MISSION ASSURANCE AND FLIGHT SAFETY OF MANNED SPACE FLIGHT: IMPLICATIONS FOR FUTIRE EXPLORATION OF THE MOON AND MARS M. T. Kezirian, University of Southern California, Los Angeles, CA 90089; The Boeing Company, HZ1-10, 13100 Space Center Blvd., Houston, TX, 77059. (Kezirian@usc.edu).

Introduction: As NASA implements the nation's Vision for Space Exploration [1] to return to the moon and travel to Mars, new considerations will be be given to the processes governing design and operations of manned spaceflight. New objectives bring new technical challenges; Safety will drive many of these decisions.

Historical Context: For the Apollo program, safety requirements were individual standards for individual subsystems or components.

The Space Shuttle Program (SSP) combined these requirements into a uniform standard, "Fail Operational, Fail Safe" or FO/FS. If any one failure occurs then the Shuttle can continue to operate and complete all flight mission objectives. Following a second failure, FO/FS specifies that the vehicle is Safe, able to return home safely, though may not be able to complete all mission objectives.

Payload Safety Process instituted Two Fault Tolerant (2FT) Requirements to add an additional layer of protection between Crew/Shuttle and Payloads.

The International Space Station (ISS) based their safety analysis on the Payload standard of 2FT, motivated by the lack of ground servicing of the ISS following failures of safety-critical hardware. The Shuttle has the option to perform an emergency deorbit, in the event of a major failure. There is no similar contingency option for the ISS.

Safety Requirements Allocation. System engineering calls for breakdown of requirements by function and allocation of portions of requirements to separate subsystems. Unfortunately, safety requirements can not follow this model. Safety requirements generally are required to be applied to all of the lowest level specifications intact.

Achieving 2FT. There are numerous ways to achieve satisfactory compliance of requirement. One could use independent, triple-redundant must-work systems or independent three inhibit most-not-work systems throughout the vehicle. Unfortunately, such design standard is not possible due to restrictions of weight and volume. Additionally, it is not necessary as there are other ways to meet 2FT: Use of Unlike Redundancies. Separate systems working together can provide an overall higher level of safety. Use of Other Available Margins, taking advantage in margin in a different system to meet 2FT requirement.

Non-Compliance of 2FT. Alternate approaches, when necessitated by design are acceptable.

Competing Must-Work and Most-Not-Work Functions. Consider rendezvous. No single or double events can result in collision. Crew controlled flight via joystick is inherently vulnerable to crew error. Instead, training, design of approach corridor and control of approach speed allow crew to recognize errors and adjust.

Equivalent Safety. This is used when risk to Crew/Vehicle is very low with just Single Failure Tolerance Implemented. The emphasis is on other controlling factors and not just probability numbers. For example, a single failure tolerant system with large time to effect is considered acceptable 'equivalent' risk to a 2FT system because there is plenty of time to avert undesired effect after the failure using operational controls.

Design for Minimum Risk (DMR): From the ISS Safety Requirements [2]: Design for minimum risk are areas where hazards are controlled by specification requirements that specifiy safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance criteria. The failure tolerance criteria … shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety properties of the design. Examples are mechanisms, structures, glass, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Safety Analysis Documents. Safety engineering analyses are documented in Hazard Reports, Failure Mode Effects Analysis (FMEA) and the Critical Items List (CIL) [3].

Hazard Reports. Hazard Reports [4] capture the risks that do not meet the FO/FS requirement. Each cause is assigned a Severity and Likelihood of Occurrence, and corresponding Hazard Classification.

The Severity level is an assessment of the worst-case effects of a hazard for a given cause. By definition, Catastrophic severity is a hazard which could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility. Critical severity is a hazard which could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay. Marginal severity is a hazard which could result in a mishap of minor nature inflicting first-aid injury to personnel and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant program delay.

The Likelihood of Occurrence assesses the probability that the worst-case hazard will take place, with the controls in place. Probable: expected to happen in the life of the program; Infrequent: could happen in the life of the program, controls have sig-

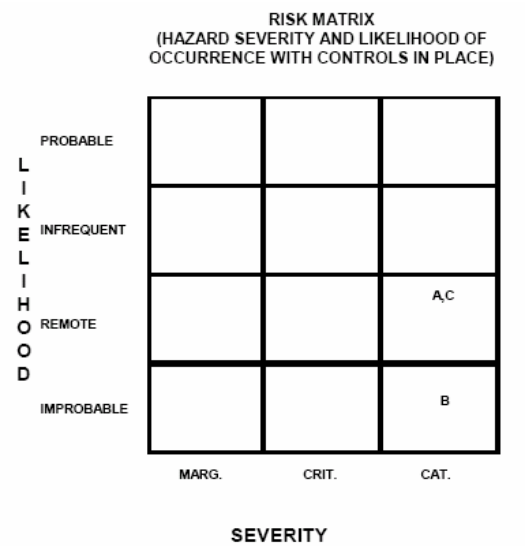

Figure 1: Sample Hazard Report Risk Matrix. Identifies the Likelihood of Occurance and Severity of each Cause.

nificant limitations or uncertainties; Remote: could happen in the life of the program, but is not expected, controls have minor limitations or uncertainties; Improbable: extremely remote possibility to happen in the life of the program; there are strong controls in place.

The risk matrix places each cause into a grid in a matrix, with the Likelihood of Occurrence on the vertical axis and the Severity on the horizontal axis. For the sample Risk Matrix with three causes (Fig. 1), two causes (A&C) are Remote/Catastrophic; one cause (B) is Improbable/Catastrophic.

Failure Mode Effects Analysis (FMEA) and the Critical Items List (CIL). FMEA/CILs identify specific potential hardware failures and describe the root cause of failures for components and subsystems. [5]

Each FMEA/CIL is assigned both a 'functional criticality/hardware criticality' as follows: '1/1' Single failure which could result in loss of life or vehicle; '1R/2' Redundant hardware item(s), all of which failed, could cause loss of life or vehicle. First failure would result in loss of mission, or the next failure could cause loss of life or vehicle; '1R/3' Redundant hardware item(s), all of which failed, could cause loss of life or vehicle. First failure has no effect on mission; second failure may result in loss of mission; '2/2' Single failure which could result in loss of mission; '2R/3' Redundant hardware item(s), all of which failed, could cause loss of mission. First failure has no effect; '3/3' All others.

FMEAs are included on the CIL if they are of criticality '1/1', '1R/2', and, for some cases, '1R/3'.

Spacecraft Operations Considerations. During Shuttle Flight Operations, the Mission Management Team (MMT) assesses on-orbit anomalies. Engineering teams review relevant FMEA/CILs and Hazard Reports. The relative positions in the risk matrix are used to guide actions to protect against the highest risk. Each anomaly is assigned a position on the Anomaly Risk Matrix, shown in Figure 2. The Fault Tolerance Remaining compared to the Next Failure Consequence are tracked. Subseqent to the anomaly, it is frequent that the position in this matrix moves. That can be because the mission circumstances change and the next failure consequence becomes less significance or it can be moved because more flight data is obtained or further analysis has been performed.

ISS operations are handled slightly differently. Following the an anomaly, the engineering investigation team assesses the Magnitude of Potential Consequences compared to the Likelihood Probability the corresponding condition or event will happen. Subsequently, the team presents options and identifes the associated risk and the corresponding reliability after implementation.

Conclusion NASA has continued to develop processes for design and operations to flight safety. The Vision for Space Exploration will bring new technical challenges and necessitate new apporaches to design and operations.

References: [1] NASA Vision for Space Exploration, February, 2004. [2] SSP 50021, ISS Safety Requirements, Appendix B, Glossary. [3] Kezirian, M. et al (2006) AIAA-2006-5110, 42nd AIAA/ASME /SAE/ASEE Joint Propulsion Conference and Exhibit. [4] Methodology for Conduct of Space Shuttle Program Hazard Analyses, NSTS 22254, Rev. B, NASA, December 10, 1993. [5] Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL), NSTS 22206, Rev. D, NASA, December 10, 1993.

Fault Tolerance Remaining	ANOMALY RISK MATRIX					
	0 – Fault					
	1 – Fail Safe					
	2 – Fail Ops					
	3 – or Greater /INSTR					
		Nominal End of Mission (NEOM)	EVA/ IFM/ Jettison	MDF / Loss of 2nd Mission Objective	NPLS/ Loss of Primary Mission Objective	Emergency Deorbit/ CSCS/ LOV
	NEXT FAILURE CONSEQUENCE					