PREFERRED RELIABILITY PRACTICES

QUANTITATIVE RELIABILITY REQUIREMENTS USED AS PERFORMANCE-BASED REQUIREMENTS FOR SPACE SYSTEMS

Practice:

Develop performance-based reliability requirements by considering elements of system performance in terms of specific missions and events and by determining the requisite system reliability needed to achieve those missions and events. Specify the requisite reliability in the system specifications in quantitative terms, along with recommended approaches to verify the requirements are met. Require the system provider to demonstrate adherence to the reliability requirements via analysis and test.

Benefits:

Quantitative reliability requirements provide specific design goals and criteria for assuring that the system will meet the intended durability and life. Early in the design process, the system developer will be required to consider how the design will provide the requisite reliability characteristics and must provide analyses to verify that the delivered hardware will meet the requirements. Assessment of the early design's ability to meet quantitative reliability requirements will support design trades, component selection, and maintainability design, and help assure that appropriate material strengths are used as well as the appropriate levels and types of redundancy.

Program that Certified Usage:

International Space Station Program

Center to Contact for more Information:

Johnson Space Center (JSC)

Implementation:

The missions and scientific objectives of the subject space system are used to define quantitative reliability goals and objectives. In general, the quantitative reliability goals and objectives are stated as requisite probabilities of achieving specific missions or scientific objectives under stated operating conditions and environments. The probability values specified as being required are established through a process of trading off a desire for very high value against the cost and design constraints of achieving that value. The specified level will also determine an accepted level of risk or likelihood that the mission objective will not be met. Very often, the acceptable level may be negotiated between the science community or user, the contractor, and the

various responsible NASA organizations.

The use of quantitative performance-based reliability requirements does not supersede or negate the need for specifying fault tolerance or other classical reliability requirements. Fault tolerance requirements and reliability design criteria should also be levied to ensure the proper separation of redundancy, and the avoidance of failure propagation. Quantitative requirements are levied to ensure that the operational performance and missions can be met with an accepted probability level or likelihood. Table 1 shows examples of several different types of quantitative reliability requirements that can be levied on a space hardware program. The importance of using both types of requirements lies in the need to ensure that the system design is as robust as necessary and that it meets the verifiable performance goal. These types of requirements, if utilized correctly, will work hand in hand to provide the contractor direction on developing a more reliable product. The quantitative requirements are levied to ensure that operational needs can be met based on pre-set conditions.

Table 1: Examples of Quantitative Reliability Requirements:

Requirement Type	Location	Requirement Example
Probability of success	System Requirements Documentation	"The on-orbit Space Station shall be capable of operating in the microgravity mode, as defined in paragraph...., for 30 day continuous periods per the mission profile ....with a reliability of 0.80."
Goal for failure free performance	System Requirements Documentation	The vehicle shall provide 40 days of failure free performance verified by demonstrating to a 95% level of confidence that the 40 day success probability is greater than .99.
Operational goal for systems	System Requirements Documentation	Satellite communication shall provide 6 out of 12 channels of downlink at 10 Mbits/sec rate for two years of continuous operation.

A quantitative reliability requirement by definition means that the reliability is expressed in a measurable quantity. Performance-based reliability requirements are generally stated in terms of the probability of properly performing a mission phase or objective without a failure (or sequence of failures) that will terminate the mission phase. An example is the International Space Station reliability requirement in SSP 41000, "System Specification for the International Space Station (ISS)." The reliability requirement in SSP 41000 states that the Space Station

shall provide an operational capability to provide a microgravity environment for 50 percent of the internal payload locations for at least 180 days per year in continuous periods of no less than 30 days with a reliability of 0.80 or better. This requirement holds the ISS prime contractor responsible for providing a vehicle design that will operate continuously for 30 days without suffering a system failure that would exceed the conditions necessary for microgravity science, and do so at least 4 out of 5 of the periods. The system reliability, given its associated components and redundancy configuration, can be measured against that quantitative requirement. Also, during design reviews, consideration must be given to reliability assessments of the design because of such requirements, thus heightening the awareness of program risks that may otherwise go uncovered.

Other requirement statements might relate to the launch phase of a space system or simply to the normal operation phase. However, the specific elements of the requirement statement include the description of the desired performance, usually a direct or indirect reference to the amount of time involved, and the probability value needed. The mission/objective specified in a reliability requirement may deal with a major portion of the entire mission or may be a very specific portion of the mission. For instance, a reliability requirement may be specified for the ability to maintain attitude or perform a significant mission event.

The specification values used for the reliability requirement depends on the criticality of the mission or objective and the consequences of failure. In the Space Station case, loss of the microgravity capability is not inherently catastrophic, and a repair capability is available. Four successful 30-day periods out of five was considered to be reasonably achievable, and was deemed to be acceptable to the scientific user community. In man-rated vehicles, determining an acceptable value for the likelihood of mission success (hence loss of mission) may be more difficult. However, specifications for the reliability may then address the probability of avoiding mission aborts or loss of function. An example might be "the item shall perform its functions during the launch phase without losing any of the defined capabilities or functions with a probability of 0.98." The Federal Aviation Administration relates the consequence of failure and the probability of its occurrence in its consideration of risk, and is shown in Figure 1. By defining quantitative reliability requirements as those involving failure events throughout a flight leading to emergency procedures or immediate landings (mission aborts), the quantitative values for commercial vehicles would be specified in the 0.999 to 0.99999 range, (or conversely 1 out of a thousand to 1 out of 100 thousand).

In non-man rated vehicles or systems, the emphasis is on specifying a requirement that is sufficient to ensure a high likelihood of mission success, but not so high as to drive cost and weight beyond reasonable bounds. The use of function and item redundancy for increasing the likelihood of mission success will likely be necessary to meet high quantitative reliability specifications, but redundancy can also add significant program costs. Again, trade studies may

be necessary to balance requirements for the likelihood of meeting a mission objective against the reliability achieved with current manufacturing technologies and against various design options. For instance, it would be extremely difficult at current technology levels to meet a 0.999 reliability on a lengthy mission of high complexity without the use of functional redundancy. For quick-development, highly cost-restrictive programs with limited objectives, a performance-based reliability requirement of 0.9 or less may be appropriate to keep the acquisition costs within bounds.

To verify the fulfillment of a quantitative requirement, reliability analysis such as reliability block diagram analysis (RBDA) is used. The attribute of reliability, by definition, lies in the probabilistic realm while most performance attributes or parameters such as temperature, speed, thrust, voltage, or material strength contain more deterministic characteristics. Within the accuracy of the measuring devices, one can directly measure performance attributes in the deterministic realm to verify compliance with requirements. No such measuring device exists for probabilistic parameters like reliability; it is usually estimated through comparison to similar components or systems through inference, analysis, and the use of statistics. Verification that quantitative requirements have been met also provides answers to questions such as "how reliable is this system?"

Table 2: Quantitative Reliability Requirement Verification Techniques

Verification Method	Program Phase	Necessary Inputs
Reliability Analysis (Block Diagram Assessments, Availability Simulation)	Design, or Phase B	System architecture, mission time, appropriate component failure data, etc.
Probabilistic Risk Assessment (Fault Tree Analysis, Event Tree Analysis)	Design and Test, Phase	System architecture, test results.
Reliability Qualification or Acceptance Testing	Phase B and C.	Failure Data, test results|

A reliability requirement specified without a probability value such as "the vehicle shall perform xyz mission on-orbit without failure for 5 years" is impossible to verify during qualification or acceptance testing. The likelihood, or probability, that the requirement will be met is assessable, and this activity is inherently equivalent to assessing the reliability. Without quantitative requirements, it is left to the certification assessor to evaluate an estimate of the probability of success and to decide if that is sufficient, which places the risk on the program.

A great deal of preliminary analysis may be necessary in the requirement specification process

that considers the capability of the technology to various levels of reliability. This preliminary analysis helps avoid setting quantitative requirements too high or too low. Development of quantitative reliability requirements must represent a balance between the operational performance requirements of the system and the ability to restore and maintain the system through maintenance and sparing.

Establishment of quantitative requirements as high as possible is necessary to maximize the probability that the system will complete the mission without failure. However, achieving high reliability or probability of mission success increases cost by generally requiring redundant equipment and fail-safe devices as well as high margins of safety in the material properties used. Thus, meeting unrealistic and unnecessary reliability requirements can lead to program weight and volume problems as well as cost inflation Based on the stress-strength concept of failure, perfect reliability could be achieved by building a system whose strength is greater than any conceivable stress put on the system. In reality, weight, volume, and cost constraints usually limit the strength of the design. Although perfect reliability from space systems cannot be expected, consideration of the needs of the operational community as well as the budget of the program will help in determining a requirement level. Also, if reliability goals are not met, it may be necessary to initiate a reliability growth scenario in which failure modes are analyzed and designed out of the system. This may or may not cost the program extra money, as reliability growth testing may not have been part of the original life cycle plan.

As mentioned above, the International Space Station Program has levied a quantitative performance requirement on the Prime Contractor. Arrival at that requirement came through rigorous coordination with operational elements of the program, including the Mission Operations Directorate and the Science and Utilization community. The actual benchmark of 0.8 was derived from analysis of the operational needs of the program, the number of failures that could be tolerated, and an early analysis of what the space station design concept could provide. This number was a mutual agreement between the product assurance community and the operations community. As a result of this requirement, the prime is undergoing an effort as part of it's reliability group to maintain a running tally of the overall station reliability via reliability block diagram analysis. Every design change, program change, or other input is reflected in the running tally to ensure that the design meets the requirement.

Technical Rationale:

Many previous NASA program development efforts have relied on specific design requirements such as redundancy to minimize risk and the likelihood of failure. Quantitative reliability requirements augment qualitative reliability analysis such as failure tolerance, but more importantly, gives teeth to a requirement that may otherwise slip from the design. Designers and contractors are held responsible for designing systems and to demonstrate analytically that the

system or function will have a sufficient likelihood of failure-free mission operations.

Impact of Nonpractice:

Program teams and/or contractors will not be obligated and/or held accountable to design for reliability, and reliability issues may be overlooked. Also, operational design goals may not be met due to less than expected vehicle availability because of failed critical items. Program cost as well as risk will probably increase.

Related Practices:

PD-AP-1313, "System Reliability Assessment Using Block Diagraming Methods."

References:

SSP 41000, "System Specification for the International Space Station (ISS)," November 1, 1994, Contract NAS15-10000.

NASA Risk Management Program Tools and Techniques Handbook, Draft, July 1988, NASA Headquarters, Code QS.

NASA Safety Risk Management Program Plan, Sections 1-5, NASA Headquarters, Code QS.

QUANTITATIVE RELIABILITY REQUIREMENTS USED AS PERFORMANCE-BASED RELIABILITY REQUIREMENTS FOR SPACE SYSTEMS

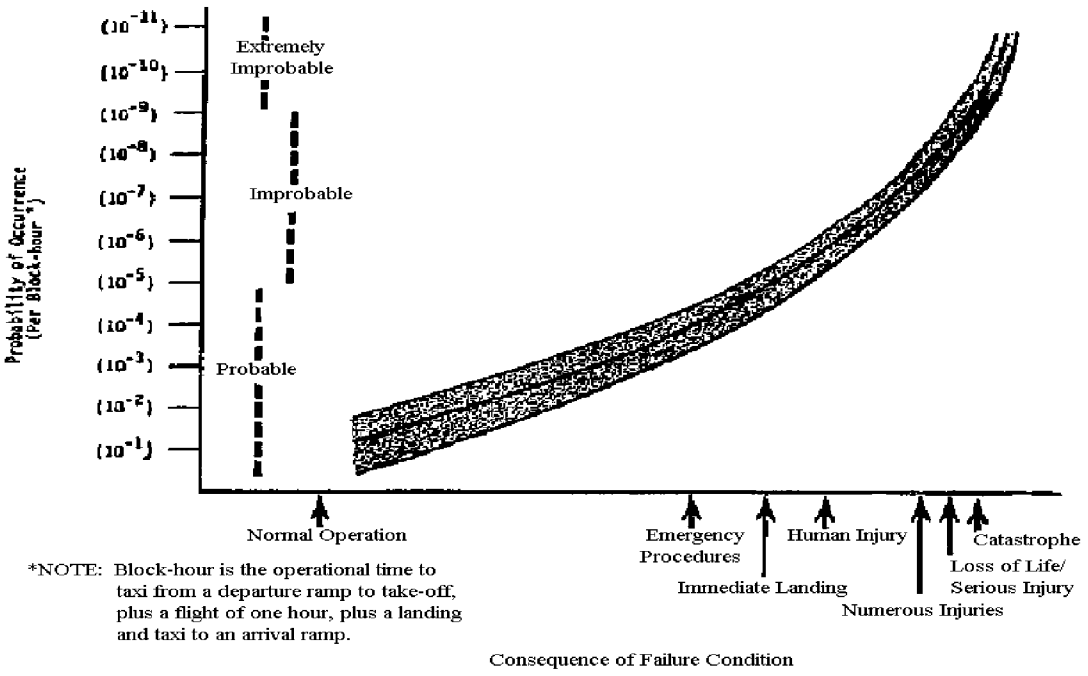

Figure 1. An Illustration of the Relationship Between Consequence of Failure and the Probability of Its Occurrence (FAA, Updated)