An Innovative Goddard Space Flight Center (GSFC) Methodology for using FMECA as a Risk Assessment and Communication Tool

Nancy J Lindsey, Goddard Space Flight Center (Code 371)

Key Words: FMEA/FMECA, Failure Analysis, Risk Assessment, Risk Priority Number, Goddard Space Flight Center, NASA

SUMMARY & CONCLUSIONS

Functional and Interface Failure Mode, Effects and Criticality Analyses (FMECA) investigate the following types of detailed potential failure origin and failure impact questions:

- What interfaces dependencies or performance issues exist as a result of each potential functional failure or input loss?
- If a component fails or exhibits intermittent functionality, is a redundant component available to mitigate the failure effects?
- If a failure occurs internal to the component's electronics is there the potential for collateral damage of adjacent systems (i.e., Is propagation possible? Will a system failure "Do No Harm" to other systems?)?
- Can any single failure mode of the instrument lead to total loss of science/data from the instrument or other flight systems?

The answers to these questions help to identify Single Point Failures (SPFs), Critical Items, and have the potential to characterize and quantify risk if a risk assessment methodology is used throughout the FMECA process. The following FMECA risk assessment methodology has been developed by GSFC's Reliability and Risk Analysis Branch to assess and communicate failure risks: 1) Correlate Mission Success Requirements-to-GSFC Risk Management Consequence Definitions (GPR 7120.4D); 2) Correlate Failure Severities (NASA/GSFC FMECA Procedures)-to-GSFC Risk Management Consequence Definitions (GPR 7120.4D); 3) Correlate Mission Failure and Duration-to-GSFC Risk Management Likelihood Definitions (GPR 7120.4D); 4) Analyze and characterize each failure mode using these correlations; 5) Assess the Failure Modes as risks, and 6) Communicate risks to mission risk managers. This methodology has already been successfully used on the following NASA GSFC projects: ICESAT-2, OSIRIS-Rex, Robotic Refueling Mission (RRM), Gravity and Extreme Magnetism SMEX (GEMS), and Nuclear Spectroscopic Telescope Array (NuSTAR) to assess and communicate risks including single point failure risks based on FMECA results. Thus it can be considered valid and useable for other missions.

1 BACKGROUND

"Risk is a potential threat with sufficient information to indicate a negative consequence when measured against a safety, technical, cost or schedule performance objective. Risk is also the potential inability to fully implement agreements with NASA stakeholders or partners (commercial, governmental, or international). Resolution requires focused management attention." [Per NASA GPR 7120.4D]

1.1 Risk Management

NASA/GSFC employs Continuous Risk Management (CRM)/Risk Informed Decision Making (RIDM) to make decisions on design, manufacturing, and operations of on-orbit assets based on the risk against achieving mission success. In continuous risk management risks are identified and analyzed/ researched then a plan is developed to handle (e.g., mitigate, watch, accept, or escalate) the risk and ultimately the risk is monitored for occurrence and or modification.

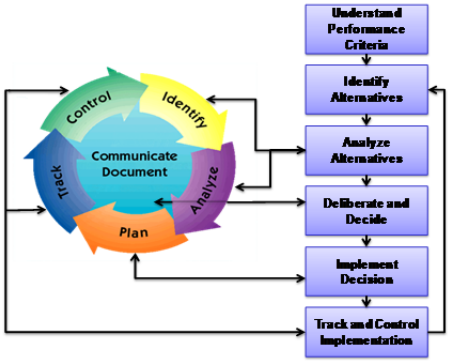

Figure 1- RIDM-CRM Risk Management Process Flow

1.2 FMECAs

Failure Mode Effects and Criticality Analysis is a bottoms-up inductive analysis of potential system failures. The three general approaches used to perform a FMECA are: *functional, interface, and detailed*. Variations in design complexity and data availability will dictate the analysis approach that is used. Some cases may necessitate that part of the analysis be performed at the functional level and other portions at the interface and detailed levels. In other cases, initial needs may be for a functional FMECA that would

progress to an interface FMECA, and then finally to a detailed FMECA. Traditionally the purpose of any FMECA is to:

- Identify where there is the potential for irreversible physical and/or functional damage;
- Identify how damage/failures propagate or not;
- Identify how damage/failures impact the system (locally and globally);
- Identify the means available for failure detection, isolation, and/or compensation;
- Recommend corrective actions and follow up on corrective action implementation/effectiveness including FMECA re-analysis.

While all resultant failure modes can be viewed as or considered identified mission success risks, formal risk assessment has not routinely been an output of the FMECA while Critical Items Lists and Single Point Failure lists have been.

2 FMECA RISK ASSESSMENT METHODOLOGY

GSFC has found enhancing the traditional FMECA methodology for risk identification, characterization, and quantification can be completed by using mission specific severity and likelihood correlations to standard risk management and FMECA definitions (See Sections 2.1 - 2.4); and identifying, analyzing, and assessing the Failure Modes/Critical Items/Single Point Failures as risks. Although identifying and analyzing risks is essential, full risk assessment and management (see Figure 1) also needs an effective way to document and communicate risks to mission risk managers in an actionable manner. In this new FMECA Risk Assessment Methodology that is done by use of the GSFC Risk matrix and FMECA identifiers (See Section 2.5). See each subsection below for each step's details and implementation strategies at GSFC.

2.1 Correlate Mission Success Requirements-to-GSFC Risk Management Consequence Definitions

At GSFC each project or mission has unique mission success requirements while the center on the whole has standard consequence risk scale definitions (See Figure 2). This would lead to difficulty in establishing the appropriately represented severity of the failure effect or risk consequence

Consequence Categories					
Risk	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Safety	Negligible or No impact.	Could cause the need for only minor first aid treatment .	May cause minor injury or occupational illness or minor property damage.	May cause severe injury or occupational illness or major property damage.	May cause death or permanently disabling injury or destruction of property.
Technical	No impact to full mission success criteria	Minor impact to full mission success criteria	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin	Major impact to full mission success criteria. Minimum mission success criteria is achievable	Minimum mission success criteria is not achievable
Schedule	Negligible or no schedule impact	Minor impact to schedule milestones; accommodates within reserves; no impact to critical path	Impact to schedule milestones; accommodates within reserves; moderate impact to critical path	Major impact to schedule milestones; major impact to critical path	Cannot meet schedule and program milestones
Cost	<2% increase over allocated and negligible impact on reserve	Between 2% and 5% increase over allocated and can handle with reserve	Between 5% and 7% increase over allocated and can not handle with reserve	Between 7% and 10% increase over allocated, and/or exceeds proper reserves	>10% increase over allocated, and/or can't handle with reserves

Figure 2 – GSFC Risk Scale Consequence Defiintions

in the analysis process if the FMECA analyst does not correlate these two before the analysishas begun. With a good understanding of successful performance criteria (re: Figure 1) the relaibility analyst simply translates a project requirement such as: *The mission shall produce at least Threshold Science measurements but shall be designed for Threshold and Baseline Science measurements;* to consequences levels for each risk scale consequence category as shown in below:

Technical Consequence	
1 Very Low	No impact to full mission success criteria → Threshold and Baseline Science can still be achieved
2 Low	Minor impact to full mission success criteria → Threshold Science can still be achieved; Baseline Science may be degraded or performed at a reduced level
3 Moderate	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin → All of the Threshold Science is still achievable; Not all Baseline Science is achievable (e.g., Cannot perform science at one or more Baseline Science performance levels)
4 High	Major impact to full mission success criteria. Minimum mission success criteria is achievable → Threshold Science is still achievable; Cannot meet any Baseline Science performance requirements
5 Very High	Minimum mission success criteria is not achievable → Threshold and Baseline Science is not achievable. (e.g., Cannot perform science at one or more Threshold Science performance levels)

Table 1 – Technical Consequence Correlation

With this scale the failure mode in the FMECA can now be characterized by the analyst consistently with project and center-wide criteria, but not the standard FMECA severity categories (1, 1R, 1S, 2, 2R, 3, 4) shown and defined in Figure 3. Direct usage of this scale would allow the analyst to proceed but would eliminate the routine correlation of severity to critical items and the full differentiation of gained with redundancy. Thus, several GSFC projects have found it best to continue the correlation process to failure severity categories (see section 2.2).

2.2 Correlate Failure Severities-to-GSFC Risk Management Consequence Definitions

GSFC has defined its tailorable severity categories with consideration of safety as shown in Figure 3 so the worst case severity equals 1 and the least severe case equals 4. Although these correlate well with the hazard severities as defined in NASA-STD-8719.24 ANNEX (Change 2). This is the reverse numerical value order needed to calculate a Risk Priority Number (RPN) in the FMECA's action/risk prioritization process (Pareto Analysis), and thus would produce erroneous results since the RPN is the product of the Likelihood, Severity, and Detection/Prevention values (rankings). The faulty RPN would reverse the determination of the order in which recommended actions should be developed to address potential failure modes and would waste time and effort without improving the reliability of the equipment at risk. Therefore, several GSFC projects have also correlated failure severity categories, as shown in Table 2, to the consequence risk scale definitions allowing for project tailoring so appropriate prioritizations can be communicated to mission

engineers/managers to formulate risk based action plans (re: Figure 1).

Category	Severity	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life (flight or ground personnel), or total loss of mission.
1R		Failure modes of identical or equivalent redundant hardware items that, if all failed, could result in Category 1 effects.
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2	Critical	Failure modes that could result in loss of one or more minimum mission objectives as defined by the GSFC project office.
2R		Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.
3	Significant	Failure modes that could cause degradation to full mission objectives and still meet a minimum mission.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

Figure 3 – GSFC Severity Categories

Technical Consequence		Failure Severity
1 Very Low	No impact to full mission success criteria → Threshold and Baseline Science can still be achieved	**Minor or no impact on mission life or performance:** noticeable or no degradation, that does not lead to loss of science or significant peril to mission. (Category 4)
2 Low	Minor impact to full mission success criteria → Threshold Science can still be achieved; Baseline Science may be degraded or performed at a reduced level	**Potential for major or significant degradation of mission or performance:** no immediate impact on mission, but potential exists for future loss, at level 5-3, if adequate alternatives or measures are not implemented. (Category 3)
3 Moderate	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin → All of the Threshold Science is still achievable; Not all Baseline Science is achievable (e.g., Cannot perform science at one or more Baseline Science performance levels)	**Significant loss or degradation of mission:** significant loss of mission function leading to a significant loss of data, or a significant reduction in life of the mission. (Category 2 or 3) Or **Loss or degradation of a redundant subsystem** or science instrument producing levels 4 or 3 severity, if remaining redundancy is lost. (Category 2R)
4 High	Major impact to full mission success criteria. Minimum mission success criteria is achievable → Threshold Science is still achievable; Cannot meet any Baseline Science performance requirements	**Major loss or degradation of mission:** capability to complete some mission objectives (Category 2) Or **Loss or degradation of a redundant subsystem** producing levels 4 or 5 severity, if remaining redundancy is lost. (Category 1R)
5 Very High	Minimum mission success criteria is not achievable → Threshold and Baseline Science is not achievable. (e.g., Cannot perform science at one or more Threshold Science performance levels)	**Complete loss of mission:** complete loss of primary mission capability. (Category 1) Or **Loss or degradation of a subsystem or science leading to safety or hazard monitoring system failure** that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Severity 5 consequences (Category 1S)

Table 2 - Technical Consequence & Failure Severity Correlation

2.3 Correlate Mission Failure and Duration-to-GSFC Risk Management Likelihood Definitions

Risks are defined with both a consequence and likelihood, so for a failure mode to be translated to a risk in this FMECA risk assessment process it must not only have impacts assessed but it must also have the occurrence frequency or likelihood assessed as well. Two methods used at GSFC to determine the likelihood based on failure probabilities used at GSFC are 1) rating of likelihood using heritage performance or expert opinion and 2) quantification of likelihood based on failure rates and mission/use duration. To facilitate the use of either or both methods as needed for each failure mode's assessment and to remove the qualitative nature of these assessments it is essential that the GSFC risk likelihood scale (See Figure 4) be correlated to system failure rates. This is done by first assuming a failure distribution for all the system's items. For many space applications this can be assumed to be exponential for all components since spacecraft environments can be assumed to be fairly benign (or controlled), thus failure rates would remain constant. However, any appropriate distribution can be used to correlate each failure mode's or system's failure rate to the GSFC risk likelihood scale.

Likelihood	Safety (Estimated likelihood of safety event occurrence)	Technical (Estimated likelihood of not meeting performance requirements)	Cost/Schedule (Estimated likelihood of not meeting cost or schedule commitment)
5 Very High	($P_{SE} > 10^{-1}$)	($P_T > 50\%$)	($P_{CS} > 75\%$)
4 High	($10^{-2} < P_{SE} \leq 10^{-1}$)	($25\% < P_T \leq 50\%$)	($50\% < P_{CS} \leq 75\%$)
3 Moderate	($10^{-3} < P_{SE} \leq 10^{-2}$)	($15\% < P_T \leq 25\%$)	($25\% < P_{CS} \leq 50\%$)
2 Low	($10^{-5} < P_{SE} \leq 10^{-3}$)	($2\% < P_T \leq 15\%$)	($10\% < P_{CS} \leq 25\%$)
1 Very Low	($10^{-6} < P_{SE} \leq 10^{-5}$)	($0.1\% < P_T \leq 2\%$)	($2\% < P_{CS} \leq 10\%$)

Figure 4 - GSFC Risk Likelihood Scale

For example: given a mission that must last 3.16 years with exponential failure distributions then equation (1) can be used to calculate the failure rate (λ) for each likelihood value rating. Results are shown in Table 3.

$$\lambda = \frac{\ln(1-P_f)}{-time} = \frac{\ln(1-P_f)}{-27720\ hrs} \qquad (1)$$

Value	Occurrence or Likelihood
5	Very High ($0.50 < P_F$) Or ($2.5 \times 10^{-5} < \lambda$ for mission duration)
4	High ($0.25 < P_F \leq 0.50$) Or ($1.03 \times 10^{-5} < \lambda \leq 2.5 \times 10^{-5}$ for mission duration)
3	Moderate ($0.15 < P_F \leq 0.25$) Or ($5.9 \times 10^{-6} < \lambda \leq 1.03 \times 10^{-5}$ for mission duration)
2	Low ($0.02 < P_F \leq 0.15$) Or ($7.3 \times 10^{-7} < \lambda \leq 5.9 \times 10^{-6}$ for mission duration)
1	Very Low ($0.001 < P_F \leq 0.02$) Or ($3.6 \times 10^{-8} < \lambda < 7.3 \times 10^{-7}$ for mission duration)
< 1	Very Very Low ($P_F \leq 0.001$) Or ($\lambda < 3.6 \times 10^{-8}$ for mission duration)

Table 3 – Mission Failure Rate to Likelihood Example

2.4 *Analyze and Characterize each failure mode using these correlations.*

Once the aforementioned likelihood and consequence correlations are complete, which can be formulated in any order, the reliability analyst can fully analyze and characterize each failure mode in terms of risks. This is done by postulating all potential failure modes with their causes and defining through analysis the impact of each at the subsystem/component level (Local Effect); the system level (for sub- system) or subsystem level (for component) (Next Higher Level Effect); and mission or end item effect level (Ultimate Effect). In addition this approach can be used to identify each failure mode's or cause's available prevention and/or mitigation strategies and detection capabilities to make the FMECA not only a design tool but a failure or root cause analysis tool too as well. Then using the correlations as described in previous sections (Example shown in Table 4) and an agreed upon detection/prevention scale (Example shown in Table 4, column 4) each failure mode can have its occurrence, consequence, and detection/prevention value quantified. The results (See example in Table 5) can then be shared as risks with mission personnel and filtered/prioritized for potential actions to be taken. It should be noted that these results would be potentially 100's to 1000's of line items for each potential failure mode so they must be filtered and communicated well to be useful.

2.5 Assess and Communicate risks to mission risk managers

FMECA results are normally reported or communicated to the project in Single Point Failures (SPFs) Lists and Critical Items Lists (CILs) but these lists don't communicate the FMECA's entire findings and in many cases can also be quite extensive as well. However, with risk correlated failure mode characterization GSFC (as described in section 2.4) reliability personnel can now use the GSFC 5x5 Risk Matrix, as defined in GPR 7120.4D and enhanced as shown in Figure 5, to effectively communicate the entire FMECA findings. This is done by entering each failure mode reference designator into the matrix in accordance with its characterization values and categories. This enables the entire FMECA's results to be assessed, captured, and communicated with risk priority in two matrices to supplement the Critical Items and Single Point Failure lists as well as FMECA risk proposals. Thus this completes the GSFC FMECA Risk Assessment Methodology being presented.

3 METHODOLOGY APPLICATION AND LESSONS LEARNED

This methodology has already been successfully used on many NASA GSFC projects (See Examples in Figure 6) including the following missions: Ice, Cloud, and Land Elevation Satellite-2 (ICESAT-2), OSIRIS-Rex, Robotic Refueling Mission (RRM), Gravity and Extreme Magnetism SMEX (GEMS), and Nuclear Spectroscopic Telescope Array (NuSTAR). As a result GSFC has found that use of this method:

1. Easily shows and begins action / risk management on critical failure modes or the items these modes are associated with;
2. Provides a quick communication mechanism of failure risks and FMECA results for milestone presentations (i.e., Prelimanary Design Review (PDR), Critical Design Review (CDR), etc.);
3. Offers a direct translation of SPFs to risks as required by GSFC Single Point Failure Policy;
4. Is easily tailored for mission length and risk tolerance profile (e.g., 2 and 2R correlation variations);
5. Requires care in implementation by reliability personnel to account for and ensure consistency in the application of the one-to-many cases in the correlations of Technical Consequence to Failure Severity Categories;
6. Makes the formulation of CIL and SPF lists and communication of safety issues efficient and verifiable.

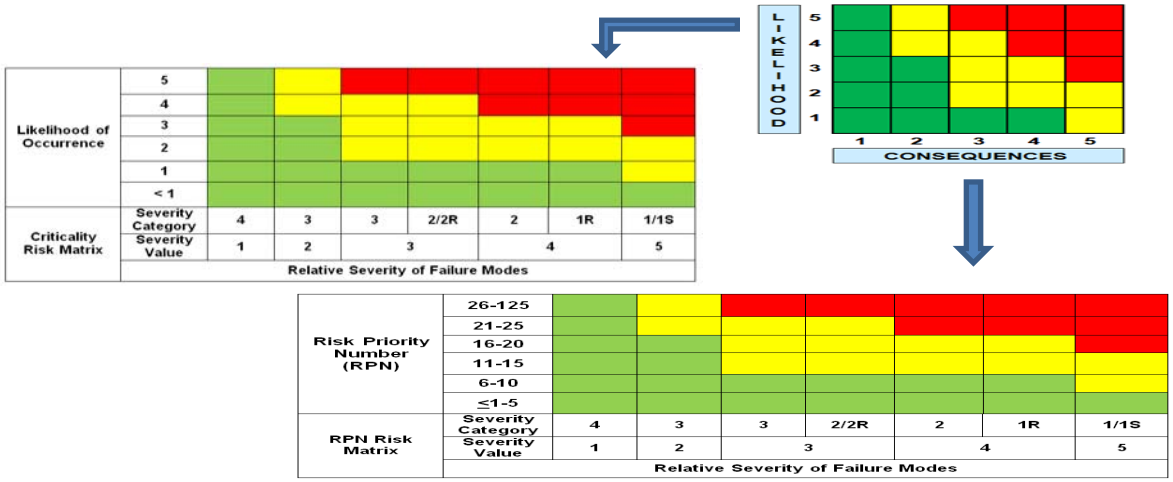

Figure 5 – FMECA Enhanced GSFC Risk Matrices

	Occurrence or Likelihood	Technical Consequence	Failure Severity	Detection/Prevention
< 1 Very Very Low	Very Very Low ($P_F \leq 0.001$) Or ($\lambda < 3.6 \times 10^{-8}$ for mission duration)	N/A	**N/A**	**N/A**
1 Very Low	Very Low ($0.001 < P_F \leq 0.02$) Or ($3.6 \times 10^{-8} < \lambda < 7.3 \times 10^{-7}$ for mission duration)	No impact to full mission success criteria → Threshold and Baseline Science can still be achieved	**Minor or no impact on mission life or performance:** noticeable or no degradation, that does not lead to loss of science or significant peril to mission. (Category 4)	Certain - failure will be detected and prevented or mitigated
2 Low	Low ($0.02 < P_F \leq 0.15$) Or ($7.3 \times 10^{-7} < \lambda \leq 5.9 \times 10^{-6}$ for mission duration)	Minor impact to full mission success criteria → Threshold Science can still be achieved; Baseline Science may be degraded or performed at a reduced level	**Potential for major or significant degradation of mission or performance:** no immediate impact on mission, but potential exists for future loss, at level 5-3, if adequate alternatives or measures are not implemented. (Category 3)	Moderate to High - Failure is likely to be detected before occurrence and has a good chance of being prevented or mitigated
3 Moderate	Moderate ($0.15 < P_F \leq 0.25$) Or ($5.9 \times 10^{-6} < \lambda \leq 1.03 \times 10^{-5}$ for mission duration)	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin → All of the Threshold Science is still achievable; Not all Baseline Science is achievable (e.g., Cannot perform science at one or more Baseline Science performance levels)	**Significant loss or degradation of mission:** significant loss of mission function leading to a significant loss of data, or a significant reduction in life of the mission. (Category 2 or 3) Or **Loss or degradation of a redundant subsystem** or science instrument producing levels 4 or 3 severity, if remaining redundancy is lost. (Category 2R)	Low to Moderate - Failure may be detected and may be prevented or mitigated
4 High	High ($0.25 < P_F \leq 0.50$) Or ($1.03 \times 10^{-5} < \lambda \leq 2.5 \times 10^{-5}$ for mission duration)	Major impact to full mission success criteria. Minimum mission success criteria is achievable → Threshold Science is still achievable; Cannot meet any Baseline Science performance requirements	**Major loss or degradation of mission:** capability to complete some mission objectives (Category 2) Or **Loss or degradation of a redundant subsystem** producing levels 4 or 5 severity, if remaining redundancy is lost. (Category 1R)	Remote - Unlikely failure will be detected or prevented or mitigated
5 Very High	Very High ($0.50 < P_F$) Or ($2.5 \times 10^{-5} < \lambda$ for mission duration)	Minimum mission success criteria is not achievable → Threshold and Baseline Science is not achievable. (e.g., Cannot perform science at one or more Threshold Science performance levels)	**Complete loss of mission:** complete loss of primary mission capability. (Category 1) Or **Loss or degradation of a subsystem or science leading to safety or hazard monitoring system failure** that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Severity 5 consequences (Category 1S)	None - Failure will not be detected and will not be prevented or mitigated

Table 4 – Detection/Prevention Scale Example

Ref. No.	Component Name	Component Function	Potential Failure Mode	Potential Cause of Failure	Occurrence Value	Potential Effects of Failure			Severity Value	Severity Category	Mitigating Factors (Detection/Prevention)	D/P Value	RPN
						Local Effect	Subsystem Effect	Mission Effect					
MEB-6	Ultra-Stable Oscillators (USO)	Provides clock signal	USO frequency change/drift	No autonomous switching Thermal control (internal) loss	1	Degraded performance parameter	Inaccurate synchronization between systems using USO	Degraded Science	3	2R	Detection: USO drift identified in science data Mitigation: switch to redundant USO Prevention: High Quality Parts and Design, and workmanship with robust testing,	3	9

Table 5 – Example FMECA Worksheet Item from GSFC Project

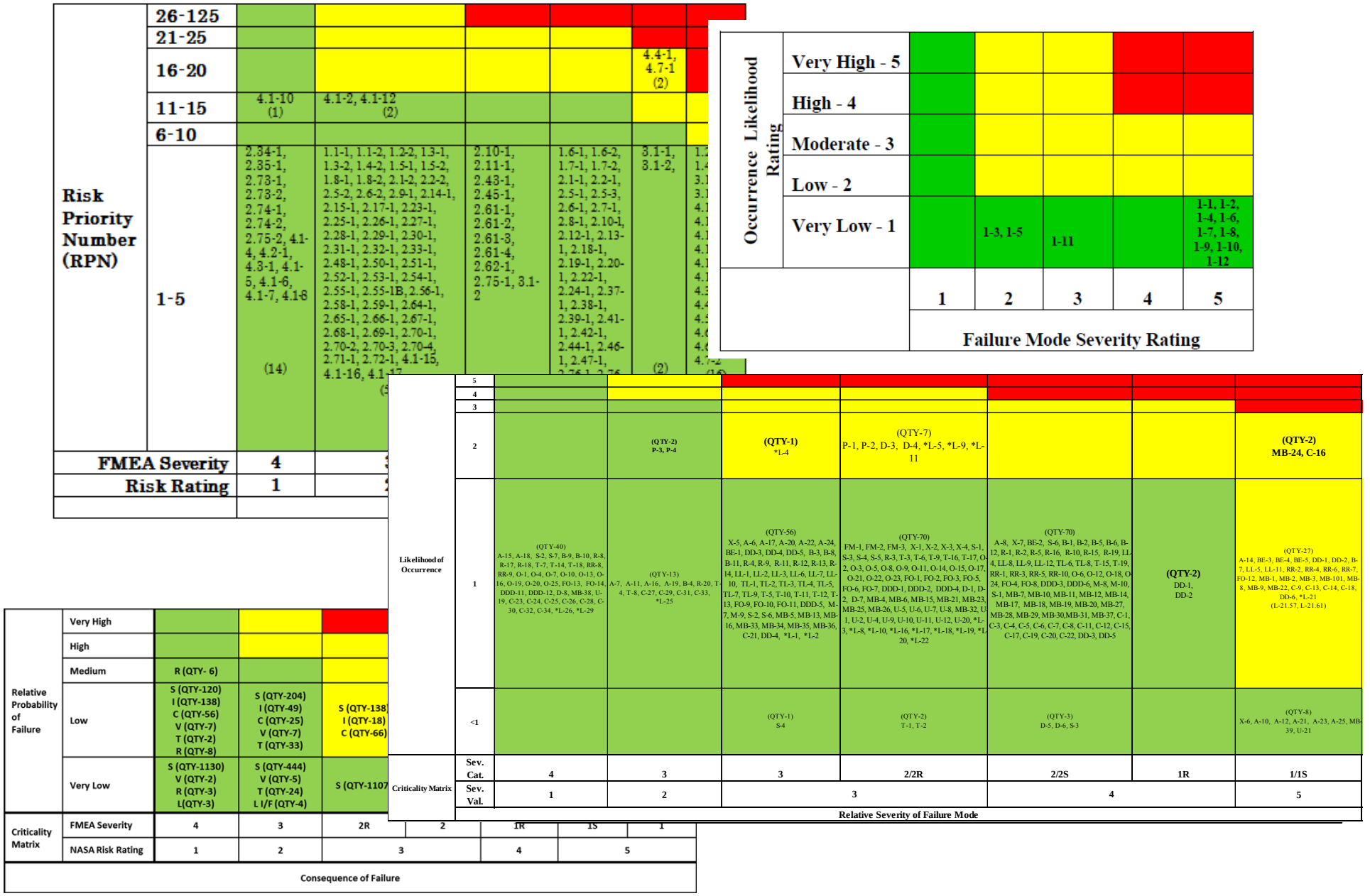

Figure 6 – Typical Mission FMECA Risk Matrix Examples
(Entries are FMECA IDs & Quantities)

4 CONCLUSIONS & RECOMMENDATIONS

GSFC has seen FMECA generated risks submitted, accepted, and managed by ICESat-2 mission team which has ensured that adequate caution has been used in integration and test decisions. GSFC has also seen that the FMECA risk matrices when presented at mission milestones reviews by OSIRIS-Rex, ICESat-2, and RRM served to eliminate the potential for action items and clearly depicted the risk posture to the review team. While these are specific and more visible GSFC successes for this methodology the capturing and communication of FMECA risk, using the methodology and tools shown in this paper, in standard FMECA reports has been found to more effectively develop an understanding of FMECA results between reliability engineering and project management/systems engineering. These and other successful uses of this FMECA risk assessment and communication methodology on multiple and diverse GSFC missions has established that this method can be considered valid and useable for other space flight missions. Further it can be inferred that this method would be applicable to any industry or subject matter that uses FMECAs as a design/system analysis tool or root cause identifier and uses risks to maximize the chances of objectives being achieved.

However, to implement this methodology successfully it is recommended that the analyst, project, and/or organization:

- Define up-front risk definitions for consequence and likelihood;
- Establish and understand the mission/project/system success criteria and allowable degradations or mitigation strategies within the success criteria;
- Agree and implement risk management strategies and philosophies consistent with mission/project/system and or organizational risk tolerance intensities;
- Acquire up-front agreement on FMECA correlations especially criticality levels;
- Involve designers, safety, quality, management, and systems engineering in the failure postulation and analysis.

Ultimately, using FMECA as a risk assessment tool as well as a design tool and failure or root cause analysis tool is a value-added endeavor and is highly recommended.

REFERENCES

1. Goddard Procedural Requirements for Risk Management, Goddard Space Flight Center Code 300, GPR 7120.4D.
2. Agency Risk Management Procedural Requirements, NASA, NPR 8000.4A.
3. GSFC Single Point Failure (SPF) Policy, GSFC Code 300 Chief Safety and Mission Assurance Engineer, 28 Aug 2013.
4. Standard Mission Assurance Requirements, GSFC Code 320, 320-MAR-1001B, 20 May2010.
5. FMEA & FMECA, https://en.wikipedia.org/wiki/FMEA
6. Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, MIL-STD-1629, 04-AUG-98.
7. Performing a Failure Mode and Effects Analysis (FMEA), GSFC Flight Assurance Procedure, P-302-720 (Rev -)
8. NASA Expendable Launch Vehicle Payload Safety Requirements, NASA-STD-8719.24 and Annex, 19 Jun 2012.
9. Criticality Analysis Presentation, FMEA INFO Centre, http://www.fmeainfocentre.com/updates/criticality-analysis-milstd1629-approach.ppt.

BIOGRAPHY

Nancy J Lindsey
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771

e-mail: nancy.j.lindsey@nasa.gov

Nancy Lindsey has spent 30+ years in aviation and aerospace engineering performing a variety of engineering tasks across the entire gamut of space vehicle life cycles and program types including Defense Communications Satellites, Commercial Communications and Television Missions, Space-based Astronomical Observatories, and Earth Science Monitoring Systems. She is a recognized innovator at GSFC based on her architecting and leading the development of the NASA GSFC Mission Configuration Tool, Failure Integration and Analysis Tool (FIAT), and the Code 300 Career Path using agile program management.

She is currently a Senior Systems Reliability Manager at the NASA GSFC in Greenbelt MD performing Life, Failure Mode, Fault, and Risk Analyses for many GSFC missions. As such she communicates findings, insightful recommendations, and/or risks to diverse audiences and performs/manages the performance of probability estimations for availability, success, and impact using reliability modeling and statistical tools (i.e., Bayesian Analysis, Monte Carlo Simulations, and Stochastic Statistics and tools). Further she assesses the risk of having a failure or a mission limiting scenario or component by performing Failure Mode, Fault Tree, or Probabilistic analyses and life assessments (using experience and/or test data). Ms. Lindsey's analyses are not limited to flight or ground system hardware and software but have also included human error estimation and mitigation strategy evaluation (e.g., her US Navy work on Controls and Displays for F-14 Out-of-Controlled flight situations).

She has a Bachelor of Science degree in Computer Science & Aeronautical Engineering and a Master's of Science degree in Space Studies. Nancy's independent research efforts can be viewed via her personal website: www.rcktmom.com.