Mission Success Starts With Safety

Introduction

• Welcome!
• Points of Contact:
  - Mike Dook, OSMA - Tel: (202) 358-0226; michael.dook@nasa.gov
  - Cal Staubus, NASA KSC - Tel: (321) 867-8757; calvert.a.staubus@nasa.gov
  - Tom Palo, NASA KSC - Tel: (321) 867-8726; thomas.e.palo@nasa.gov
  - Shawn Donovan, SRS Technologies - Tel: (321) 867-6240; shawn.t.donovan@nasa.gov
  - Marv Becker, SRS Technologies - Tel: (321) 867-3266; marvin.l.becker@nasa.gov
  - Program Website: www.ksc.nasa.gov/elvpayloadsafety

Topics

• Background
  - Current NASA ELV Payload Safety Review Process Standard
  - Issues Needed to be Addressed by New Program
• New Program Development
  - Program Development Working Group
  - Program Development Executive Team
  - Accomplishments/Activities
  - Tasking and Funding
  - Schedule
• NPR 8715.3, Chapter 3, Payload Safety
  - NASA Payload Safety Policy
  - NASA ELV Payload Safety Program
    - Applicability
    - Roles and Responsibilities

Topics (continued)

• Proposed NPR 8719.XX, NASA ELV Payload Safety Program
  - Chapter 1, Program Overview
  - Chapter 2, Safety Review and Approval Process
    - Mission Roles & Responsibilities
    - Flow of Activities and Deliverables
    - Website
  - Chapter 3, Requirements
    - Design, Ground Operations, etc.
    - Variance
    - Training Program
• Open Discussion

Background

  - Applies to Orbital and Deep Space ELV Missions (unmanned)
  - Focus on safety of processing at launch site, including payload processing facilities at or near launch site
  - Designed for missions involving numerous organizations and various vehicle/launch site combinations (derived from Shuttle PSRP/OSRP with appropriate differences)

Background (continued)

• NASA STD-8719.8 (continued)
  - Has been successful (with ad hoc changes) for a majority of NASA ELV payloads
  - Certain complications evolved after the Process was developed:
    - Complicated roles for projects involving multiple NASA Centers
    - Projects involving International Partners
    - Lack of approval process for use of common spacecraft bus
    - Lack of process for resolving dissenting opinions within NASA and with external organizations
    - Lack of acceptance of external approving authority and requirements
Launched successfully from VAFB SLC2, April 2006
(Example) Entailed many administrative and technical complications
Highlighted weaknesses in current payload safety process
- Goddard Science Program – Langley Project – KSC Launch Services
- Co-manifested with CLOUDSAT – led by Goddard
- NASA provided CALIPSO instrument – France provided spacecraft bus
- "Off the shelf" hydrazine-fueled Proteus spacecraft manufactured by Alcatel
Space Industries and provided by the Centre National d'Etudes Spatiales (CNES) as the "contribution" to the joint mission
- Joint Mission Agreement – not your typical contract
- Proteus flown successfully in 2001 on the Jason-I – led by JPL
- Goddard SMA and Engineering raised concerns with Proteus:
  - Fuel tolerance for leakage of hydrazine, hardware safety, battery safety, others
  - Resolution via Formal Variance Process:
    • Personal safety ensured via implementation of NESC recommendations
    • Mission success risk accepted via NASA Variance

Background (continued)
- Requires "Tailoring" of requirements for each payload
  • Subject to misunderstanding the process and benefits, and poor implementation
  • Current Process lacks the strict and consistent oversight from one project to the next needed for proper implementation
  • Relies heavily on the ability of the PSWG to reach consensus
  • Current process does not identify a decision-making authority
  • No clear direction for when consensus cannot be reached
  • Resolution of contentious issues can drag on until the "final hour"
  • No clear direction on the applicable Safety Variance Process

Program Development Working Group
- Established via Letter From Dr. Stamatesiatos, March 24, 2004
- Open to all NASA Centers and other appropriate organizations:
  • APL Clay Smith
  • GRC Bill Schiemen
  • HQ Mike Dost, Steve Voigt
  • KSC Cal Mabitis, Tom Palo
  • LaRC Jose' Caraballo
  • WFF Gerald Morris, Tom Morello
  • 45SW Jeffrey Wethern
- Provide technical expertise
- Provide Center/s' organization's perspective
- Identify needs of future projects
- Participate in Program document development and other activities
Mission Success Starts With Safety

Program Development (continued)

Executive Team (Established via letter from Bryan O'Connor, March 2006)

GSFC
Karen Fisher

KSC
Cal Staubs, Tom Palo

JPL
Jim Lumsden

HQ
Mike Dook

(Contractor support at GSFC and KSC by SSR Technologies)

- Draft Program Process/Requirements (NPD/ NPR)
- Organize and facilitate Working Group activities
- Resolve Working Group comments
  - Striving to build consensus on Program Elements
  - HQ Chief, SMA has final decision
- Ensure Program is consistent with current Agency implementation of Technical Authority
- Coordinate with external organizations
  - Strive for a joint approval process with Air Force Range Safety

Program Development (continued)

Activities/Accomplishments

- Program Development Objectives and Concepts (Charter)
  - Helped to help resolve philosophical differences as a first step
- Fact Finding/Program Development Meetings During 2005 @ HQ, KSC, Patrick AFB, Vandenberg AFB, JPL, WFF, and JSC
- Briefed SMA Directors, August 11, 2006, on Objectives and the Program Concepts/Approach - Obtained OK to Proceed
- Published new Payload Safety Policy, Roles, and Responsibilities, September 2006:
  - NPR 8715.3, General Safety Program Requirements (Chapter 3)
  - Includes Agency Safety Policy applicable to all types of payloads
  - Establishes NASA ELV Payload Safety Program

Program Development (continued)

Approach

- Build on the current PSWG approach and augment as needed to address lessons learned
- New Agency Safety Program to include:
  - 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 Decision Making Authorities
- Formal process for resolving differences within the PSWGs
  - Formal variance process
- Enhance and formalize key partnerships (e.g., Air Force and other ranges, commercial launch service providers, etc.)

Program Development (continued)

Continuing Development/Implementation Led by KSC

- Drafting new ELV Payload Safety Program specific NPR
  - Safety Review Process and Technical Requirements
  - Coordinate with all Center/Working Group Representatives
  - Review and Approval of NPR via NODIS
  - Develop MOAs with 30/45th SW for concurrence on NPR
  - Ensure NPR written into contracts/agreements for ELV missions
  - Developing Website, Tools, Training ...
  - Implementation kick off activities with payload projects

Program Development (continued)

Tasking and FY06 Funding by QSM:

- KSC: ($300k) Safety Review Process Development, Overall Program
  - Manager: Cal Staubs, Technical Lead: Tom Palo, Contractor: SSR
  - Developing: Tools and Training Program for project management and personnel
  - Coordinating with Range and other partners
  - Program Website: www.ksc.nasa.gov/ELVpayloadsafety
  - Repository for applicable policy, requirements, standards, and guidance
  - Process schedules and checklist for use by payload projects
  - Status tracking of ELV payload projects
- GSFC: ($300k) Technical Requirements Development, Executive Team
  - Member: Karen Fisher
- JPL: ($200k) Input to all Program Development Activities, Executive Team
  - Member: Jim Lumsden
- GSFC: ($100k) ELV Payload Safety and Mission Success Conference

ELV Payload Safety Program Schedule

<table>
<thead>
<tr>
<th>2007</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDR DEVELOPMENT</td>
<td></td>
<td>▲</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPR ET REVIEW</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPR VQG REVIEW</td>
<td>▲</td>
<td></td>
<td>▲</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPR NOLOGO REVIEW</td>
<td>▲</td>
<td></td>
<td>▲</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Center NPR Familiarization</td>
<td></td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTATION</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>- Mission Phase-In</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>- Work Instructions</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
<tr>
<td>- Assessments</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
</tr>
</tbody>
</table>
NASA Payload Safety Policy

- Published in Chapter 3 of NPR 8715.3, General Safety Program Requirements, September 2006
- Applies to all payloads controlled by NASA
- Distinguishes:
  - Manned Space Flight Payloads: Payloads that fly on, or interface with a manned space launch vehicle, spacecraft, or entry vehicle
  - Unmanned Suborbital Payloads: Payloads that fly on an unmanned suborbital vehicle (e.g., sounding rocket, balloon, or experimental aeronautical vehicle)
  - Return-to-Earth Payloads: Payloads that will return to Earth for recovery or purposes other than disposal
  - ELV Payloads: Unmanned orbital and unmanned deep space payloads
- Establishes the NASA ELV Payload Safety Program

NASA ELV Payload Safety Program (continued)

NPR 8715.3

3.13.4.1 Payload Safety Policy. It is NASA policy to safeguard people and resources (including flight hardware and facilities) from hazards associated with payloads controlled by NASA and hazards associated with payload-related Ground Support Equipment (GSE) by eliminating the hazards or reducing the risk associated with each hazard to an acceptable level. To accomplish this policy NASA shall:

a. Establish and maintain technical and procedural safety requirements applicable to the design, production, flight area processing and testing, vehicle integration, flight, and planned recovery of NASA payloads.

b. Coordinate with U.S. or foreign entities that participate in NASA payload projects as needed to ensure compliance with all safety requirements that apply to each payload.

c. Incorporate all applicable safety requirements into the overall requirements for each NASA payload, the contracts for any related procurements, and any related cooperative or grant agreements.

d. Maintain an independent payload safety review and approval process designed to ensure that each NASA payload project properly implements all applicable safety requirements and to facilitate safety risk management appropriate to each payload.

NASA ELV Payload Safety Program Integration

Headquarters

Mission Directories

- Exploration
- Science
- Space Ops
- OSMA

ELV Payload Safety Program

Executive Team

Program Manager

Safety Review
Process Participants
(PSSWG)

Mission Centers
NASA ELV Payload Safety Program (continued)

NASA ELV Payload Safety Manager:
• Lead the NASA ELV Payload Safety Program and serve as the Agency focal point for all matters involving ELV payload safety...
• Develop and maintain Agency-level safety policy and requirements...
• Develop and administer the safety review and approval process...
• Provide payload projects with guidance on implementation of policy, requirements, and processes...
• Provide input and guidance... for development of... contracts, grants, and cooperative agreements...
• Report to the NASA Headquarters Office of Safety and Mission Assurance...
• Element of the HQ SMA Audits, Reviews, and Assessments program...

NASA ELV Payload Safety Executive Team:
• Element of HQ Office of Safety and Mission Assurance
• Functions to provide Agency-wide perspective and insight on ELV payload safety related activities
  – Members from appropriate NASA Centers designated by OSMA
• Assess payload projects/PSWG activities to assure NPR requirements are consistently implemented throughout Agency
• Assess early identification of payload safety concerns and any applicability to other NASA payloads
• Report to the NASA HQ OSMA on ELV payload safety concerns...
• Participate in the NASA Safety and Mission Success Review (or equivalent)

Executive Team Lead: (proposed in new NPR)
• Establish and document the activities and processes needed for the Executive Team to satisfy its responsibilities
• Ensure coordination with all Executive Team members on all Executive Team decisions
• Serve as the approving (signing) official for the Office of Safety and Mission Assurance for any variance to a requirement contained in the NPR

Center Director: (Responsible for a Payload, Processing Facility, or Launch Site)
• Establish Center-level processes and requirements to ensure Agency policy and requirements are satisfied for each ELV payload project that uses the Center’s resources
• Support safety assessments of ELV payload activities and respond to all findings and recommendations, for which the Center is responsible
• Ensure that Center personnel involved in payload projects complete training offered by ELV Payload Safety Program
• Ensure that Center support, including GSE and facilities used in processing, testing, vehicle integration, launch, and planned recovery of NASA ELV payloads comply with applicable NASA and Center technical and procedural requirements (proposed in new NPR)
Mission Success Starts With Safety

NASA ELV Payload Safety Program (continued)

**Center S&MA Director**: (proposed in new NPR)
- Ensure implementation of Agency policy and requirements for each ELV payload project that uses the Center's resources in coordination with the NASA ELV Payload Safety Manager
- Provide each payload project with safety engineering, safety analysis, and other safety expertise needed to ensure the project successfully completes the safety review and approval process
- Ensure that processes exist and assessments are conducted to ensure compliance with this NPR and the safety of activities within the scope of their authority

**ELV Payload Project Manager**: (proposed in new NPR)
- Ensure that funding and other resources are allocated for payload projects to satisfy all aspects of the NASA ELV Payload Safety Program...
- Ensure that the payload project's timeline provides for compliance with the established payload safety review and approval process
- Establish and implement any project-level processes and requirements needed to satisfy safety requirements and successfully complete the payload safety review and approval process
- Ensure all personnel ..., possess the necessary certification, training, judgment and abilities (proposed in new NPR)
- Prepare and approve any variance to a safety requirement...

**NASA Contract, Grant, Cooperative Agreement, or Other Agreement Officer**: (proposed in new NPR)
- Coordinate with the NASA ELV Payload Safety Manager and Payload Project Managers to ensure that all applicable safety and mission assurance requirements necessary for payload safety are incorporated into the contracts and agreement(s) governing each payload...

**Proposed NPR 8715.xx ELV Payload Safety Program**

**CHAPTER 1 Program Overview**
- Payload Safety Policy (consistent with general policy in NPR 8715.3)
- Roles and Responsibilities (moved from NPR 8715.3 and updated)
- Variance Process (consistent with NPR 8715.3)

**CHAPTER 2 Safety Review and Approval Process**
- Payload Safety Working Group
- Roles and Responsibilities
- Flow of Activities and Deliverables
- Content of Deliverables

**CHAPTER 3 Payload Design and Ground Operations Safety Requirements**
- General Payload Flight Hardware and GSE Safety Design
- Safety Critical Software
- Ground Operations
- Payload Flight Hardware and GSE

**Goals**
- Assure the appropriate representation and involvement of all organizations that support the mission.
- Identify and resolve any safety concerns as early as feasible during the project timeline.
- Assure that the project obtains the formal approval of all safety authorities for the mission (internal and external to the Agency).
Payload Safety Working Group Membership

**Mission PSWG**

- Launch Vehicle Contractor Safety
- Air Force 45/50 BW Range Safety
- Mission Center NASA & Contractor Safety
- Payload Organization Safety Engineer
- System or Subject Matter Expert (As Needed)
- Payload Project Manager (cont.):
  - Ensure all project personnel involved in the review process are experienced and trained as needed
  - Ensure that the payload organization plans for and fully participates in all safety review and approval process activities
  - Concur on all safety review and approval process deliverables prior to submittal to the PSWG
  - Ensure that all approved safety plans and procedures are implemented
  - Notify the NASA ELV Payload Safety Manager of the new project and provide contact information for the appointed Payload Organization Safety Engineer
  - Ensure safety status and any safety concerns are presented at mission design reviews, including the Preliminary Design Review and Critical Design Review

Payload Project Manager:
- Ensure that a Payload Organization Safety Engineer is appointed no later than the Confirmation Review or 90 days prior to the PDR
- Coordinate with the Payload Organization Safety Engineer to establish the PSWG and include the following members as applicable to the mission:
  - NASA Payload Organization Safety Engineer
  - Payload contractor safety representative
  - NASA Launch Services Division Safety Engineer
  - Launch vehicle contractor safety engineer
  - Payload processing facility safety representative
  - Range safety organization representative(s) responsible for launch
  - NASA Launch Services Program Launch Site Integration Manager (invited participant)

Executive Team:
- For each mission, Team shall designate a member to serve as the Team's primary interface for the safety review and approval process
- Develop a mission specific assessment plan prior to the Payload Safety Introduction Meeting.
- Review all safety review submittals, participate in safety review activities as needed, and approve any alternative approaches for satisfying safety requirements
- Coordinate on guidance provided to a PSWG that has not been previously documented as an official ET position.
Payload Organization Safety Engineer (cont.):
- Ensure that released technical operating procedures are reviewed and approved by facility safety and other responsible organizations
- Participate in Payload Design Reviews presenting mission safety status
- Ensure that the PSWG and Executive Team are notified whenever a mishap or close call takes place involving their payload
- Mishap reporting will be conducted in accordance with contractual documentation and NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping

PSWG Members:
- Participate in the safety review/approval process
- Assist the payload project to comply with applicable safety requirements
- Within their scope of authority, assess for safety the payload design, fabrication, testing, integration, pre-launch and launch operations, planned recovery of the payload, and mission specific GSE, and interfaces with other supporting GSE, facility systems, and launch vehicle systems and GSE
- Review and comment on all payload safety review deliverables and meeting minutes
- Assess and concur with any variance to a safety requirement within their scope of authority
- Coordinate with the Executive Team and others as needed to resolve payload safety concerns

PSWG Members (cont.):
- Coordinate with other PSWG members to identify a PSWG chairperson
  - Note: A member of the responsible NASA launch site safety organization typically serves as the PSWG Chairperson. Depending on the mission specifics, there may be advantages to having a PSWG representative from one of the other NASA organizations involved in the mission perform this function. Example, for missions involving significant contributions from international partners, communications and coordination efforts may be more easily facilitated if the Payload Organization Safety Engineer performs as the PSWG Chairperson. A Co-Chairperson may also be appointed if deemed necessary for any mission.

PSWG Chairperson:
- Schedule and conduct PSWG meetings
- Ensure that PSWG activities and decisions include the collective input and participation of all PSWG members
- Ensure PSWG participation, as required, at payload/launch vehicle integration working group meetings (e.g. Ground Operations Working Group (GOWG), Mission Integration Working Group (MIWG))
- Facilitate the signing of the Certificate of Safety Compliance by appropriate PSWG members, compile any constraints, and ensure delivery to the ELV Payload Safety Program Manager
- Ensure that all mission support and safety related documents are filed for access by the PSWG members, Executive Team and the NASA ELV Payload Safety Manager
Mission Success Starts With Safety

Proposed NPR 8715.xx, Chapter 2
Safety Review and Approval Roles and Responsibilities

NASA Launch Services Program Manager:
- Notify the PSWG of Ground Operations Working Group and Ground Operations Review activities
- Ensure that the NASA Launch Services Division Safety Representative is notified of any payload/launch vehicle interface concerns
- Ensure launch vehicle and commercial payload processing facility contracts provide the provisions of the NPR

NASA ELV Payload Safety Manager:
- Track the status of each payload project as it proceeds through the safety review/approval process and provide guidance on the associated activities, tools, and deliverables as needed
- Issue a letter indicating that the project has successfully completed the payload safety process

Chapter 2.4 Overview
Identifies the required safety documentation, safety reviews, and sequence of submittal of the associated deliverables
NPR 8715.xx will define more specifically:
- Topics to be covered in required safety briefings
- Support materials for briefings
- Submittal dates for safety documentation

Tailored Safety Requirements
Tailored Safety Requirements result from the process of reviewing requirements to ensure applicability and compliance by the project, as written, or whether the project will achieve an equivalent level of safety through an acceptable alternative requirement.
- Joint activity by all PSWG members
- Identifies applicable requirements
  - NASA, Range Safety, other Government and consensus standards
  - Documents the interpretation of requirements or applicability of a requirement to a specific mission activity
- Implements lessons-learned as applicable
- Consolidates interim policy/guidance/requirements
- Documents the rationale for addition/deletion/change in requirements
- Resulting Tailored Requirements are a safety requirements for a specific mission
Tailored Safety Requirements (cont’d)

The Tailoring process aids in identifying potential non-compliances and safety issues
- Interpretation or compliance assessment performed early
- Alternative approaches that provide an equivalent level of safety determined and finalized
- Early resolution of issues reduces risk, enhance safety, and minimizes impact to project

NPR 8715.xx will define the format for the tailored requirements, approval process, and provide by Attachment a baseline of tailored requirements.

Payload Safety Introduction Briefing

Payload Safety Introduction (PSI) Briefing is the introduction of the mission by the project, with emphasis on safety aspects and issues
- First formal meeting with the PSWG and Executive Team
- Includes briefing of preliminary hazard analyses, Hazard Reports, Systems Safety Program Plan, and review of Draft Tailoring

NPR 8715.xx will expand the typical agenda to include project lifecycle safety issues and the time period for the PSI to occur.

Payload Safety Introduction Briefing (cont’d)

Topics include:
- Applicable compliance documents (new)
- Contractual requirements and relationships (new)
- Systems Safety Program Plan
- Description of payload, instruments, GSE, operations
- Presentation of preliminary Hazard Reports (new)
- Spacecraft failure modes/probability during ground operations
- Discussion of potential non-compliances
- Description of Planned studies and analyses
- Description of flight path and launch vehicle options

Payload Safety Introduction Briefing (cont’d)

Topics include (cont’d):
- Description of processing flow, schedules, milestones
- Identification of facility requirements
- Description of launch vehicle interfaces and mission unique GSE and operations at the launch pad
- Contingency Operations (new)
- Planned recovery activities (new)
- Pre-launch mishap response and reporting (new)
- Draft Tailored Requirements with critical assumptions
- Recommendations for future TIMs, working groups, studies, etc.

Systems Safety Program Plan (SSPP)

Systems Safety Program Plan is a comprehensive description of how project safety activities will be executed to meet safety requirements.
- Systems Safety Program Organization
  - Role, responsibility, and qualification of key safety personnel
  - Review and approval authority
  - Interfaces with other disciplines
  - Lines of communication with management

Systems Safety Program Plan (cont.)

- System Safety Program Milestones
- System Safety Data
  - Deliverables/non-deliverables
- Systems Safety Integration
  - Identifies interfaces with other external organizations and safety authorities

NPR 8715.xx will require increased emphasis on defining how safety activities are integrated throughout the project lifecycle.
Hazard Reports

Hazard Reports identify the potential hazards of a system, and define the causes, controls and verifications and assessment of risk:
- Report required for each unique hazard
- Drafts required at PSI based on payload conceptual design and planned operations (new)
- Reports address each operational phase and/or facility (new)

Hazard Report Format

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Design Review Presentation

Safety activities and issues are presented at the CDR & PDR by the Payload Organization Safety Engineer:
- 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 issues
- Risk matrix chart (new)

Safety Data Package (SDP)

Safety Data Package 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:
- Includes hazard reports, safety assessments, inhibits, and mitigations
- Together with the Ground Operations Plan, it is one of the media through which prelaunch safety approval is obtained.

Ground Operations Plan

Ground Operations Plan (GOP) provides a detailed description of hazardous and safety critical operations for processing a payload and its associated ground support equipment:
- Includes analysis of project-supplied GSE, description of planned operations, Operating and Support Hazard Analysis, procedure descriptions and task summaries, and contingency, training, and emergency response plans
- Together with the Phase III Safety Data Package, it is one of the media through which prelaunch safety approval is obtained.
Mission Success Starts With Safety

Ground Operations Plan (cont.)

- If operations occur at a NASA facility, or facility where NASA personnel controls the operation, or are required to perform a task during an operation, applicable portions of the GOP and hazard reports are to be approved NLT 30 days prior to hardware arrival. (new)

NPR 8715.xx expands the scope of ground operations requirements to include all NASA processing locations; GOP is also identified as the mechanism for submitting GSE and operations data to provide for earlier (than SDP) approval requirements.

- Issue: AFSPCMan 91-710 requires GOPs to be submitted 45 days prior to design reviews; NPR 8715.xx proposes 30 days.

Phase III Payload Safety Review Presentation

Phase III Payload Safety Review is a review of safety activities and issues, and is presented by the Payload Organization Safety Engineer (new)

- Presented to PSWG and Executive Team prior to pre-ship review
- Summary of safety activities and reviews, and status of any in-process safety related work
- Overview of non-compliances and risks
- Provides a verification that all safety requirements and activities have been met, or review of plan to bring project into compliance
- Status of SVTL Items
- Certificate of ELV Payload Safety Compliance is signed (new)

Safety Verification Tracking Log (SVTL)

Safety Verification Tracking Log identifies the required verifications from the Hazard Reports that are constraints to payload activities and operations.

- Required to be developed from hazard reports
- Updated as required if open verifications exist that are constraints to payload processing
- After payload arrival at the launch site processing facility, updated at least weekly
- Reviewed at the Phase III Final Safety Review (new)

Technical Operating Procedures

Technical Operating Procedures provide a step-by-step description of the manner in which hazardous / safety critical operations will be accomplished. Procedure approval is required prior to the start of a hazardous / safety critical operation.

- All procedures are identified in the GOP, providing substantiation of classification, task summaries, and OSHA
- Released hazardous procedures are to be submitted to safety approving authorities (for KSC, 55 days before use; 10 days on-the-shelf)

NPR 8715.xx will define the technical operating procedure requirements for submittal, content, format, etc. that are currently in place

Website Demonstration

ELV PAYLOAD SAFETY PROGRAM
Mission Success Starts With Safety

Website Demonstration

ELV PAYLOAD SAFETY PROGRAM

Mission Success Starts With Safety

Website Discussion

• Safety Data Package Management
  - Options
    1. Program Office as part of normal data management/config
    2. LSP via their KSC website: https://elvprogram.ksc.nasa.gov
    3. Agency ELV Payload Safety Office via this website: http://www.ksc.nasa.gov/elvpayloadsafety
    4. PBMA website: http://pbma.nasa.gov
  - Issues/Concerns
    • Need to select and develop process
    • Assured access for all "partners"
    • Website support/cost – government vs contractor
    • In place or development required
    • Reliability
    • Customer Friendly

Mission Success Starts With Safety

Website Discussion

PROs

PBMA
- Developed
- Funded by HQ
- Support in place
- Security functions

EPSP
- Can design in function
- Tech Docs secure
- Exec Team coordinated

SV Contr
- Use contr current system
- Less duplication of effort
- More current infodata

CONs

PBMA
- Off-site control/maintenance
- Unknown reliability/dependence
- No access when system is down

LSP
- Access may be an issue
- User-friendly?

EPSP
- Development required
- May need additional manpower

SV Contr
- Less govt control over data
- Dependent on contractor
- Require PO oversight?
- May charge for services

Mission Success Starts With Safety

Website Discussion

Agency ELV Payload Safety Office Website Will Keep:
- Safety Data Package Archives
- Payload ES&H Lessons Learned
- Variances
- Forms/templates

Mission Success Starts With Safety

Proposed NPR 8715.XX, Chapter 3
Design and Ground Operations Requirements

Development:
- Consistent with the general system safety policy of NPR 8715.3
- Capture NASA and Air Force requirements as tailored for NASA ELV missions
- Obtain Air Force by-in on the use of these requirements for launches at the Eastern and Western Ranges
Goal: Consistent interpretation and implementation of design requirements Agency-wide

Approach:
- Provide clear requirements, associated definitions, and guidance, including examples applicable to NASA ELV payload projects
- Address:
  - Hardware Design Inhibits/Failure Tolerance
  - Design for Minimum Risk
  - Design for High Reliability

Hardware Design Inhibits/Failure Tolerance
- The hardware design of each payload system (including flight hardware and associated GSE) that controls a hazard shall incorporate a minimum number of design inhibits against each credible hazardous system failure (EXCEPTION: Design for High Reliability)
  - A hazardous system failure is a failure of the overall system, subsystem, or component that can result in injury to people or loss of resources, including damage to flight hardware or facilities
  - A hazardous system failure is credible if it can occur and is reasonably likely to occur. A quantitative guideline is a probability of occurrence \( p \leq 10^{-3} \)
  - Failures of components that meet specific Design for Minimum Risk requirements are not considered credible

Required Minimum Number of Design Inhibits:
- Dependent on the potential consequence(s) associated with each credible hazardous system failure
- The design of a system that controls a hazard shall incorporate no less than:
  - Three design inhibits (dual failure tolerant) against each credible system failure that can lead to loss of life
  - Two design inhibits (single failure tolerant) against each credible system failure that can lead to injury of people or loss of resources, but not loss of life

Determination of Credible Hazardous System Failures:
- Coordinated effort between payload organization and the PSWG
- Account for potential failure of all system components that do not meet specific Design for Minimum Risk requirements
- Without consideration of any procedural hazard controls
- If dependent on quantitative probabilistic analysis:
  - Formal written probabilistic risk assessment
  - Incorporate system and component reliability data
  - Account for uncertainty in input data and any models
  - Subjected to peer review and approval

Determination of Required Number of Design Inhibits for each Credible Hazardous System Failure:
- Coordinated effort between payload organization and the PSWG
- Account for both immediate and long term potential injury or illness effects associated with each hazard
- If based on an assessment that the hazard level will not exceed an injury/fatality threshold:
  - Formal written technical analysis
  - Demonstrate that the hazard level will not exceed the injury/fatality threshold
  - Subject to peer review and approval
- Design inhibits shall consist of electrical and/or mechanical hardware and be independent of any other inhibit or hazard control

Design Inhibits:
- Shall consist of electrical and/or mechanical hardware
  - An operator control is not considered a design inhibit
  - Implementation of operator controls may be used as justification for a variance to the requirements for design inhibits
- Each design inhibit shall be independent of any other inhibit or hazard control
- Design inhibits that protect against a specific hazardous system failure shall have design and/or implementation differences between them to protect against a common cause failure of the inhibits
- Each design inhibit shall be verifiable after installation or through a process of pre-installation testing and implementation of written procedures that ensure the inhibit's integrity during and after installation
- The system design shall allow for the system to be brought to a safe state in the event of the loss of a design inhibit.
Design for Minimum Risk

- Components may be eliminated from consideration as a potential source of a credible hazardous system failure by complying with requirements that have been developed specifically for each such component.
  - For example: structures, pressure vessels, pressurized line and fittings, and functional pyrotechnical devices.
- Proposed NPR 8715.XX, Appendixes D and E identify specific components and provide the associated Design for Minimum Risk requirements.
- Any proposed use of Design for Minimum Risk for a component not specifically addressed in Appendix D or E requires approval by the NASA ELV Payload Safety Executive Team in coordination with any other responsible technical authority.

Design for High Reliability (consistent with NPR 8715.3)

- A system may be exempted from the requirements for design inhibits if the system has high reliability that is verified by a formal reliability analysis:
  - Using accepted data in which uncertainties are incorporated
  - Subject to the requirements of NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
  - Regarding ELV payload, high reliability is defined as ≥ 0.999 with 95% confidence (not specified in NPR 8715.3)
- Approach might not be acceptable to all safety authorities involved in a NASA ELV payload mission
  - Approval to use this approach must be obtained from all PSWG members as early as possible in the project timeline.

Safety Critical Software:

- Payload systems that incorporate safety critical software that are used to support NASA missions shall have an independent verification and validation plan in accordance with NPD 8730.4, Software Independent Verification and Validation (IV&V) Policy.

Ground Operations:

- Safety requirements applicable to ground operations associated with flight-area processing (including testing and vehicle integration) and any planned recovery of payloads provided in NPR 8715.XX, Appendix D (in work).
- Requirements tailored for NASA ELV payload projects and augmented with implementation guidance NASA projects.
Proposed NPR 8715.XX, Chapter 3
Flight Hardware and GSE Safety Design (continued)

- Ground Operations (Appendix D) (cont.)
  - Material Handling Operations
  - Acoustic Hazards
  - Pressurized Systems & Vacuum Systems
  - Ordnance
  - Electrical System Operations
    - Grounding
    - Bonding
    - Battery Operations
    - Energized systems
    - Launch Operations

Ground Operations (Appendix 0) (cont.)
- Material Handling Operations
- Acoustic Hazards
- Pressurized Systems & Vacuum Systems
- Ordnance
- Electrical System Operations
- Grounding
- Bonding
- Battery Operations
- Energized systems
- Launch Operations

NPR 8715.xx Technical Safety Requirement – Development Approach

Goals
- Develop a NASA ELV payload safety document
  - Capture NASA requirements, interpretations, processes
  - Include NASA's role in evaluating and data approval
  - Increase commonality among NASA Centers and with Ranges
  - Ranges' acceptance of tailored requirements in lieu of AFSPCMAN 91-710

Approach
- Use AFSPCMAN 91-710 as baseline document
  - Strong heritage and comprehensive
  - Compliance required for processing and launch

Tailored AFSPCMAN 91-710 becomes Appendix E of NPR 8715.XX

Tailoring Approach Details
- Maintain 91-710 chapter layout and paragraph numbering, to extent possible
- Tailoring focuses on applicable payload requirements and credible contingencies
  - Capture NASA requirements and interpretations
  - Resolve longstanding issues
  - Continue to utilize 'text boxes' to propose design solutions
  - Use applicable documents sparingly as a method to identify specific requirements
  - Maintain 'stand alone' documentation philosophy for ease of mission specific tailoring
  - Reference/applicable documents identified for informational purposes
  - Change the unilateral Range-required approval of specific requirements to include all safety approving authorities/FPSWO
  - Add NASA Requirement Identifier after each specific requirement
  - Tailor Attachment I to provide references to data matrices

Tailoring - Example

12.1.3.3. If the Range User and Range Safety approving safety authorities decide that depressurizing and/or offloading the pressure systems of a mated spacecraft is prohibited at the launch pad, spacecraft offload-demating procedures shall be approved by Range Safety prior to use. (Requirement)

Rationale: Clarify requirement, as an approving authority would also be the NASA Launch Services Division Safety Office. Replace 'offload' with 'demating', as offload procedures are required to be approved prior to spacecraft mating; contingency demating procedures may have to be tailored to address the circumstances of the contingency.

Tailoring - Example (cont'd)

12.1.3. Flight Hardware Pressure System Offloading.

12.1.3.1. For contingency safety operations, hazardous pressure systems shall be designed so that depressurization and drain fittings are accessible and do not create a personnel or equipment hazard for offloading hazardous fluids at the launch complex, commodities. (Requirement)

Rationale: The commodity to be offloaded could be non-hazardous, or not a fluid; applicability at the launch complex was deleted, as capability to offload is also required at the payload processing facility.

12.1.3.2. The philosophy to be adopted for Propulsion system design shall permit the offload of these pressure systems at any point after pressurization or loading, including the ability to offload all systems at the launch pad without demating of the spacecraft from the launch vehicle or any other disassembly of vehicle systems. (Requirement)

Rationale: Because of the hazard potential, the ability to offload is a requirement, not a design goal.
Tailoring Example — Text Box (cont’d)

System design and contingency planning shall permit for safe movement of the payload to a payload processing facility. Planning shall address the worst-case scenario.

Accessibility through payload fairing doors is the desired approach. Verification/validation of the design for accessibility is best achieved through a high fidelity model, mock-up of hardware, GSE, tooling, PPE, etc., or by demonstrating similarity to accepted design and processes.

Coordination with the launch vehicle contractor is necessary for allowable payload fairing door size and placement, operational support, and ability to perform contingency support in hazardous and/or explosive environments.

Rationale: Design solution added to ensure early coordination and planning for access to hardware in the event of a leak contingency.

Linking Tailoring to Data Requirements

15.2.1.4 Plastic materials that may pose a hazard because of hypergolic ignition breakthrough shall be treated in accordance with the requirements described in PRA 95E (I.3.1). Procedures for Calculating Decomposition Rate, Evaluation Reaction Method (Requirement).

15.2.2.1.4 Hypergolic The HS-APP may require the testing of materials whose hazard properties are not well defined (Requirement).

16.6 Hazardous Material Data Requirements. Hazardous material data requirements are in accordance with an identified in Attachment 1 (A.2.2.1.5).

AFSPC-4 91-710 (T) Vol 3, Attach 1

Linking Tailoring to Data Matrices

NPR 8715.xx, Appendix E (T) (Vol) Requirements

Safety Data Matrix — EGSE Example

Safety Data Matrix — Pyro and NEI Devices

Inhibit Status Summary

Operational Phase / Event

System (Inhibit) Ref# | Inhibit Status |
<table>
<thead>
<tr>
<th align="left">:-----------------</th>
<th>----------------</th>
</tr>
</thead>
<tbody>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td align="left">:-----------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
Mission Success Starts With Safety

Safety Data Submittals

Impact of Late Deliverables
- Increases the potential of a safety issue requiring resolution late in safety review process
- Mission may not be able to implement an optimum solution to resolve (engineering, science and safety impact)
- Resulting risk may be unacceptable or higher than desired
- Impacts the safety review process
- Cost and schedule impacts trickle-down throughout project and support
- Noncompliance to Range Safety Requirements

Impact to Safety and Risk
- Safety requirements may not be implemented (fully) if discovered late, or after critical milestones in the design phase
- Required design changes may be constrained
  - Engineering capability or feasibility
  - Cost
  - Schedule
  - Mission goals
- Effectiveness (if instituted) of engineering solutions
  - Safety tradeoffs may result
  - Integrated hazards

Impact to Safety and Risk (cont’d)
- Additional hazard mitigations may result
  - Necessary inhibits and monitoring capability may not be optimal due to technical limitations
  - Additional cost may be incurred to implement
  - Impact to schedule; support requirements
  - New or revised of procedures may be required
  - Implementation may still result in level of risk
- Potential increase in risk
  - Compromise to spacecraft and launch vehicle safety, systems, facilities, and GSE
  - Risk to processing and pad personnel; public safety
  - Risk to mission success

Impact to Safety Review Process
- Late submittal reduces allocated safety review time
  - Increases the potential of omission/oversight
  - Cause further delays if additional data/clarification is needed
- Systems, safety and mitigation changes add to the review process
  - Additional analysis/test/reports required
  - Ensure adequate mitigation
  - Demonstrate an equivalent level of safety

Impact to Safety Review Process
- Disrupts the planned work schedule of reviewers
  - May infringe on data review required for other missions
- Potentially could result in submittal of a Mission Risk, with associated briefings, documentation, and tracking
- Affects the release of other mission documents (e.g., Interface Control Document, Launch Site Support Plan)
  - Safety inputs are required
  - Impacts the OPR’s schedule for document development

Impact to Safety Requirements
- Noncompliance to NPR
  - NASA policy requires a variance to be submitted
    - Missed delivery milestones
    - Potential for an additional non-compliance to a technical requirement
    - Impact to payload project (associated cost and schedule) for variance preparation, briefings, coordination
    - Cost and time for variance review/approval by OBMA, ELV Payload Safety Program, Center Director(s), PSWG, Range, etc.
    - Terms of acceptance may include additional mitigations, process/procedural changes, or non-concur
- Noncompliance to other requirements (e.g., Range, OSHA)
Mission Success Starts With Safety

Impact to Launch Vehicle Contractor

- Spacecraft safety data package is needed for preparation of the launch vehicle mission-specific safety data package
  - Contract deliverable requirement
- May require unanticipated support requirements, or modifications to vehicle / pad activities
  - Mission-specific GSE requirements
  - Procedural changes for pad operations
- Changes to established procedures/processes or need for out-of-sequence work increases risk
  - Schedule changes
  - Support availability

Corrective Action - Goals

- Ensure that safety and ELV Payload Safety Program objectives are achieved
  - Safety is adequately performed in a timely and efficient manner consistent for all missions
  - Mission objectives are met
- Minimize cost and schedule impacts
- Ensure requirements and associated corrective actions are defined and implemented consistently
- Required actions are value-added
  - Provide an equivalent means to ensure safety is appropriately in-step with mission activities, not a paperwork exercise

Corrective Action - Options

- Potential options to achieve safety confidence and manage risk increase in severity:
  - 'Get-well' schedules from Project Management for milestones / deliverables
  - Risk process / watch item used to monitor status and resolution
  - Variance (Level I)
  - Formal project assumption of risk / cost / schedule impact due to potential 'safety-driven' changes
  - 'Delta' safety reviews
  - System Engineering briefings to provide data
  - Additional interim safety data submittals
  - Variance (Level II)
  - Audits of Engineering Data
  - Project Milestone Reviews (PDR, CDR, FRR, LRR, etc.) are kept 'OPEN' to completion
- Goal is to prevent a delay in payload shipping, processing, transportation to the pad, or launch

Implementation Methods

Example #2: Late submittal of hazardous technical operating procedure.
- Considerations:
  - Extent of delinquency; frequency
  - Impact to processing if safety approval is delayed
  - Criticality and probability of potential safety risk
  - Remedial action required: Compliance (delay performing operation), or Variance (level I) required; Project awareness/assumption of risk; Occurrence tracked by Payload Safety Program

Process Improvements

- Data Requirements and Development
  - Prioritization of safety data requirements to a specific submittal phase
  - Develop data matrices
  - Consistent format and content defines the standard for assessment and expedites compilation of required data
- Document Submittal
  - Electronic transmittal will eliminate delay in data transfer
- Variance Approval Process
  - Potential for approval of certain variances to be delegated to the SMA Director
  - Approval process for Project and ELV Payload Safety Program would not change
- Propose Change to Range Safety Requirements
  - Reduce required delivery date of safety data packages from 45 days prior to design review, to 30 days.
**Summary**

- Late submittals can have a wide range of impacts:
  - Technical, cost, and schedule impacts to project and safety activities
  - Impacts can flow to other organizations and other missions
- Design and safety activities have to be synchronized:
  - Mission engineering milestones are established by project
  - Safety involvement and input need to be timely
  - Safety-related requirements/changes imposed late have a higher likelihood of major impact
- Process changes can provide some improvement:
  - Resolutions (data preparation and submittal, variance approval, etc.) will require a change to current way of doing business
  - Other factors...Training? Communication? Staffing? Safety culture?
- Alternative (back-up) data sources need to be identified in advance, and be utilized when primary sources can not deliver as required.
  - Risks must be acknowledged by Project Management

**Mission Success Starts With Safety**

**Proposed NPR 8715.XX, Chapter 1**

**Variance Process**

Consistent with NASA safety variance requirements in NPR 8715.3:
- A variance consists of documented and approved permission for relief from an established SMA requirement
- Exception authorizes permanent relief from a specific requirement and may be requested at any time during the project life cycle
- Deviation authorizes temporary relief in advance from a specific requirement and is requested during the formulation/planning/design stages
- Waiver authorizes temporary relief after the fact from a specific requirement and is requested during the implementation of a project or operation to address situations that were unforeseen during design or planning
- Each variance type may involve approval of alternative means that provide an equivalent or lower level of risk or formal acceptance of increased risk (inconsistent with AF Range policy)
- Approval authorities vary based on the type/level of requirement (design/technical, administrative/milestone, HQ/local) and on whether approval includes acceptance of increased risk

**"New" Waiver Process**

- Non-conformance – the state or situation of not fulfilling a requirement
- Waiver - a written authorization allowing relief from a requirement (Note: The relief can be temporary)
- Exception - A written authorization granting permanent relief from a specific, non-applicable requirement
- Variance - This term has specific significance in the administration of OSHA requirements and will only be used in relation to OSHA regulations and requirements
- Deviation - encompassed by the terms exception and waiver

**Training Program**

2 Courses to be developed and offered:
- ELV Payload Safety Process
  - 1 - Day process and requirements course for program managers and center S&MA managers
- ELV Payload Safety Analysis
  - A detailed 3 - Day process and analysis course with panel and working group exercises for PSWG members

**The PSWG and the Executive Team:**

- Ensure request and accompanying data are correct and complete
- Ensure any residual risk is properly characterized (quantitatively or qualitatively) and any increase in risk is properly identified
- Assess effects on requirements or other ELV payload projects and initiate any actions needed to address such effects
- Ensure request identifies all needed signatures for approval, concurrence, and any risk acceptance
  - NASA and external approval authorities
  - Technical authority (or equivalent) responsible for the requirement
  - Center Directors or other NASA officials responsible for people or property exposed to any risk associated with the variance
- The Chief of OMSA may delegate his approval authority for HQ level NPR safety variances
ELV Payload Safety Process – 1 day course
- System Safety Requirements Overview
- Management Roles & Responsibilities
  - Safety Requirements in Contracts
  - Resources (Budget/Manpower)
  - Reviews & Approvals
  - Mission Assurance & Personnel Safety
- ELV Payload Safety Review and Approval Process
  - NPR Chapter 2 Requirements
  - Additional Roles and Responsibilities (PSWG & others)
  - Deliverables & Schedule
  - NPR Chapter 3 Payload Design and Ground Operations Safety Requirements Summary
  - Requirements
  - Format
  - Examples

ELV Payload Safety Analysis – 3 Day course
- Payload Mission Life Cycle
- Roles & Responsibilities
- Payload System Safety Unique Requirements
- Compliance Documents
- Process Requirements
  - Phase reviews
  - Variances
  - Approval/certification
- Payload Design Requirements
- Payload Ground Processing Requirements
- Requirements Verification

ELV Payload Safety Analysis – 3 Day course (cont.)
- Technical Operating Procedures
- Deliverables
  - Schedule
  - Content
  - Forms
- Presentations
  - Phase I, II, III Safety Reviews
  - SARR/MARR
- Launch Site "Protocol"
  - Communications/Coordination
  - Anomaly & mishap reporting
- Communication Interfaces
- Issue Resolution
- Lessons Learned

Questions or Comments?
Action Items
**Title and Subtitle:** NASA ELV Payload Safety Program Information Exchange

**Author(s):**
- Calvert A. Staubus
- Thomas E. Palo
- Michael Ooook
- Shawn T. Donovan

**Date:** 23-02-2007

**Abstract:**
This presentation details the Expendable Launch Vehicle Payload Safety Program in its development and plan for implementation. It is an overview of the program's policies, processes, and requirements.

**Subject Terms:**
- PSWG - Payload Safety Working Group

**Security Classification of:**
- Report: U
- Abstract: U
- This Page: U

**Limitation of Abstract:**
- Number of Pages: 14