Quick Start Guide to Payload Design

PAYLOAD SAFETY OVERVIEW

March 2, 2022

Payload Safety Overview

Don't try this at home

Safety Reviews are required for all spaceflight hardware going to the ISS, including payload, science, equipment and commercial. These reviews span all aspects of the payload's development and performance. Reviews consider the design, operations, functional capabilities of the payload's flight hardware and the associated ground support equipment a payload needs throughout its entire lifecycle.

There are four levels, or phases, of Safety Reviews aligned to the design maturity of the payload.

The payload will need to meet safety requirements associated with each stage.

- Phase 0: Safety Technical Interchange Meeting (TIM)
- Phase I: Safety Review for payload's Preliminary Design
- Phase II: Safety Review for payload's Critical Design
- Phase III: Safety Review for payload's Final Acceptance

Documentation of a payload's potential hazards and controls matures over the course of these reviews, ending with verifications for all controls. The Safety Review phases act as milestones and gates for payloads along the path to ISS.

The ISS Safety Team provides safety oversight, guidance and review during the phased Safety Review process. Much of the team's time is dedicated to ensuring successful and active safety engagement as part of the payload integration process. They work with all payload teams, from first time Payload Developers (PDs) to repeat PDs.

Your Payload Integration Manager (PIM) will connect you with personnel to help shepherd you through the multi-staged safety process.

At the payload Kickoff meeting, you are introduced to the Safety Review Process and are provided preliminary information on important safety concepts such as the meaning of a payload being designated "Safety Critical." The Kickoff's safety presentation provides insight into how safety requirements, issues and concerns are managed throughout the payload development and integration process.

You will receive a large amount of information at the Kickoff, including an explanation of the Safety Process. However, it is not necessary to understand fully the entire process and elements at this early stage. PIMs and safety personnel will guide you on how best to prepare for each Safety Review Phase and associated milestone review meeting.

Your PIM can provide clarification regarding safety requirements and receive recommendations for avenues to get help. If anything seems unclear, ask! In addition, specific requirements vary for individual payloads. Understanding fundamental safety requirements up front will help you lay a solid foundation for upcoming ISS Safety Review Panel (ISRP) Reviews.

During the Kickoff meeting, be sure to take time to discuss safety with your team as well as with NASA experts who can provide valuable guidance up front, saving disappointing setbacks. This interaction is especially important if you are new to ISS or if you were PD for a different payload.

Note that the Safety Review Process can be taxing, and you may require extra or more personalized and intensive guidance/assistance. Receiving assistance is especially important when approaching a formal Safety Phase Review to mitigate schedule risks and stay on track for mission success.

Payloads can have many safety requirements, and information overload can result in inefficient and incomplete data for a phase review.

To keep safety in perspective, two Space Station Program (SSP) documents are key:

SSP 30599 Safety Review Process: Contains process description and data requirements

SSP 51721 ISS Safety Requirements: Contains top-level NASA technical requirements for experiment and non-experiment hardware.

Your PIM can provide clarification on important aspects of safety requirements documents as they relate to your payload.

THE SAFETY REVIEW PROCESS

The Safety Review Process is a joint responsibility of the PD, NASA ISRP, and visiting vehicle (VV) owners. ISS Program and VV owners manage requirements. The ISRP and technical support evaluate payload compliance throughout the phased process. You likely will interact mostly with the ISRP.

To succeed at Safety Reviews, begin early to establish safety as an integral part of hardware design/development process. A best practice is to assess payload hardware for all potential hazards throughout all mission phases and maintain good documentation on configurations, materials and parts. These documents may be key evidence for meeting a safety requirement.

> ***Make sure safety is part of your design.***

Expectations grow at each phased Safety Review:

- Phase 0 TIM: seeks images, diagrams and other informal documentation to inform the ISRP of payload objectives and concepts for design and operations and to enable provide recommendations.

- Phase I: This phase corresponds to the Preliminary Design Review and delves deeper into evolving payload needs and hazards. Initial Hazard Reports, which define causes and controls, are due. Preliminary verification methods may be presented, but full development is not yet required.

- Phase II: This phase corresponds to the Critical Design Review. Design iterates to ~60 percent completion, and final planned verification methods are identified.

  Note: Payloads that undergo major change or have incomplete products entering advanced safety reviews may need to return to earlier phases.

- Phase III: With the design finalized, the status of verifications that were successfully performed/completed are reported. All analysis is completed with only nominal open work remaining; e.g., late inspections, late filling operations, etc. Special TIMs can be held to address any problems or necessary changes to previously agreed-upon designs or hazard control/verification approaches.

The types of reviews and the relative depth of detail required depend on payload hardware complexity, technical maturity, and hazard potential and may be modified by the ISRP chairperson in conjunction with you as PD. Additionally, the Safety Review Process may be tailored as appropriate and agreed to between the PD and ISRP. By the end of the process, there may be some residual safety risk the ISS Program could consider to help you achieve the requested science objectives.

As part of the ISS Safety Review Process, payloads are required to demonstrate compliance with applicable ISS requirements. Assigned ISRP members and technical support staff perform independent reviews of each payload's safety assessments and provide input to the ISRP.

Many PDs think they can complete all the safety documentation to the satisfaction of the ISRP singlehandedly. However, experienced safety engineers are able to more easily and thoroughly identify potential hazards and develop controls that instill confidence among safety representatives. Best practice suggests that including a safety expert on your team to help you through these phases is optimal. This additional support allows you to focus your attention on managing the process, consulting with the Safety Payload Engineer (SPE) and Client Safety Engineer (CSE) (described in the next section) and engaging other members of your team as needed.

Even if you do not have a dedicated safety engineer on your team, it is recommended that you designate an individual as an ISS representative (such as a systems engineer or safety expert) as a liaison who attends the formal Safety Reviews for each phase in person. Other experts should be on call during these meetings to answer questions in real-time.

Ultimately, the purpose of the Safety Review Process is to ensure that payloads do not compromise the safety and health of the crew nor the capabilities of the ISS.

RESOURCES FOR SAFETY ADVICE

The Safety Payload Engineer (SPE)

assigned to each payload executes the Safety Review process and helps assure payload safety on behalf of the ISRP. While their primary duty is independent safety review and evaluation of the PD-provided safety analysis, they are committed to helping the payload succeed.

The SPE is your primary safety resource and helps communicate safety expectations and their intent so you can design hardware/software to an acceptable level of risk to the crew and vehicle. More generally, the SPE will advise you on reaching and passing each of the Safety Review gates. Like the PIM, the SPE can leverage the help of various discipline experts who can take on issues and be instrumental in helping you succeed while preserving safety.

While these experts are available to assist you through the process, you are responsible for completing the safety documentation. You have the most knowledge about and are ultimately responsible for the payload and related documents.

For some PDs, an additional level of support may also be available. The Client Safety Engineer (CSE) is a senior SPE authorized to provide additional tailored services to PDs in safety analysis and safety product development. The CSE serves independently from the SPE during ISRP reviews. CSEs are assigned in response to authorization/agreement from the ISS Program.

For integrated help with a multi-discipline challenge, you can work with the assigned SPE and request informal working group meetings prior to phased Safety Reviews to receive support resolving an issue. Making use of these groups is an excellent way to engage expertise within NASA. Experts can assist you by providing their understanding of any technical safety constraints that could affect a project.

Working group experts can suggest potential means to control hazards based on previously successful implementation approaches. They can help guide you through the safety process and steer your team to develop practical hardware designs and proven methods of operation, avoiding payload characteristics and thresholds that necessitate additional tests, controls, redundancy, and complication.

Bottom line: Safety experts are here to help get your payload through the integration process while assuring your payload meets all safety requirements. Be sure to ask for safety contacts by discipline and reach out to them early in the project lifecycle.

HAZARD ANALYSES AND HAZARD REPORTS

Performing Hazard Analyses and preparing Hazard Reports (HRs) are two crucial tasks for any PD. Hazard Analyses involve systematically identifying hazards, causes, controls, and associated verification methods. Hazard Reports summarize how payload design and operations demonstrate compliance with requirements and prevent hazards.

Payload hardware and software are assessed for all potential hazards throughout all mission phases. If a hazard cannot be eliminated in design, the hazard will be controlled to mitigate the likelihood and the consequences of the risk to an acceptable level.

HRs can be time- consuming to complete, and the standard templates are written to address many different types of hardware and cases in one document. Your Hazard Report will never use all the possible cases, so you will need to delete all the irrelevant cases from your payload-specific HRs.

Since the HR template is a guideline intended to be tailored or customized to the needs of the specific payload, using HR templates without customizing them may raise concerns with the Safety Panel. Since each payload is unique, you will demonstrate to the panel you and your team understand the logic and approaches defined within the generic HR templates by modifying them as appropriate for your specific design and operations.

Controlling hazards by design

In the event it is impossible to remove a hazard completely, there are two options for controlling hazards during payload hardware development/ design. Each of these terms carries specific meanings and ramifications.

Design to Tolerate Failures indicates hazard controls are required.

Design for Minimum Risk requires only minimum supporting data and relies on design robustness.

Hazard severity classifications are defined as follows:

- Marginal - Any condition that may *(a)* cause damage to an ISS end item, the loss of which itself does not constitute a critical or catastrophic hazard, and/ or *(b)* an injury that does not require medical intervention from another crewmember nor consultation with a Flight Surgeon.
- Critical - Any condition that may cause *(a)* a non-disabling personnel injury or illness, *(b)* loss of a major ISS end item, *(c)* loss of redundancy (i.e., with only a single hazard control left) for on-orbit life sustaining function, or *(d)* loss of use of systems needed for essential logistics.
- Catastrophic - Any condition that may *(a)* cause a disabling or fatal personnel injury or illness, *(b)* loss of ISS, *(c)* loss of a crew-carrying vehicle, or *(d)* loss of a major ground facility.

For additional rationale, explanation and examples for each of these severity definitions, see *SSP 51721, ISS Safety Requirements.*

! During a safety review, the ISRP may deem an item to be "Safety Critical." This designation indicates the item has a feature/aspect whose failure may result in a critical or catastrophic hazard. Safety experts are familiar with this designation and can provide guidance on typical hazard controls and verification methods to consider should the hardware contain Safety Critical elements.

THE SAFETY DATA PACKAGE

To meet ISS Program safety and interface requirements and guidelines, you must provide evidence that the payload meets the requirements described in program documents. You will demonstrate this evidence by providing information through the Safety Data Package (SDP), which ISRP technical reviewers evaluate. Updated and refined by the PD team throughout Safety Review Process, the SDP typically includes details for the payload, including hardware design information and the Concept of Operations. The ISRP expects you to provide an assessment of potential hazards, detailing your approach towards hazard control and associated verification activities.

The SDP defines hazards, hazard controls, and verification of hazard controls. The PD identifies all hazards and ensures that proper hazard controls have been developed and implemented for each hazard.

The SDP encompasses all safety-related information pertaining to a payload, including hazard identification, classification, issue(s) resolution, if applicable, and a record of all failures/anomalies with special emphasis on those pertaining to safety. Note: The ISRP has available supplemental information on assessing hardware for safety, performing a Hazard Analyses, and constructing an SDP. These resources can be provided by the assigned SPE/CSE.

> 💡 A good SDP follows a logical, structured format, using a common application with a reader-friendly platform; e.g., Word, PowerPoint, PDF, but not Excel. Charts, diagrams and other helpful elements are recommended for conveying information as clearly as possible to the ISRP.

Through developing the SDP and HRs, you communicate with NASA that your team has addressed safety throughout the development of the payload.

Upon completion of each phased Safety Review, the Safety Data Package with approved Hazard Reports serves as formal documentation that a payload has been evaluated for any potential safety risks and that the mitigation of these risks has been thoroughly considered and adequately controlled.

> 💡 The SDP should evolve with additional details added to it throughout the phased Safety Review process. See Figure 1, Schematic process flow for SDP.

By working together, you and the NASA safety representatives can find ways to mutually succeed in fulfilling the obligation to fly safely.

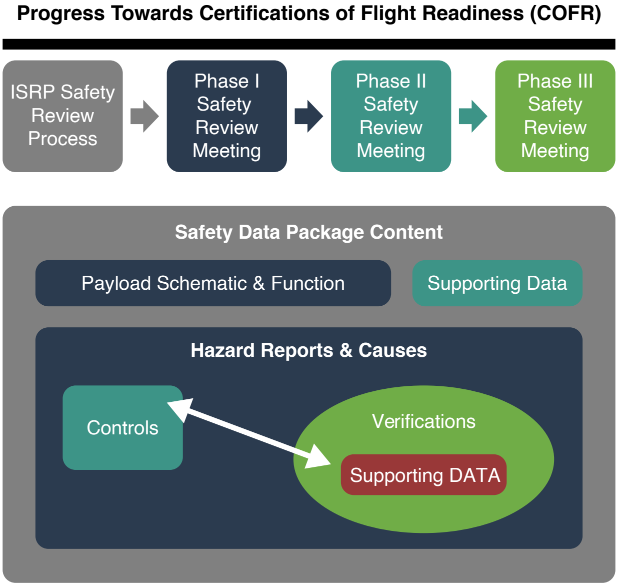
SAFETY REVIEW OVERVIEW – PHASE 0 EXAMPLE

The ISRP Chair is responsible for determining whether a payload is safe for flight based on the recommendations of panel members. The Chair's focus is on HRs and safety Non-Compliance Reports generated throughout the Safety Review. The Chair aims to approve the payload; however, it is your responsibility to provide enough rationale to enable them to do so.

> 💡 Although the Phase 0 TIM is not required for PD teams, having this standalone TIM early in the process is an excellent way for you and the ISRP to begin to reach a common understanding regarding the payload. For PD teams that opt for a Phase 0 TIM, this is the first opportunity for the ISRP Chair and PD team to meet.

Phase 0 is an opportunity to convey your research objectives as well as the design and operations concepts to the ISRP. Sketches

figure 1
A schematic process flow for the Safety Data Package.


Progress Towards Certifications of Flight Readiness (COFR)
ISRP Safety Review Process
Phase I Safety Review Meeting
Phase II Safety Review Meeting
Phase III Safety Review Meeting
Safety Data Package Content
Payload Schematic & Function
Supporting Data
Hazard Reports & Causes
Controls
Verifications
Supporting DATA

and preliminary payload design information are acceptable at this phase; plan to include as much detail as possible.

Since your field of expertise is likely very different from those of the panel members, articulate information thoroughly but in layperson-level terms. Since the ISRP is more familiar with the ISS and its capabilities, the ISRP may be able to advise you on design or operational concepts that will facilitate easier flight certification, and the panel is expected to convey their information in understandable language to you.

Approximately two weeks prior to the Phase 0 review, provide presentation material to the ISRP that covers:

- What you want to achieve with your experiment/ demonstration.
- What you think the hardware will do.
- How the payload could potentially cause harm to the crew, the ISS or VV if it did not operate correctly.
- What the sources of the hazards are in the payload.
- What data are available to support the details?
- What major components your payload will include, such as lasers, sources of high temperature, toxic chemicals, biological samples, etc.

This information helps the panel envision the payload in context.

When needed, you may be referred to specific technical experts to receive the best assistance/resources to resolve any anticipated safety challenges as you progress through the phases of the Safety Review Process.

Unless the payload has flown routinely and no design or operational changes or anomalies that would require more extensive in-panel discussions have been identified since the previous flight, it is recommended that you attend all formal Safety Phase Reviews, either in person or remotely. Alternately, a safety representative on your PD Team can fulfill this function.

There are phase-level checklists (available from the SPE/CSE) to assist the PD to help clarify expectations of the SDP, accompanying Hazard Reports and other supporting data and to ensure all necessary technical data are included. It is your responsibility to ensure quality control of the data and to know how and when this information needs to be provided.

When preparing presentation materials for Safety Reviews, your objective is to explain how the payload works and why the payload is safe to fly. You will provide evidence that you have consistently prioritized safety throughout the design process, providing grounds to establish the desired rapport of trust. Aim to make your presentation comprehensible and succinct and include an orientation overview and illustrations.

The SPE/CSE will clarify what to expect at these reviews. Have experts on call during the review to help answer technical questions during the meeting. Unanswered questions are tracked, and you will be asked to respond to them at the next review if an answer is unavailable when asked during the review meeting.

The job of the ISRP is to ensure the safety of the crew and vehicles, so the ISRP Chair will ask questions and provide feedback in order to gather ample evidence to approve the payload to fly. A PD who listens carefully at reviews and takes the advice of the panel — particularly regarding appropriate hazard definitions and controls — will be able to successfully navigate the safety review process.

A successful review demonstrates that the PD is thorough, has thought things through, knows the payload design well, understands the requirements, and has anticipated questions and prepared answers.

PAYLOAD SAFETY SUMMARY

Over the years of ISS research utilization, safety representatives have learned many lessons to apply to future development activities. PDs who approach the review process with a willingness to invest time early, demonstrate a thorough understanding of potential safety hazards and who display a willingness to have candid discussions will reap rewards in the later Safety Review phases. As is the case with each phase of the payload project lifecycle, communication and collaboration are key.

> If a requirement is unclear, ask for clarification. When possible, ask to connect with experts or specialists and get their feedback before design decisions are made. If only preliminary information is available, identify it as such and share it. Test prototypes and always keep complete records on materials, parts, and configuration.

Since it is the responsibility of ISS safety personnel to ensure the safety of the crew and the vehicle, be prepared when safety personnel ask questions to highlight missing information. Incomplete data can lead to rework and reconvening of phase meetings.

> The Safety Review Process can be facilitated by having a dedicated safety expert on the PD team, by designating an ISS representative (such as the team's project systems engineer) to attend each phase review. These highly recommended best practices are worthwhile investments for every PD to consider as part of their budget/resource planning.

> ! Seasoned ISS safety personnel may be able to assist with simpler or more reliable design/operational considerations. At a minimum, they will be able to help identify areas to improve efficiency, including solutions for reducing paperwork while continuing to meet ISS safety requirements.

While it is always the goal to eliminate or fully control hazards whenever possible, safety personnel understand that in some cases, an easy design solution is neither practical nor possible. In such cases, understand that the ISRP will continue to work jointly with you on the problem and explore options to determine the best solution — together.

A payload may be able to receive an Exception/Waiver for a particular requirement if the safety community understands the hazard, the environment, and the controls to the point that the ISS Program is willing to accept the residual risk.

The goal of everyone involved is to fly the payload safely in space. The PIM is your main source of support through the integration process, and there are multiple people available — Research Portfolio Managers (RPMs), SPEs/CSEs, and ISRP representatives with a variety of discipline experts — to support achieving this goal and the desired mission success.