop the systems and subsystems that MSFC S&MA is attempting to assess.

Communication. The CAIB noted communication shortcomings between Space Shuttle project offices and the S&MA organizations during the periods preceding both the *Challenger* and *Columbia* accidents. The Rogers Commission reported the absence of any safety organization participation in the *Challenger* launch decision in spite of the fact that MSFC S&MA had declared a launch constraint (Rogers et al., 1986). The CAIB reported, "The exchange of communications across the Shuttle program hierarchy is structurally limited" (Gehman et al., 2003). The CAIB also observed a Shuttle program tendency to oversimplify issues and concerns in the course of communicating and resolving the issues and concerns.

At MSFC, the practice of co-locating S&MA employees in the project offices has promoted good communication. Project managers customarily chair problem review boards which assure that MSFC project managers are aware of the content, status, and disposition of problem reports in the MSFC-managed problem reporting and corrective action system.

Qualified Personnel. The CAIB concluded that NASA's safety organization was not an effective voice in discussing STS-107 issues due to a lack of capability independent of the Shuttle program (CAIB, 2003). The CAIB also observed that NASA managers at many levels are placed in positions without completing a standard training and education program to prepare them for their roles (CAIB, 2003). Program and project managers, although ultimately responsible for the safety of their programs and projects, are not required to complete system safety training.

Historically, NASA (including MSFC) has not required PE or CSP credentials for selection for or retention in engineering and management positions in S&MA organizations. Pursuit of professional credentials and training is the employee's prerogative. For employees who choose to participate, NASA offers

a wide variety of Web-based courses, on-site and off-site classroom courses, and university programs. While MSFC's policy permits maximum flexibility and initiative on the individual engineer's part, it does not assure that employees will be properly prepared to function in system safety engineer positions.

Employees in MSFC program/project offices and engineering organizations are not required to complete basic or advanced system safety training. S&MA personnel are not required to have previous project experience. Both groups gain knowledge and experience as they perform their respective roles.

Well-Defined Roles, Processes, and Tools. MSFC internal procedures (Marshall Work Instruction (MWI) 1700.2 'System Safety Program' and the MSFC Organization charter (MSFC, 2002)) communicate the requirement for a system safety program, but do not assign specific implementation roles to either the MSFC S&MA Office or program/project offices. This gives MSFC S&MA the option to provide three system safety roles: (1) MSFC S&MA may perform the role of expert consultant by preparing program/project system safety program plans, (2) S&MA may prepare hazard analyses for projects, and (3) S&MA provides an audit or review function of program/project system safety activities. In those cases where MSFC S&MA both prepares and reviews hazard analyses, an independent review conflict may exist.

Methodologies for performing hazard analysis, fault tree analysis, FMEA, etc. are documented in NASA handbooks and standards. These documents levy few requirements or standards. This approach maximizes flexibility and permits extensive tailoring; it complicates the task of assuring that the hazard and failure modes analyses are credible. CAIB "investigators found that a large number of hazard reports contained qualitative judgments such as "believed" and "based on experience from previous flights this hazard is an 'Accepted Risk'" (Gehman et al., 2003).

Although MSFC S&MA has participated in the development of a lessons-learned database managed by NASA Headquarters, "design engineers and mission assurance personnel use it only on an ad hoc basis, thereby limiting its utility" (Gehman et al., 2003).

MSFC S&MA employs the NASA Engineering Quality Audit (NEQA) process to audit contractors that provide flight hardware and associated ground support equipment for NASA programs and projects. The NEQA process, defined in MWI 5330.2 'NASA Engineering and Quality Audit', clearly and thoroughly addresses system safety considerations relevant to the contracts. MSFC S&MA also provides representation to project/program review boards for contracted and in-house programs and projects.

Unlike Air Force programs, MSFC does not employ system safety working groups either within individual projects or collectively by including all projects in a Center-led system safety working group.

MSFC S&MA maintains both problem reporting and mishap reporting databases that could support the lessons learned and the issue/concern communication tasks. The problem report and mishap report databases are supported by trend analysis features. MSFC S&MA personnel report significant trends to the relevant program or project manager; however, internal project or program communication channels usually provide earlier notice to project managers. Additionally, many of the small projects do not participate in the problem reporting system due to budget limitations.

Sufficient Resources. Exhibit 3 states that insufficient resources for system safety characterized the periods preceding both the *Challenger* and *Columbia* accidents. In the case of *Challenger*, the reduced resources were the consequence of management's view that the Space Shuttle fleet had transitioned from a developmental status to an operational status (Rogers et al., 1986). Management believed that an operational vehicle required less expenditure for safety assurance than a developmental vehicle (Rogers et al., 1986). In the case of *Columbia*, NASA was adjusting to reductions in annual budgets and the Agency was attempting to do its work better, faster, and cheaper while maintaining a very aggressive set of goals (Gehman et al., 2003). In both cases, catastrophic accidents followed.

Conclusions

The preceding analysis yields the following conclusions:

1. Agency, Center, and Shuttle program managers have not consistently addressed all the attributes required for an effective system function. For MSFC, improvement of hazard analysis and FMEA, documentation, and communication appears to be the key issue.
2. The MSFC safety culture requires improvement in upward communication of safety concerns and issues.
3. The organizational independence of the MSFC S&MA organization is hampered by dependence on programs and projects for funding, and is further diminished by the limited technical engineering expertise allocated to S&MA organizations.
4. NASA, including MSFC, does not prescribe professional development requirements for employees involved in the implementation of the system safety function.
5. S&MA organizations, including MSFC S&MA, have been chronically underfunded and understaffed.

6. S&MA organizations, including MSFC, have not universally and consistently maintained technical rigor in the hazard analysis process and in the process of documenting hazards.
7. There is potential for compromising independence of S&MA reviews if the same S&MA personnel prepare and review the same hazard analysis.
8. S&MA organizations have not universally and consistently maintained problem reporting and corrective action systems that are complete, useful for trend analysis, and user friendly.
9. S&MA organizations, including MSFC, have not universally and consistently supported a disciplined lessons-learned program.
10. MSFC has not advocated the use of system safety working groups, which is a practice that is employed and valued by the Air Force aerospace community.

Recommendations

The following recommendations address the issues identified in the Conclusions section:
1. MSFC management should reassess commitment to safety and the health of the MSFC safety culture. The Shuttle project management decision processes should be emphasized, and should include assuring that all safety-related information resources are fully integrated and used in decision making.
2. NASA should provide direct funding for S&MA organizations as recommended by the Rogers Commission and the CAIB to enable organizational independence.
3. MSFC S&MA should conduct a thorough review of information and issue/concern communication processes. The review should include the relevancy of S&MA-maintained databases and the technical capability of S&MA personnel engaged in these processes.
4. MSFC S&MA should maintain sufficient staff and work assignment controls to assure independence of reviews of hazard analyses if the present S&MA policy of preparing hazard analyses is continued.
5. NASA S&MA organizations should conduct a collaborative effort, including program and engineering organizations, to review and standardize processes for problem and mishap reporting, hazard analysis, trending analysis, and lessons learned.
6. NASA, including MSFC, should investigate the use of standardized development programs for technical and managerial employees associated with implementation of the system safety function. The approach employed by the Air Force may provide a useful model.
7. MSFC S&MA should assess the potential value of implementing system safety working groups.

During the Space Shuttle return-to-flight process, MSFC S&MA should take the opportunity to assess the applicability of the CAIB findings to the processes, practices, and behaviors that comprise the MSFC S&MA organization. By doing so, MSFC S&MA will be able to either improve organizational performance or validate that MSFC S&MA employees are presently doing the right things.

NASA is presently responding to the CAIB report. An Agency wide initiative to strengthen safety culture is underway. S&MA organizations are now funded independently of the programs/projects they assess. Additional resources are now allocated to S&MA organizations to provide for improved performance. Independent technical resources are now available through the NASA Engineering and Safety Center, which assesses technical issues Agencywide. At MSFC, an independent technical authority is being created to provide independent technical assessments from a team comprised of S&MA and engineering resources. The MSFC S&MA organization has created a system safety working group and has established a specific development program for safety, reliability, and quality engineers. The authors recommend that NASA pursue the remaining recommendations to minimize the likelihood of another accident with management and organization failures as contributing factors.

For engineering managers in general, the lesson learned from NASA's experience is that management process and organization errors can contribute to catastrophic accidents. Careful observance of the criteria previously presented is necessary to keep an organization's management system functioning in support of safety rather than unwittingly working against it.

References

Air Force Safety Agency, Air Force System Safety Handbook (July 2000), pp. 1.

Bahr, Nicholas J., *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor and Francis (1997), pp. 36-70.

Bowman, F. L., Statement to the House Science Committee (October 29, 2003).

BST, Assessment and Plan for Organizational Change at NASA (March, 15, 2004), Appendix D.

Federal Aviation Administration, FAA System Safety Handbook (December 30, 2000), p. E-3.

Gehman et al., Columbia Accident Investigation Board Report Volume 1 (August 2003), pp. 97-223.

Grubbe, Deborah L., Statement to the House Science Committee (October 29, 2003).

Johnson, Ray F., Statement to the House Science Committee (October 29, 2003).

Leveson, Nancy G., *Safeware System Safety and Computers*, Addison-Wesley (1995), pp. 227-285.

Leveson, Nancy G., A New Approach to System Safety Engineering, MIT (June 2002), pp. 57-130.

Marshall Space Flight Center, Safety and Mission Assurance Office Mission Statement (February 4, 2002), p. 1.

Rogers, William, et al., Report of the Presidential Commission on the Space Shuttle Accident (June 6, 1986), pp. 152-161 and 198-201.

Roland, Harold E., and Brian Moriarty, *System Safety Engineering and Management*, revised edition, John Wiley (1990), p. 6.

Sullivan, Paul E., Statement to the House Science Committee (October 29, 2003).

About the Authors

Edward H. Kiessling received his M.S. degree in Engineering Management from The University of Alabama in Huntsville. He is manager of the Engineering Business and Integration Office at NASA Marshall Space Flight Center. He is a registered Professional Engineer in Alabama.

Donald D. Tippett holds master and doctor degrees in industrial engineering from Texas A&M University, and a bachelor's degree in mechanical engineering from the U.S. Naval Academy. He is a member of the engineering management faculty at The University of Alabama in Huntsville. His previous experience includes 10 years active duty as a carrier-based naval aviator with the U.S. Navy. He held a project management position in materials management systems with Union Carbide Corporation and served as an advanced technology program manager with Newport News Shipbuilding.

Charles Herbert Shivers received his Ph.D. from The University of Alabama in Huntsville in Industrial and Systems Engineering and Engineering Management. He is Deputy Manager, Engineering Systems Department, of the NASA MSFC Engineering Directorate and has over 25 years experience in Industrial and Systems Safety for the Department of the Army, the Tennessee Valley Authority, and NASA. He also holds degrees from Auburn University, Bachelor of Industrial Engineering; and Texas A&M University, Master of Engineering, Industrial Engineering. He is a registered Professional Engineer in Alabama and a Certified Safety Professional.