Managing SRM & QA Throughout the Project Life Cycle

by George A. Rodney

Program and project managers often ask me how they can gain maximum benefit from their safety, reliability, maintainability, and quality assurance (SRM&QA) engineering and technical support. My answer is that it is vital to develop a "team" culture within the program or project that includes SRM&QA support. Managers stand to benefit most when their management procedures and techniques are designed to ensure that safety, reliability, maintainability, and quality are built into the design plans of products and services up-front. They benefit least when safety, reliability, maintainability, and quality have to be built into the products and services at a later date, with the associated high costs of inspection and rework as well as the consequent impact on schedule and budget. You cannot "inspect" quality in.

The purpose of this article is to discuss the role of NASA's SRM&QA capability as a valuable resource to assist program and project managers in managing risk throughout the life cycle of their programs and projects and to show the importance of utilizing SRM&QA resources and total quality management (TQM) principles to achieve excellence. The principles embodied in the philosophy of TQM range from proper planning to total involvement of the workforce to assure quality products and services. Therefore, it is important to understand more fully the benefits that SRM&QA support has to offer. TQM principles include the following:

- Creating a "team" culture characterized by quality, innovation, goal-setting, two-way communication, and participation;
- Ensuring top management leadership and involvement in quality;
- Focusing on the customer and customer requirements;
- Pursuing continuous improvement; and
- Working towards prevention instead of correction.

The underlying theme of my discussion is that, because application of TQM principles encourages appropriate consideration of all factors (including SRM&QA-related ones), the end product or service will have safety, reliability, maintainability, and quality designed in, thereby reducing rework. The consequent impact on cost and schedule will show that SRM&QA can help conserve budget and time resources while ensuring safer mission performance.

SRM&QA Support at Agency, Center, and Project Levels

SRM&QA expertise spans a wide range of knowledge, skills, and experience available to the project manager throughout the life cycle. SRM&QA engineering and technical personnel at three levels assist project managers endeavoring to address risk management issues during the design, development, implementation, and evaluation phases of their projects.

At the agency level, the Office of SRM&QA at NASA Headquarters is responsible for developing and implementing firmly defined agency-wide SRM&QA policies. These policies, found in a variety of NASA Management Instructions (NMIs) and NASA Handbooks (NHBs), provide a foundation for project efforts to address risk. The Office of SRM&QA also tracks and analyzes trends and provides independent assessments of major programs. Finally, as NASA's safety and mission assurance advocate, the office acts on behalf of project managers in helping secure resources and scheduling that promotes safety and mission assurance.

At the Center level, each Center's SRM&QA organization develops and implements its SRM&QA policies. It performs trend tracking and analysis and provides independent assessments of programs and projects in a manner similar to the Office of SRM&QA at Headquarters. Also, the Center SRM&QA organization provides project managers with the engineering and technical support to perform the required SRM&QA design, implementation, and evaluation functions.

At the project level, SRM&QA personnel use a variety of tools and techniques, within the framework of agency and Center SRM&QA policies, to assess risk.

SRM&QA Tools and Techniques

Managers should become familiar with the tools and techniques that their SRM&QA support personnel use to assist them in designing and implementing product or service plans. Information concerning these tools and techniques can be gained from discussions with the supporting SRM&QA personnel and by being familiar with the requirements set out by the NHB 5300.4 series and other applicable agency and Center SRM&QA directives. The tools and techniques described in the following paragraphs are some of the principal ones with which managers should be familiar.

Failure Modes and Effects Analysis (FMEA). A FMEA is a systematic analysis performed on each component of a system to identify those components that are critical to the performance and safety of the crew, vehicle, or mission. The analysis includes identifying all system components, determining the potential modes of failure for each component, and recommending corrective actions.

Critical Items List (CIL). Based on a FMEA, a CIL is developed, consisting of a summary of single critical failure points and a summary of redundant elements, the failure of which could cause loss of crew, vehicle, or mission. As such, the CIL contains the same information as the FMEA, except that it includes the rationale justifying retention for redundancy of any critical item not meeting design specifications.

Hazard Analysis (HA). HAs are performed after the FMEA/CIL and are designed to identify, analyze, and categorize safety hazards, and subsequently track them to closure or resolution. Closure or resolution includes elimination of the hazard or control of the hazard through development of acceptable safety measures.

Problem Reporting and Corrective Action (PRACA). PRACA is a system for reporting all problems (failures and unsatisfactory condition reports) and establishing the necessary corrective action.

Electrical, Electronic, and Electromechanical (EEE) Parts and Mechanical Parts Control. These parts control systems are designed to control the selection, reduction in number of types, specification, failure analysis, stocking and handling methods, installation procedures, and reliability requirements of EEE and mechanical parts.

Qualitative Risk Assessment (QRA). QRA is a nonmathematical review of all factors affecting the safety of a system (hardware, software, etc.). It examines actual designs, processes, and parameters against a predetermined set of risk acceptability parameters.

Probabilistic (or Quantitative) Risk Assessment (PRA). PRA, a more rigorous engineering review than QRA, generates numerical probabilities of risk by considering reliability and probability estimates of risk occurrence.

Risk assessment, whether qualitative risk categorization or quantitative risk estimation, must be followed by the evaluation of risk significance. It is important to note that numbers per se are not the most important result from risk assessment. In fact, numbers can sometimes be deceiving. Program and project managers must keep in mind that, in reviewing risk assessment results, the most important result is an increased understanding of the system that leads to the discovery of ways to fix weak spots. Efforts can then be aimed at eliminating hazards where possible through redesign or through controlling hazards, by developing acceptable safety measures, in those cases where elimination is not possible.

Cost, Schedule, Performance, and Risk Management

Sound decision-making for program and project managers requires assessing each decision's impact in three areas: cost, schedule, and performance. Managers face immense pressure to keep cost within budget, schedule according to plan, and performance according to assigned mission objectives. Therefore, much of their time is spent reconciling the three. Since there is an element of risk to budget, schedule, or performance associated with every decision or non-decision, managing risk is a primary component of this process.

Risk, as it relates to performance, is defined as exposure to the chance of loss or injury to personnel, loss or damage to equipment, or loss or delay to the mission. It is a function of the following three factors:

- The frequency with which a hazard occurs;
- The potential severity of the resulting consequences; and
- The probability of those consequences occurring when the hazardous situation exists.

We at NASA have learned all too well that performance failure can mean more than just failure to accomplish a mission objective. It can mean tragic loss of personnel and equipment, sometimes with long-term consequences to cost and schedule.

Risk management is the decision-making process concerned with the balancing of performance-related risk with cost, schedule, and other programmatic considerations. It consists of the following four steps:

- Identifying risk;
- Assessing risk;
- Making decisions regarding the disposition of risk; and
- Tracking the effectiveness of the decisions made.

Safety is defined as the measure of freedom from occurrence or risk of loss or injury during use of a system or equipment through the elimination or control of hazards or the reduction of risk to an acceptable level. For example, SRM&QA engineers for the Galileo program had to identify and analyze the potential hazards related to the vehicle's nuclear power source. These analyses helped planners to eliminate some hazards and develop measures to control others. The effectiveness of these controls is continuously tracked and evaluated and change recommendations are developed, as required.

Reliability is the measure of assurance that a system or equipment will perform as designed by reducing risks of failure. As the life cycle for NASA programs and projects lengthens, increasing emphasis will be placed on the increasing reliability of systems as a method of eliminating or controlling hazards. High reliability in the Apollo and Voyager programs contributed to their success.

Maintainability is the measure of ease and rapidity with which a system or equipment can be restored to operational status following a failure or be maintained as a preventive measure prior to failure. Increased maintainability contributes to managing risk since it helps compensate for reliability shortcomings in current technology. Space Station Freedom, with an expected life of 30 years, will require systems with an increased degree of maintainability since the space station cannot return to Earth for repair. SRM&QA support can assist by performing integrated logistics support and configuration management studies.

Quality assurance is the measure of assurance that a system or equipment is produced or implemented as designed or intended through design review, inspection, and evaluation. High reliability systems are useless if they are not produced to high quality standards. For example, the quality of fasteners is becoming an important quality issue of international proportions. Also, new nondestructive evaluation technology is assisting managers in ensuring the quality fabrication of hardware.

Conclusion—SRM&QA Contributes to Good Management

The principles of TQM provide the foundation for decisions. Successful managers have learned the importance of continuous improvement in providing products and services and are designing in quality to achieve excellence. Less successful ones risk dooming their program or project to struggling to "inspect quality in" and reworking problems in their products and services that could have been resolved during the design process.

From my standpoint, risk management is a decision-making process when the manager balances performance-related risk with cost, schedule, and other programmatic considerations. Stated this way, performance should receive somewhat greater consideration in the decision-making process than do cost and schedule, at least to the extent that acceptable safety and mission assurance standards are met. While no one wants to make decisions that have a negative impact on cost and schedule, cost and schedule decisions cannot result in the kind of loss, in terms of resources and equipment, that performance failures can.

Performance objectives and mission success must come first, as they did in past programs such as Apollo, Voyager, and Viking. SRM&QA expertise is a critical element of the project team's ability to develop solutions to eliminate or control risk, attaining continued objectives and mission successes within budget, on time, and according to specifications.

Quality is planned in, designed in, and built in. Quality is not inspected in. Quality starts before designs are drawn and well before metal is bent. The main message here is that each person and organization in the program must understand and believe in the need for quality performance from the onset of the program. You cannot wait until the hardware is built to decide you want quality and then attempt to "inspect" it in. I have often seen this tried, but never successfully or economically. Quality encompasses more than just the delivered hardware. It includes management, requirements, design, development, testing and documentation.. Simply stated, the quality of every person's output is very important to the outcome of the program. — James B. Odom, "Guiding Principles for the Space Station Program," in Issues in NASA Program and Project Management, NASA SP-6101 (1988).