ENHANCING THE NASA EXPENDABLE LAUNCH VEHICLE PAYLOAD SAFETY REVIEW PROCESS THROUGH PROGRAM ACTIVITIES

Thomas E. Palo

National Aeronautics and Space Administration – Kennedy Space Center, Florida USA
Email: Thomas.e.palo@nasa.gov

ABSTRACT

The safety review process for NASA spacecraft flown on Expendable Launch Vehicles (ELVs) has been guided by NASA-STD 8719.8, Expendable Launch Vehicle Payload Safety Review Process Standard. The standard focused primarily on the safety approval required to begin pre-launch processing at the launch site. Subsequent changes in the contractual, technical, and operational aspects of payload processing, combined with lessons-learned supported a need for the re-assessment of the standard. This has resulted in the formation of a NASA ELV Payload Safety Program. This program has been working to address the programmatic issues that will enhance and supplement the existing process, while continuing to ensure the safety of ELV payload activities.

PREFACE

This is a factual (though at times tongue-in-cheek) account of payload safety program activities. Any similarities to Dorothy's trip to Oz, and the events and characters she encountered along the way, are purely coincidental. Fortunately for Dorothy, her adventure was only a dream.

NOTE: The views expressed in this paper are solely those of the author, and do not necessarily represent those of NASA or its employees.

1. THE HISTORY

Not unexpectedly, a collection of individual, common place events led to the present situation. NASA-STD 8719.8, Expendable Launch Vehicle (ELV) Payload Safety Review Process Standard, released in 1998, was the official beginning. Developed through an aptly named process called SPAT - Safety Process Action Team - this standard was to define the never before documented safety approval process for NASA ELV payload processing. It was the result of the efforts of a dedicated team of hardworking, intelligent individuals, each with one goal in mind... satisfying their own interests. At least as an outsider that was my impression; as an ad hoc member of the team working for the 45 Space Wing at the time (with no dreams of rainbows), the inside story was that it would give payload project safety personnel some representation against those feared safety guys when they came to process at Kennedy Space Center (KSC). Was it successful? Surprisingly, yes -- for everyone.

NASA-STD 8719.8 accomplished many important things. It established payload safety working groups (PSWG), a distinguished body composed of safety personnel representing the various organizations including the payload contractor, spacecraft center, launch vehicle, processing facility, and Air Force Range Safety. It also defined typical milestones for submittal of safety data, and an approval process of the payload safety documentation. We were brave in those days, and there wasn't an issue we didn't think we couldn't handle ourselves.

We were also tremendously successful for years, surviving all the other external influences such as re-organizations, NASA initiatives (e.g., Faster, better, cheaper), organizational restructuring, changes in management, and organizational re-alignments. With no real visibility, we avoided many obstacles. Unfortunately, the formal implementation of the standard was virtually non-existent and its presence in a contract seemed to be the rare exception. With limited support, we imposed it on projects the best we could; there seemed to be a 'gentlemen's agreement' that this was something good.

Often we would be confronted with a unique situation, not addressed by the standard. Left to our own methods, we addressed the issue and our solutions, and although they maybe not have been perfect or well documented, we accomplished our safety objectives. We avoided all the bureaucracy, management interference, politics, turf battles, etc. that are known to exist outside of NASA. We knew what the issues were, what had to be done, and how to fix it. OUR process actually worked.

1.1 The B.C. Years – (i.e., Before CALIPSO)

It's hard to pinpoint the exact time when the speed bumps appeared in the 'yellow brick road'. Again, there was not one individual event that was the root cause. A combination of the Air Force Range Safety reducing their oversight to the public safety of civil and commercial launches (effectively transferring the safety responsibilities), and increased competition between spacecraft contractors and their efforts to maintain market share were probably the major contributors. Overhead cuts were made and trickled down resulting in smaller safety staffs. Lower paid (inexperienced) safety personnel were hired to replace those fortunate enough to embark on more fulfilling career paths (if they were replaced at all), decreasing the quality of safety assessments, timeliness of data submittals, etc. Unknowingly, the good old days were about to end as project managers saw the safety folks as an independent bunch that "needed some learnin'" in principles of corporate finance. Unfortunately, a few project managers didn't read the paragraph in the NASA Policy Directive that requires safety approval of payloads.

As hard as we tried (and seriously, we did), the past user-friendly, flexible, trust-me, teamwork approach wasn't getting the results that it once did during the era of Air Force assistance and larger safety staffs. Reluctantly (it was an impact on us, too) we started to really push the implementation of NASA-STD 8719.8, requiring new program introductions, regularly scheduled PSWG meetings, firm submittal dates for safety data packages – the requirements to ensure that we received the stacks of safety data we needed. Then the name calling began (a little nastier than 'lions, and tigers, and bears'), but our firm stand resulted in some slow improvements.

Who knows when or if we would have ended up at Emerald City, as we were certainly on the road to Abilene. Fortunately, the road divided with a sign pointing toward CALIPSO. Maybe a bit of a long way off (as the distance conversion was verified by the Jet Propulsion Laboratory), but still 'close enough for government work'. Suddenly, our wishes and dreams came true and we received more management support and assistance than ever thought possible (thanks to Dr. Laurence J. Peter).

1.2 Program Establishment

Without getting into the technical issues, safety requirements, or management issues of CALIPSO, it was really a blessing in disguise. CALIPSO motivated safety personnel and agency and center management to work together as a team to define short-term solutions, realize that indeed, programmatic issues existed, and develop long-term solutions for some long-standing problems. After CALIPSO, NASA quickly created a team that immediately identified the objectives, approach, processes, and requirements. Well, maybe not quickly, but it was the first step in resolving some of the issues that evolved since the release of NASA-STD 8719.8 and the lessons learned from CALIPSO.

CALIPSO raised some specific problem areas that needed resolution. They included:

- Complicated roles for projects involving multiple NASA Centers
- Dealing with projects that involved international partners
- Lack of an approval process for the use and re-flight of a common spacecraft bus
- Lack of a process for resolving dissenting opinions within NASA and with external organizations
- Lack of acceptance of external approving authority and requirements

From these issues, an approach was identified:

- Build on the current PSWG approach and augment as needed to address lessons learned
- Develop a new NASA ELV Payload Safety Program (PSP) to:
  - Establish and maintain NASA ELV payload safety policy, roles and responsibilities, and associated requirements
  - Ensure consistent interpretation of safety requirements
  - Define and oversee implementation of the safety review process
  - Provide payload projects with training, tools, and guidance
  - Identify the decision making authorities
- Develop a formal processes for:
  - Resolving differences within the PSWGs:
  - Variance approval
- Enhance and formalize key partnerships (e.g., Air Force and other ranges, commercial launch service providers, etc.)

2. ELV Payload Safety Program Scope

In NASA-STD 8719.8, the focus of the requirements concentrated on the approval of the safety data package

to obtain approval for processing at the launch site and subsequent launch. Obviously, to meet the agency safety (and mission success objectives) the scope of the program had to be increased to address the complete lifecycle. Anything less would result in a program with gaps, or an approach where safety is only selectively implemented. To achieve a robust program, the NASA-STD 8719.8 scope was expanded to include systems safety participation in such areas as contracts and safety requirements identification, design, assembly, integration and test at NASA facilities, pre-launch processing and launch site operations, and planned recovery of capsules and sample return. This is in keeping with the similar lifecycle philosophy of MIL-STD 882.

2.1 Program Organization and Structure

When originally discussed, one option considered was adopting a 'panel' type structure, similar to the Shuttle Flight Review Panel. This would certainly accomplish the objectives and provide the benefit of a strong, authoritative panel, but the cost to support such an organizational structure was deemed a prohibiting factor. In addition, the added complexity of multiple launch vehicles and launch sites would increase the complexity of support required. The approach finally adopted was to keep the successful structure of the PSWG intact as defined in NASA-STD 8719.8. The PSWG members would continue to support mission safety activities through better defined roles, and to provide the agency perspective, an ELV Payload Safety Program Manager and an Agency Team, was identified by NASA Headquarters (HQ) Office of Safety and Mission Assurance (OSMA). The agency team and program manager will provide support to the PSWG, and to ensure agency objectives are met, facilitate center and agency communications.

The core agency team representatives will come from the Jet Propulsion Laboratory, Goddard Space Flight Center, and KSC, with specific roles and responsibilities should be defined. This cross-section of centers will provide varied perspectives (and agendas), and should facilitate the exchange of information between centers for current and future missions.

The agency team will support the program in two phases. The first phase consists of a development phase where the program activities, requirements, and processes are developed and finalized. The follow-on phase, the implementation phase, is where the program-defined requirements and activities are instituted, with the agency team acting to ensure that program/agency objectives are met.

One of the misconceptions that needs to be addressed is that the PSWG is 'certifies' the safety of the payload. This is really done by the project office safety engineer. The PSWG provides a top level assessment to ensure the safety in their limited areas of authority. Many project managers think they have a 'safe' payload because the PSWG provides approval, but in reality the burden falls upon the payload center Safety and Mission Assurance Office to ensure the appropriate review for the entire lifecycle.

2.2 Program NASA Procedural Requirements Development

The policy establishing the protection of the public, workforce and assets of NASA ELV payloads is defined in NASA Procedural Requirements (NPR) 8715.3, NASA General Safety Program Requirements. This NPR also defines the HQ level responsibilities associated with the program. As stated earlier, the program activities include the development of a new NPR that will supersede NASA-STD 8719.8 and define the program, operating structure, roles and responsibilities, processes, and technical safety requirements.

A major area of concern was the lack of NASA ELV payload safety design requirements. As nearly all NASA ELV payloads are launched from Air Force Ranges, the Eastern and Western Range (EWR) Requirement 127-1 (superseded by Air Force Space Command Manual (AFSPCMAN) 91-710), was specified by NASA as the applicable safety requirement document for all flight hardware, ground support equipment, and operations conducted on Air Force property. At times, there are concerns that it is difficult to enforce requirements that NASA does not 'own', or that the Air Force is queried for requirement interpretations for NASA programs.

These concerns will be alleviated by the development of technical safety requirements for NASA ELV payloads. The safety requirements will be based upon Air Force requirements, but will be tailored for payloads and include any NASA requirements that are more stringent or unique, and lessons learned. AFSPCMAN 91-710 was chosen as the baseline for the NASA requirements, because of its strong heritage, the mandatory compliance document for launches, and as wise man (me) one said,

Hardware is dumb; it doesn't care what it's flying on or where, the hazards on the ground are all the same.".

In addition to safety design requirements, applicable operational safety requirements are required. Disparity exists between centers' requirements and these differences become apparent especially when hardware is transferred to another center for additional integration and test, or to the launch site for pre-launch processing. A common core of operational safety requirements would ensure safer, seamless operations with fewer confusion and delays.

3. Program Elements

From these objectives, the specific elements of the existing process were reviewed to identify the areas which required enhancing or supplementing to ensure that the agency objectives were reflected in the PSP.

The following sections identify the areas addressed, options considered, actions proposed, and the expected results.

3.1 Contract Assessment and Requirements Identification

These activities require a thorough identification of compliance requirements, standards, and codes to ensure that all applicable safety requirements necessary for payload safety are incorporated into the contracts and agreement(s). These requirements encompass all safety activities and should address flight hardware systems, ground support equipment, facilities, institutional safety, applicable launch range safety requirements, etc. Experience has shown that failure to identify applicable safety requirements for inclusion into contracts results in flight hardware design paths being taken that may result in costly redesign and/or risk to personnel or hardware.

Related to requirement identification is a review of the contractual requirements. NASA occasionally enters into unique contractual agreements including grants or cooperative agreements. These agreements sometime impair the ability to impose the appropriate safety requirements, or prevent the required changes to achieve compliance to safety requirements. These contracting arrangements effectively 'tie the hands' of a safety office, and could result in project and safety risks.

3.2 Systems Safety Program Plan

The Systems Safety Program Plan (SSPP) defines the payload project office safety organization, roles, responsibility, authority, lines of communication, and interfaces with other disciplines both internal and external to the mission. NASA-STD 8719.8 previously specified only external (PSWG) review of the document, not approval. As this document can be considered as a contract between the payload safety office and the payload project that defines the function and support provided to the project and how the PSP objectives will be met, approval of this document will now be required.

An important change to the SSPP contents will be the increased emphasis on how the safety activities are integrated throughout the project lifecycle. This is the result of PSP's expansion of the safety review activities, and problems with past SSPPs where roles and responsibilities were undefined, such as during certain project phases or integrated activities.

The timing of the submittal and approval of the SSPP will also be better defined. The importance of safety participation at the beginning of a mission cannot be over emphasized, and a sound plan is needed to guide the safety activities. Without a complete and robust safety process identified and implemented early, this too may jeopardize project goals and safety activities.

3.3 Requirements Tailoring

'Tailoring' is probably one of the least understood, most ignored and abused, but most beneficial process to the project and safety authorities. Tailored safety requirements result from the process of reviewing requirements to ensure the applicability and compliance by the project, as written, or whether the project will achieve an equivalent level of safety through an acceptable alternative requirement.

The tailoring process is performed to aid in the interpretation of requirements and identify potential non-compliances; this facilitates the early resolution of issues to reduce risk, enhance safety, and minimizes impact to project.

Tailoring is not a unilateral activity. The project office safety engineer should prepare a draft in coordination with payload systems engineers. This draft is reviewed by all PSWG members for their respective areas of responsibility to:

- Identify applicable requirements -- NASA, Range Safety, other Government and consensus standards
- Document the interpretation of requirements or applicability of a requirement to a specific mission activity
- Implement lessons-learned as applicable
- Consolidate interim policy/guidance/requirements
- Document the rationale for addition/deletion/ change in requirements

The resulting tailored requirements become the safety requirements for that project, therefore it is important that tailoring is performed early, so design and operations can implement the safety requirements; accurately, to ensure safety and project goals are achieved; and consistently, to meet the PSP objectives.

In the past, some tailoring efforts took the approach of a 'compliance checklist', resulting sometimes in combinations of undefined requirements, key requirements being deleted, and requirements incorrectly interpreted. Alternative approaches have been poorly documented, not documented, or accepted with a higher risk without assessments or management acceptance of risk.

If the proper proposed programmatic changes to the tailoring process are incorporated, substantial improvements should result. Specific milestones are defined for the tailoring activity. The format/process for tailoring will be defined, and rationale provided for any change, with a risk statement and assessment provided or referenced. As the tailoring is actually a modification to a NASA Procedural Requirement, it will be reviewed by the agency team to ensure that the correct interpretations of requirements have been documented, alternative approaches provide an equivalent level of safety truly do not increase risk, and adequate rationale is provided.

A review by the agency team will provide a consistent assessment for all agency payloads, and also provide insight into requirements that may be unclear or frequently misunderstood, or alternative approaches that should be incorporated in the baseline requirements. This review will also provide the agency team the opportunity to identify issues that may be applicable to other current or future projects.

3.4 Project Safety Introduction

The Payload Safety Introduction (PSI) is the fist formal meeting of the spacecraft team and the PSWG. While a requirement of NASA-STD 8719.8, its occurrence varied, and at times was held after the Preliminary Design Review (PDR), if at all. This meeting provides the project team the opportunity to introduce their organization, describe their mission, hardware, and processing activities, and provide an initial hazard assessment of their hardware and operations.

The PSP has clarified the requirements for the PSI to ensure that preliminary hazard identification and analyses, a draft systems safety program plan, and a draft of the requirements tailoring are provided for discussion at the PSI.

The agenda of the PSI has also been expanded to include discussion of the following items:

- Applicable compliance documents
- Contractual requirements and relationships
- Contingency Operations
- Planned recovery activities
- Pre-launch mishap response and reporting

3.5 Safety Data Packages

A Safety Data Package (SDP) is a data submittal that provides a detailed description of hazardous and safety critical flight hardware equipment, systems, components, and materials that comprise the payload. It includes hazard assessments, inhibits, and mitigations, and with data provided in hazard reports, the ground operations plan, and hazardous technical operating procedures, it is one of the media through which prelaunch safety approval is obtained.

The SDP is the 'objective evidence' a PSWG utilizes to assess safety compliance, and is their only official source of information. Obviously, an accurate submittal of this data is essential to ensure that the safety community is aware of the hazards, concurs with the assessments and mitigations, and the risk or effect on personnel or resources in their specific areas of responsibility (i.e., launch vehicle, public safety, NASA resources, processing facility, etc.).

Safety activities are especially important at the beginning of a project during the concept and development engineering phases. Without active safety participation, a path may be taken that could lead to a design burdened by safety requirements, or at the other extreme it could result in a design with unacceptable risk. To avoid these events, preparation, submittal, and review comments are linked to a project's PDR and CDR milestones.

The SDP not prepared or reviewed in conjunction with the design review milestone may have serious impact to the project including:

- The potential of a safety issue being discovered late(r) in the safety review process and requiring corrective action
- The project not being able to implement an optimum solution to resolve the safety issue (compromising engineering, science and/or safety)
- The residual risk from any design change or mitigation may still result in a risk that is higher than desired
- Cost and schedule impacts to the project to accommodate design reviews and changes, hardware re-work or software modifications, testing, procedural changes, waiver processing, and management briefings.

Previously, submittal dates were poorly defined and the requirements for the number of submittals, content and required delivery dates were creatively interpreted. Payload project safety offices pointed to the systems engineers as the source of the problem, as systems engineers were busy preparing for the PDR/CDR, and could not provide the required support to safety. To be effective, safety must actively participate in the design assessments, and be synchronized with the project engineering tasks. Systems safety is not an after-the-fact activity; it is an activity that must be performed concurrently with engineering. It can't be 'designed-in' afterwards.

In addition to the NASA-STD 8719.8 prescribed PDR, CDR, and 'final' submittals, an additional SDP submittal is being proposed post-CDR that would capture CDR changes and open comments from the Phase I and II submittals.

While the post-CDR submittal may appear as an additional burden to the payload project, historically, a minimum of 4 submittals is typically required to fully address the PSWGs concerns. From a cost standpoint, there may be a slight increase due to an additional internal review cycle, but the total level of effort in compiling the project's SDPs would remain the same, as the data required overall does not change. Likewise, requiring SDPs to be submitted before the project milestones is the only way to ensure timely feedback to the project and avoid the previously mentioned impacts. The preparation cost of an additional SDP is insignificant cheap when contrasted with the expense of a major design change.

3.6 Design Review Presentations

Safety compliance is a project management gate, and safety activities and issues are required to be presented at the PDR and CDR by the payload organization safety engineer. Although NASA-STD 8719.8 identified specific topics to be presented at the design reviews, many presentations lacked substance and at times offered little more than the status of safety milestones.

The PSP will require the following areas be presented at the PDR and CDR:

- Summary of safety activities and reviews, with dates and overview of upcoming safety milestones
- Summary of hazard reports and hazard resolutions
- Overview of non-compliances and potential safety issue

One alternative considered would have the individual sub-system engineers address the safety aspects of their systems in their presentations, in lieu of the project office safety engineer providing a summary. A benefit would be that the sub-system engineers would be more conscious of the safety requirements and implementation in their designs.

3.7 Phase III Payload Safety Review Presentation

The Phase III Payload Safety Review Presentation is a new initiative instituted to provide a summary review of safety activities prior to the pre-ship review. The project office safety engineer will present to the PSWG and agency team the following:

- A summary of safety activities and reviews, and the status of any in-process safety related work
- An overview of non-compliances and risks
- Verification that all safety requirements and activities have been met, or review of the plan(s) to bring the project into compliance
- Status of safety verification tracking log items
- The Certificate of ELV Payload Safety Compliance

3.8 Certificate of ELV Payload Safety Compliance

Although 8719.8 required a documented, coordinated approval from the PSWG, this rarely happened. PSWG members would provide individual approvals, at a schedule that coincided with their mission support milestones. In addition, a PSWG member approval did not always identify the scope of their approval or authority. This of course was confusing to project

managers, as they were unsure of the number of approvals they needed, or would receive. Occasionally, it also led to subtle pressure by project managers against a PSWG member that might still be trying to resolve a safety concern.

The revised process will consolidate the PSWG approvals through a certificate of compliance, with the goal of approval prior to the pre-ship review.

3.9 Dissenting Opinions

NASA-STD 9719.8 did not establish a formal voting process to resolve payload safety issues that had reached a stalemate within the PSWG. PSWG members always operated under the premise that all members would reach a unanimous position, or work until one was achieved. CALIPSO was the first mission where the PSWG could not reach agreement, and the need for a process to elevate and resolve dissenting opinions was evident.

New program requirements will specify that a dissenting opinion from a PSWG member can be brought forward to the agency team. If necessary, the agency team will use independent resources such as subject matter experts to guide the determination. If the agency team also cannot reach a consensus, or provide a solution to satisfy a dissenting PSWG member, the issue will be further elevated to HQ OSMA.

The agency team will rely upon the PSWG to raise any issues of concern before prolonged discussion occurs, or where an impasse is expected, and long before a critical milestone. The agency team will provide support and recommendations to the PSWG, and also advise HQ OSMA if a potential controversy appears to exist.

3.10 Training

NASA Standard 8719.8 never prescribed required training, nor was training for compliance to the Standard or its elements ever developed. Previously 'training' consisted of a short presentation at the PSI, primarily identifying roles, responsibilities, and description of the required data submittals.

Two training classes are being proposed. A shorter version will have a target audience of NASA center and spacecraft contractor project managers, spacecraft systems engineers, safety and mission assurance directors and managers, and mission integration managers. The focus of the training will be toward roles, responsibilities, and processes. A longer class will provide greater detail in these areas and more specific instruction with respect to the required safety data submittals. This class will be aimed to PSWG members and safety engineers.

The PSP will also define minimum experience requirements for project safety personnel. Payload project office safety engineers will be expected to have the required systems safety engineering training, and will be required to have on-the-job experience assisting in a previous mission, before being the lead of a mission under the watchful eye of an experienced project office safety engineer.

4. Program Development Lessons Learned

Lessons learned is a misnomer because every new initiative probably reflects on decisions made in the same areas of communication, adequate funding or resources, and planning and scheduling. Then there are some circumstances that even the Wizard couldn't fix, but a few suggestions:

- Apply a systems engineering approach. Issues and potential resolution should be defined in an increasingly greater level of detail, with stakeholder buy-in obtained at each phase. Issues/actions should be well defined, documented, prioritized, and dispositioned through a logical, integrated process. The time taken to clearly define in detail the approach and actions would have saved much time in the disposition of comments, clarifying incorrect assumptions, recalling the rationale for past changes and decisions, re-formulating, and writing of requirements.

- Process changes are best implemented in phases. Beta testing of portions of the process would have provided confirmation of the validity of approaches and provide opportunity to adjust. Easy 'fixes' should be implemented on an interim basis; it would provide a sense of accomplishment for team, and address current issues now. Phasing-in changes also prevents an overload during implementation, and early success makes the team more receptive to additional changes.

- Continually review program objectives and original lessons learned, and periodically assess to ensure that objectives are being met. Changing the scope or dismissing a previous objective because a hard

decision is required doesn't make a problem disappear.

- Be realistic and honest in planning, scheduling and communications, and critique of your work. Processes that are developed might look good on paper, but they have to survive the real world and 'human factors'.

- Avoid new inventions; systems safety wasn't discovered yesterday. Try to employ proven processes and common requirements and apply them to all activities – Not only is hardware dumb, it has no sense of direction. Selective application of requirements doesn't solve problems, they just occur somewhere else.

5. Summary

While NASA-Standard 8719.8 provided instruction that facilitated the safe processing of scores of NASA ELV payloads, the evolution of the industry and agency concerns necessitated an expansion of policy scope, activities, and requirements to achieve the intended goals.

Clarification and formalization of existing requirements for day-to-day project activities will help achieve the goals. Well-defined roles, responsibilities, and requirements will reduce confusion and provide a more effective safety process for the projects. The broader agency goals of consistent interpretation and implementation of requirements and processes should be achieved through the creation of the program and utilization of the new agency team.

Collectively, these programmatic changes should result in a significant improvement of the safety of NASA ELV Payloads.