Use of Preliminary PRA to Inform Decisions During Initial NASA Gateway Development

Teri Hamlin[a]
[a] NASA Johnson Space Center, Houston, USA, teri.l.hamlin@nasa.gov

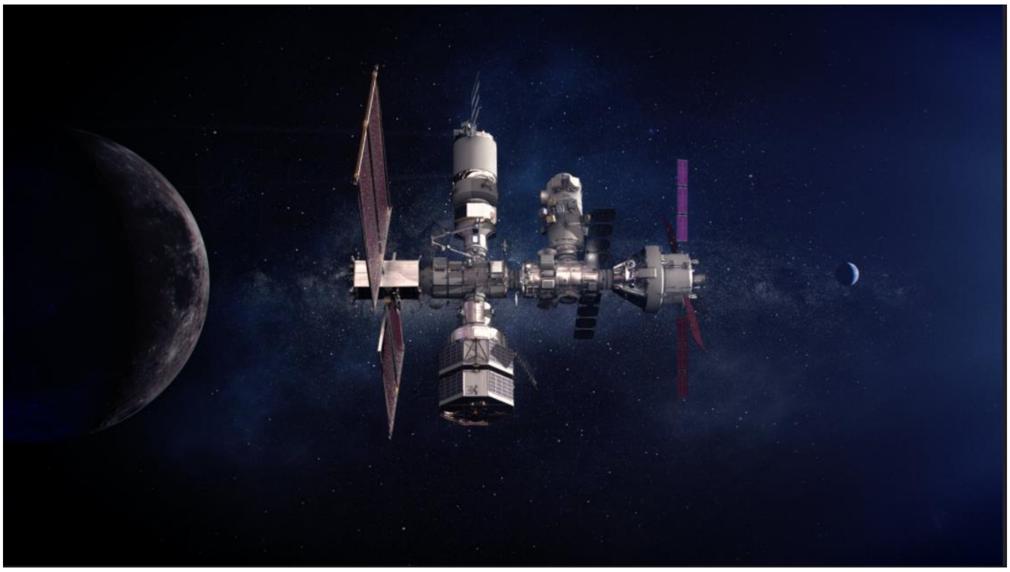
Abstract: How do you use Probabilistic Risk Assessment (PRA) to support a program in development before designs are even known? Traditional PRAs require detailed design information and early in a program life cycle such information is not available. National Aeronautics and Space Administration (NASA) Safety and Mission Assurance (SMA) developed a preliminary PRA for the Gateway Program based upon NASA reference designs utilizing data and models from previous PRA studies as surrogates for the Gateway systems. Gateway will be a lunar outpost that supports missions to the moon and includes several elements/modules developed by NASA and International Partners. NASA SMA began supporting Gateway in fall 2017 during initial formulation and continues to support the Gateway Program today. This paper will explore how the NASA SMA developed preliminary PRA was used to inform Gateway Program decisions with specific examples provided.

1. INTRODUCTION

How do you use Probabilistic Risk Assessment (PRA) to support a program in development before designs are even known? Traditional PRAs require detailed design information and early in a program life cycle such information is not available. National Aeronautics and Space Administration (NASA) Safety and Mission Assurance (SMA) developed a preliminary PRA for the Gateway Program based upon NASA reference designs utilizing data and models from previous PRA studies as surrogates for the Gateway systems.

Gateway will be a lunar outpost that supports missions to the moon and includes several elements/modules developed by NASA and International Partners. It is a critical component of NASA’s Artemis program. Figure 1 shows Gateway at assembly complete with the Human Landing System (HLS) and Orion vehicles docked. The assembly complete Gateway includes the Power and Propulsion Element (PPE), the Habitation and Logistics Outpost (HALO) module, the International Habitation (IHAB) module, the European Space Agency (ESA) System Providing Refuelling Infrastructure and Telecommunications Refuelling Module (ESPRIT-RM), the Deep Space Logistics (DSL) Module, the Robotic Arm, and the Airlock module. Gateway is intended to be uncrewed most its 15-year life.

Figure 1: Assembly Complete Gateway, Human Landing system and Orion [1]



NASA SMA began supporting Gateway in fall 2017 during initial formulation and continues to support the Gateway Program today. This paper will explore how the NASA SMA developed preliminary PRA was used to inform Gateway Program decisions on requirements and design options with specific examples provided.

The Gateway preliminary PRA is also used to compare against Loss of Crew (LOC) and Loss of Mission (LOM) requirements which will eventually be verified by the Gateway PRA. Although not discussed in this paper, the risk trade studies help ensure LOC and LOM requirements are met by helping identify areas to reduce risks.

2. Methodology

Early in the program formulation before contractors had been selected, NASA had developed reference designs for Gateway elements/modules. These NASA designs were based upon assigned functions, safety and design requirements and historical designs for similar systems. These NASA designs are replaced with the actual designs as the contractors are selected and their designs are matured.

The Gateway preliminary PRA is a high-level model that utilizes data and models from previous spacecraft PRAs such as those developed for the International Space Station (ISS) and Orion. Each Gateway module was broken down by critical system (e.g., Power, Thermal Control System (TCS), Avionics, etc.). In addition to the critical systems, which were mainly capturing functional loss, there were contributors associated with human error, software, fire, Micro-Meteoroid and Orbital Debris (MMOD), and tank rupture. The PRAs from previous programs were manipulated to represent the NASA designs. For example, if the ISS is two failure tolerant to loss of a system but Gateway only single failure tolerant the models were pruned to eliminate a leg of failure tolerance.

The Gateway preliminary PRA evaluates two end states, Loss of Crew (LOC) and Loss of Mission (LOM). LOC is evaluated for a crewed mission to Gateway and includes all credible, quantifiable events that result in death of or permanent debilitating injury to one or more crew members initiated by Gateway starting from crew entering the rendezvous sphere of Gateway to crew departure from the sphere. LOM is evaluated over a one-year period and includes all credible, quantifiable events that result in the loss of a defined major mission objective (as agreed to by the Gateway Program) initiated by Gateway such as LOC, Loss of Gateway, Inability to dock with a major element, etc. LOM is evaluated over one year because the expected crewed mission flight rate to Gateway is once a year.

Initiated by Gateway includes external events which result in Gateway failure (e.g., MMOD, radiation, etc.) and includes human error associated with operating Gateway but excludes events initiated by other programs such as Orion or HLS. Events initiated by other programs such as Orion or HLS are captured in the Orion or HLS LOC/LOM estimates (e.g., medical and docking events initiated by Orion).

3. Risk Trade Examples

The Gateway preliminary PRA has been utilized by the Gateway Program to inform decisions through numerous risk trades. Early in the program formulation it was used to help establish requirements and to evaluate design options. Several risk trades will be highlighted in this paper.

3.1. Micro-Meteoroid and Orbital Debris Requirement

Gateway is going to be positioned in a Near Rectilinear Halo Orbit (NRHO) around the moon. In orbit, Gateway is exposed to impacts from Meteoroids which could result in LOC or LOM. To mitigate this risk and to ensure a robust design, Gateway has a Probability of No Penetration (PNP) requirement similar to ISS. This requirement varies in magnitude depending upon the size and duration of exposure. This allows for larger permanent elements/modules to have higher overall risk than smaller temporary elements/modules but set a consistent requirement per square meter/year.

Initially the Gateway PNP requirement was modeled after the ISS visiting vehicle requirement which utilizes the following equation:

$$PNP = 0.99998^{A*T} \tag{1}$$

Where A equals the critical surface area in square meters and T equals the exposed time in years. The equation sets the requirement value which is then verified by MMOD analysis. The verification is successful when the results of the MMOD analysis meets or exceeds the calculated requirement value.

Many of the Gateway initial requirements were based upon ISS requirements because of the similarities between the two vehicles. Based on the initial size of Gateway during formulation, the ISS visiting vehicle requirement was used rather than the ISS permanent module requirement because Gateway was planned to be smaller than ISS and therefore could accept a higher risk per element/module. However, Gateway grew, and preliminary MMOD risk estimates showed significant margin to the requirement. For this reason, the requirement was re-visited.

The preliminary PRA was utilized to evaluate changing the above requirement to be consistent with the ISS permanent module equation:

$$PNP = 0.99999^{A*T} \tag{2}$$

This change resulted in decreasing MMOD LOC and LOM by ~50%, overall Gateway LOC by 21% and overall Gateway LOM by ~8.3% as shown in Table 1.

Table 1: Gateway Risk Reduction with Updated MMOD Requirement

	MMOD % Change	**Gateway % Change**
LOC (30 days)	**50% decrease**	**21% decrease**
LOM (1 year)	**50% decrease**	**8.3% decrease**

This risk trade was brought forward to the Gateway Program and the MMOD requirement was changed.

3.2. Habitable Volume Valves Remote Isolation Capability

All crewed spacecraft have valves which connect the internal pressurized habitable volume to the vacuum of space. For example, Positive Pressure Relief Valves (PPRVs) provide protection in the event of an overpressure event and Vent Valves are nominally used to vent overboard. However, these valves provide potential leakage paths which could exceed the capability of the pressure control system and result in Gateway depressurization. For a crew tended vehicle such as ISS, caps can be installed by the crew in the event of such leaks. However, because Gateway is uncrewed most of the year, caps would only mitigate a fraction of the risk.

In the early NASA designs it was not clear whether there would be a capability to isolate these valves remotely. There was no requirement to provide a remote isolation capability although there is a general requirement for fault isolation and recovery. The Gateway preliminary PRA model was utilized to show the importance of having remote isolation capability because without it risk of Gateway depressurization would have been a top LOM risk driver. It was shown that the risk per PPRV is reduced by ~99% with this capability.

3.3. Thermal Control System Cross Strap Capability

Initial concepts for the Gateway Modules' Thermal Control Systems (TCS) were independent of each other (i.e., no capability to connect the cooling loops between two modules). There was no requirement to be able to cross-strap between two modules. Loss of TCS was a top LOM risk contributor to overall Gateway LOM.

In order to inform design decisions, the Gateway PRA team worked with engineering to evaluate six TCS configurations. The first three configurations included 1) dual external and internal cooling loops (referred to as "dual") with no cross strapping, 2) fluid exchange cross strapping and 3) heat exchanger (Hx) cross strapping shown in Figure 2. The Interface Hx (IFHX) shown in the figure is where the internal and external loops interface. The second three configurations included 1) dual external and single internal cooling loops (referred to as "dual/single") with no cross strapping, 2) fluid exchange cross strapping and 3) heat exchanger cross strapping shown in Figure 3. Cross-strapping the internal loops allow for the internal loops to utilize heat rejection capability of the other module in the event of a dual external loop failure. The fluid exchange cross-strapping physically connects the two module internal loops together such that they are exchanging fluid between the two modules potentially mitigating failures of the internal pumps as well as external loop failures. The heat exchanger cross-strap maintains the separation of the internal loops connecting the two through a heat exchanger mitigating only external loop failures. In addition, the heat exchanger adds a potential leakage path for the module for which it resides.

Figure 2: Dual External and Internal Loops (Dual)

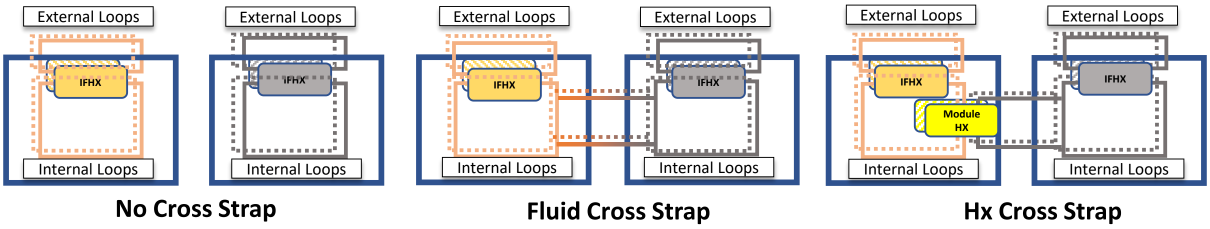


Figure 3: Dual External and Single Internal (Dual/Single)

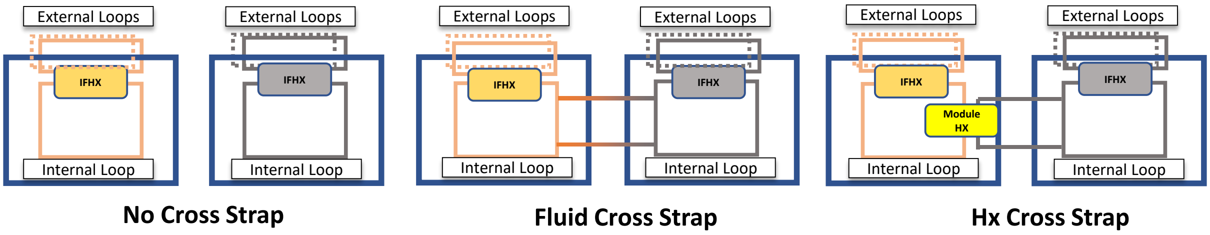


Table 2 summarizes LOM results for all six configurations. In this risk trade, the dual no cross-strap was considered the baseline case for which the percentage change was calculated.

Table 2: Summary of LOM Results for TCS Configurations

	Gateway TCS LOM % Change	**Gateway LOM % Change**
No Cross- Strap (Dual)	N/A	N/A
Dual Fluid Cross Strap (Parallel)	**51% decrease**	**3.5% decrease**
Dual Hx Cross Strap	**34% decrease**	**2.4% decrease**
No Cross Strap (Dual/Single)	**100% increase**	**7% increase**
Dual/Single Fluid Cross Strap (Parallel)	**24% decrease**	**1.6% decrease**
Dual/Single Hx Cross Strap	**71% increase**	**5% increase**

Although dual fluid exchange cross strapping provided the biggest risk reduction, the dual Hx cross strap option was selected for implementation. This is because the fluid exchange cross strapping would have been more difficult to implement.

Follow up risk trades were performed with detailed modeling of each of the modules designs as the heat exchanger cross strapping requirements were defined.

4.0. LOC/LOM Trending and Mission Duration

The Gateway PRA supports the Gateway Program Integrated Analysis Cycles (IACs) and trending those assessments provides insight into how risk estimates have changed since initial formulation. Some changes are the result of changing the the Gateway architecture (e.g. eliminating a module or a capability), some are the result of design maturity (e.g. replacing surrogate models with detailed models of provider designs), and some may be the result of data maturity (e.g. availability of operational data). Figures 4 and 5 provide a normalized look at the Gateway LOC and LOM estimates over time. Each has been normalized by the original upper scale value that was presented to the Gateway Program in order to maintain the shape of the graphs.

Mission duration is a major factor in LOC/LOM assessments. It is fairly intuitive that the longer a mission, the higher the likelihood something can go wrong. For Gateway, which is uncrewed most of the year, a longer crewed mission increases LOC risk but could mean lower LOM risk over the year due to increased capability to perform corrective maintenance while the crew is present. For this reason, as well as the general uncertainty associated with projected mission durations, the Gateway PRA team started evaluating 60 and 90 day missions to Gateway along with the baseline of 30 days. Normalized values for those estimates are also provided in Figures 4 and 5.

Figure 4: Gateway LOC Trend

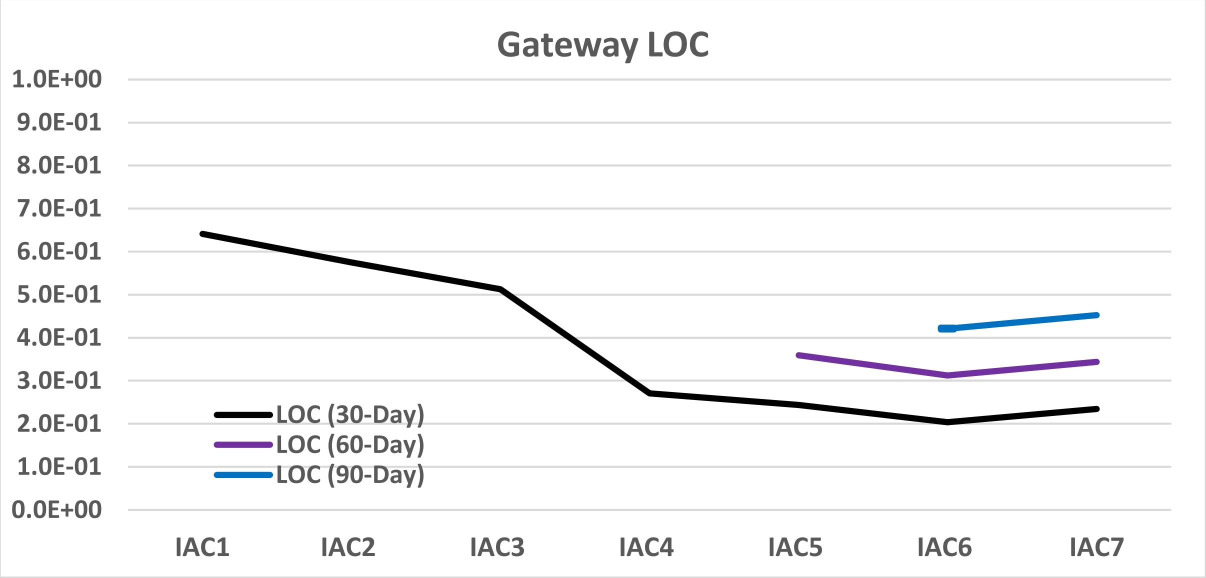
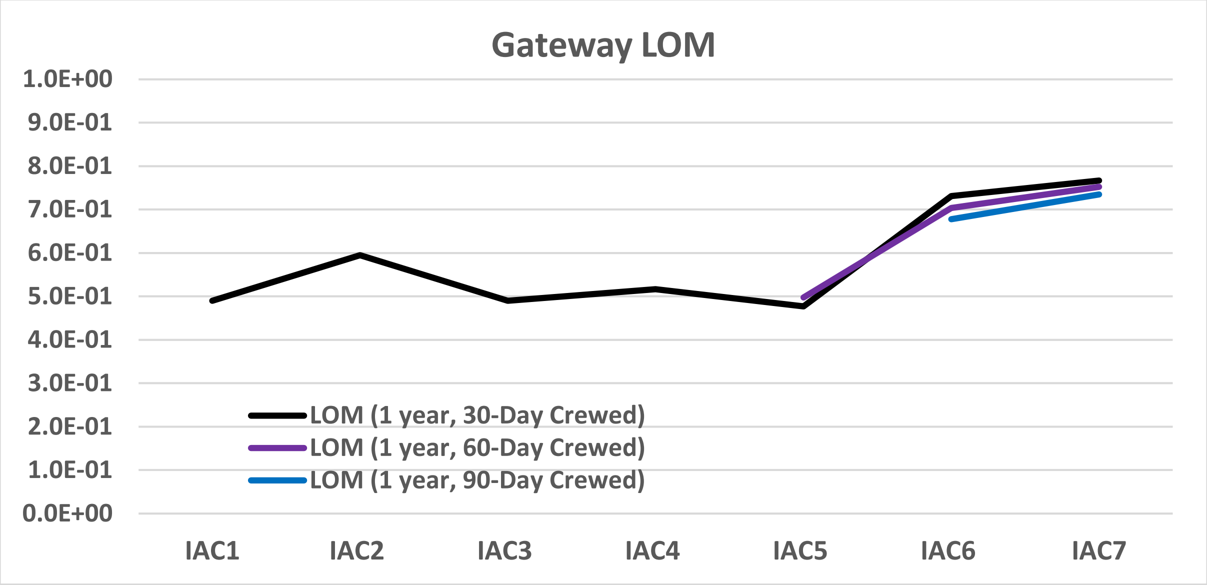


Figure 5: Gateway LOM Trend



The large change in LOM estimates between IAC 5 and IAC 6 was mainly the result of eliminating a mitigation capability from the model which was not being developed by the Gateway program. There were Gateway requirements to develop the capability, but no capability existed and no funding was available to create the capability. Therefore, IAC 6 and subsequent updates more correctly reflect the Gateway risk all along and is not the result of a particular Gateway decision.

5. CONCLUSION

The Gateway Program has utilized a preliminary PRA built from previous spacecraft PRAs to inform decisions on requirements and design options. The MMOD and habitable volume valves remote isolation risk trades are examples of how the preliminary PRA was used to inform design requirements. The TCS risk trade is an example of how the preliminary PRA was used to inform design options. This preliminary PRA is being replaced over time with detailed modeling using more traditional PRA techniques as designs become more mature. Trending has shown how the Gateway LOC and LOM estimates have changed over time and the impact of mission duration changes.

Acknowledgements

The author would like to thank the Gateway Program for supporting PRA and using it to inform decisions.

References

[1] A. Bertolin, jsc2021e047255, https://www.flickr.com/photos/nasa2explore/51670491734/in/photolist-2mHWM29