Artemis Missions Probabilistic Risk Assessment (PRA) & Reliability Assessment Overview

Roger Boyer, CRE

Lunar Surface Innovation Consortium (LSIC)
Power System Reliability Workshop

July 26, 2023

Roger L. Boyer Bio

Roger L. Boyer, CRE

Roger is the Associate Division Chief of the Space Transportation Systems Division with the National Aeronautics and Space Administration (NASA) at Johnson Space Center (JSC) in Houston, Texas. Roger is responsible for overseeing Probabilistic Risk Assessments (PRAs) of all Artemis missions to the lunar surface and the lunar Gateway space station. His experience includes mission analyses supporting the Space Shuttle, Mars, Constellation, Orion, Commercial Crew, Deep Space Gateway, and the new lunar lander and surface programs. He currently serves as NASA's Cross Program PRA lead responsible for integrating the various human exploration program PRAs (i.e. spacecraft, launch vehicle, lunar surface operations, human reliability, crew medical, external events, and pre-launch and post-landing ground operations on Earth) as well as overseeing the development of several new PRA methods for future use and serving on NASA's system safety steering group, human factors technical discipline team, and the integrated medical model steering committee.

Roger's career has evolved from performing deterministic thermal-hydraulic analyses, nuclear safety analyses, and PRA in the nuclear power industry to advanced automation Fault Detection, Isolation, and Recovery (FDIR) and PRA in the aerospace industry. Over a six-year period, he was instrumental in introducing PRA to the oil and gas industry (both on the commercial and government sides) and supported a couple of related National Academy of Science ad hoc committees, as well. He now serves on the National Academies Transport Airplane Risk Assessment Methodology (TARAM) Community of Experts (CoE). The common theme has been promoting and supporting management's risk-informed decision-making (RIDM) process from concept to design to operations with high quality risk assessments. He has 40 years of experience providing both technical analyses and leadership in risk, reliability, thermal-hydraulic and accident analysis, to the nuclear, aerospace, and oil & gas industries.

Roger holds BS degrees in both Nuclear and Mechanical Engineering as well as a MS in Nuclear Engineering from the University of Missouri at Rolla. He recently received NASA's Outstanding Leadership Medal and several other awards / commendations over the years. He is a Certified Reliability Engineer (CRE) with the American Society for Quality and held offices with the local section. He is an Eagle Scout, Vigil Honor member of the Order of the Arrow, and VP of Programs for his local Boy Scouts of America council. He volunteers for high school robotics competitions at the District, Regional, and National levels. His daughter and son are mechanical and nuclear engineers, respectively.

Glossary

- **Artemis Missions –** current follow on to Apollo missions to lunar surface
- **Agency LOC Threshold – Metric used to inform the NASA Administrator when the estimated mission risk becomes higher than previously approved**
- **Moon-to-Mars (M2M) program – new** overarching program encompassing Artemis Missions, as well as future Mars missions
- **Probability of Loss of Crew (LOC) –** is the death or permanently debilitating injury to one or more "flight" crew members.
- **Probability of Loss of Mission (LOM) –** is the loss of or inability to complete significant / primary mission objectives, which includes Loss of Crew.
- **Probabilistic Risk Assessment (PRA) -** is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes.
- **Cross Program PRA (XPRA) -** Integrated mission PRA
- **Technical Performance Metric (TPM) –** serves as a "warning track" or "trip wire" before reaching a requirement level.

Purpose

- To show how NASA's Moon-to-Mars (M2M) program can use hardware reliability assessments and comprehensive PRAs to estimate risk of future missions and manage risk via safety and mission success requirements from the top down, so that this risk can be balanced with other program metrics like cost and schedule.
- To provide some thoughts on how the NASA process can be utilized for the Lunar Grid development.

Background

- **NASA establishes Agency Loss of Crew (LOC) thresholds for mission classes as part of human rating requirements.**
  - An Agency LOC threshold provides a reporting threshold for risk, so programs can balance cost, schedule, and risk together and not overly constrain one at the expense of the other.
- **Mission classes define the major characteristics of a mission such as destination. For example, "Lunar Surface" or "Gateway Assembly".**
- **A mission class can involve several NASA vehicle programs (e.g., Orion, Gateway, or Human Landing System).**
- **NASA programs set requirements to ensure Agency LOC thresholds are met.**

Artemis Missions LOC Requirement Hierarchy

- NASA HQ establishes Agency LOC Thresholds for upcoming human Artemis Missions via defined mission classes, such as lunar surface mission class.
- M2M program establishes overall mission LOC Requirements (i.e. From crew ingress to Orion on the launch pad to crew recovery post-landing) to ensure that it meets the corresponding Agency LOC Thresholds with margin.
- Each vehicle program works with M2M program to establish vehicle program level LOC, LOM, and hardware reliability requirements which are consistent with the Agency LOC thresholds for each mission phase of each mission class.
- Each vehicle program flows hardware reliability requirements to the providers to enable the program to meet its LOC and LOM requirements.
- Each provider can establish its own internal requirements, as needed.

Why Not Allocate LOC & LOM to Providers?

- **Rather than allocating LOC & LOM requirements to program providers, Artemis programs established hardware reliability requirements. This was done for the following reasons:**
  - PRA is a specialized field and for those not familiar with performing a PRA, it may take years to develop the expertise needed.
  - A reliability requirement is more straightforward to verify because traditional reliability methods could be utilized.
  - Due to the integrated nature of Artemis (distributed functions), it would be difficult to allocate LOC to each provider.
  - Several sub-disciplines to PRA (e.g. Human reliability, software reliability, common cause, external events, etc.) are difficult to ensure consistency across multiple practitioners.

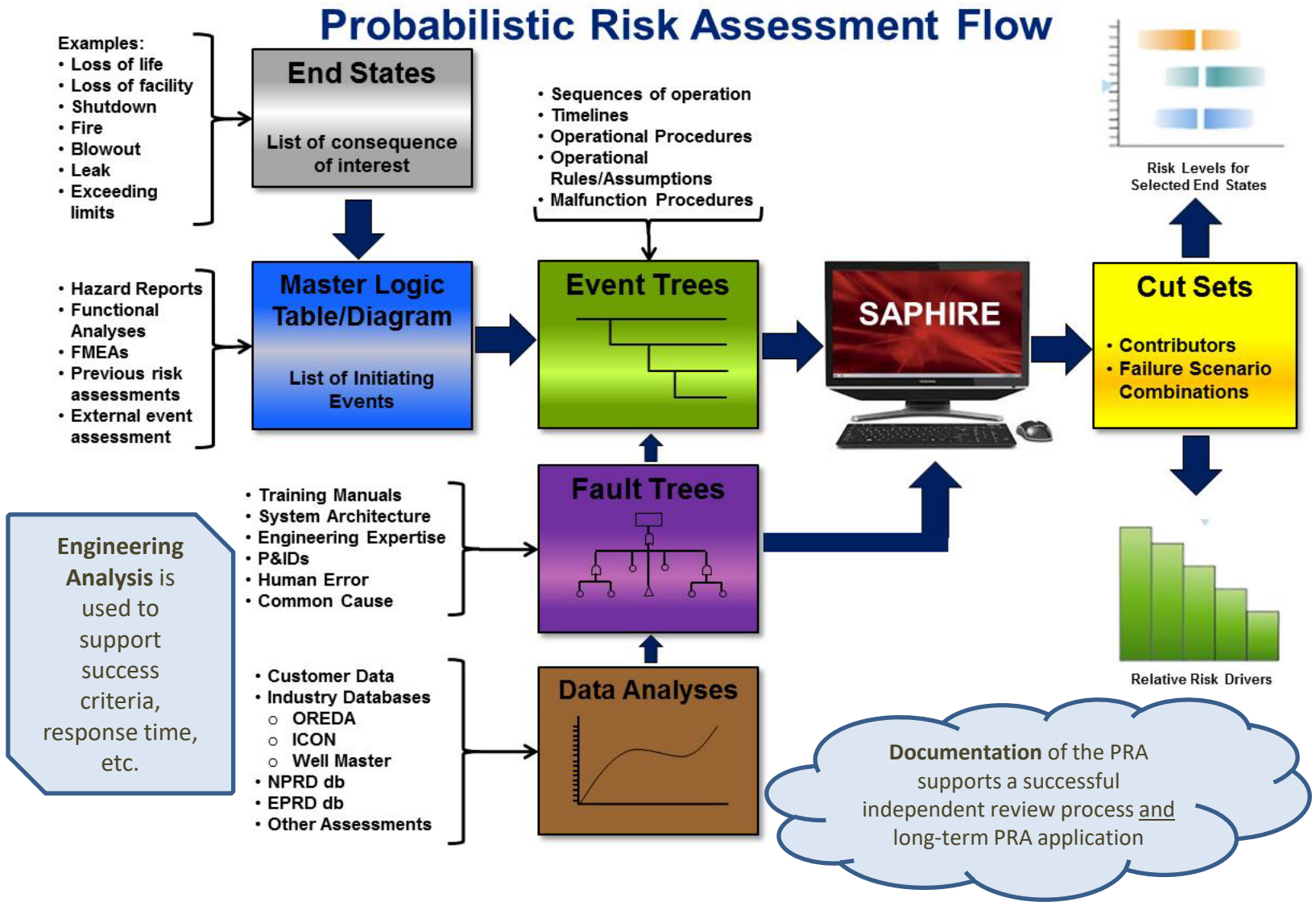
What Do Companies Do with a Hardware Reliability Requirement?

- **Further allocate it to sub-systems / components**
  - How it is allocated is up to the company, there are multiple allocation methods
  - Allocation facilitates management of the reliability across vendors, but could lead to a less optimal design
- **Utilize the reliability requirement to inform the design for example:**
  - Level of redundancy
  - Component selections
  - Vendors
- **Verify by analysis**
  - What does it take to verify by test? What would "test demonstration by V&V" look like?
    - In order to verify a 0.999 with 90% confidence reliability requirement by test, >1000 tests would be needed
  - There are a variety of hardware reliability prediction methods
    - MIL-HDBK-217F is still currently used in the Satellite industry for reliability prediction, but has not been updated since 1995
    - Generally, recommend utilizing data in the following order for reliability estimation
      1. Flight History data for any well established and proven design being considered for the mission
      2. Actual experience data from very similar equipment
      3. Life test or Accelerated life test data
      4. Commercial, NASA, or military reliability databases
      5. Reliability handbook data
      6. Expert elicitation

PRA Overview

- **PRA is the analysis tool NASA uses to verify programs meet LOC & LOM requirements**
  - PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes.
  - PRA process involves both system analysts and domain experts (Engineering, Operations, Crew etc.).
  - Numerical uncertainty communicated as part of model results (Band-Aid chart) is the result of propagating the data uncertainty. Uncertainty associated with logic is captured through sensitivity analyses.
  - When comparing risk estimates with uncertainty, it is important to consider the level of dependence between the two results.
  - PRA has limitations as all models do. Two of the biggest limitations is that it does not capture unknown risks and can yield underappreciated risks via biased analysts.
  - PRA has been used on Shuttle, and ISS for risk informed decision making and on Orion, Cross Program, and Commercial Crew as for risk informed design and decision making as well as LOC / LOM requirement verification.

PRA Event Tree / Fault Tree Process



PRA Process

- **Define the scope of the PRA**
  - Consequence – e.g. LOC / LOM
  - Mission Scope – e.g. Crew ingress to Crew egress
  - Establish mission phase(s) – e.g. Ascent, In-space, Entry & Landing
- **Develop Logic Models**
  - PRA Lead works with system analysts to develop event trees using master logic table / diagram
  - System analysts work with domain experts to develop fault trees
  - System analysts work with data analysts and domain experts to determine level of detail and failure logic
    - Develop fault trees to the level that data exists
  - Obtain concurrence on models from domain experts
- **Develop failure data**
  - Data analysts calculate failure probabilities based on best available data and approved methods
  - Includes expert elicitation and engineering judgement
- **Quantify the model, perform sanity checks, re-iterate until PRA Team is in agreement (Analysts and domain experts)**
- **Share results**
  - Risk drivers and insights
  - Incorporate feedback and update the model

PRA and Hardware Reliability Assessment Comparison

PRA

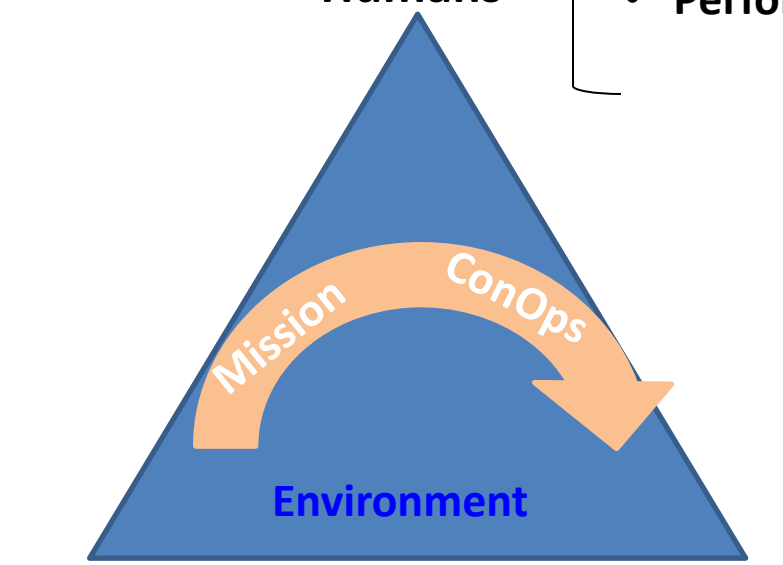
- Models specific end state scenarios, e.g., Loss of Crew (LOC) and Loss of Mission (LOM)
- Includes all failures that could result in end states:
  - Hardware
  - Software
  - Human Error & Medical Events
  - Common Cause
  - Phenomenological (MMOD, Tank Ruptures, etc.)
- Includes data uncertainty to estimate end state likelihood distribution
- Takes credit for shared capabilities across different vehicles / Programs

Hardware Reliability

- Models reliability for critical hardware that could impact end states
  - Does not account for mitigations that may prevent end states, such as aborts
- Includes hardware failures only
- Does not include data uncertainty (point estimate)
- Does not account for shared capabilities across different vehicles/Programs

PRA and hardware reliability assessment results cannot be directly compared. They are two analytical techniques that work together, not one or the other.

PRA and Human Systems Interface Relationship



- Health
- Performance

- Medical
- Human Factors
- Tasks
- Physiology
- Cognitive

Human Reliability

Based on Performance Shaping Factors, e.g.

- Working conditions
- Availability of procedures/plans
- Available time
- Training & Experience

PRA Limitations

- **PRA is not the answer to all questions. It has limitations, just as any model (for example engineering analysis of abort performance).**
  - It only captures the "known" (explicitly modeled) and "known-unknown" (captured as part of the uncertainty of the known risks) risks. PRA does not capture the "unknown-unknown" risks.
    - Limited to non-existent Program specific data, which results in extensive use of surrogate data.
      - Debate over the direct applicability of surrogate data to Human Spaceflight vehicle designs remains (NASA flight rates insufficient to gain design specific data).
    - "Unknown-unknown" and "underappreciated" risks are more prevalent with early flights because of lack of data about how the integrated system behaves in the integrated environment. This is evidenced in comparing PRA estimates to early Launch Vehicle failure rates.
      - Early flight risk assessments attempt to capture the impact of unknown-unknown risks to inform the risk-takers but are not incorporated into the PRA because the PRA is meant to inform risk decisions and it is impossible to provide insight into unknown risk.
  - It can not tell you what to change in a pump with a high failure probability. That requires reliability engineering and analysis to include material selection, test plan, manufacturing process, and design specifications.
  - PRA uses time and demands to determine failure probabilities, but it is not a dynamic change-of-state model (like a discrete event simulation).
    - However, dynamic models can serve as inputs to PRAs and conversely PRAs can be used to provide inputs to dynamic models.

Proposed Thoughts for Lunar Grid Development

- **Assuming solar arrays are planned for North Pole and all lunar surface ops are planned for South Pole, then some power transmission system is needed to get the generated power to the point of need. Correct?**
  - If so, then
    1. The solar array field needs to be built at the North Pole.
    2. Power needs to be stepped up at North Pole (transformers / switchyard), transmitted via "power lines" to South Pole, then stepped down via a switchyard for use.
    3. Post-construction maintenance plans at both poles, as well as along the transmission line(s)
    4. What experience do we have with transmitting power on the Moon and for that distance? Does our Earth-based systems experience apply to the Moon?
    5. Construction time? Level of effort? Equipment? Material? ConOps? Etc.
    6. Construction, operations, and maintenance by **robotics or astronauts**?
       a) Health, medical, and human reliability applies for crew / astronauts.
       b) Robotic hardware reliability applies for robotics as well as human operator reliability (auto vs manual).

Proposed Thoughts for Lunar Grid Development (Cont'd)

- **Alternative plan: build one or two small auxiliary nuclear plants (e.g. Radioisotope Thermoelectric Generators) at the South Pole to minimize power transmission needs, construction time, maintenance, distance covered, and maintenance / ops of remote solar arrays.**
  - If so, then
    1. Remove solar array field and transmission lines, then add RTGs at South Pole and any associated maintenance and ops needs.
    2. The rest is similar to the solar array field option.

- **PRA can be used to assess overall risk of both approaches ➔ Risk trade study**
  - Use PRA during their Conceptual, Design, and Operational phases.
  - Reliability assessment can be used to provide input to PRA and feedback into system design process
  - Failure data will be challenging due to environment concerns for both the hardware as well as the construction workers and operators.
  - How many Earth launches will be required to get material, hardware, and crew to Moon for both options.
  - Perform Human Reliability Analysis (HRA) using a consistent approach.
  - Determine what data and corresponding uncertainty is used in PRA.
  - Communicate the results of PRA used to support risk-informed decision-making (RIDM).

In Closing

- NASA sets Agency LOC thresholds, so programs can balance cost, schedule, and risk together and not overly constrain one at the expense of the other.
- Program LOC, LOM, and reliability requirements ensure LOC thresholds are met.
- PRA is used to verify LOC and LOM requirements and as part of the risk-informed design process.
- Reliability requirements are flowed to providers to enable the programs to meet LOC and LOM requirements.
- Providers utilize the reliability assessments to verify requirements and to inform their design.
- PRA and reliability analysis can be utilized in the development of the lunar grid development to help inform the design and to ensure crew safety as well as mission success.

Backup

LOC Definition & General Ground Rules

- **Loss of Crew (LOC) is the death or permanently debilitating injury to one or more "flight" crew members.**
  - Mission Duration: from crew ingress on the pad to crew egress post-landing on Earth.
  - LOC occurs when the complete loss of a critical vehicle system (e.g. Power, ECLSS, Propulsion, etc.) occurs. The exception is Gateway, who counts on Orion for evacuation.
  - LOC occurs when the crewed vehicle has a catastrophic failure, such as a critical MMOD hit, uncontrolled cabin fire, uncontained explosion, etc. and evacuation is assumed impossible.
  - JSC Human Health & Performance (HHP) also estimates medical risk based on the Integrated Medical Model (IMM).

LOM Definition & General Ground Rules

- **Loss of Mission (LOM) is the loss of or inability to complete significant / primary mission objectives, which includes Loss of Crew. Each mission is defined with different assumptions and mission objectives. Therefore, specific mission LOM assessments are accomplished evaluating attainment of specific mission objectives, using methods tailored to the specific mission risk drivers and each specific program but consistent with defined NASA Probabilistic Risk Assessment (PRA) standards (ESD 10002).**
  - Once the significant / primary mission objectives are complete (e.g. Post-lunar surface ops), then LOC is the only LOM risk contributor remaining prior to the safe return of crew post-landing on Earth.
  - Early termination is typically assumed to occur when only one more layer of redundancy remains before a LOC will occur.
  - An abort occurs due to a survivable initiating event that results in an early mission termination.
  - HHP's IMM also estimates the probability of an emergency medical return of one or more flight crew members.

What is Probabilistic Risk Assessment (PRA)?

- **PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes. It attempts to quantify rare event probabilities of failures. It attempts to take into account all possible events or influences that could reasonably affect the system or process being studied. It is inherently and philosophically a Bayesian methodology.**

- **In general, PRA is a process that seeks answers to three basic questions:**
  - What kinds of events or scenarios can occur (i.e., what can go wrong)?
  - What are the likelihoods and associated uncertainties of the events or scenarios?
  - What consequences could result from these events or scenarios (e.g., Loss of Crew (LOC) and Loss of Mission (LOM))?

- **The models are developed in "failure space"**
  - Fault trees are developed using failure criteria (e.g. what needs to fail in order to fail function/system)
  - Component failure rates/probabilities are used rather than component reliability

- **PRAs are often characterized by (but not limited to) event tree models, fault tree models, and simulation models**