View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by NASA Technical Reports Server

Technical Excellence and Communication, The Cornerstones for Successful Safety and Mission Assurance Programs

Roy W. Malone, *Marshall Space Flight Center, MSFC, Mail Code QD-01, Huntsville, AL, USA, 35812*
Email: roy.w.malone@nasa.gov
John M. Livingston, *Bastion Technology, MSFC, Mail Code QD-01(Bastion), Huntsville, AL, USA, 35812*
Email: john.m.livingston-1@nasa.gov

ABSTRACT

The paper describes the role of technical excellence and communication in the development and maintenance of safety and mission assurance programs. The Marshall Space Flight Center (MSFC) Safety and Mission Assurance (S&MA) organization is used to illustrate philosophies and techniques that strengthen safety and mission assurance efforts and that contribute to healthy and effective organizational cultures. The events and conditions leading to the development of the MSFC S&MA organization are reviewed. Historic issues and concerns are identified. The adverse effects of resource limitations and risk assessment roles are discussed. The structure and functions of the core safety, reliability, and quality assurance functions are presented. The current organization's mission and vision commitments serve as the starting points for the description of the current organization. The goals and objectives are presented that address the criticisms of the predecessor organizations. Additional improvements are presented that address the development of technical excellence and the steps taken to improve communication within the Center, with program customers, and with other Agency S&MA organizations.

1. INTRODUCTION

There are a number of factors that need to be considered in the development of a sound and effective S&MA organization. Most importantly there is a need to make sure that organizational capabilities are consistent with organizational responsibilities. Technical excellence and communication skills are a necessary foundation for any successful effort.

2. BACKGROUND

The development of the major elements of the S&MA function at the MSFC has followed different paths. At the time of the Challenger accident, the differences in the safety, reliability, and quality assurance functions were both organizational and functional in nature.

The MSFC Safety Office had both a System Safety Office and an Industrial Safety Office; however, the Safety Office heritage was based on its role as an Industrial Safety organization. The System Safety effort was a relatively new effort in response to an Agency level initiative after the Apollo I fire. System Safety Engineering was a "foreign" concept from the aviation and defense industries; introduced after the Saturn V launch vehicle design and development was completed. Flight safety for MSFC systems had been achieved by a combination of conservative design and extensive testing supported by active reliability and quality assurance functions.

The reliability and quality assurance functions were in the Quality and Reliability Laboratory and closely tied to the Center Engineering effort by tradition and organizational structure. The major Reliability Analyses Tools which include Failure Modes and Effects Analysis (FMEA), and the Critical Items List (CIL) were familiar to the engineering community, with the CIL having been introduced during the Saturn V development. At this time there were reliability and quality assurance groups within the Program offices who provided insight and coordination between the Lab and the respective projects.

For the System Safety effort, it was a question of a general lack of "clout", not organizational position, since the organization reported directly to the Center Director. In this context, clout is the power to direct, shape, or otherwise influence conditions that have to do with flight safety and mission success. There are four organizational attributes that promote clout:

organizational mass (size), organizational skills (knowledge and ability to apply), organizational responsibilities, and organizational connections (formal & informal). Conversely it follows that for any S&MA organization, the lack of, or weakness in any of those characteristics reduces that organization's clout. It is important that management constantly review their organization's performance to assure the most effective and relevant effort is being made.

The lack of organizational mass impacts an organization's ability to assess potential issues or concerns. This leads to a lack of independent assessment and the tendency to accept the status quo. In a design and development phase, where a number of product development teams are active, the lack of personnel limits the system safety organizations ability to interact directly with the design teams. Opportunities are lost to achieve design solutions to potential safety risks with the minimum impact on system design. It also deprives the system safety team insight and understanding of design and operational details that could adversely affect their ability to provide effective system safety support for the life cycle of the program/project.

Shortcomings in an organization's defined, or assumed, role in a parent organization can also contribute to the underperformance of an S&MA effort. S&MA roles and responsibilities need to be clearly defined and reflected in the program/project and the general organizational structure. Customer feedback is another important form of communication to assure the effectiveness of an S&MA program. Evaluations of the quality of service, products, and personnel should be solicited periodically from customers at both the working and management levels. Internal surveys provide an opportunity for self-assessment and a vehicle for employees to offer suggestions for improving the organizations performance. The information collected can then be utilized to update strategic planning and the structure of the day-to-day program support.

While some compensations and adjustments can be made, major shortcomings in any of those general characteristics will increase the likelihood of unsatisfactory performance by the assurance organization. Clout and performance has a direct relationship (not necessarily one-to-one).

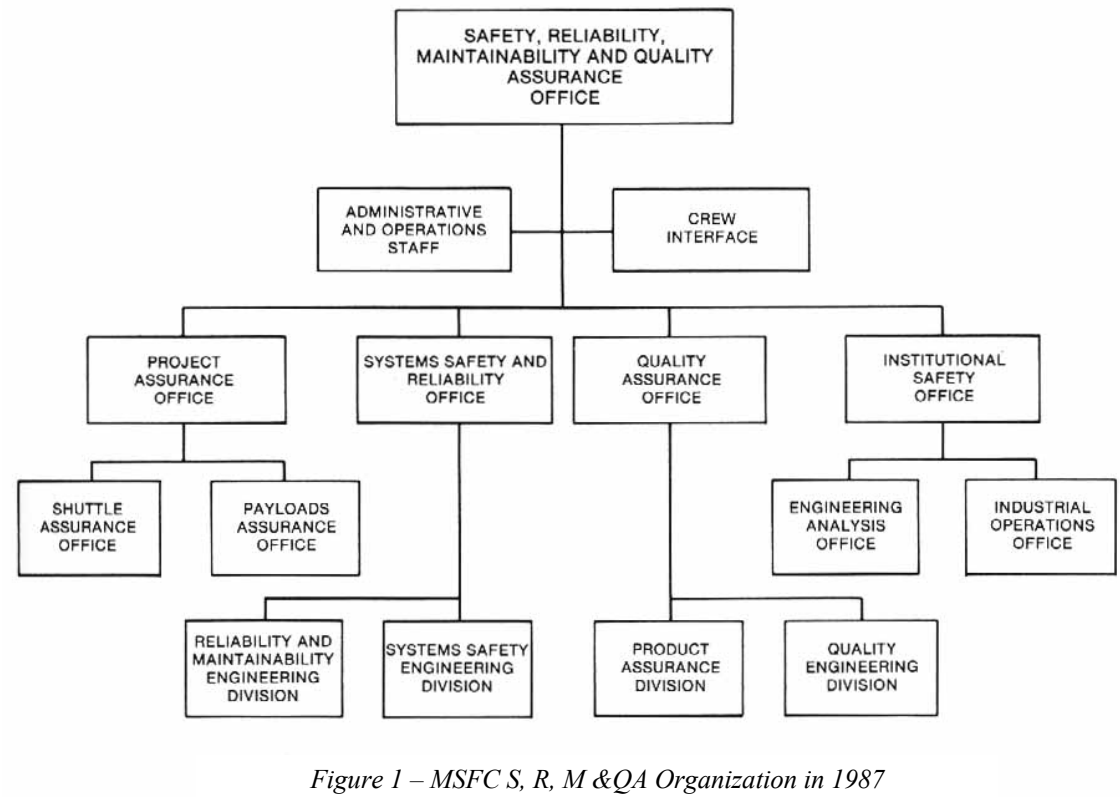

Figure 1 – MSFC S, R, M &QA Organization in 1987

Following the Challenger accident in 1986, the Rogers Commission was critical of the fact that, "Safety, Reliability, and Quality Assurance representatives were not included in technical issue discussions on the evening prior to the fateful flight." The Commission also noted inadequate S&MA staffing at MSFC; "Reductions in the safety, reliability and quality assurance work force at Marshall and NASA Headquarters have seriously limited capability in those vital functions (safety program responsibility) to ensure proper communications." [1]

In direct response to the Rogers Commission findings on the Challenger accident, a new Safety and Mission organization was established at MSFC as shown in Figure 1. The functions of the Center Safety Office (Industrial & Systems Safety) were combined with the Reliability, Maintainability, and Quality Assurance functions that had been formerly part of the center Science and Engineering Directorate. The new Safety, Reliability, Maintainability, and Quality Assurance Office reported directly to the Center Director. A mission support contractor function was also established to provide technical support for the different disciplines that made up the new organization. Within a short time, the organization was re-named the Safety and Mission Assurance Office to better reflect the major objectives of the office.

Soon after the Space Shuttle Program (SSP) completed the return-to-flight activities and resumed its flight program, the S&MA disciplines came under pressure to reduce the size of the new organization at MSFC. Successful flights and a general shift in the NASA Shuttle role from an insight (assurance) role to an over-sight role were coupled with a lack of appreciation for the importance of the role of the S&MA organization. This led to the perception that such reductions would be beneficial, or at least not harmful. The reductions were promoted as reducing unneeded "duplicate" functions that would not have a negative impact on the Shuttle program.

3. ISSUES AND CONCERNS

In 1999, the Space Shuttle Independent Assessment Team (SIAT) cautioned, "that oversight processes of considerable value, including Safety and Mission Assurance, and Quality Assurance, have been diluted or removed from the program. The SIAT feels strongly that NASA Safety and Mission Assurance should be restored to the process in its previous role of an independent oversight body, and not be simply a safety auditor." [2]

The SIAT review findings were consistent with alarms raised by other outside assessment teams which shared similar concerns about the state of the SSP S&MA efforts. The concerns fell into five general conditions with the same basic fault:

- Lack of resources
- Lack of independence
  - Funding
  - Authority
- Lack of discipline and domain expertise
- Lack of engagement in technical decision making
- Lack of respect for technical capability

The basic problem was that S&MA had often not been funded at the levels required to carry out its assignments. Almost all S&MA efforts were directly funded by programs and projects which required S&MA to compete for funding with engineering and program/project requirements. Even S&MA staffing levels were negotiated with and directly funded by the Center's programs and projects. This resulted in an S&MA organization that was beholden to programs and projects for people, tools, and travel. The lack of an independent source of funding limited S&MAs ability to levy requirements on programs and projects beyond the program's expectations which further clouded the S&MA lines of authority.

Adding to the difficulty in securing proper support, was the fact that the S&MA organization was often seen as overhead by Center programs and projects. In addition, there was a general lack of customer understanding of the total S&MA equity in the program effort. Customers had a limited view of S&MA as strictly a regulatory organization.

From an engineer talent perspective, a career in S&MA was not usually the first choice of NASA's best and brightest engineers and the S&MA grade structure was not on a par with engineering counterparts. Another factor was that S&MA's downsizing in the 1990's required the civil servant engineering workforce to become S&MA generalist at the expense of discipline expertise.

In the area of discipline expertise, since the S&MA disciplines of systems safety, reliability and maintainability, and quality engineering are not normally offered as university degree majors, S&MA discipline expertise had to be developed and cultivated within an organization's S&MA community. Unfortunately the NASA training and development programs after the Challenger accident were still inadequate to address S&MA development needs. There were no formal programs for S&MA discipline development and qualification. Shortcomings in institutional training capabilities could not be offset by out-side sources because of shortages in formal training and related travel dollars. Use of outside training also adversely impacts minimally staffed S&MA organizations which have to choose between getting the job done and providing "off-the-job" time for engineers to obtain training.

Unfortunately the reduction in the capabilities of the NASA S&MA organizations continued from just after the Challenger accident in 1988 until the Columbia accident in 2002. Generally organizations with a history of weak safety cultures have difficulty maintaining improved cultures even in the aftermath of major accidents unless there is a true shift in the culture of the organization. The Columbia Accident Investigation Board (CAIB) report on the Space Shuttle Columbia accident stated that, "NASA's organizational culture and structure had as much to do with this accident as the External Tank foam." The Board had expected to find vigorous safety organization with strong processes and an effective safety effort based on the changes put in place in response the findings of the Rogers Commission. It was disappointed to find that, "Shuttle Program safety personnel failed to adequately assess anomalies and frequently accepted critical risks without qualitative or quantitative support, even when the tools to provide more comprehensive assessments were available." The Board also was critical of the NASA Safety and Mission Assurance organization's performance in key program meetings during the STS-107 mission; noting the absence of any dissenting opinions and the silence of program-level safety participants that undermined their oversight role. "When they did not speak up, safety personnel could not fulfill their stated mission to provide checks and balances." The Board found a pattern of acceptance of the foam loss problems without sufficient engineering justification that was not challenged by S&MA. [3]

4. CURRENT S&MA FOCUS

The current S&MA organizational focus is on the implementation of the S&MA Mission & Vision Statements. The S&MA Mission is to enable NASA's success through proactive engagement of S&MA expertise. The S&MA Vision is to contribute to NASA success through Safety and Mission Assurance excellence. Technical excellence and communication provide the cornerstones for the current efforts to conduct a successful Safety and Mission Assurance program.

4.1. Technical Excellence

Three efforts were instrumental to the development of technical excellence: the development of discipline expertise within S&MA; improvement in the role in technical issue discussions; and the development of the necessary resources to the meeting the challenges of the desired organizational roles and contributions.

Discipline expertise is developed via a Professional Development Program. All S&MA personnel are required to select an S&MA discipline as their primary area of expertise. Professional Development Roadmaps (PDRMs) were created to identify and list the courses, knowledge and the experience necessary to be qualified at the various levels of S&MA discipline development. Discipline Champions were established to train and mentor S&MA personnel in their efforts to develop individual discipline knowledge and expertise. Mandatory discipline working groups were established to provide a forum for discipline development and knowledge sharing conducted by the individual Discipline Champions. [4]

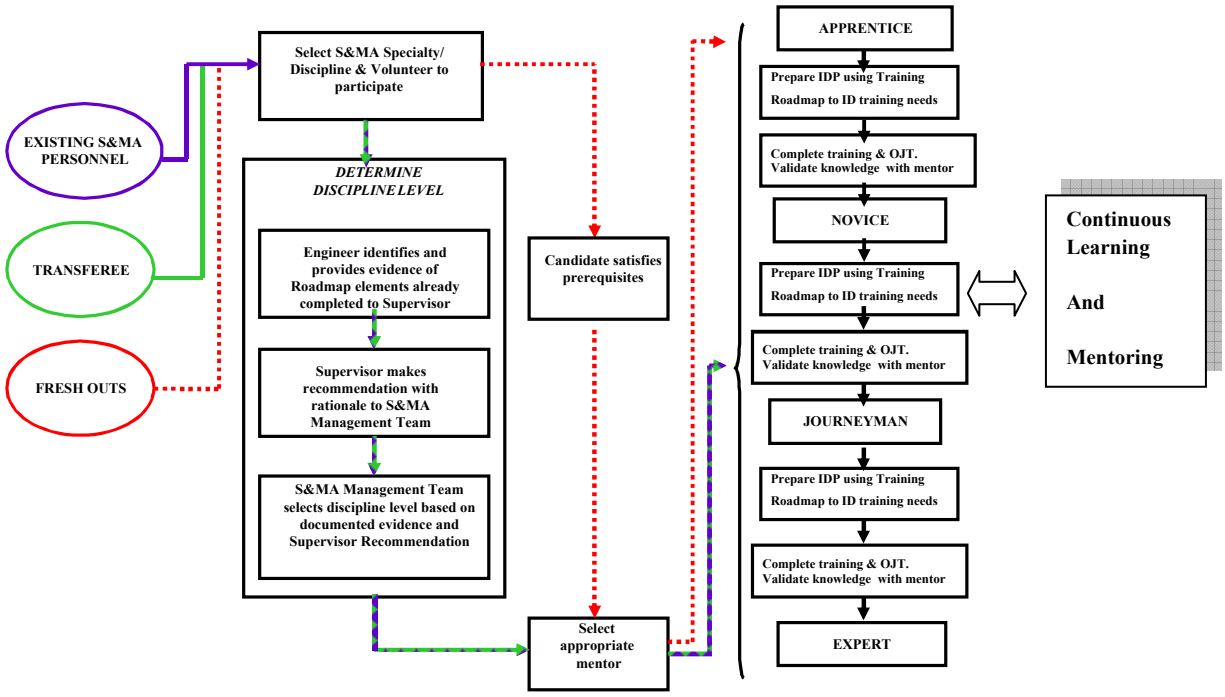

Figure 2. PDRM Flow Chart

4.2. Communication

For any S&MA effort to be effective there must be meaningful communication with the customer. The objective is the exchange of relevant information. While the skills and effort needed may vary with the type of information involved, the basic principles remain the same. For example, risk information may be a combination of data, knowledge, and professional opinions. The S&MA team must be able to communicate with design and engineering staff about details of the product and the associated operational environment to build their technical data base. The resulting risk assessments must address the basic elements of risk source identification, risk analysis, determination of controls, and follow-though of the disposition. The S&MA efforts are of no value unless the information is properly communicated to program management. [5]

Efforts were made on several fronts to improve communications with the S&MA customers as part of the current S&MA focus activities. One of the first steps taken was to conduct a general survey of the S&MA Directorate customers seeking: feedback from leadership customers on the overall service and quality of the S&MA effort; to garner feedback from civil servant employees and contractor support staff regarding the organization's performance over the past year and to solicit their suggestions for improvements; and to update its strategic plan based upon continuing development of its mission-related environment to support major NASA projects.

A number of organizational changes were made. An S&MA Deputy for Program Assurance was established. The position was staffed with a senior (SES) manager rotated from outside the organization. Steps were made to improve organizational understanding and communication both within and external to the S&MA organization. Outside hiring was utilized to strengthen areas where technical expertise was lacking.

The Safety and Mission Assurance Council (SMAC) was developed and implemented. The SMAC provided a direct role in the MSFC governance process; providing a forum for the review of issues critical to S&MA and a setting for technical dialogue with the MSFC engineering community via panel membership.

There was also an increased emphasis on early involvement in MSFC projects and programs. For the Constellation Program, members of the S&MA team were actively involved in the establishment of the program S&MA requirements and definition of needed program elements. Several S&MA trade studies were conducted to support vehicle architecture assessments and major system selections. The wide range of safety review experience within the S&MA organization was utilized in providing inputs to the development of the Constellation Safety Review Process.

5. THE S&MA COMMITMENT

The current MSFC S&MA organization is founded on and committed to the following key tenants:

- The development and maintenance of an organization that is respected for its technical expertise where NASA's best and brightest want to work.
- An organization that actively trains and develops its people to assure that the discipline technical expertise is consistent and reliable.
- An organization that is known for rewarding and acknowledging superior performance by its members.
- An organization which brings unique engineering expertise to the table in support of programs and projects.
- An organization that programs see as a must have - not a forced to have - and programs request S&MA support beginning with formulation.
- An organization that not only identifies issues, but also helps identify solutions.

6. REFERENCES

1. *Report of the Presidential Commission on the Space Shuttle Challenger Accident (1986)*, National Aeronautics and Space Administration, Washington, D.C.

2. Space Shuttle Independent Assessment Team, *Report to Associate Administrator, Office of Space Flight (2000),* National Aeronautics and Space Administration, Washington, D.C.

3. *The Report of Columbia Accident Investigation Board (2003),* Government Printing Office Washington, D.C.

4. Malone, Roy W, *Changing the S&MA Paradigm (2006)*, HRC INCOSE Meeting

5. Livingston, John M, *How to Build a Better System Safety Program based on a Little Common Sense (and 25 years of Trial and Error (2000)),* 18th International System Safety Conference, System Safety Society.