QUO VADIS PAYLOAD SAFETY?

Michael P. Fodroci(1)**, MaryBeth Schwartz**(2)

(1)*NASA, 2101 NASA Parkway, Mail Code NE, Houston, TX, USA 77058, Email: Michael.Fodroci-1@Nasa.gov*
(2)*NASA, 2101 NASA Parkway, Mail Code NE, Houston, TX, USA 77058, Email: Mary.B.Schwartz@Nasa.gov*

ABSTRACT

As we complete the preparations for the fourth Hubble Space Telescope (HST) servicing mission, we note an anniversary approaching: it was 30 years ago in July that the first HST payload safety review panel meeting was held. This, in turn, was just over a year after the very first payload safety review, a Phase 0 review for the Tracking and Data Relay Satellite and its Inertial Upper Stage, held in June of 1977.

In adapting a process that had been used in the review and certification of earlier Skylab payloads, National Aeronautics and Space Administration (NASA) engineers sought to preserve the lessons learned in the development of technical payload safety requirements, while creating a new process that would serve the very different needs of the new space shuttle program. Their success in this undertaking is substantiated by the fact that this process and these requirements have proven to be remarkably robust, flexible, and adaptable. Furthermore, the payload safety process has, to date, served us well in the critical mission of safeguarding our astronauts, cosmonauts, and spaceflight participants. Both the technical requirements and their interpretation, as well as the associated process requirements have grown, evolved, been streamlined, and have been adapted to fit multiple programs, including the International Space Station (ISS) program, the Shuttle/Mir program, and most recently the United States Constellation program.

From its earliest days, it was anticipated that the payload safety process would be international in scope, and so it has been. European Space Agency (ESA), Japan Aerospace Exploration Agency (JAXA), German Space Agency (DLR), Canadian Space Agency (CSA), Russian Space Agency (RSA), and many additional countries have flown payloads on both the space shuttle and on the ISS. Our close cooperation and long-term working relationships have culminated in the franchising of the payload safety review process itself to our partners in ESA, which in turn will serve as a roadmap for extending the franchise to other Partners.

But what may we say then, about the future of payload safety? Where are we going? While its heyday may indeed be yet to come, with three large laboratories now up and running on board the ISS, beyond that, the future holds both great opportunities, and even greater challenges. As we move beyond Earth orbit, constraints on upmass will begin to impact the way we select payloads for flight, as well as the way in which we design them. Current projections for the Altair Lunar Lander indicate that only 500 kg will be reserved for cargo to the lunar surface, and only 150 kg for return, with only two missions planned per year. Further, it should be recognized that out of this small amount, some mass will need to be dedicated to payload secondary structure, so the actual mass to and from the lunar surface will be even less. When compared to the approximately 25,000 kg of payload upmass that can be accommodated by the space shuttle (with an average of four flights per year), it is clear that opportunities for flying payloads beyond Earth orbit will be extremely limited. It is also clear that manifest trades will become absolutely critical, as every kilogram of payload cargo will be displacing critically needed consumables and equipment. We presume that strict criteria for scientific merit will be invoked to assure that only the most significant experimentation is performed.

And while two-fault tolerance has long been the hallmark of the NASA payload safety program, mass constraints may force a rethinking of basic fault tolerance requirements, just as the design of the Altair vehicle itself is, in many cases, zero-fault tolerant and has adopted a risk informed design philosophy across the board. Such an approach may well be required for all payloads destined for the lunar surface.

Finally, everything we take to the moon must work. There is no such thing as a category D payload, or a piece of Criticality 3 hardware. A fifty-kilogram payload on the surface of the moon that fails to function represents ten percent of the total lunar cargo downmass that could have been used to transport oxygen, or critical repair parts, or another payload that would have functioned properly. Reliability requirements may well find their place alongside safety requirements in the effort to assure that every device we take to the lunar surface is able to perform its intended function.

Understanding the origin and the evolution of payload safety technical requirements as well as the payload safety process, can help guide our understanding of how they may evolve in the future, as they are once again adapted to meet the needs of a very different program:

payload safety in transit between the Earth and the Moon, on lunar sortie missions, and as a part of a program of investigation and experimentation in a lunar outpost.

1. ORIGINS

In June of 1977, the Payload Safety Review Panel (PSRP) convened for the first time to review the hazards associated with a Space Shuttle payload. The payload in question was the Inertial Upper Stage/Tracking and Data Relay Satellite (IUS/TDRS). The task before them was formidable. The IUS was a large two stage solid fuel upper stage, which would be used to propel the TDRS satellite from low earth orbit to its final geosynchronous operational altitude. The TDRS itself used a hydrazine propellant system for attitude control. The entire IUS/TDRS stack would have to be erected and then deployed from the payload bay of the Space Shuttle orbiter. The first stage would then need to be ignited, while still no more than a few miles from the orbiter. The technical requirements used in the review still existed only as a "white paper" ("Initial Issue of Safety Policy and Requirements for Payloads Using the Space Transportation System", dated June 16, 1976.) No detailed process requirements were yet officially documented. But this was the beginning of a process that resulted in the safe and successful flight of five TDRS satellites on the space shuttle, and countless other payloads in 125 different space shuttle missions, ten years of ISS operations, and seven Increments on the Russian *Mir* space station. It did not spring into being fully formed on that day in 1977, and it would change significantly over the years, but by understanding the origins of that process, and by studying how it has changed, we can prepare ourselves to deal with some of the challenges that lie ahead, in assuring the safety of payload activities that we pursue beyond earth orbit.

The roots of Payload Safety as we know it today can be traced back to the National Aeronautics and Space Administration (NASA) Skylab program (1973-74). The Skylab space station hosted three crews, who performed a variety of experiments, during a total of 178 days on-orbit. NASA and its SR&QA contractor (Boeing) established a small team of Skylab experiment safety engineers, who traveled to the development centers for each experiment, and supported every experiment design review with the sole purpose of assuring the safety of these experiments. There were no documented payload/experiment safety requirements; they just depended on these senior safety engineers to assure that hazards associated with Skylab payload operations were properly identified and controlled.

With the conclusion of the Skylab Program, and the advent of the Space Shuttle, this team of engineers (most notably Robert (Bobby) Miller from NASA, and William (Bill) Powell and James (Jim) Mello from Boeing) turned their attention to the question of assuring the safety of Space Shuttle payloads. They knew that the approach they had used during Skylab was impractical – Skylab had a defined ending date, and a known, finite number of experiments, all of which would be flown within less than a two year period. The Shuttle Program, however, was open-ended, with a vastly greater scope – far more payloads, far more hazards, a much wider variety of potential experiments, and an international customer base. It was clear that their traveling team of safety engineers could not support such a program – the travel requirements alone would exceed any reasonable expectations for funding. Instead, a centralized panel would review all payloads from a single location, and payload organizations would travel to the Johnson Space Center in support of their safety reviews. Thus was born the concept of the Payload Safety Review Panel – A group of technical experts, led by a Chairman from the Program Office, who would review all Shuttle payloads for safety. The idea of a phased approach to safety reviews followed naturally, because the developers of the process tended to think in terms of supporting design reviews. From these two concepts came JSC 13830 "Implementation Procedure for STS System Safety Requirements", dated May 1979 – the first document defining the process for first delivering the data necessary to support payload safety reviews, and then conducting payload safety reviews. In parallel, the team was also developing the safety policy and technical requirements for payloads. Since they knew that it was not feasible to impose NASA quality and reliability standards on the paying customers of the Shuttle, they decided to adopt a strict policy of defense in depth (fault tolerance), plus design to minimum risk, where fault tolerance was infeasible. The initial thrust of the early requirements was directed at upper stages such as the IUS, the Centaur, and the PAM (Payload Assist Module), and at the first major Shuttle-launched satellites – the Hughes 376, the TDRS, and the interplanetary missions such as Magellan, Galileo, and Ulysses, with much attention focused on such things as rotation of safe and arm devices, monitoring of inhibits, and the opening of propellant isolation valves.

2. EVOLUTION

The first version of the NHB 1700.7 was released in May of 1979. A revision followed quickly (December of '80), then again in January of '89. The ISS Addendum was released in December of '95. Payload safety requirements have been adapted for many uses – for the Shuttle/Mir Program, as the starting point for the Space Station Safety requirements, and as the basis for NASA Government Furnished Equipment (GFE) safety requirements. They have been revised, improved, clarified, interpreted, streamlined, and sometimes deleted. In general, the PSRP has consistently worked to streamline the payload safety review process as well as the technical requirements both to create efficiencies for the customers of the process (the payload organizations), and to allow the panel to focus on the most significant hazards for a given payload.

2.1. Interpretation

The guiding philosophy behind the development of payload safety technical requirements has always been to leave payload organizations as free as possible to design their payloads as they wished, without unnecessary constraint. This proved to be a less than satisfactory approach, and resulted in what we at NASA often refer to as the "Bring me a rock" syndrome, where a payload organization would repeatedly present designs to the PSRP, only to be told that the designs were unacceptable. A good example of this is associated with the selection of circuit protection devices. Designers naturally wanted to protect wires from overcurrents, but tended to want to err on the side of sizing such devices larger rather than smaller, to prevent loss of function in the event of a current spike. The PSRP, on the other hand, wanted to err on the side of caution, and protect the space shuttle from a potential fire by requiring circuit protection devices to be sized smaller. This resulted in much frustration, until the PSRP finally issued NSTS 18798, "Interpretations of NSTS Payload Safety Requirements". Where requirements were open-ended or ambiguous, the Interpretations document provided guidance and clarification. The document is actually a collection of formal letters and memoranda documenting panel positions on a wide variety of requirements, which had often been in use by the PSRP internally for years before eventual dissemination to the payload community. Interpretations continue to be promulgated, updated, and refined to this day.

2.2. Streamlining

In 1995, the PSRP began an effort to evaluate whether payload safety reviews could be streamlined, so as to spend less time on some (presumably less hazardous) payloads, while allowing the panel to spend more time focusing on unique and significant hazards. This effort gave rise to the development of the Form 1230, "Flight Payload Standardized Hazard Report," often referred to as the Payload Hazard Report EZ. This effort was also accompanied by an attempt to reduce the number of reviews held to assess the safety of a payload. Up until that time, all payloads went through four reviews, starting with Phase 0 and proceeding through Phase III, although reviews were sometimes combined together (e.g., a combined Phase I and II safety review.) This further reduced workload on both the PSRP and on the payload community, and allowed even more focus on truly hazardous payloads. In addition, an effort was begun to approve hazard reports outside of the formal panel meetings, resulting in even more time savings. In support of these efforts, the panel created three categories of payloads: Basic, Intermediate, and Complex, to allow discrimination between simple, non-hazardous flight articles, and larger, more complex and hazardous payloads. In general, the initial thought was that hazard reports would be required only for those payload hazards that were unique, that is, hazards with controls and verifications that are not generic in nature. In other words, if all of your hazards were generic, you could fill out the Form 1230, have one review, and be done. Unique hazards would require additional reviews, up to the full complement of three or more phased safety reviews. While these categories have undergone some modification over the years, they remain essentially the same, and today are defined as follows:

2.2.1. Basic Payloads

- All identified hazards and their hazard controls are "standard" as specified on JSC Form 1230 "Flight Payload Standardized Hazard Control Report"
- No unique hazards / hazard reports (HR)
- Usually an informal Out-of-board review by PSRP Chairman

2.2.2. Intermediate Payloads

- In addition to the Form 1230 standard hazards, the payload has unique hazards and requires unique HR's
- Unique hazards have proven and/or passive controls and standard verification methods
- One or two formal safety reviews with the PRSP
- Typically one face-to-face and one via telecon

2.2.3. Complex Payloads

- In addition to the Form 1230 standard hazards and unique passively controlled hazards, the payload also has unique hazards with active controls/must work functions, operational hazard controls; or passive hazards with non-standard control and verification methods
- Three or more formal safety reviews with the PSRP
- Typically face-to-face reviews, but telecons may be held after the first review if appropriate
- Splinter and/or Working Group meetings with technical support may be required before and during reviews to discuss major issues

Coincidentally, at about this same time, a similar effort was underway to develop a scheme for categorizing cargo that would be carried up by the Shuttle to the Russian Mir space station. RSA/Boris Sotnikov, working with NASA/Gary W. Johnson and others to develop a proposal for dividing all cargo into two categories. In a similar fashion to that described above, Category1 items would be those with no hazards, controls and verifications other than those listed in what is now the JF 907 checklist. Category 1 items would be certified by the providing organization only, with an information copy provided to the other partner. Any items with unique, non-generic hazards would require the submittal of hazard reports, and the hazard reports and the associated certification would require approval by both partners. This process too, is still in use today.

2.3. ISS Addendum

The payload requirements established in NSTS 1700.7, Safety Policy and Requirements for Payloads Using the Space Transportation System preceded the development of the ISS. As the ISS was beginning to prepare for utilization of the orbiting laboratory, there was a need to provide payload developers the appropriate safety requirements. In January 1989, an addendum to NSTS 1700.7 was developed to expand and modify existing Space Shuttle payload requirements for ISS applicability. The addendum included labeling of each paragraph to relate the applicability compared to Space Shuttle payload requirements. This approach prevented duplication of payload requirements documents and enabled the addendum to address ISS unique requirements. NSTS 1700.7 and the ISS addendum together provide requirements that enable development of safe payloads for STS transportation phases, Space Shuttle operations, and ISS on-orbit operations. Additionally, the addendum approach leveraged payload organizations' familiarity with STS requirements. With the impending retirement of the Space Shuttle, the requirements are planned to be restructured to eliminate the Space Shuttle addendum approach.

So it can be seen that over the years, there have been many efforts made to improve the efficiency and effectiveness of the payload safety process. These efforts have been primarily in three areas: providing clarification and interpretations of technical requirements, reducing or combining the number of safety reviews required, and reducing the number of hazard reports required for submittal. Another significant step is currently in work: The effort to "Franchise" the payload safety process, whereby the authority to conduct safety reviews is ceded to international partners. This will be discussed in greater detail later.

3. THE PRESENT

Dividing the Shuttle program history into three distinct phases allows us to recognize how payload priorities and risk posture has changed over the years. The first phase occurred prior to the Challenger accident. During this phase, capability was proved and we rapidly moved into complex scientific accomplishments. The Shuttle era of space exploration began in April 1981 with Columbia's first voyage into space. The Shuttle's first scientific payload was flown aboard the same vehicle just seven months later. The payload consisted of remote sensing instruments which provided an evaluation of Earth resources, environment quality and weather conditions. As our experience grew, so did the complexity of payloads. During June 1983, Shuttle Pallet Satellite (SPAS-l) built by Messerschmitt-Bolkow-Blohm, a German aerospace firm, flew beside and above the Shuttle for several hours recording images of various orbiter maneuvers. In 1984, the first capture, repair and redeploy of a malfunctioning satellite was successfully accomplished. The EVA crewmember flew to the satellite using the Manned Maneuvering Unit (MMU) and attempted to capture it with the Trunnion Pin Acquisition Device (TPAD). After three attempts, the satellite began to tumble and the effort was halted. Eventually, ground controllers were able to stabilize the tumbling action providing a second opportunity the following day to grapple the satellite with the Shuttle Remote Manipulator System SRMS. It was successful, and resulted in the first repair mission of an orbiting satellite; the Solar Maximum Mission (Solar Max) satellite launched 4 years earlier.

Following the Challenger accident, President Reagan directed that the shuttle cease carrying commercial satellite payloads and expendable launch vehicles to be greater utilized for placing satellites into space. Additionally, payload requirements were revised to reflect the increased safety awareness brought about by the Challenger accident.

During the post Challenger era although there was an increased safety and risk awareness, some very complex and challenging missions were conducted. For example, in 1989 the Galileo Planetary mission included an orbiting spacecraft launched into the inner solar system from the Shuttle using an inertial upper stage rocket. To achieve the power needs, solar panels 65 m^2 in size would have been required along with unacceptably massive batteries. As a result, the payload utilized two radioisotope thermoelectric generators which powered the payload through the radioactive decay of plutonium-238. The heat emitted by this decay was converted into electricity providing a reliable and long-lasting source of electricity unaffected by the cold space environment and high radiation fields. More than 100 scientists from the United States, Great Britain, Germany, France, Canada and Sweden conducted Galileo experiments. As commitments prior to the Challenger accident were completed, the focus shifted toward development of a space station. In June 1995, the third mission of the US/Russian Shuttle-MIR

Program, the Shuttle docked to the MIR creating the largest spacecraft ever in orbit. By December 1998, building of the International Space Station was underway with the attachment of Node 1 to the orbiting Functional Cargo Block (FGB.)

After the Columbia accident, President Bush called for the retirement of the space shuttle after completion of the International Space Station. As the ISS nears completion, the payload focus has moved to ISS utilization. At completion, the ISS is slated to have five laboratories, the US Destiny, the European Columbus, and Japanese Kibo, the Russian Multipurpose Laboratory Module and Mini-Research Module 2.

3.1. Franchising, the Challenge of Consistency

The PSRP franchising effort initiated in June 2002 will facilitate the increasing volume of payload reviews required with the presence of five orbiting laboratories. One challenge the franchised panels face is maintaining consistency with requirement implementation and interpretations. Charters and Memorandums of Agreement have been established which outline planned process audits and joint safety reviews. Relationships between panel experts have been established to help provide consistency across the panels. With more laboratories to conduct science and increased partner vehicle traffic to the ISS, franchising complexity increases. Open communication between the panels, safety engineers and topic experts will be the cornerstone of maintaining consistent safety assessments. The ability to understand and implement lessons learned from one another will be of utmost importance in an ever growing busy environment. Close attention to the details is extremely important; knowing who is responsible for the equipment configuration and understanding what, if any changes, have been implemented. Identifying all features that may present hazards when incorporated in the ISS environment and assuring that all relevant parties have a common understanding must be accomplished to maintain a safe ISS. The implementation of franchised safety reviews will truly present challenges that, when safely accomplished, will be a great achievement.

4. THE FUTURE

The future of payload safety will see an extreme path bifurcation. Payloads destined for the ISS will continue to enjoy a wealth of available space, upmass, electrical power, and many different opportunities for transport, with up to seven possible transport vehicles, even after the retirement of the Shuttle (Soyuz, Progress, ATV, HTV, Orion, Dragon, and Cygnus.) There is every expectation that the efforts that have characterized payload safety to date, i.e., efforts to continuously search for efficiencies and cost-saving measures, will continue, and that the worldwide payload community will reap the benefits of these activities in reduced costs. Efforts to franchise the process will continue, as well as efforts to streamline and ensure consistency in the approach to mutual multilateral certification. The ISS will no doubt prove to be a space laboratory of great effectiveness, with many, many users throughout the world.

But what about payload operations beyond the ISS? What about payloads operated on the surface of the moon, or en route to the moon? It is safe to say, even from this distant vantage point, that payload operations on the lunar surface and payload safety in particular, will look very different indeed, and for one simple reason: severe limitations on down mass to the lunar surface. Although the Altair Project is still in its infancy, current projections indicate that there will be two manned missions to the lunar surface per year, with 500 kg allocated for payload mass per mission. This is actually a total figure, and out of this must be subtracted mass for structural supports, containers, foam, etc., so that the actual payload mass to the lunar surface will be somewhat less. Two additional unmanned, “cargo-only” flights, capable of delivering 14.5 metric tons to the lunar surface may also be conducted, although there are no figures available on the amount of that mass which will be made available to payload activities. Experience tells us however, that this number will be highly variable, and also highly dependent on the immediate needs of the lunar surface outpost for consumables, spares, replacement parts, and new equipment critical to the functioning of the outpost. This severe limitation on mass and space (payload volume) has many implications:

4.1. Scientific Merit

Only the most productive, meaningful, and scientifically desirable experiments will be flown to the lunar surface. While today each partner in the ISS has their own methods for evaluating scientific merit, it is a sure bet that this process will become far more stringent when applied to lunar surface payloads.

4.2. Reliability

Payload requirements for reliability in the Shuttle and the ISS Programs have typically been left entirely to the discretion of the payload owner, with predictable results: some payloads have performed reliably and well; others have failed almost upon reaching orbit. This will have to change. We will not be able to afford to take anything to the moon that is not designed to provide the maximum chance of successful operation. Everything we take to the moon must work. A fifty-kilogram payload that fails on the lunar surface has just displaced fifty kilograms of air, food, water, or desperately needed spares. Discussions with the Altair Project Manager Laurie Hansen confirm that a set of reliability requirements aimed at payloads, and documenting the need for the appropriate design philosophies, analysis requirements, parts selection procedures, etc. is highly likely. This in turn will necessitate a set of reviews aimed at assuring compliance with these requirements, well beyond the scope of current payload safety reviews.

4.3. Safety Requirements Philosophy

Ultimately, the severe constraints on mass for lunar payloads may even impact the philosophy for assuring the safety of lunar payloads. During the Shuttle/ISS era, we have depended on a philosophy of defense in depth (fault tolerance) as well as design to minimum risk (materials selection, factors of safety on structures and pressure vessels, etc.) to assure the safety of payloads. This too, may have to change. In the Altair Project today, the vehicle design was stripped down to only those functions absolutely required to perform the mission of the vehicle. Redundancy was then added back in on a case-by-case basis, evaluating complex trades among functionality, safety, reliability, and mass for each vehicle function under consideration. Single fault tolerance has been achieved for most cases; zero fault tolerance is still present in some cases, offset by dependence on extreme reliability.

For payloads, requirements for factors of safety in structures and pressure vessels will almost certainly have to be revisited. But what about fault tolerance? Adding redundancy adds weight, and in some cases reduces reliability. Will we retreat to single fault tolerance, given extensive insight into inherent reliability? Or will we, perhaps, adopt an approach of picking risk “targets” as is currently done in the Constellation Program in lieu of prescriptive requirements for fault tolerance?

The adoption of such an approach would come with a significant price tag. First, risk targets (i.e., probability of causing Loss of Crew of no greater than 1-in-100,000, for example) would have to be allocated to each payload. Then trade studies would have to be conducted to determine the most effective and least costly (in terms of mass) means of achieving that target. Then analyses and tests would have to be performed to verify that requirements had been met. Designs might ultimately consist of a mixture of two-fault tolerance, design to minimum risk, and high reliability. Arguments for reliability in lieu of fault tolerance would need to be supported by detailed analysis, and would require extensive review, all of which points to a lengthy and expensive process.

4.4. Commonality and Interoperability

While it may never be ensconced in formal requirements, the desire for common parts in a mass-constrained environment cannot be overstated. On the ISS, when the Elektron vacuum vent valve became contaminated, the Russians were able to re-plumb the Elektron vacuum line to the vent valve for the Harmful Contaminants Filter, which was identical. This practical and robust approach simultaneously simplifies sparing logistics, and creates options for recovery in the event of a parts failure.

5. SUMMARY

In adapting a process that had been used in the review and certification of earlier Skylab payloads, NASA engineers sought to preserve the lessons they had learned in the development of technical payload safety requirements, while creating a new process that would serve the very different needs of the new Space Shuttle program. Their success in this undertaking is attested to by the fact that this process and these requirements have proven to be remarkably robust, flexible, and adaptable. Furthermore, the payload safety process has, to date, served us well in the critical mission of safeguarding our astronauts, cosmonauts, and spaceflight participants. Both the technical requirements and their interpretations, as well as the associated process requirements have grown, evolved, been streamlined, and have been adapted to fit multiple programs, including the International Space Station program, the Shuttle/Mir program, and most recently the US Constellation program.

Understanding the origin and the evolution of payload safety technical requirements as well as the payload safety process, can help guide our understanding of how they may evolve in the future, as they are once again adapted to meet the needs of a very different program: payload safety in transit between the Earth and the Moon, on lunar sortie missions, and as a part of a program of investigation and experimentation in a lunar outpost.

Quo Vadis Payload Safety?

IAASS Conference

Rome, 2008

MaryBeth Schwartz and Michael Fodroci

Quo Vadis Payload Safety?

- **Agenda**
  - **Introduction**
  - **Origins**
  - **Evolution**
  - **The Present**
  - **The Future**
  - **Summary/Conclusions**

Quo Vadis Payload Safety?

- **Introduction**
  - **Thirty Years of Payload Safety**
  - **The Road We’ve Traveled**
  - **The Road Ahead**

Quo Vadis Payload Safety?

- **Origins**
  - **Skylab**
  - **The Space Shuttle**
  - **The Technical Requirements**
  - **The Process**

Quo Vadis Payload Safety?

- **Evolution**
  - **Interpretations**
  - **Streamlining/Combining Reviews**
  - **Basic, Intermediate, and Complex**
  - **Category 1 & 2 – The Shuttle/Mir Program**
  - **The ISS Addendum**

Quo Vadis Payload Safety?

- **The Present**
  - **The Shuttle**
  - **The International Space Station**
  - **Franchising, and the Challenge of Consistency**
  - **Export Control**
  - **The End of the Shuttle Program**

Quo Vadis Payload Safety?

- **The Future – Two Paths**
  - **The International Space Station**
  - **Lunar Missions**
    - **Scientific Merit**
    - **Reliability**
    - **Fault Tolerance and Factors of Safety in a Mass Constrained Environment**
    - **Safety “Targets” vs. Fault Tolerance**
    - **Commonality and Interoperability**

Quo Vadis Payload Safety?

- **Summary/Conclusions**