The NASA Radiation Hardness Assurance (RHA) Process Standard

Razvan Gaza[1], Gregory R. Allen[2], Michael J. Campola[3], Kenneth A. LaBel[4], Raymond L. Ladbury[3], Jean-Marie Lauenstein[3], Joshua Pritts[5], Ted Wilcox[3], Peter J. Majewicz[3], Robert F. Hodson[6]

[1]NASA Johnson Space Center, Houston, TX, USA

[2]NASA Jet Propulsion Laboratory, Pasadena, CA, USA

[3]NASA Goddard Space Flight Center, Greenbelt, MD, USA

[4]Science Systems and Applications, Inc. at NASA Goddard Space Flight Center, Greenbelt, MD, USA

[5]Jacobs Technology Inc. at NASA Johnson Space Center, Houston, TX, USA

[6]NASA Langley Research Center, Hampton, VA, USA

2024-09 RADECS

List of Acronyms

CCA: Circuit-Card Assembly

COTS: Commercial-off-the-Shelf

D&C: Design and Construction (Standards)

DDD: Displacement Damage Dose

DSEE: Destructive SEE

EDD: Environments Definition Document

EEEE: Electric, electronic, electro-magnetic and electro-optical

FY: Fiscal Year

HEO: Human Exploration and Operations Mission Directorate

HW: Hardware

IRCP: Ionizing Radiation Control Plan

LET: Linear Energy Transfer

MEAL: Mission, Environment, Application, and Lifetime

MIL-SPEC: Military Specification

NDSEE: Non-destructive SEE

NEPP: NASA Electronic Parts and Packaging Program

NESC: NASA Engineering & Safety Center

NSPAR: Non-Standard Part Approval Request

NVROM: Non-Volatile Read-Only Memory

OSMA: (NASA) Office of Safety and Mission Assurance

(NASA) Program: A strategic investment by Mission Directorates or mission support offices with a defined architecture and/or technical approach, requirements, funding level, and a management structure that initiates and directs one or more projects.

(RHA) program: The detailed implementation of the RHA approach. The hierarchical structure for implementation and tracking of RHA activities including decomposed requirements and (references to) specific procedures and techniques for test and analysis.

RHA: Radiation Hardness Assurance

RHA Part: Radiation Hardness Assured Part

RHARD: RHA Requirements Document

SEB: Single-Event Burnout

SEGR/SEDR: Single-Event Gate/Dielectric Rupture

SEE: Single-Event Effect(s)

SEECA: SEE Criticality Analysis

SEFI: Single-Event Functional Interrupt

SEL: Single-Event Latchup

SET: Single-Event Transient

SEU: Single-Event Upset

SME: Subject Matter Experts

SMD: Science Mission Directorate

SRR: System Requirements Review

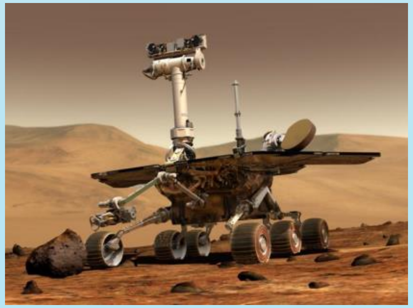
SW: Software

TID: Total Ionizing Dose

TNID: Total Non-Ionizing Dose

Motivation

- The NASA portfolio consists of a wide variety of missions
  - Subject to a wide range of MEAL (Mission, Environment, Application and Lifetime) criteria
- No single RHA program can feasibly envelop all these missions
  - Historically, Radiation Hardness Assurance (RHA) was left to the NASA Centers and Programs
- In 2019, the NASA Engineering and Safety Center (NESC) commissioned a task to formulate a set of RHA Guidelines for Exploration missions
  - TI-19-01489, https://ntrs.nasa.gov/citations/20210018053
  - The study concluded that successful RHA programs share specific characteristics, and recommended the development of a NASA Agency-level RHA Standard
- In 2022, the NASA Electronic Parts and Packaging (NEPP) Program commissioned a task to develop the NASA RHA Standard
  - A draft document was completed in 2023 and distributed for peer review
  - Comments have been incorporated and the document is ready for NASA Centers Review
- It is expected that the document will be formally baselined during FY 2025

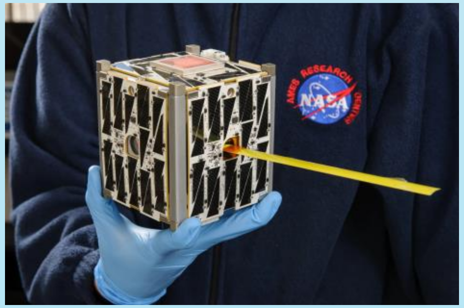



Image credits: nasa.gov

Agenda

- Requirements and challenges
- RHA Taxonomy
- Process to baseline an RHA Program
  - Fundamental Concepts: MEAL, risk
  - Compliance Matrices
  - Process
- RHA Schedule and Deliverables
- Conclusion

Requirements and Challenges

The RHA Standard must:

- Envelop the entire portfolio of NASA programs & projects
- Address modern technology needs of NASA Programs
  - Use of non-RHA parts, balancing system- and part-level RHA
  - Flexibility: Allow for non-traditional RHA approaches while providing radiation assurance commensurate with the mission-applicable success- and safety requirements
- Augment but not override existing Center, Program, or International Partners RHA Standards
- Include technical rationale “the why”
  - Technology maturation leads to new threats
  - Not intended as a comprehensive RHA textbook
- Stay clear of ambiguities in the RHA vernacular
  - Avoid terms like “Radiation hard” “Radiation tolerant” “COTS” “EEEE Parts Grade”
- Be consistent with existing NASA processes

RHA **Process** Standard - Prescribes the process of baselining Program- and project- RHA approaches consistent with the applicable MEAL criteria including the programmatic constraints and risk posture

RHA Taxonomy

- Taxonomy definition:
  - A system for naming and organizing things, especially plants and animals, into groups that share similar qualities (https://dictionary.cambridge.org/us/dictionary/english/taxonomy)
  - The study of the general principles of scientific classification, especially orderly classification of plants and animals according to their presumed natural relationships (https://www.merriam-webster.com/dictionary/taxonomy)
- An initial attempt was made to categorize electronic components based on their RHA characteristics, similar to the EEEE Part Grades
  - This proved insufficient as it failed to account for the system implementation
- Instead, the NASA standard provides a taxonomy of RHA approaches
  - A number of criteria grouped self-consistently
  - The criteria are organized into three classes: RHA Scope and Assurance, System-level, and EEEE-part-level
  - Separate taxonomies are provided for single-event effects and total dose

RHA Taxonomy Example

Table 6. SEE Taxonomy – RHA Scope and Assurance

RHA Category	S1	S2	S3	S4	S5
Risk tolerance posture	Low	Low-Medium	Medium-High	High	Very High
Purpose of SEE RHA	Assures reliability (DSEE) and	Assures reliability (DSEE) and	Provides targeted assurance	Provides some assurance of	N/A
Surviva					
A prior will be					
Availab produc					
A prior availab					
Anticip testing					

[6-1]"Targ
[6-2]Proto
[6-3]This
[6-4]Risk
[6-5]See
[6-6]Refer to Ap
[6-7]High energy

Table 7. SEE Taxonomy – System-level RHA criteria

RHA Category	S1	S2	S3	S4	S5
RHA integral to the design process	Yes	Yes	Yes	Selectively at project discretion	Not required
System-level LOE	SEE threats to reliability and	SEE threats to reliability and	SEE threats to availability do	None to interface-limited[7-2]	None to interface-limited[7-2]
SEEC					

[7-1]Par
[7-2]E.g
[7-3]For

Table 8. SEE Taxonomy – EEEE-part-level criteria

RHA Category	S1	S2	S3	S4	S5
SEE part selection criteria	**Enforced**	**Enforced**	**Enforced**	**Enforced**	**Not enforced**
SEE data type[8-1,8-2, 8-3]	Piece-part	CCA- and/or piece-part	CCA- and/or piece-part	CCA-level test	None
SEGR/SEB/SEDR acceptance criteria[8-4]	Risk avoidance (commonly, $37\ MeV\cdot cm^2/mg$)	Risk avoidance (commonly, $37\ MeV\cdot cm^2/mg$)	Risk avoidance (commonly, $37\ MeV\cdot cm^2/mg$)[8-5]	High energy protons for DSEE[8-6]	None
SEL/other DSEE acceptance criteria[8-6]	Risk avoidance (commonly, $75\ MeV\cdot cm^2/mg$) or quantification	Risk avoidance (commonly, $37\ MeV\cdot cm^2/mg$) or quantification	Risk avoidance (commonly, $37\ MeV\cdot cm^2/mg$) or quantification[8-5]	High energy protons for DSEE[8-6]	None
NDSEE acceptance criteria	Likelihood and criticality assessed and meet project requirements.	Likelihood and criticality assessed and meet project requirements.	Likelihood and criticality assessed and meet project requirements for critical systems.	Likelihood and criticality assessed and meet project requirements for critical systems.	None
SEE data representative of flight parts[8-7]	Required	Required	Recommended	Recommended as feasible	

[8-1]RHA guarantees are provided by US military standard, other government/industry organizations, or manufacturer/vendor. RHA parts are subject to lot traceability and manufacturing process change controls that vendor data may or may not provide. The radiation designator in MIL-PRF-38534/5 and MIL-PRF-19500 refers to TID only and is not indicative of any SEE guarantees. Data sheets often guarantee specific SEE characteristics only (e.g., SEL LET threshold) and must be supplemented by manufacturer/vendor- or application specific testing on flight-lot representative samples.

[8-2]Refer to Appendix G: RHA Evidence Hierarchy and definitions of "acceptable data" available in the literature (e.g., Poivey, 2002; Gonzales, 2018)

[8-3]Compliant to national and international standards to the extent practical

[8-4]Based on structure layout of the device

[8-5]Test LET may be reduced to program-agreed level (e.g., to 20-30 $MeV\cdot cm^2/mg$) due to practical considerations

[8-6]DSEE risk remaining for specific part types e.g., with thick sensitive regions [RHA guidelines]

[8-7]Analysis required to validate applicability of previous test data to the flight design

RHA Taxonomy Example

Table 6. SEE Taxonomy – RHA Scope and Assurance

RHA Category	S1	S2	S3	S4	S5
Risk tolerance posture	Low	Low-Medium	Medium-High	High	Very High
Purpose of SEE RHA	Assures reliability (DSEE) and	Assures reliability (DSEE) and	Provides targeted assurance	Provides some assurance of	N/A
Surviva					
A prior will be					
Availab produc					
A prior availab					
Anticip testing					

[6-1]"Targ

[6-2]Prot

[6-3]This

[6-4]Risk

[6-5]See F

[6-6]Refer to Appendix G: RHA Evidence Hierarchy and definitions of "acceptable data" available in the literature (e.g., Poivey, 2002)

[6-7]High energy protons (~200 MeV) often used as the main test solution. Heavy ion testing performed for specific part types e.g., with thick sensitive regions

Table 7. SEE Taxonomy – System-level RHA criteria

RHA Category	S1	S2	S3	S4	S5
RHA integral to the design process	Yes	Yes	Yes	Selectively at project discretion	Not required
System-level LOE	SEE threats to reliability and availability drive the mission success criteria. Systems architecture, circuit design, parts selection, and SW/VHDL are carefully managed throughout project or program lifecycle to meet all SEE requirements.[7-1]	SEE threats to reliability and availability drive the mission success criteria. Systems architecture, circuit design, parts selection, and SW/VHDL are carefully managed throughout project or program lifecycle to meet all SEE requirements.[7-1]	SEE threats to availability do not directly drive mission success. The system's tolerance inherent to the design, rather than extensive part test data, is expected as a primary mitigation for nondestructive SEE. Destructive SEE is managed by a strategic combination of parts testing and system design to assure reliability.[7-1]	None to interface-limited[7-2]	None to interface-limited[7-2]
SEECA	Required for all systems[7-3]	Required for all systems[7-3]	Required for critical systems	Recommended to identify driving risk to reliability, availability, and performance. Required for do-no-harm if not guaranteed by system-level mitigation	Do-no-harm strategy completely relies on system-level mitigation

[7-1]Part selection for risk avoidance (e.g., SEE rad-hard vs. rad-tolerant) lowers the scope of system-level LOE vs. risk quantification and analysis-driven design mitigation implementation

[7-2]E.g., implementation of current monitoring and power cycling capability external to the CCA

[7-3]For equivalent risk posture, decreased assurance at piece-part level requires increased scope at systems level for RHA design and analysis.

RHA Taxonomy Example

Table 6. SEE Taxonomy – RHA Scope and Assurance

RHA Category	S1	S2	S3	S4	S5
Risk tolerance posture	Low	Low-Medium	Medium-High	High	Very High
Purpose of SEE RHA	Assures reliability (DSEE) and availability (NDSEE) consistent with the program risk tolerance posture	Assures reliability (DSEE) and availability (NDSEE) consistent with the program risk tolerance posture	Provides targeted assurance of reliability (DSEE) and availability (high impact NDSEE)[6-1]	Provides some assurance of reliability (DSEE) and availability (NDSEE).	N/A
Survivability assurance result	Verified risk avoidance or quantification	Verified risk avoidance or quantification	Limited risk analysis[6-2]	Limited risk analysis[6-2]	None
A priori confidence reliability will be met[6-3]	High[6-4]	Limited[6-4]	Limited[6-4]	None	None
Availability assurance product	Probability quantification of all unmitigated SEE impacting mission success criteria	Probability quantification of all unmitigated SEE impacting mission success criteria	Limited risk analysis[6-5]	Limited risk analysis[6-5]	None
A priori confidence availability will be met[6-3]	High[6-4]	Limited[6-4]	Limited[6-4]	None	None
Anticipated scope of SEE testing[6-6]	Piece-part heavy ion characterization test data if not already available. Additional testing as needed for NDSEE characterization, low-LET-threshold parts proton susceptibility, CCA-level for complex system interactions (e.g., SW and HW) and NDSEE mitigation and correction validation, etc.	Combination of CCA- and piece-part-level, high-energy proton and heavy ion testing. Additional testing as needed for NDSEE characterization, low-LET-threshold parts proton susceptibility, CCA-level for complex system interactions (e.g., SW and HW) and NDSEE mitigation and correction validation, etc.	Combination of CCA- and piece-part-level, high-energy proton and heavy ion testing[6-7]	CCA-level high energy proton testing	None

[6-1]"Targeted" definition: focused on project priorities and within budget and schedule constraints
[6-2]Proton-data-derived heavy ion DSEE susceptibility quantification is unreliable
[6-3]This refers to the ability to guarantee at the inception of the RHA effort that the program required reliability and availability goals will ultimately be met.
[6-4]Risk avoidance provides guarantees. Risk quantification can be effective subject to successful implementation of RHA processes.
[6-5]See RHA Guidelines Document for CCA-level test limitations
[6-6]Refer to Appendix G: RHA Evidence Hierarchy and definitions of "acceptable data" available in the literature (e.g., Poivey, 2002)
[6-7]High energy protons (~200 MeV) often used as the main test solution. Heavy ion testing performed for specific part types e.g., with thick sensitive regions

RHA Taxonomy Example

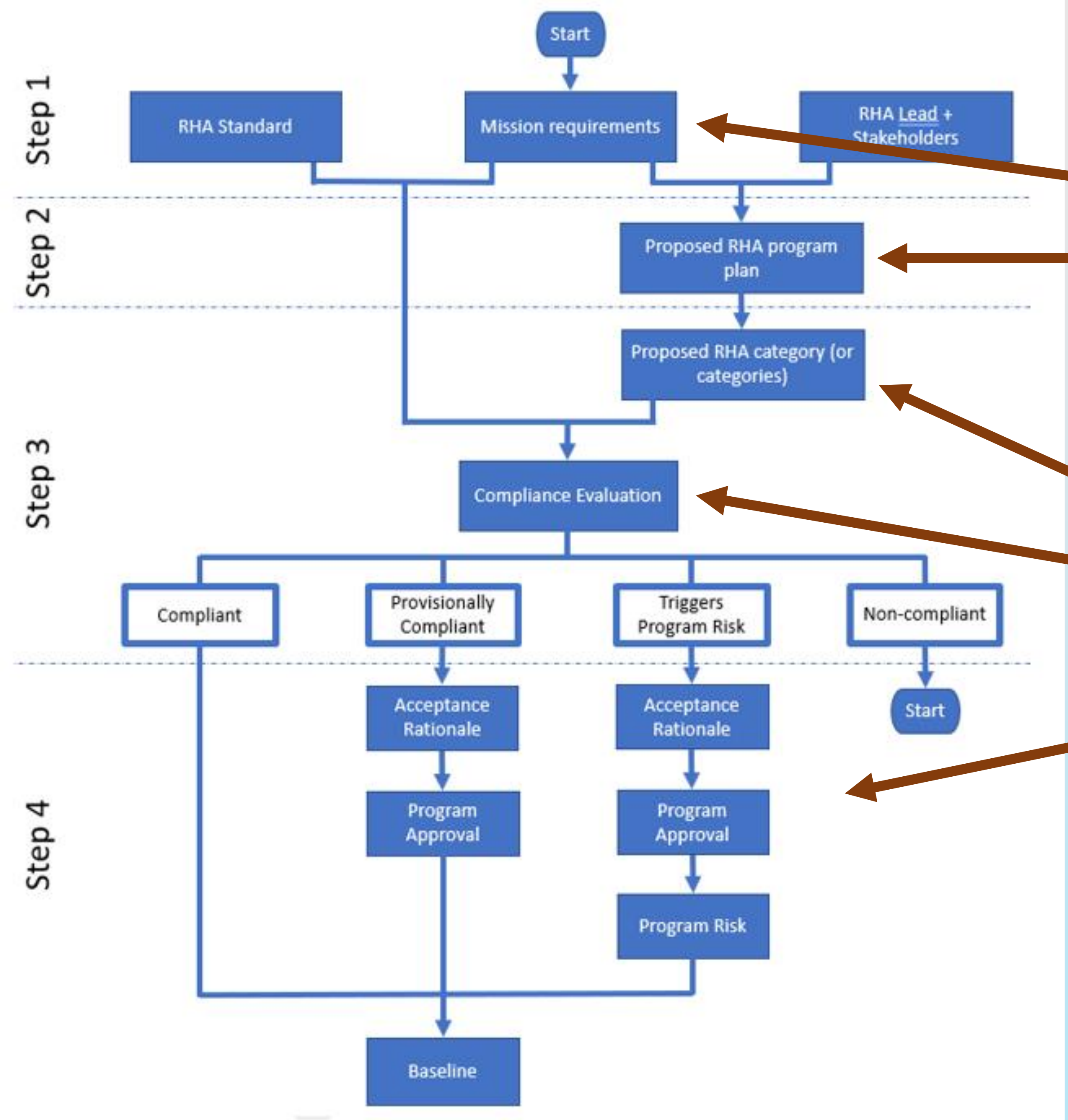
Table 6. SEE Taxonomy – RHA Scope and Assurance

RHA Category	S1	S2	S3	S4	S5
Risk tolerance posture	Low	Low-Medium	Medium-High	High	Very High
Purpose of SEE RHA	Assures reliability (DSEE) and availability (NDSEE) consistent with the program risk tolerance posture	Assures reliability (DSEE) and availability (NDSEE) consistent with the program risk tolerance posture	Provides targeted assurance of reliability (DSEE) and availability (high impact NDSEE)[6-1]	Provides some assurance of reliability (DSEE) and availability (NDSEE).	N/A
Survivability assurance result	Verified risk avoidance or quantification	Verified risk avoidance or quantification	Limited risk analysis[6-2]	Limited risk analysis[6-2]	None
A priori confidence reliability will be met[6-3]	High[6-4]	Limited[6-4]	Limited[6-4]	None	None
Availability assurance product	Probability quantification of all unmitigated SEE impacting mission success criteria	Probability quantification of all unmitigated SEE impacting mission success criteria	Limited risk analysis[6-5]	Limited risk analysis[6-5]	None
A priori confidence availability will be met[6-3]	High[6-4]	Limited[6-4]	Limited[6-4]	None	None
Anticipated scope of SEE testing[6-6]	Piece-part heavy ion characterization test data if not already available. Addi[illegible] for N[illegible] low-[illegible] proto[illegible] level[illegible] inter[illegible] HW) [illegible] and correction validation, etc.	Combination of CCA- and piece-part-level, high-energy proton and heavy ion testing. [illegible] and correction validation, etc.	Combination of CCA- and piece-part-level, high-energy proton and heavy ion testing[6-7]	CCA-level high energy proton testing	None

[6-1]"Targeted" definition: focused on project priorities and within budget and schedule constraints
[6-2]Proton-data-derived heavy ion DSEE susceptibility quantification is unreliable
[6-3]This refers to the ability to guarantee at the inception of the RHA effort that the program required reliability and availability goals will ultimately be met.
[6-4]Risk avoidance provides guarantees. Risk quantification can be effective subject to successful implementation of RHA processes.
[6-5]See RHA Guidelines Document for CCA-level test limitations
[6-6]Refer to Appendix G: RHA Evidence Hierarchy and definitions of "acceptable data" available in the literature (e.g., Poivey, 2002)
[6-7]High energy protons (~200 MeV) often used as the main test solution. Heavy ion testing performed for specific part types e.g., with thick sensitive regions

Relaxation of EEEE-part-level criteria may to an extent be mitigated by an increase in system-level effort and result in comparable assurance, but with lower a priori confidence

RHA Baseline Process



Step 1: Evaluate mission

Step 2: Define the proposed RHA program plan

Step 3: Determine the programmatic activities required to baseline the proposed RHA approach

- Categorization per taxonomy
- Compliance evaluation

Step 4: Execute the required programmatic activities to baseline the proposed RHA approach at SRR

- Different levels of program visibility
  - “Provisionally compliant” requires program approval
  - “Triggers risk” requires programs to carry a radiation risk

Compliance Matrices

- The standard provides compliance matrices associating different mission classes (or safety-criticality levels) with RHA categories
  - Four compliance matrices are provided for robotic- and crewed spaceflight, SEE and total dose
- For example, compliance matrix for crewed space flight, SEE

S2: Requirement relaxation at the part level is allowed only with systems-level mitigation and program visibility via the Risk process

Criticality 1 (loss of life)

S1: compliant

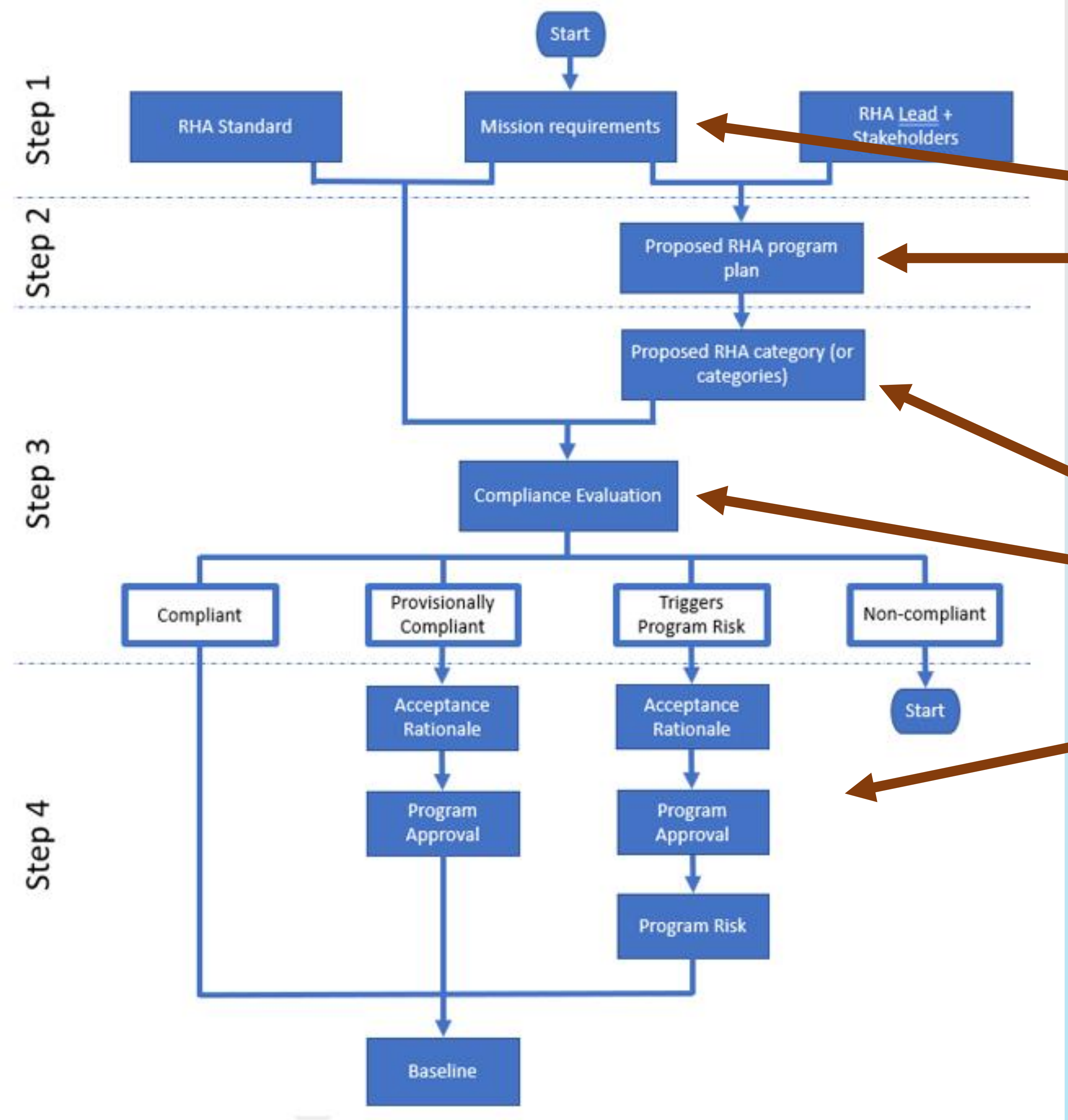
S3: Requirement relaxation at the part level without systems-level mitigation is not allowed

Table 12. RHA compliance matrix: SEE, Crewed Space Flight

Crewed Space Flight	S1	S2	S3	S4	S5
Crit1	Compliant	Triggers Program Risk	Non-compliant	Non-compliant	Non-compliant
Crit2	Compliant	Provisionally Compliant	Triggers Program Risk	Non-compliant	Non-compliant
Crit3/Non-critical	Compliant	Compliant	Provisionally Compliant	Provisionally Compliant	Non-compliant

For Criticality 2 (loss of mission) the bar is slightly lower, and then even lower for Criticality 3

RHA Baseline Process



Step 1: Evaluate mission

Step 2: Define the proposed RHA program plan

Step 3: Determine the programmatic activities required to baseline the proposed RHA approach

- Categorization per taxonomy
- Compliance evaluation

Step 4: Execute the required programmatic activities to baseline the proposed RHA approach at SRR

- Different levels of program visibility
  - "Provisionally compliant" requires program approval
  - "Triggers risk" requires programs to carry a radiation risk

The NASA risk management process

- “Risk” has a very specific meaning in the NASA vernacular
- The risk management process is a formally established NASA process (NPR 8000.4C)
- Utilizes tools such as the risk matrix to communicate how individual issues (e.g., schedule, cost, and technical) related to a given mission are classified and prioritized to one another.
- Every risk is formulated as a triplet: scenario, likelihood, and consequence
- Each program has its own scorecard reflecting MEAL criteria
- Leveraged in the RHA standard to ensure that projects benefit from Program visibility and system-level resources towards meeting mission goals.

Page 1 of 2

ORION (CEV) RISK SCORECARD

ORION

LIKELIHOOD RATING

5 Very High	Qualitative: Likely to occur.
	Quantitative: $10^{-1} < P$ (for risks with primary impact on human safety) or $P > 50\%$ (for risks with primary impact on cost, schedule, or performance)
4 High	Qualitative: Probably will occur.
	Quantitative: $10^{-2} < P \leq 10^{-1}$ (for risks with primary impact on human safety) or $33\% < P \leq 50\%$ (for risks with primary impact on cost, schedule, or performance)
3 Moderate	Qualitative: May occur.
	Quantitative: $10^{-3} < P \leq 10^{-2}$ (for risks with primary impact on human safety) or $10\% < P \leq 33\%$ (for risks with primary impact on cost, schedule, or performance)
2 Low	Qualitative: Unlikely to occur.
	Quantitative: $10^{-6} < P \leq 10^{-3}$ (for risks with primary impact on human safety) or $1\% < P \leq 10\%$ (for risks with primary impact on cost, schedule, or performance)
1 Very Low	Qualitative: Occurence improbable.
	Quantitative: $P \leq 10^{-6}$ (for risks with primary impact on human safety) or $P \leq 1\%$ (for risks with primary impact on cost, schedule, or performance)

RISK MATRIX

LIKELIHOOD	1	2	3	4	5
5	10	16	20	23	25
4	7	13	18	22	24
3	4	9	15	19	21
2	2	6	11	14	17
1	1	3	5	8	12

CONSEQUENCES

TIMEFRAME

Near	0 to 3 months
Mid	3 to 9 months
Far	> 9 months

Time to Initiate Handling Strategy

Conseqeuence Rating

IMPACTS TO CEV GOALS		1 Very Low	2 Low	3 Moderate	4 High	5 Very High
SAFETY	Personnel	A condition that could cause the need for minor first aid treatment though would not adversely affect personal safety or health (Class IV)	A condition that may cause minor injury or occupational illness. (Class III)	A condition that may cause severe injury or occupational illness (Class II)	A condition that may cause permanently disabling injury (Class I-B)	A condition that may cause death or loss of crew (Class I-A)
SAFETY	Facilities, Equipment, or Other Assets	A condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear (Class IV)	A condition that may cause minor property damage to facilities, systems, equipment, or flight hardware (Class III)	A condition that may cause major property damage to facilities, systems, equipment, or flight hardware (Class II)	A condition that may cause destruction of non critical facilities or assets (Class I-B)	A condition that may cause destruction of critical facilities on the ground, major systems, or vehicle during the mission (Class I-A)
SAFETY	Environment	Negligible OSHA/EPA violation - non reportable	Minor reportable OSHA/EPA violation	Moderate OSHA/EPA violation which requires immediate remediation	Major OSHA/EPA violation causing temporary stoppage	Serious or repeat OSHA/EPA violations resulting in action terminating project
PERFORMANCE (Mission Success) Including impacts to operations and supportability		Negligible impact to requirements, mission objectives or technical goals	Minor Impact to requirements, mission objectives or technical goals	Moderate impact to requirements, mission objectives or technical goals	Major impact to requirements, mission objectives or technical goals	Technical goals not achievable with existing engineering capabilities/ technologies
COST		<\$100K (Negligible impact to budget)	>\$100K but ≤\$1M (Minor impact to budget)	>\$1M but ≤\$10M (Moderate impact to budget)	>\$10M but ≤\$50M (Major impact to budget)	>\$50M (Possible project cancellation)
SCHEDULE		Negligible schedule impact	Minor overall schedule impact (Accommodate with reserve, no impact to critical path)	≤1 month impact to critical path/ milestones	>1 and ≤5 month impact to critical path/milestones	>5 month impact to critical path/ milestones or possible project cancellation

September 2006

Oscar Gonzales et al., “Space System Verification Approach Based on MEAL and Mission Risk Posture”
https://ntrs.nasa.gov/api/citations/20180007359/downloads/20180007359.pdf

Jeevan S. Perera, “NASA’s Enterprise Risk Management System”
https://ntrs.nasa.gov/api/citations/20110020315/downloads/20110020315.pdf

RHA Schedule and Deliverables

- Timing of the RHA activities is important
  - Budget commensurate with requirements
  - Early architecture, part selection strategy consistent with mission requirements
- Specific “shall” statements associated with RHA deliverable schedule and contents

	Project or Program Formulation				Project or Program Implementation						Program
	Pre- Phase A	Phase A		Phase B	Phase C		Phase D		Phase E	Phase F	
	KDP A	KDP B		KDP C	KDP D		KDP E		KDP F		
Milestone	MCR	SRR[1]	SDR	PDR	CDR	SIR	ORR	FRR	DR	DRR	FRR
RAD2	RHA SME	Assign RHA Lead									
RAD3	RHA Feasibility	Update as necessary									
RAD4		RHA Baseline									
RAD5	Preliminary Estimates	Initial ERD/EDD		Mature ERD/EDD	Final ERD/EDD						
RAD6 RAD7		Baseline RHARD	Update as necessary (CR required)								
RAD8				Initial RAR							
RAD9					Mature RAR						
RAD10											Final RAR
RAD11	Manage risk										
Parts List Rad Review		Critical Devices	Initial		Update	Update as necessary					
Test Schedule Plan incl RLAT[2]				Initial	Update	Update as necessary					
Subsystem Rad Req Allocations[3]		Initial		Update	Final						
System-level Rad Analysis & Report[4] RAD10					Inputs	Update as necessary					Final RAR

RHA Schedule and Deliverables

- Timing of the RHA activities is important
  - Budget commensurate with requirements
  - Early architecture, part selection strategy consistent with mission requirements
- Specific "shall" statements associated with RHA deliverable schedule and contents

RAD9 At CDR, programs and projects shall provide a mature version of the Radiation Analysis Report (RAR) containing at minimum the items shown in Table 4.

Rationale: RHA activities must be fundamentally complete by CDR. Tailoring of the RAR contents is acceptable for mission class[10] D and some C, and for Crit 3 projects.

Table 4. Minimum required CDR RAR contents

Validation of previous assumptions and documentation updates including the PDR RAR and EDD.
List of hardware to be addressed in the radiation review. This information establishes the scope for the radiation effects review.
Total dose (ionizing and non-ionizing) radiation analyses and requirements compliance status
Single-event effects piece-part level requirements compliance status
Final single-event effects criticality analysis (SEECA) including impact characterization
The complete list of SEE that are not mitigated at component level (i.e., SEE propagating through the interfaces) and requirements for external mitigation.
Impact description of high-risk SEE modes with sufficient detail to enable system-level radiation integration (e.g., information on system response, existing and required mitigation at both circuit and system level, and any forward work required to reduce risk)
Summary of radiation requirements compliance, margins, remaining radiation testing, open items / liens and path to closure
References to deviations/waivers approvals
References to the RHA-relevant objective evidence, e.g., design data, radiation test reports, parts lists, NSPAR and deviations/waivers approvals, radiation data applicability / similarity to the flight design, analyses requiring radiation inputs such as WCCA, FMECA, etc.

Conclusion

- The NASA RHA Process Standard is in an advanced formulation stage and will undergo a Centers Review process before being baselined
  - It prescribes the process to be used by NASA Programs and projects to baseline their RHA programs
  - Allows Programs and projects flexibility in balancing EEEE-part-level- and system-level RHA
  - While utilizing established processes to ensure sufficient program visibility and resources to meet mission requirements

Thank you for your attention

razvan.gaza@nasa.gov

Backup

Process to baseline an RHA Program: MEAL

- Mission, Environment, Application, and Lifetime

Risk Classification
(NPR 7120.5 Projects)

- Class A: Lowest risk posture by design
  - Failure would have extreme consequences to public safety or high priority national science objectives.
  - In some cases, the extreme complexity and magnitude of development will result in a system launching with many low to medium risks based on problems and anomalies that could not be completely resolved under cost and schedule constraints.
  - Examples: HST and JWST
- Class B: Low risk posture
  - Represents a high priority National asset whose loss would constitute a high impact to public safety or national science objectives.
  - Examples: GOES-R, TDRS-K/L/M, MAVEN, JPSS, and OSIRIS-REX
- Class C: Moderate risk posture
  - Represents an instrument or spacecraft whose loss would result in a loss or delay of some key national science objectives.
  - Examples: LRO, MMS, TESS, and ICON
- Class D: Cost/schedule are equal or greater considerations compared to mission success risks
  - Technical risk is medium by design (may be dominated by yellow risks).
  - Many credible mission failure mechanisms may exist. A failure to meet Level 1 requirements prior to minimum lifetime would be treated as a mishap.
  - Examples: LADEE, IRIS, NICER, and DSCOVR

Risk Classification
(Non-NPR 7120.5 Projects)

- **NPR 7120.8 "class" – Technical risk is high**
  - Some level of failure at the project level is expected; but at a higher level (e.g., program level), there would normally be an acceptable failure rate of individual projects, such as 15%.
  - Life expectancy is generally very short, although instances of opportunities in space with longer desired lifetimes are appearing.
  - Failure of an individual project prior to mission lifetime is considered as an accepted risk and would not constitute a mishap. (Example: ISS-CREAM)
- ***"Do No Harm" Projects*** – If not governed by NPR 7120.5 or 7120.8, we classify these as "Do No Harm", unless another requirements document is specified
  - Allowable technical risk is very high.
  - There are no requirements to last any amount of time, only a requirement not to harm the host platform (ISS, host spacecraft, etc.).
  - No mishap would be declared if the payload doesn't function. (Note: Some payloads that may be self-described as Class D actually belong in this category.) (Example: CATS, RRM)

7120.8 and "Do No Harm" Projects are not Class D

Jesse Leitner, "Risk Classification and Risk-based Safety and Mission Assurance
https://ntrs.nasa.gov/api/citations/20150001352/downloads/20150001352.pdf

Process to baseline an RHA Program: MEAL

- Mission, Environment, Application, and Lifetime
  - Mission class is not defined for crewed missions
  - Criticality is the equivalent for crewed missions

Monitoring Safety Critical Items

As part of the safety, reliability and quality assurance effort, components of the Shuttle system are assigned to criticality categories as follows:

Criticality 1	Loss of life or vehicle if the component fails.
Criticality 2	Loss of mission if the component fails.
Criticality 3	All others.
Criticality 1R	Redundant components, the failure of both could cause loss of life or vehicle.
Criticality 2R	Redundant components, the failure of both could cause loss of mission.

"Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident"
https://www.nasa.gov/history/rogersrep/v1ch7.htm

RHA Ecosystem

RAD2 During Pre-Phase A, programs and projects shall assign an experienced RHA engineer as RHA lead responsible for implementing the RHA program and establish an-, or integrate into the existing RHA ecosystem.

Rationale: Responsibilities of the RHA lead include planning and execution of the RHA effort, coordination with the RHA customer, coordination with the design- and system engineering teams, ownership of radiation deliverables, status reporting, etc. RHA being a specialized field, the experience of the RHA lead is often a success predictor for the RHA program. Radiation topics are often dispositioned by SME agreement. For this reason, a program RHA ecosystem (i.e., system of checks and balances) is critical to successful execution of RHA. Such an ecosystem can for example consist of a program-established radiation working group with sufficient participation, or be provided as insight/oversight from other SMEs. Projects are urged to assign the roles of RHA leads to engineers other than program-level RHA leads to ensure meaningful review.

Standard-at-a-glance

Prescribes the process for radiation program integration

- Levies requirements for:
  - RHA schedule
  - RHA deliverables
- Requires programs & projects to accept a risk if the schedule / deliverables are not met

Prescribes the process for programs and projects to baseline their RHA approach

- Defines RHA process taxonomy & correlation w/ MEAL
- Prescribes the program scrutiny required to baseline the RHA approach
  - Up to accepting a risk

- Leverages NASA Risk Management Process
  - Mitigation plan, risk tracking to closure

Highlights

- This is a process standard
  - How to implement an RHA program consistent with the MEAL criteria
    - Mission, Environment, Application, and Lifetime
- Provides a framework for RHA integration at system level
  - Establishes a schedule for RHA activities and deliverables
- Establishes a taxonomy of RHA approaches “Categories of RHA programs”
  - Much more than a radiation taxonomy of EEEE parts
  - Scope of RHA, System-level aspects/criteria, EEEE-Part-level criteria
- Establishes a process for baselining the program or project RHA approach
  - Allows for alternative RHA approaches with risk-informed program-level buy-in
  - The RHA taxonomy and MEAL factors determine the required level of program scrutiny
- Leverages the NASA risk process
  - Risks are not intended as a negative, but as a visibility & resource focus tool
- Additional non-prescriptive information critical to the correct interpretation of the intent of the standard is provided in the appendix sections