NASA/TM–2015-218676/Volume II
NESC-RP-14-00929

Review of Exploration Systems Development (ESD) Integrated Hazard Development Process

Appendices

Michael D. Smiles/NESC
Langley Research Center, Hampton, Virginia

Michael P. Blythe
Johnson Space Center, Houston, Texas

Bohdan Bejmuk
Analytical Mechanics Associates, Houston, Texas

Nancy J. Currie/NESC
Langley Research Center, Hampton, Virginia

Robert C. Doremus
Johnson Space Center, Houston, Texas

Jennifer C. Franzo
Stennis Space Center, Mississippi

Mark W. Gordon
Kennedy Space Center, Florida

Tracy D. Johnson
Marshall Space Flight Center, Huntsville, Alabama

Mark M. Kowaleski
Glenn Research Center, Cleveland, Ohio

Jeffrey R. Laube
The Aerospace Corporation, Houston, Texas

January 2015

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question to help@sti.nasa.gov

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2015-218676/Volume II
NESC-RP-14-00929

Review of Exploration Systems Development (ESD) Integrated Hazard Development Process

Appendices

Michael D. Smiles/NESC
Langley Research Center, Hampton, Virginia

Michael P. Blythe
Johnson Space Center, Houston, Texas

Bohdan Bejmuk
Analytical Mechanics Associates, Houston, Texas

Nancy J. Currie/NESC
Langley Research Center, Hampton, Virginia

Robert C. Doremus
Johnson Space Center, Houston, Texas

Jennifer C. Franzo
Stennis Space Center, Mississippi

Mark W. Gordon
Kennedy Space Center, Florida

Tracy D. Johnson
Marshall Space Flight Center, Huntsville, Alabama

Mark M. Kowaleski
Glenn Research Center, Cleveland, Ohio

Jeffrey R. Laube
The Aerospace Corporation, Houston, Texas

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

January 2015

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Review of Exploration Systems Development (ESD) Integrated Hazard Development Process

Volume 2: Appendices

November 20, 2014

Table of Contents

Appendix A. Interviews Conducted and Documents Reviewed

Interviews conducted by the assessment team included:

- Exploration Systems Development (ESD) personnel:
  - Integrated Hazard Analysis Working Group (IHAWG) Chairman
  - System Safety Functional Area Lead
  - Chief Safety and Mission Assurance (S&MA) Officer (CSO)
  - Crew Survivability Integrated Task Team (ITT) Lead
  - Multi-Purpose Crew Vehicle (MPCV)/Space Launch System (SLS) Abort Integration Team (MSAIT) ITT Lead
- Stakeholders:
  - ESD Chief Engineer – Paul McConnaughey
  - NASA Chief Engineer – Ralph Roe
  - Chief, S&MA – Terry Wilcutt
  - Director, NASA Engineering and Safety Center (NESC) – Tim Wilson
  - ESD Deputy Associate Administrator – Dan Dumbacher
  - ESD Assistant Deputy Associate Administrator – Bill Hill
  - Former Chief, S&MA, Current Aerospace Safety Advisory Panel Member – Bryan O'Connor

ESD and Program documentation reviewed by the assessment team included:

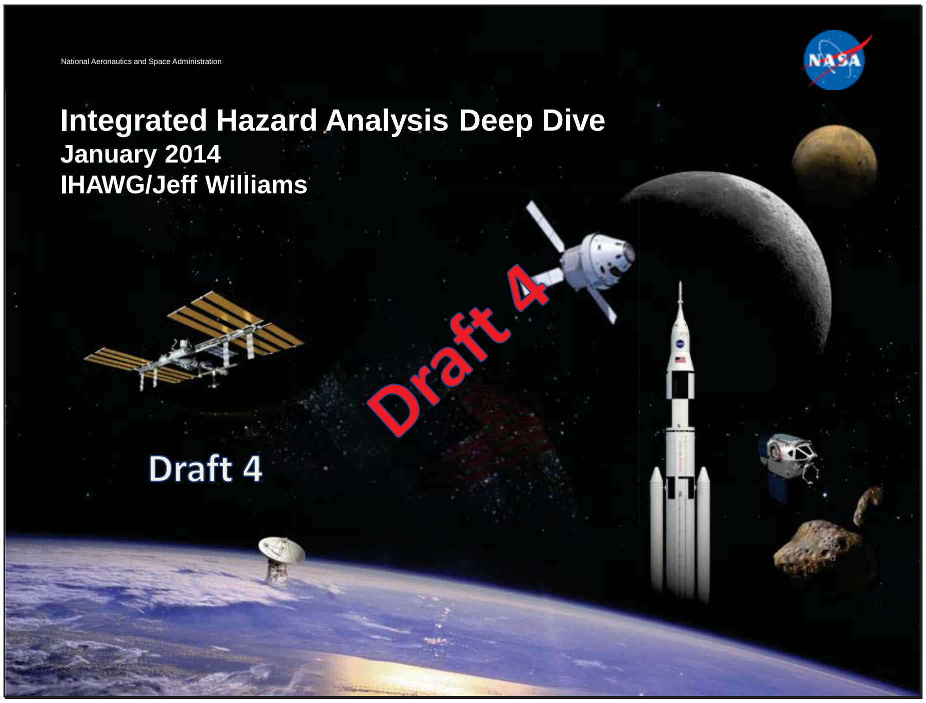
- "Integrated Hazard Analysis Deep Dive" presentation
- Program documentation
  - Cross-Program S&MA Plan (ESD 10010)
  - ESD Systems Safety Analysis Report (10015)
  - IHAWG Task Agreement
  - IHAWG Guidance for Analysis Causes
  - Ground Systems Development and Operations (GSDO) S&MA Plan (GSDO-LN-1036)
  - Multi-Purpose Crew Vehicle (MPCV) S&MA Plan (MPCV 70294)
  - SLS S&MA Plan (SLS-PLAN-013)

- SLS Abort Triggers Definition Document (SLS-SPEC-197)
- GSDO Top Level Operational Hazard Analysis Fault Tree
- MPCV Master Hazards List
- SLS Master Hazards List (SLS-RPT-076)
- ESD Risk Management Plan (ESD 10003)
- ESD Implementation Plan (ESD 10001)
- Charter for the ESD Control Board (ESD-MD-12002)
- Joint Program Control Board Charter (JPCB 0001)
- Cross-program Ascent Aborts Analysis Methodology (MPCV 72519)
- Orion MPCV Crew Survival Analysis Exploration Mission 2 Reference Missions (MPCV 72532)
- Orion MPCV Vehicle Integration Control Board/Joint Integration Control Board Charter (MPCV 0074)
- SLS Chief Engineer Control Board/Joint Integration Control Board Charter
- Selected Cause Records and Cause Trees

Other documentation reviewed by the assessment team included:

- Prior human spaceflight (HSF) program related documentation
  - Apollo Safety Program Plan
  - KSC Apollo Safety Systems Program Plan
  - Apollo Failure Mode Effects and Criticality Analysis procedure
  - Shuttle Integrated Hazard Report IPYR-01, Pyrotechnic System Malfunction
- Tim Wilson's integration white paper "Improving Exploration Systems Integration, 29 January 2014"

Appendix B. "Integrated Hazard Analysis Deep Dive" Presentation to ESD Management



Purpose

- Provide overview of ESI Integrated Hazard Analysis approach, structure, and content.
- Discuss selected details of IHA.
- Discuss forward work.

2

Agenda

- Approach to ESI IHA:
  - Benefits and limitations of hazard analysis
  - IHAWG Org
  - Scope – What's in and what's out
  - Methodology – Non-traditional approach: advantages, disadvantages, and lessons learned
  - Development and review for PDR
  - Deliveries for major program & integrated milestones
- Top-level view of the IHA:
  - Major hazardous conditions (by area).
  - Major causes for hazardous conditions
- Slices of the IHA:
  - High risk hazard cause summary
  - Elevated Watch Items
  - Deep dive into areas of interest
- Success stories:
  - Known areas where IHA impacted design
  - Final IHA status for GSDO PDR
- Forward Work for IHAWG:
  - Model restructuring
  - Getting to Orion delta-PDR and ESI Design-to Sync

3

Approach to IHA

4

Approach to ESI IHA

BENEFITS AND LIMITATIONS OF HAZARD ANALYSIS

5

Approach to ESI IHA: Benefits & Limitations of HA

- Why we do Hazard Analysis:
  - Influence Design and Operations
  - Identify, Communicate, Mitigate, and Accept Risk
  - Identify Hazard Controls for "Posterity" – Relate selected design and operational parameters to hazard controls to assure retention.
- Limitations of HA:
  - Primarily Qualitative – no cumulative assessment of risk
  - Can't capture all the unknowns

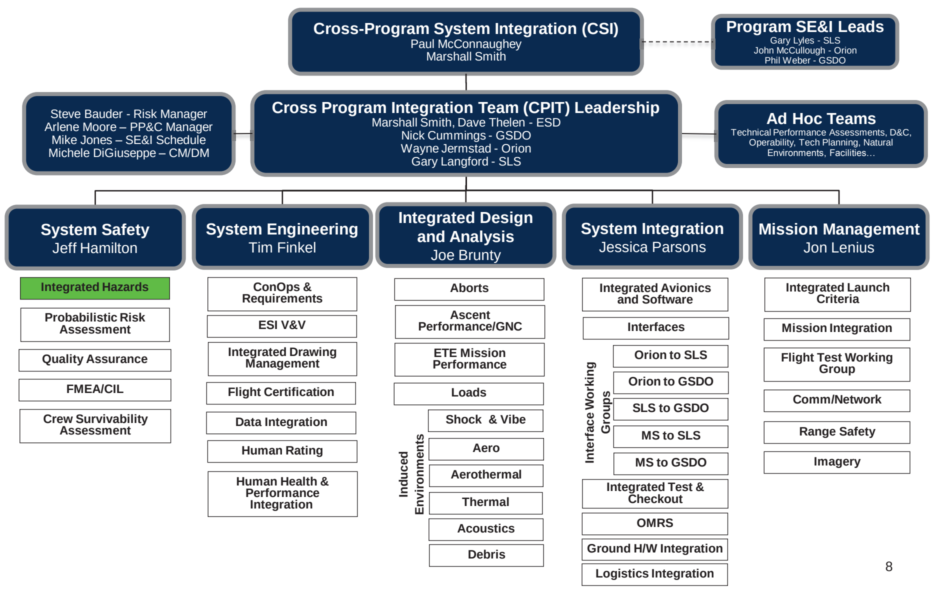
6

Approach to ESI IHA

ESI IHA ORGANIZATION

7

Approach to ESI IHA: ESI IHA Organization



8

Approach to ESI IHA: IHAWG Organization (Membership)

- Per IHAWG Task Agreement, IHAWG membership includes:
  - Core members:
    - CSI - IHAWG Lead
    - GSDO, Orion & SLS SMA
    - GSDO, Orion & SLS Engineering

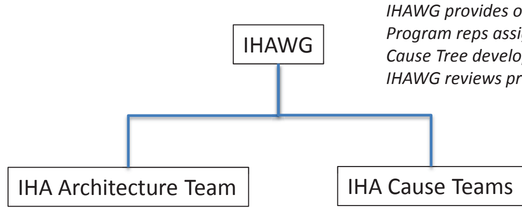
    } Reps are from center line orgs

  - Ad hoc members:
    - Health and Medical TA
    - Crew Office
    - Mission Operations
    - HQ Office of S&MA
    - ESD Chief Engineer
    - Reps from other System Safety Functional Area ITTs
    - Discipline experts
    - Safety Panel Chairs
    - Center S&MA Reps and Safety Engineers
    - Contractor Reps

9

Approach to ESI IHA: ESI IHA Organization

IHAWG Structure



IHAWG provides overall leadership.
Program reps assign resources to Cause and Cause Tree development.
IHAWG reviews products prior to release.

IHA Architecture Team: Program Engineering & S&MA; IHAWG Lead

IHA Cause Teams: Program Engineering; Program S&MA; Others as required

IHAAT coordinates development of Cause Trees. Recommends program assignments for tree and cause development.

Cause Teams develop causes.

10

Approach to ESI IHA

ESI IHA SCOPE

11

Approach to ESI IHA: ESI IHA Scope

- ESI IHA scope is established by ESD 10010, ESD S&MA Plan (section 4.1.2):
- What makes an integrated hazard or hazard cause:
  - More than one program contributes to a cause, control, or verification.
    - Example: During cryo loading, GSDO controls SLS tank pressure and SLS has independent pressure relief
  - More than one program contributes to the analysis of the system effect, the interactions/interfaces, and interdependencies of the hazard.
    - Example: All 3 Programs contribute to integrated loads analyses
- IHA timeframe: Pre-launch cryo loading start to post-flight crew egress.
- EM-1 & EM-2

12

Approach to ESI IHA: ESI IHA Scope

- What is IHA:
  - Any failures during otherwise nominal operations that result in loss of or injury to crew or loss of mission.
    - Post T-0, crew injuries are either catastrophic (result in permanent disability) or critical (loss of mission if injury requires more than first aid).
  - Error in analysis, design, or operation that may cause hazard within IHA timeframe.
  - Hazards imposed by nominal system behavior during integrated operations (e.g., build-up of hazardous gases due to allowable leakage from more than one program).
  - Hazards associated with on-pad engine shut-down.
  - Hazards imposed by the presence of emergency systems (e.g., abort systems).
- What is not IHA:
  - Loss of crew/vehicle during use of emergency system or operation. → Failure to abort or perform emergency egress when needed or failure to survive abort/emergency egress are exempted from HA by the ESD S&MA Plan.
    - IHA Causes do capture potential crew survival methods in the Crew Survival Notes field.
  - Interfaces between an individual Program and external entity such as those between SLS and Range Safety.
  - Interfaces between Program elements that do not impact other Programs.

13

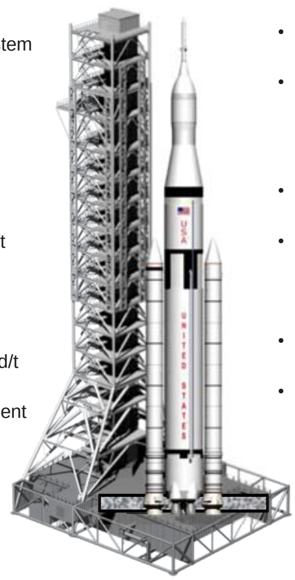
Approach to ESI IHA: ESI IHA Scope

Integrated HAs vs. Program HAs – Examples

- IHA: Loss of comm due to system characteristics
- Not IHA: Loss of comm d/t hardware failure.

- IHA: Collision with tower d/t improper vehicle OML
- Not IHA: Collision w/ tower d/t GN&C failure

- IHA: Hazardous environment d/t combined sources of H2.
- Not IHA: Hazardous environment d/t H2 leak.



- IHA: Inadvertent abort due improper notification.
- Not IHA: Inadvertent abort d/t premature LAS firing.

- IHA: Geysering in LOx line due to contamination.
- Not IHA: Geysering in LOx line d/t Ghe supply system failure.

- IHA: Under-/Over-fill of prop leading to off-nominal engine performance
- Not IHA: RS-25 failure due to engine component failure

NOTIONAL

14

Approach to ESI IHA

ESI IHA METHODOLOGY

15

Approach to ESI IHA: Methodology

- In order to provide a product within required timeframe and to provide more opportunity to influence design, the IHAWG adopted a streamlined approach. This approach focused on the following major aspects:
  - Interfaces (Program-to-Program IRDs/ICDs):
    - "Middle out" assessment based on the functions of the interface such as:
      - Structural
      - Electrical, data, or fluid pass-through
  - Operations (specifically, the ESD Con Ops):
    - Hazards imposed by planned ops.
  - Environments (Thermal, winds, plume, etc.)
  - Experience of Past Programs (SSP, CxP)

16

Approach to ESI IHA: Methodology

- Methodology adopted was "non-traditional" when compared to approaches used in past HSF programs.
- ESI IHA Cause Trees are not part of a single, comprehensive hazard model such as:
  - Top-down fault tree
  - Functional hazard analysis
  - Hazard checklist
- With this methodology, classic hazard reports (a high-level hazard broken into causes) are not produced.
  - Cause trees are needed to relate individual causes to each other and to higher level Hazardous Conditions.

17

Approach to ESI IHA: Methodology

Preliminary Architecture Assessment

Cross Program architecture was assessed to identify hardware interfaces (i.e., mechanical, electrical, fluid, etc.), system interactions, and interdependencies to define a comprehensive list of hazardous conditions/hazard topic areas. Approximately 270 hazardous conditions were identified.

Closely coupled Engineering and S&MA teams identified ~270 hazardous conditions.

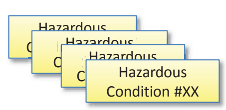
18

Approach to ESI IHA: Methodology

Preliminary Architecture Assessment

Cross Program architecture was assessed to identify hardware interfaces (i.e., mechanical, electrical, fluid, etc.), system interactions, and interdependencies to define a comprehensive list of hazardous conditions/hazard topic areas. Approximately 270 hazardous conditions were identified.

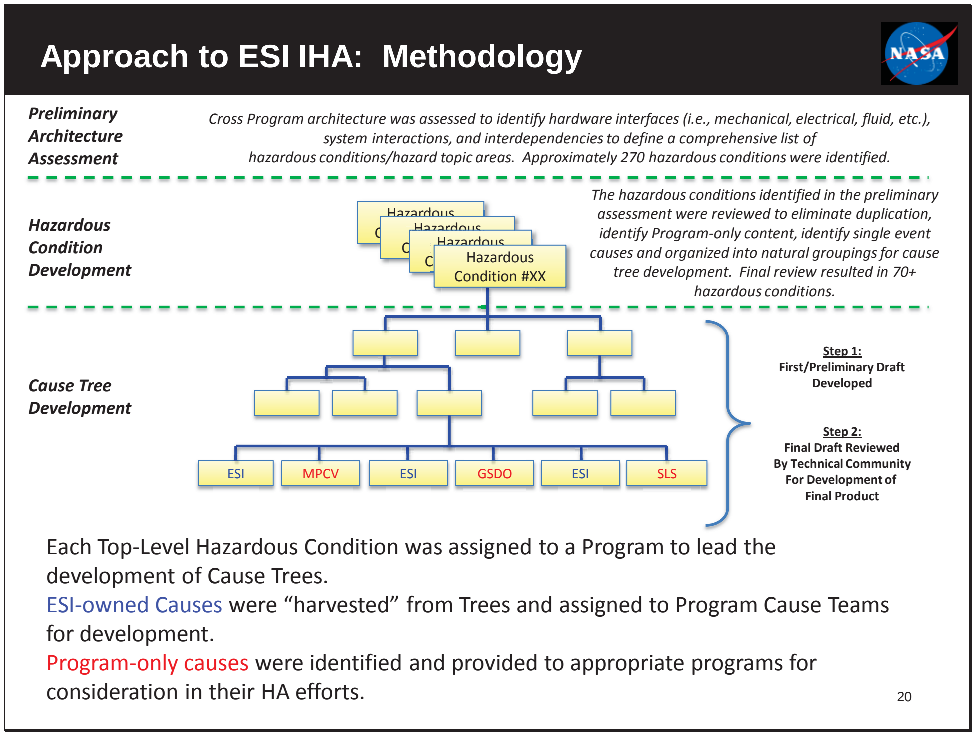
Hazardous Condition Development

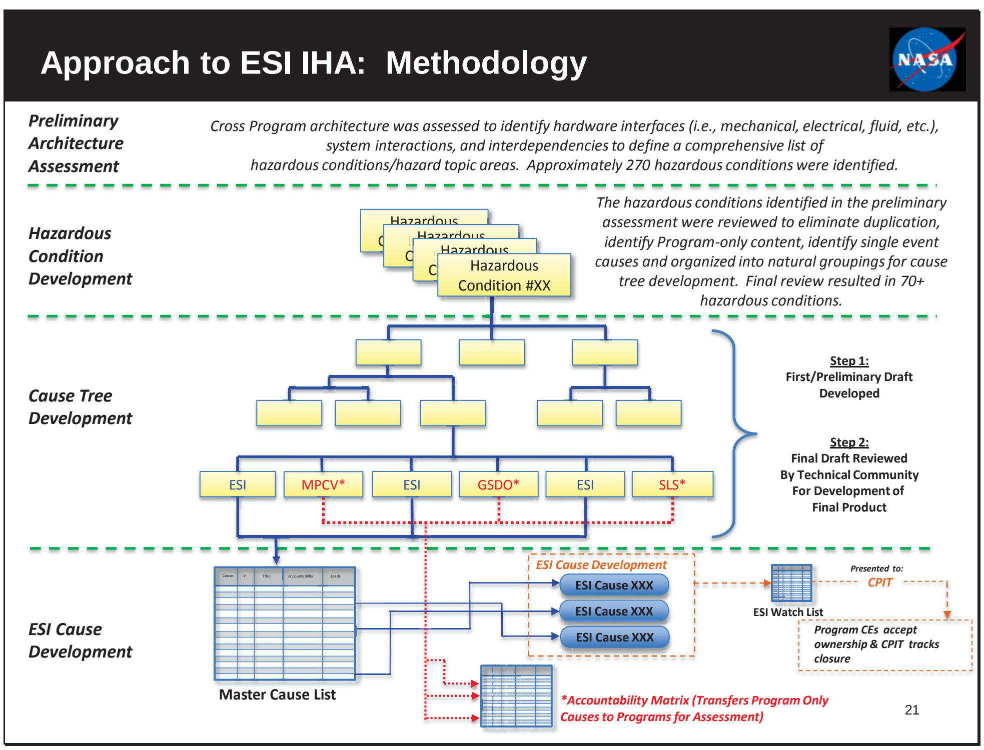


The hazardous conditions identified in the preliminary assessment were reviewed to eliminate duplication, identify Program-only content, identify single event causes and organized into natural groupings for cause tree development. Final review resulted in 70+ hazardous conditions.

270 conditions assessed by CSI, Program S&MA, and Program Engineering and placed into logical groupings.
Groupings would become the starting point for next step – Cause Tree development.

19


Approach to ESI IHA: Methodology
Preliminary Architecture Assessment
Cross Program architecture was assessed to identify hardware interfaces (i.e., mechanical, electrical, fluid, etc.), system interactions, and interdependencies to define a comprehensive list of hazardous conditions/hazard topic areas. Approximately 270 hazardous conditions were identified.
Hazardous Condition Development
Hazardous Condition #XX
The hazardous conditions identified in the preliminary assessment were reviewed to eliminate duplication, identify Program-only content, identify single event causes and organized into natural groupings for cause tree development. Final review resulted in 70+ hazardous conditions.
Cause Tree Development
ESI
MPCV
ESI
GSDO
ESI
SLS
Step 1:
First/Preliminary Draft Developed
Step 2:
Final Draft Reviewed By Technical Community For Development of Final Product
Each Top-Level Hazardous Condition was assigned to a Program to lead the development of Cause Trees.
ESI-owned Causes were "harvested" from Trees and assigned to Program Cause Teams for development.
Program-only causes were identified and provided to appropriate programs for consideration in their HA efforts.
20


Approach to ESI IHA: Methodology
Preliminary Architecture Assessment
Cross Program architecture was assessed to identify hardware interfaces (i.e., mechanical, electrical, fluid, etc.), system interactions, and interdependencies to define a comprehensive list of hazardous conditions/hazard topic areas. Approximately 270 hazardous conditions were identified.
Hazardous Condition Development
Hazardous Condition #XX
The hazardous conditions identified in the preliminary assessment were reviewed to eliminate duplication, identify Program-only content, identify single event causes and organized into natural groupings for cause tree development. Final review resulted in 70+ hazardous conditions.
Cause Tree Development
ESI
MPCV*
ESI
GSDO*
ESI
SLS*
Step 1:
First/Preliminary Draft Developed
Step 2:
Final Draft Reviewed By Technical Community For Development of Final Product
ESI Cause Development
Master Cause List
ESI Cause Development
ESI Cause XXX
ESI Cause XXX
ESI Cause XXX
ESI Watch List
Presented to:
CPIT
Program CEs accept ownership & CPIT tracks closure
*Accountability Matrix (Transfers Program Only Causes to Programs for Assessment)
21

Approach to ESI IHA: Methodology

- Advantages of chosen approach:
  - Allowed for a product with opportunity to influence design.
  - Used available cross-program products in absence of more detailed design definition.
  - Implementable with limited resources, the vast majority of which are provided by ESD Programs.
  - Easily adaptable. Can add Cause Trees and Causes as design changes. (Example: Vehicle Stabilization System)
- Disadvantages:
  - Potential to miss something due to lack of more structured model.
- Concerns and Lessons Learned:
  - Common understanding of approach by all those involved in IHA development and review (including stakeholders).
  - Difficult to see the “big picture” for causes and relationships between causes. Often results in scoping issues for these causes.
    - Example: Fire/Explosion causes are spread among multiple trees.
  - Sustainability and maintainability of the model structure over the long term.

22

Approach to ESI IHA

ESI IHA DEVELOPMENT & REVIEW

23

Approach to ESI IHA: IHA Product Development & Review

IHA Maturity for PDR

- These criteria for IHA content were approved by ESMAP and will be included in next rev of ESD S&MA Plan.
- IHA content consistent with level of PDR design definition.
  - Hazard topics showing relationship between hazard topic and causes
  - Description and effect(s) for each hazardous topic
  - Hazard causes identified
  - Elimination/Mitigation strategies or preliminary controls for the hazard causes
  - Failure Tolerance/exception approach for applicable hazard causes
  - Preliminary verification methods for each hazard control
  - Potential Crew Survival Methods (CSM) for catastrophic hazards and descriptions of their role in ensuring crew survival
  - All action items/RIDs required to be closed for phase I/PDR have been dispositioned

24

Approach to ESI IHA: IHA Product Development & Review

Products from ESI IHA

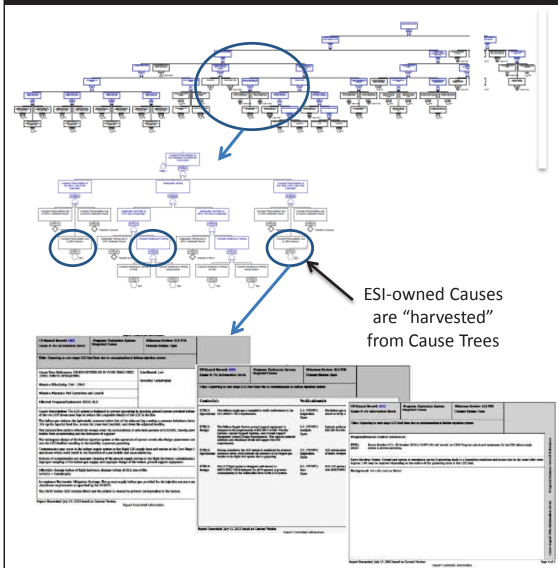
- The ESI System Safety Analysis Report (ESI 10015) is the primary IHA product for any given milestone:
  - Methodology Summary
  - **Cause Trees**
  - **ESI Cause Sheets** (aka Cause Records)
    - Cause Title
    - Description & Effects
    - Mitigation Strategy and Acceptance Rationale
    - Controls & Verifications
    - Likelihood and Severity (LxS)
    - …
  - Program-only causes
  - ESI Watch Items
  - High Risk Causes

~95% of the SSAR content

- The ESI SSAR is delivered as a draft for each Program's major milestone.
- The SSAR will be baselined before or around the ESD Design-To Sync and formally revised for subsequent ESD milestones.

25

Approach to ESI IHA: IHA Product Development & Review



TYPICAL CAUSE TREE

- 75 Cause Trees total.
- 70 Trees delivered with SSAR for GSDO PDR

TYPICAL CAUSE RECORD (partial)

- 190 Total Causes
- 149 with GSDO content (including 10 forward work Causes)

26

Approach to ESI IHA: IHA Development & Review for PDR

- Cause Tree Development & Review:
  - All Cause Trees are assigned to a program S&MA engineer who facilitates the development of the Tree in collaboration with Engineering and S&MA from impacted or contributing programs.
  - After initial drafting, a review is held with all appropriate stakeholders (including IHAWG members). Successful completion of that review results in a Cause Tree that is "Phase B complete".

- Cause Development:
  - ESI-owned Causes are harvested from Phase B Cause Trees and assigned to a Program for development.
  - After basic Cause info is drafted (description, effects, mitigation strategy), IHAWG Lead and others meet with Cause Team to review and adjust the "scope" of the cause.
  - IHAWG provided guidance on minimum content for PDR-mature causes. Also provided guidance on certain IHA cause categories to promote maturity and commonality.
  - IHAWG Program Engineering and S&MA reps assign personnel to work together on Cause.

- Cause Review:
  - Multiple reviews of IHA Causes to date:
    - IHAWG/Grey-Beard Review of Causes and Trees prior to SLS PDR
    - ESD Change Request prior to SLS PDR
    - Internal "Recovery" review by IHAWG post-SLS PDR
    - IHAWG Table-Top Review prior to GSDO PDR (continued on next chart)

27

Approach to ESI IHA: IHA Development & Review for PDR

- Cause Review (continued):
  - For GSDO PDR, the following review approach was employed:
    - IHAWG table-top reviews were convened for the purpose of reviewing each cause needed for GSDO PDR (i.e., with GSDO content) prior to delivery to the milestone review.
      - Chief Engineers and CSOs from ESI and each Program were invited to “augment” their participation in these reviews as desired.
    - Cause Teams incorporate IHAWG agreed-to comments into causes.
    - IHAWG Lead approves Cause for release to milestone review once comments (including comments from previous reviews) are verified as appropriately incorporated.
  - Typical attendance for a Table-Top Review included:

Reviewers:
- Core IHAWG Members*
- CSI CSO Rep
- CSI CE Rep
- Crew Rep
- HMTA Rep
- IHAAT Members
- Mission Ops Rep
- Orion CE Rep
- GSDO CE Rep
- SLS CE Rep
- SLS CSO Rep
- IHAWG Admin

Presenters:
- Program Engineering
- Program S&MA
- Discipline Experts

* Program Engineering/SMA & IHAWG Lead

28

Approach to ESI IHA: IHA Development & Review for PDR

- IHAWG Watch Items:
  - Watch Items are opened as needed by any IHA team member to track any number of things, from issues to open work to process improvements.
  - IHAWG periodically reviews Watch Items for status. IHAWG may elevate individual Watch Items to CPIT as needed to get help in resolving the WI. (IHAWG may also elevate certain WI’s for visibility.)
  - While IHAWG tracks multiple WI’s, only those that have been elevated to CPIT and communicated to Program stakeholders are included in the ESI SSAR.

29

Approach to ESI IHA: IHA Development & Review

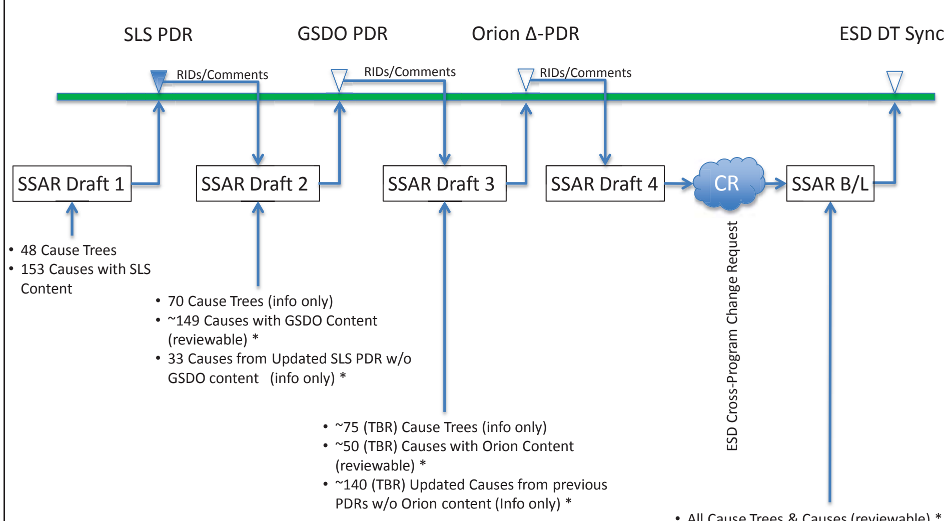
Cross Program Hazard Analysis Database

- IHAWG makes extensive use of Ames-developed CP Hazard Database:
  - Cause records
  - Cause Tree metadata
  - Watch Items
  - Review and approval for release
  - Reporting, including the bulk of the SSAR
- Database and developers are extremely flexible and responsive to changes needed by IHA Team.

30

Approach to ESI IHA: IHA Development & Review for PDR

SSAR Delivery for Program PDRs and ESD Sync



31

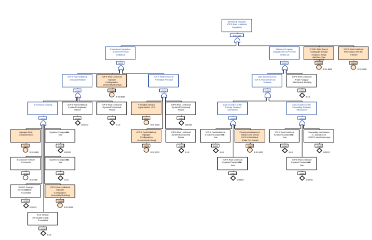
* Minus any causes that are known forward work

Top-Level View of the IHA

32

Top-Level View of IHA

CAUSE TREES



33

Top-Level View of the ESI IHA: Major Hazardous Conditions

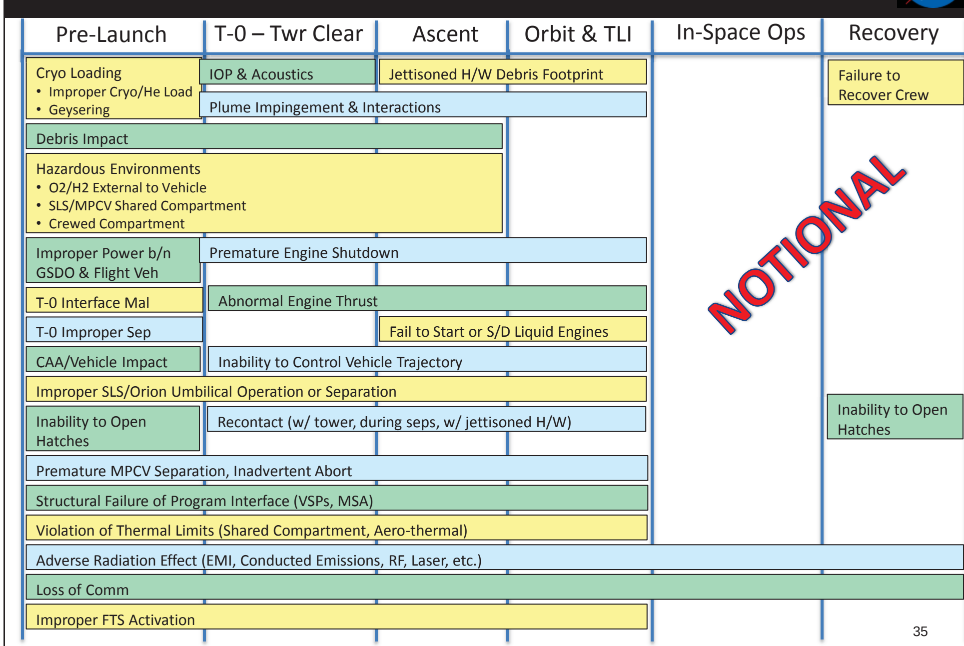
- The IHAWG currently tracks 75 top-level Hazardous Conditions as Cause Trees.
- The following table shows the major categories in which these trees fall:

Cause Tree Area	Number of Trees
Improper Cryo Load (LH2 and LOx – Core Stage and ICPS)	4
Improper Helium Load (Core Stage & ICPS)	2
LOx Geysering	1
Crew Access Arm Extendable Platform Impacts/Collides With Vehicle	1
Fire/Explosion In SLS/Orion Shared Compartment	1
Hazardous Environment External to Vehicle	2
Improper Crew Compartment Atmosphere During Launch Operations	1
Improper Operation Of FTS Leads To A Catastrophic Event	1
Improper Power Between GSDO and Flight Element	2
Structural Failure Of The MSA	1
Structural Failure Of The Vehicle Support Posts (VSPs)	1
Violation Of Thermal Environment Limits In The ISPE-SM Compartment	1
Excessive Vehicle/Tower Excursions	1
Improper Umbilical or T-0 Interface Operation Up to T-0 (1 Tree per interface)	13
Improper Umbilical or T-0 Separation (1 Tree per interface)	13
Improper Ignition Overpressure Or Acoustics During Liftoff	1

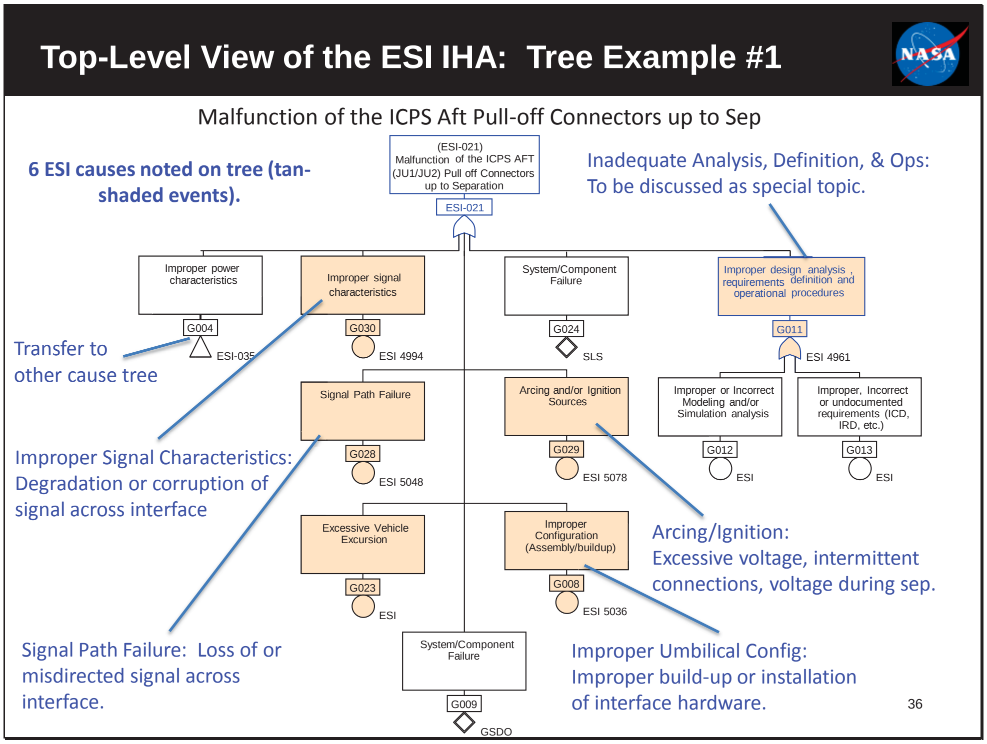
Cause Tree Area	Number of Trees
Recontact During Lift-Off or Staging	4
Improper start or shut-down of liquid engine or off-nominal performance	6
Plume Impingement & Interaction	1
Premature MPCV Separation	1
Debris Impact Results In Catastrophic Failure	1
Inadvertent Abort	1
Jettisoned Hardware Impact/Recontact With The Integrated Vehicle	1
Jettisoned Hardware/Debris Falls Outside Expected Footprint	1
Inability to Control Vehicle Trajectory (by Mission Phase)	5
Excessive Aero-Thermal Heating To The External Surface Of The Vehicle	1
Loss Of Communications During Operations	1
Adverse Radiation Effect	1
Inability To Open The LAS/CM Hatches When Required	1
Unable To Safely Recover The CM/Crew During Post Landing Operations	1
Natural Environments Mapping Tree	1
Improper Orion/SLS Umbilical Operation or Separation	2

34

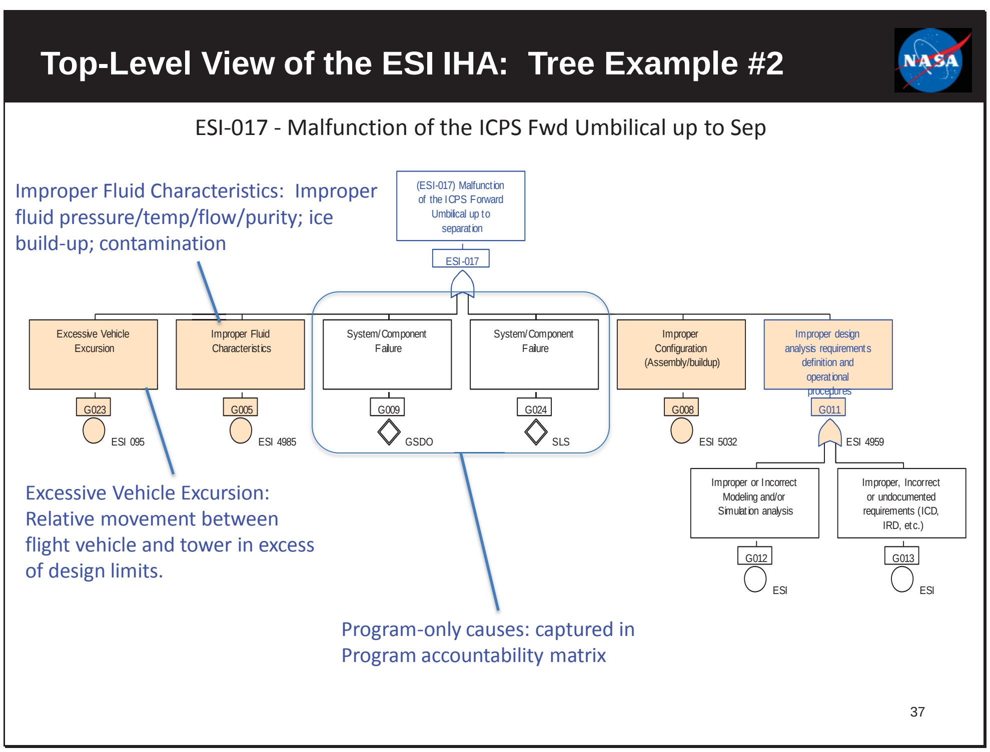
Top-Level View of the ESI IHA: Major Hazardous Conditions



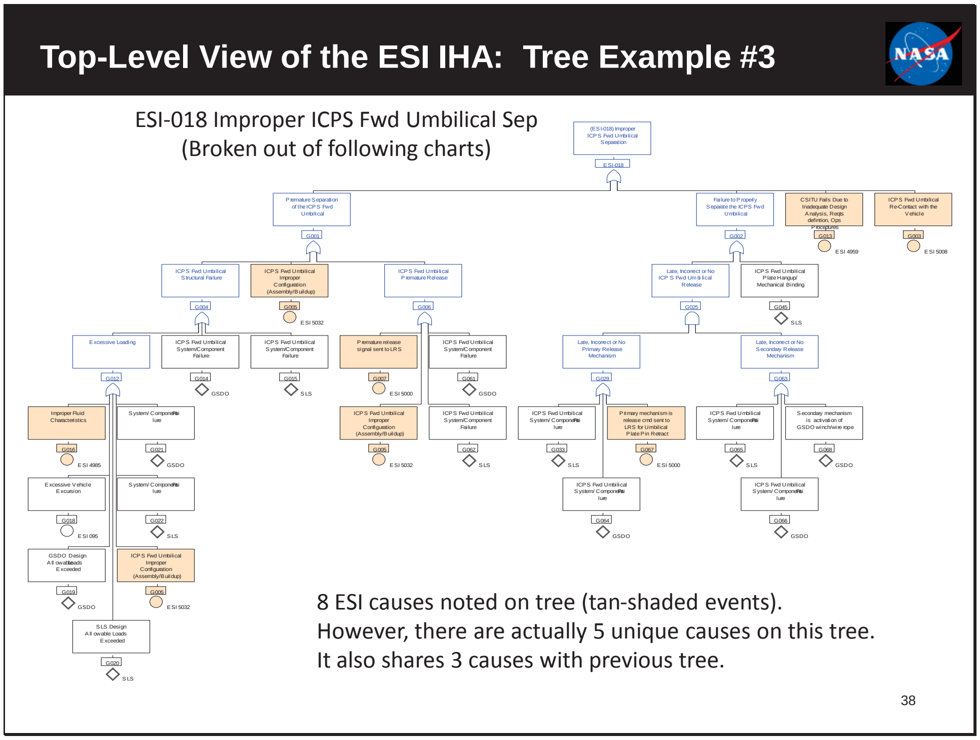
35

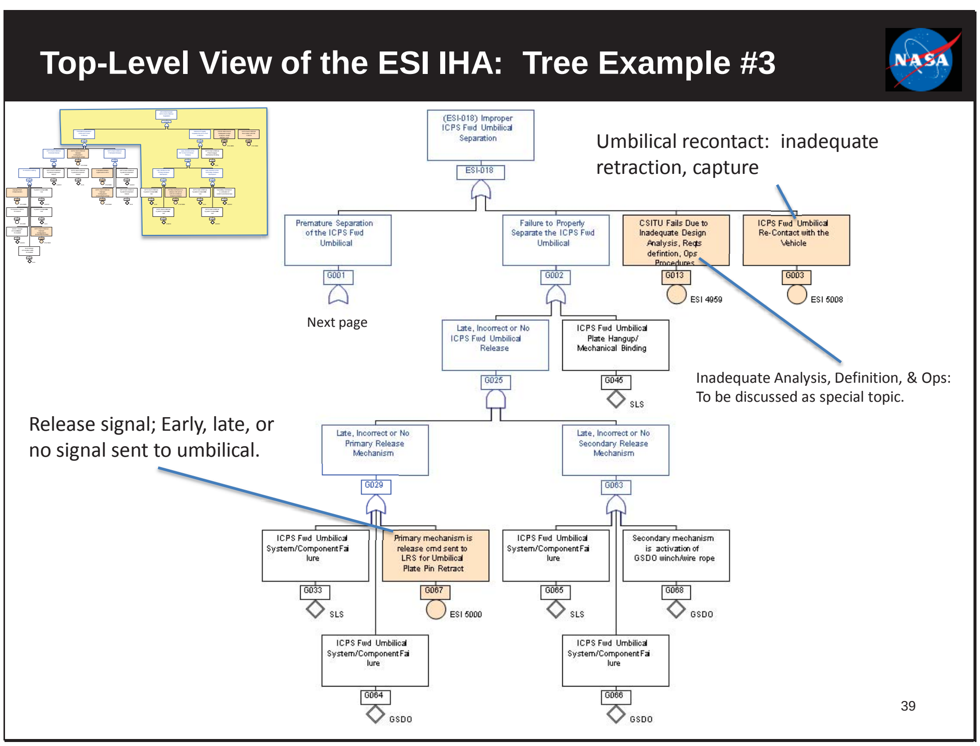


Top-Level View of the ESI IHA: Tree Example #1
Malfunction of the ICPS Aft Pull-off Connectors up to Sep
6 ESI causes noted on tree (tan-shaded events).
(ESI-021) Malfunction of the ICPS AFT (JU1/JU2) Pull off Connectors up to Separation
ESI-021
Inadequate Analysis, Definition, & Ops: To be discussed as special topic.
Improper power characteristics
G004
ESI-035
Improper signal characteristics
G030
ESI 4994
System/Component Failure
G024
SLS
Improper design analysis, requirements definition and operational procedures
G011
ESI 4961
Transfer to other cause tree
Signal Path Failure
G028
ESI 5048
Arcing and/or Ignition Sources
G029
ESI 5078
Improper or Incorrect Modeling and/or Simulation analysis
G012
ESI
Improper, Incorrect or undocumented requirements (ICD, IRD, etc.)
G013
ESI
Improper Signal Characteristics: Degradation or corruption of signal across interface
Excessive Vehicle Excursion
G023
ESI
Improper Configuration (Assembly/buildup)
G008
ESI 5036
Arcing/Ignition: Excessive voltage, intermittent connections, voltage during sep.
System/Component Failure
G009
GSDO
Signal Path Failure: Loss of or misdirected signal across interface.
Improper Umbilical Config: Improper build-up or installation of interface hardware.
36

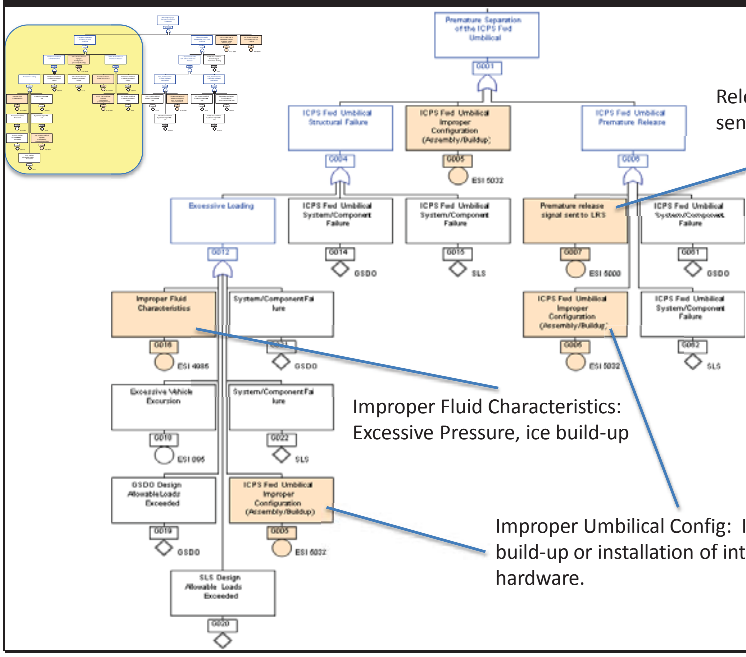


Top-Level View of the ESI IHA: Tree Example #2
ESI-017 - Malfunction of the ICPS Fwd Umbilical up to Sep
Improper Fluid Characteristics: Improper fluid pressure/temp/flow/purity; ice build-up; contamination
(ESI-017) Malfunction of the ICPS Forward Umbilical up to separation
ESI-017
Excessive Vehicle Excursion
G023
ESI 095
Improper Fluid Characteristics
G005
ESI 4985
System/Component Failure
G009
GSDO
System/Component Failure
G024
SLS
Improper Configuration (Assembly/buildup)
G008
ESI 5032
Improper design analysis requirements definition and operational procedures
G011
ESI 4959
Improper or Incorrect Modeling and/or Simulation analysis
G012
ESI
Improper, Incorrect or undocumented requirements (ICD, IRD, etc.)
G013
ESI
Excessive Vehicle Excursion: Relative movement between flight vehicle and tower in excess of design limits.
Program-only causes: captured in Program accountability matrix
37


Top-Level View of the ESI IHA: Tree Example #3
ESI-018 Improper ICPS Fwd Umbilical Sep
(Broken out of following charts)
8 ESI causes noted on tree (tan-shaded events).
However, there are actually 5 unique causes on this tree.
It also shares 3 causes with previous tree.
38


Top-Level View of the ESI IHA: Tree Example #3
(ESI-018) Improper ICPS Fwd Umbilical Separation
ESI-018
Umbilical recontact: inadequate retraction, capture
Premature Separation of the ICPS Fwd Umbilical
G001
Next page
Failure to Properly Separate the ICPS Fwd Umbilical
G002
CSITU Fails Due to Inadequate Design Analysis, Reqs defintion, Ops Procedures
G013
ESI 4959
ICPS Fwd Umbilical Re-Contact with the Vehicle
G003
ESI 5008
Late, Incorrect or No ICPS Fwd Umbilical Release
G025
ICPS Fwd Umbilical Plate Hangup/ Mechanical Binding
G046
SLS
Inadequate Analysis, Definition, & Ops: To be discussed as special topic.
Release signal; Early, late, or no signal sent to umbilical.
Late, Incorrect or No Primary Release Mechanism
G029
Late, Incorrect or No Secondary Release Mechanism
G063
ICPS Fwd Umbilical System/Component Failure
G033
SLS
Primary mechanism is release cmd sent to LRS for Umbilical Plate Pin Retract
G067
ESI 5000
ICPS Fwd Umbilical System/Component Failure
G065
SLS
Secondary mechanism is activation of GSDO winch/wire rope
G068
GSDO
ICPS Fwd Umbilical System/Component Failure
G064
GSDO
ICPS Fwd Umbilical System/Component Failure
G066
GSDO
39

Top-Level View of the ESI IHA: Tree Example #3



Release signal; Early signal sent to umbilical.

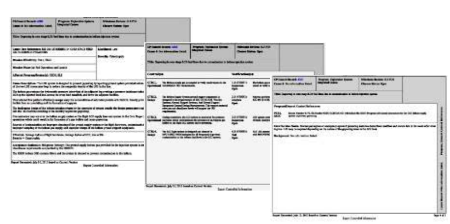
Improper Fluid Characteristics: Excessive Pressure, ice build-up

Improper Umbilical Config: Improper build-up or installation of interface hardware.

40

Top-Level View of IHA

ESI-OWNED CAUSES



41

Top-Level View of the ESI IHA: IHA Causes

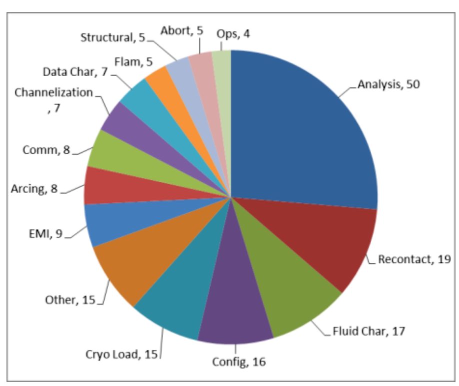
- The ESI IHA currently contains 190 ESI-owned causes.
- Number fluctuates due to:
  - New Cause Trees being developed
  - Combining of like causes where possible
  - Deletion of causes due to non-applicability, non-credibility, transfer to program-only
- Many causes share much in common with other similar causes in the general hazard scenario and mitigation approach.
- IHAWG categorizes each hazard cause to facilitate review and commonality of approach.
  - Aids in cause scoping and table-top reviews where IHAWG can review similar causes one or two sessions.
- 20+ cause categories are used as shown on following chart.

42

Top-Level View of the ESI IHA: IHA Cause Categories

Cause Categories Used by IHAWG

Cause Category	Description	Number of Causes
Analysis	Inadequate analysis, design, or ops	50
Recontact	Recontact during lift-off, sep, or jettison	19
Fluid Char	Improper fluid characteristics across interface (temp, pressure, flow, etc.)	17
Config	Improper build-up/config of interface	16
Cryo Load	Over-/under-press, geysering, over-/under-load	15
EMI	Improperly characterized or controlled EMI	9
Arcing	Arcing within T-0 electrical connection	8
Comm	Loss of or improper communication	8
Channelization	Improper signal path between elements	7
Data Char	Improper/corrupted data signal across interface	7
Flam	Flammable environment	5
Structural	Structural failure	5
Abort	Inadvertent abort	5
Ops	Ops outside certified limits	4
IOP	Excessive ignition over-pressure or acoustics	3
DOLILU	Improper or corrupted DOLILU	2
FTS	Inadvertent FTS or FTS failure when needed	2
Recovery	Unable to recover crew	2
Traj	Trajectory anomalies	2
Excursion	Excessive excursion of flight or ground elements	1
Materials	Material incompatibility	1
Power	Improper power between programs	1
Release Sig	Early, late, or no release signal to T-0's	1
Total		**190**



43

Top-Level View of the ESI IHA: IHA Causes

Example of Typical Cause Sheet

CP-Hazard: 4401 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Excessive ground winds during liftoff or on-pad engine shutdown

Cause Tree Reference: ESI-045 LOSS OF CONTROL DURING LIFTOFF,ESI-060 STRUCTURAL FAILURE OF THE VEHICLE SUPPORT POSTS (VSPs)

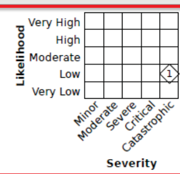
Mission Effectivity: EM-1,EM-2

Mission Phase(s): Pad Operations and Launch

Affected Program/System(s): GSDO,Orion,SLS

Severity: Catastrophic

Likelihood: Low



Basic Cause

Cause Description: If ground winds during liftoff or during an on-pad engine shutdown exceed allowable design limits due to operational procedure violations, structural damage/failure may occur at any/all of the primary loading paths of the integrated vehicle. Procedure violations may result from any one of the three following sub-causes: 1) inadequate or unclear documentation of the procedure; 2) analysis errors that drive the wrong operational ranges/parameters in the documented procedure; or 3) intentional violations that are not sanctioned by the Exploration Systems Program. Excessive ground winds due to any of these forms of procedural violations may lead to structural failure of the integrated vehicle.

Effect(s): If the actual ground winds during liftoff or an on-pad engine shutdown exceed those used for design due to various procedural violations, the result could be excessive loading on the integrated vehicle. Excessive loads can lead to damage or structural failure of the integrated vehicle. This effect may not manifest until a later mission phase (i.e. ascent). Excessive loads can lead to structural damage or failure of the integrated vehicle, leading to loss of mission and/or loss of crew.

Mitigation Strategy:
Operational controls or procedures employed at KSC are carefully documented to accurately and clearly reflect the analytical design parameters and limits such as those defined in the SLS-SPEC-159, Cross-Program Design Specification for Natural Environments (which includes ground winds while at the pad and during liftoff). The limiting wind factors are based on the integrated vehicle loads analyses and are driven by the lowest limiting case (at interface TBD).

Accurate ground wind characterization is based on years of measured environment data at Kennedy Space Center (KSC) which are used to develop models utilized in the integrated vehicle analyses. This same approach has been historically proven by the successful, 30+ year, Space Shuttle Program (SSP). Appropriate technicians/personnel are trained and certified to follow and implement the operational procedures as written. Employees/personnel performing this work are instilled with a strong sense of pride and integrity to perform exceptional work. As a result, sabotage or intentional procedures violations are considered highly unlikely.

Cause Report #

44

Top-Level View of the ESI IHA: IHA Causes

Example of Typical Cause Sheet

CP-Hazard: 4401 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Excessive ground winds during liftoff or on-pad engine shutdown

Acceptance Rationale:
See "Mitigation Strategy".

Basic Cause

Failure Tolerance:
Structural exception to failure tolerance, as allowed by SLS-SPEC-032, Space Launch System (SLS) Program Launch Vehicle Specification. Failure of structures is exempted from the Failure Tolerance requirement based on section 3.2.7 requirement SLS.10, Paragraph A. Failure tolerance for other effects are documented in lower level cause records and hazard reports.

Likelihood Justification: The likelihood applied to this cause is low due to the strength of the operational controls employed at KSC. Procedures are reviewed and assessed for accuracy and clarity and personnel are trained and certified to follow procedures as written.

Cause Report #

45

Top-Level View of the ESI IHA: IHA Causes

Example of Typical Cause Sheet

CP-Hazard: 4401 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Excessive ground winds during liftoff or on-pad engine shutdown

Control(s):		Verification(s):	
CTRL1. Design	**Design (Historical Data)** Design (historical data). Liftoff or on-pad engine shutdown ground winds used in integrated vehicle loads analyses are developed from years of measured data at Kennedy Space Center (KSC).	**1.1** (VERIF1) Analysis Open	Analysis. An extensive statistical analysis is done based on historical meterological data at KSC.
CTRL2. Design	**SLS-SPEC-159, Cross-Program Design Specifications for Natural Environments** The integrated vehicle is being designed to the natural environment specifications contained in SLS-SPEC-159, Cross-Program Design Specifications for Natural Environments (DSNE). The following section is applicable to this cause record: Section 3.1.3 Ground Winds for Transport and Launch Pad Environments Section 3.2.1 Ground Winds during Launch	**2.1** (VERIF2) Inspection Open	Inspection. The document is peer reviewed by the Natural Environments community as part of the Cross-Program Natural Environments Integrated Ad-Hoc Team (NEIAHT). It is approved by the SLS Program through the configuration management process defined in SLS-PLAN-008, SLS Configuration Management Plan.defined in SLS-PLAN-008, SLS Configuration Management Plan.
CTRL3. Design	**SLS-SPEC-044 (Volume 7), SLSP Vehicle Design Environments (Natural Environments)** SLS-SPEC-044 (Volume 7), SLSP Vehicle Design Environments (Natural Environments) allocates the applicable natural environments per Table 3-1 to the integrated SLSP system, as well as its elements per mission phase as mapped in the DSNE.	**3.1** (VERIF2) Inspection Open	Inspection. The document is peer reviewed by the Natural Environments community as part of the Cross-Program Natural Environments Integrated Ad-Hoc Team (NEIAHT). It is approved by the SLS Program through the configuration management process defined in SLS-PLAN-008, SLS Configuration Management Plan.defined in SLS-PLAN-008, SLS Configuration Management Plan.

Controls and Verifications

Cause Report #

46

Top-Level View of the ESI IHA: IHA Causes

Example of Typical Cause Sheet

CP-Hazard: 4401 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Excessive ground winds during liftoff or on-pad engine shutdown

Program/Element Control References:

PCR1. GSDO	Vertical Stabilizaton System (VSS) mitigates vehicle sway and provides stability while on the pad.
PCR2. GSDO	HR GSDO-GEN-WEA-010-C02 (High Winds) is the general processing hazard report that covers adverse weather controls for this hazard cause. Controls include real time wind warnings, use of weather forecasts 1 hour prior to move start. Also wind restrictions (TBD) are established based on Integrated Loads requirements and/or a safety engineering assessment.

Crew Survival Notes:
If the hazardous event manifests itself prior to booster ignition, but prior to LAS arming, the flight crew egresses via the Crew Access Arm (CAA). If the hazardous event manifests itself prior to booster ignition, and after LAS arming, either a LAS PAD Abort will be executed or the flight crew will egress via the Crew Access Arm (CAA). The decision to egress the flight crew is dependent upon many factors and is the responsibility of the Launch Director; in some instances, the flight crew will shelter in place until environmental conditions are safe enough for egress. If the event occurs at booster ignition and/or during initial ascent (up to tower clear), an abort through the Launch Abort System (LAS) can be accomplished.

Background:
Related Documents:

SLS-SPEC-159, Cross-Program Design Specification for Natural Environments (DSNE)

SLS-SPEC-044 (Volume 7), SLSP Vehicle Design Environments (Natural Environments)

Program/Element Control References

Cause Report #

47

Top-Level View of the ESI IHA: IHA Causes

Example of Typical Cause Sheet

CP-Hazard: 4401 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR
Title: Excessive ground winds during liftoff or on-pad engine shutdown		

Signatures

Name	Concurrence/Approval	Date
IHAWG_Concurrence		
Cause_Report_Auth-or		

Signatures

Cause Report #

48

Slices of the IHA

49

Slices of the IHA

CAUSE SPECIAL TOPICS – ANALYSIS CAUSES

50

Top-Level View of the ESI IHA: IHA Cause Categories

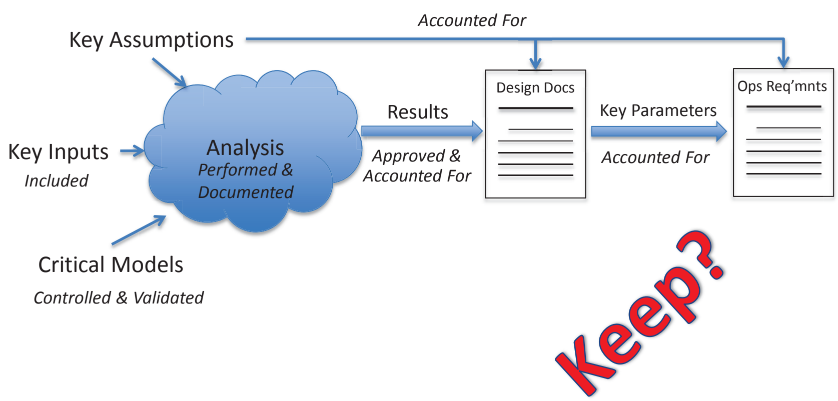
Analysis Causes

- IHAWG applied Shuttle IHA experience gained during Columbia return to flight regarding integrated design analyses.
- Primary objectives for developing these causes:
  - Determine if integrated (cross-program) analysis is needed to characterize a potential hazard, validate the effectiveness of controls, or identify controls. Assure such an analysis exists, is in-work, or planned.
  - Identify the actual analyses needed along with supporting models.
  - Capture the controls & verifications needed to provide confidence in the results of the analyses.
    - Management/Engineering processes that govern development, maintenance, approval of analyses/models and results.
    - Plans for validation of results – testing, peer review, etc.
    - Identify the critical assumptions and inputs, including those from other programs.
  - Identify the key design requirements resulting from analyses and assure requirements are implemented appropriately in IRDs/ICDs or other cross-program specs as appropriate.
  - Identify needed operational requirements or constraints needed to assure system is operated within design limits derived from key analytical inputs or assumptions.

51

Top-Level View of the ESI IHA: IHA Cause Categories

Analysis Causes (continued)



52

Top-Level View of the ESI IHA: IHA Cause Categories

Analysis Causes

- Implementation was difficult.
  - Completely different than a system HA
  - What value does this add?
  - What needs to be captured?
  - What analyses does this apply to?
- IHAWG developed guidelines for analysis-related causes for use by Cause Teams
  - Cause Scoping:
    - Identify System/Critical Functions
    - ID potential hazards associated with loss of and performance of functions.
    - ID critical attributes associated with functions: Loads/margins; pressure/temp/flow rate; data transfer; tolerances; etc.
    - ID any integrated analyses needed to characterize critical attributes: loads; CFD; tolerance stack-up; electrical; etc.
  - Controls:
    - Provide confidence in adequacy/accuracy of models: V&V; testing; conservatism; etc.
    - ID how/where resulting design parameters are documented;
    - ID any needed operational constraints required to assure system operated within limits as analyzed

53

Top-Level View of the ESI IHA: IHA Cause Categories

Analysis Causes (continued)

- Implementation was still difficult.
  - Some "integrated" analyses not really cross-program.
  - Some analyses delegated to lower levels.
  - Identifying the real critical parameters is not straight-forward.
  - Guidance doesn't fit all situations.
- Team made very good progress, but still lots of work ahead.
  - Several iterations of causes through IHAWG table-top reviews. 23 of 31 causes approved for release for GSDO PDR.
  - Have some good examples for others in team to use.

54

Top-Level View of the ESI IHA: IHA Cause Categories

Example of Analysis Cause Sheet

CP-Hazard: 4964

Cause #: No information listed

Program: Exploration Systems Integrated Causes

Milestone Review: GSDO PDR

Closure Status: Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

Cause Tree Reference: ESI-031 MALFUNCTION OF THE VEHICLE STABILIZER SYSTEM UP TO SEPARATION,ESI-032 IMPROPER VEHICLE STABILIZATION SYSTEM SEPARATION

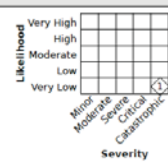
Mission Effectivity: EM-1,EM-2

Mission Phase(s): Pad Operations and Launch

Affected Program/System(s): SLS,GSDO,Orion

Severity: Catastrophic

Likelihood: Very Low



Basic Cause

Cause Description: Malfunction of the Vehicle Stabilizer during pad pre-launch and launch operations, including mechanical separation anomalies (premature separation & failure to separate properly) and loss of stability, may be caused by:

1) Improper analysis used to define design requirements and operational environments such as induced structural loads and thermals on the Vehicle Stabilizer. Improper analysis includes inadequate modeling or modeling errors, improper ground rules/assumptions (errors and omissions), or inputs to the analyses used to design and certify the integrated ground system and establish operational constraints.
2) Inadequate procedures derived from analyses resulting in improper operation of the Vehicle Stabilizer outside of its certified limits. This cause includes failure to properly define and document procedures to ensure the Vehicle Stabilizer is operated within the analyzed / certified limits but excludes improper installation and procedural errors which are covered in CR TBR.

Analyses used to define Vehicle Stabilizer (both flight half and ground half) design requirements and operational environments such as induced structural loads, connector integrity (attaching and separating), etc. will be performed by the SLS Integrated Vehicle Loads Team with inputs from a GSDO-supplied Mobile Launcher (ML) model.

Thermal analyses used to define thermal environment at the Vehicle Stabilizer will be performed by Core Stage and documented in D201-10135-1, Space Launch System (SLS) Stages Core Stage (CS) Thermal Design Data Book. Analyses used to define Vehicle Stabilizer design requirements and operational environments such as loads to vehicle due to Ground, failure of the release mechanism/release commanding (which comes from ground launch sequencer) and vehicle clearance (i.e. arm swing away) etc. will be performed by GSDO.

Effect(s): Malfunction of the Vehicle Stabilizer could result in premature separation and/or failure of the Vehicle Stabilizer to separate properly during launch and could result in catastrophic damage to the CS, ICPS, or MPCV, loss of vehicle control, loss of vehicle, and/or loss of crew.

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version

Page 1 of 9

55

Example of Analysis Cause Sheet

CP-Hazard: 4964 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

Mitigation Strategy:
Models and analysis results used to identify and define critical Vehicle Stabilizer performance parameters account for worst case expected system and environmental dispersions and are verified and validated in accordance with *SLS-PLAN-009, Verification & Validation Plan*. Critical models are documented in *SLS-RPT-105* and placed under program configuration management controls in accordance with *SLS-PLAN-008, SLSP Configuration Management Plan.*
*SLS-STD-038, Space Launch System Program (SLSP) Design Model Delivery Standard*provides controls for the Vehicle Stabilizer Operation-s Analysis by placing requirements on the model used in the analysis. *SLS-PLAN-173, SLS Program Modeling and Simulation Plan*describe the implementation and management of Models and Simulations (M&S) within the SLSP. These management practices are based on best practices, sound systems engineering, standards and guidelines, and comply with *SLS-PLAN-003, SLSP Systems Engineering Management Plan (SEMP).*

Critical Vehicle Stabilizer design parameters (tolerances, structural loads) are documented in *SLS-ICD-052-03, SLSP-to-GSDOP Interface Control Document(ICD), Volume 3, SLS Core Stage-to-GSDOP Detailed Design*, and are under program configuration management control in accordance with *SLS-PLAN-008, SLSP Configuration Management Plan*. Uncertainty factors are applied to design loads and are documented in section 3.1.3 of *SLS-RQMT-045, SLSP Vehicle Design Environments Integrated Vehicle Loads*. The results of this analysis, including the stabilizer to vehicle loads, are controlled by the Joint Loads Task Team (GSDO is a member) and documented in *SLS-RQMT-04-5.*

Operational procedures will be implemented to ensure the Vehicle Stabilizer is properly installed and operated within analyzed and certified design limits. Electrical testing procedures will be developed and inspections will be performed. Operational limits established by these procedures will include margin to account for instrumentation accuracy.

Acceptance Rationale:
No information listed

Failure Tolerance:
Failure tolerance is not applicable to analysis.

Basic Cause

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version

Page 2 of 9

56

Example of Analysis Cause Sheet

CP-Hazard: 4964 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

Likelihood Justification: Likelihood is Low due to conservatism used in the modeling and analysis of critical Vehicle Stabilizer performance parameters, adherence to established standards and requirements for verification and validation of critical math models and analysis results, and documented operational controls to ensure the Vehicle Stabilizer is operated within analyzed / certified limits.

Basic Cause

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version

Page 3 of 9

57

Example of Analysis Cause Sheet

CP-Hazard: 4964 Cause #: No information listed	Program: Exploration Systems Integrated Causes	Milestone Review: GSDO PDR Closure Status: Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

Control(s):		Verification(s):	
CTRL1. Design	**SLS M&S Master Plan** Implementation and management of Modeling and simulation (M&S) within the SLSP comply with SLS-PLAN-003, SLSP Systems Engineering Management Plan (SEMP) and is described within SLS-PLAN-173, SLSP Modeling and Simulation Plan (MSP). TBD models were used in the analysis.	**1.1** (VERIF30) Inspection Open	Inspection of the generated reports required by SLS-PLAN-173, SLSP Modeling and Simulation Plan.
		1.2 (VERIF31) Inspection Open	Inspections of the SLS Design Model Log (DML) from SLS-RPT-105. Design Math Models are documented in the SLS DML and placed under program configuration management controls in accordance with SLS-PLAN-008, SLSP Configuration Management. The SLS DML is maintained to identify versions and conventions of models and inputs used in each model/simulation run so repeatability and reliable results can be assured. Each version of the log is formally reviewed and signed.
CTRL2. Design	**SLS Prelaunch Loads Analysis** The SLS Prelaunch Loads Analysis includes the SLS vehicle model as well as the GSDO supplied ML model. Uncertainty factors are applied to design loads and are documented in section 3.1.3 of SLS-RQMT-045, SLSP Vehicle Design Environments Integrated Vehicle Loads. Vehicle Stabilizer to vehicle loads are documented in sections 4.2.4, 5.6, and 6.11 of SLS-RQMT-045, which is controlled by the Cross-Program Joint Loads Task Team.	**2.1** (VERIF25) Inspection Open	Inspection of SLS-PLAN-008, Space Launch System Program (SLSP) Configuration Management (CM) Plan. SLS-PLAN-008 defines the CM requirements, processes, procedures, and associated roles and responsibilities used in the application of CM on the SLSP at Marshall Space Flight Center (MSFC). This activity supports the required development, maintenance, and control of the technical and programmatic documentation and data that defines the performance, physical, and functional characteristics of the SLS flight vehicle, SLS software, SLS ground equipment, and delegated cross-program activities.
	The configuration included a stabilizer which was attached during the rollout, prelaunch, and liftoff events and released at the time of booster ignition. Stabilizer loads, as applied to	**2.2** (VERIF27) Inspection Open	Inspection by the Joint Loads Task Team (JLTT) and approved by the Joint Integration Control Board (JICB).

Controls and Verifications

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version — Page 4 of 9

58

Example of Analysis Cause Sheet

CP-Hazard: 4964 Cause #: No information listed	Program: Exploration Systems Integrated Causes	Milestone Review: GSDO PDR Closure Status: Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

	the vehicle, were recovered from the interface force Loads Transformation Matrix (LTM) and are listed in Table 5-2 of SLS-RQMT-045. Torque is given about the vehicle centerline.	**2.3** (VERIF28) Inspection Open	Inspection of SLS-RQMT-045, Vehicle Design Environments and Integrated Vehicle Loads Book, for Vehicle Stabilizer design loads.
CTRL3. Design	**GSDO VSS Analysis** TBD.	**3.1** (VERIF33) Inspection Open	TBD.
CTRL4. Design	**SLS-to-GSDO ICD** Vehicle Stabilizer will be designed in accordance to: SLS-ICD-052-01, SLSP-to-GSDOP Interface Control Document (ICD) Volume 1: Functional Interface Definition & SLSP Integrated Vehicle to GSDOP Detailed Design Volume 3: SLS Core Stage-to-GSDOP Detailed Design (section 4) This ICD, Volume 3, defines and controls the interface hardware design and implementation between SLSP CS Element and the GSDOP. The ICD contains drawings, definitions, characteristics, attributes, and constraints of the interfacing items, including the mechanical, structural, electrical, avionics, induced environments, data exchange, gases, fluids and envelope design agreements of the interfaces between the SLS CS and the launch site ground system. The Vehicle Stabizer design loads are documented in SLS-ICD-052-03, and are under program CM control. A 1.X factor of safety is applied to design / certification loads to	**4.1** (VERIF4) Inspection Open	Inspection of the TBD verification reports required by section 5.0 of SLS-ICD-052-01, SLSP-to-GSDOP Interface Control Document (ICD).
		4.2 (VERIF28) Inspection Open	Inspection of SLS-RQMT-045, Vehicle Design Environments and Integrated Vehicle Loads Book, for Vehicle Stabilizer design loads.

Controls and Verifications

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version — Page 5 of 9

59

Example of Analysis Cause Sheet

CP-Hazard: 4964 Cause #: No information listed	Program: Exploration Systems Integrated Causes	Milestone Review: GSDO PDR Closure Status: Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

	account for uncertainties in the induced loads environment. The ICD vehicle stabilizer load reflects the do-not-exceed limit load at the interface which were agreed upon between GSDO and Stages.		
CTRL5. Design	**Ground Systems Design** Ground systems are designed to comply with the requirements of KSC-DE-512-DM, Facility Systems, Ground Support Systems, And Ground Support Equipment General Design Requirements	**5.1** (VERIF14) Inspection Open	Inspection of the generated reports required by KSC-DE-512-DM, Facility Systems, Ground Support Systems, And Ground Support Equipment General Design Requirements.
CTRL6. Operational	**TBD OMRS Operational Procedures** From OMRS database <TBD>	**6.1** (VERIF10) Inspection Open	Inspection of the required TBD OMRS Operational Procedure.
	TBD OMRS Operational Procedure. Ground Operations installation/alignment procedures will be developed and inspections will be performed to inspect for damage/wear, cracks, degradation (corrosion, pitting, ice build-up, etc.). TBD operational constraints have been implemented to ensure the loads on the Vehicle Stabilizer due not exceed certified limits. TBD OMRS for VSS to be assembled at VAB and remain attached until T-0. TBD OMRS for VSP removal for ground ops.	**6.2** (VERIF26) Inspection Open	Inspection of operational constraint requirement defined in OMRSD TBD.

Controls and Verifications

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version — Page 6 of 9

60

Example of Analysis Cause Sheet

CP-Hazard: 4964 Cause #: No information listed	Program: Exploration Systems Integrated Causes	Milestone Review: GSDO PDR Closure Status: Final for GSDO PDR

Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures

Program/Element Control References:

PCR1. SLS — Thermal analyses used to define thermal environment at the Vehicle Stabilizer will be performed by Core Stage and documented in D201-10135-1, "Space Launch System (SLS) Stages Core Stage (CS) Thermal Design Data Book", Appendix L (pgs. 943 - 1073).

Crew Survival Notes:
If the hazardous event manifests itself prior to booster ignition, but prior to LAS arming, the flight crew egresses via the Crew Access Arm (CAA). If the hazardous event manifests itself prior to booster ignition, and after LAS arming, either a LAS PAD Abort will be executed or the flight crew will egress via the Crew Access Arm (CAA). The decision to egress the flight crew is dependent upon many factors and is the responsibility of the Launch Director; in some instances, the flight crew will shelter in place until environmental conditions are safe enough for egress. If the event occurs at booster ignition and/or during initial ascent (up to tower clear), an abort through the Launch Abort System (LAS) can be accomplished.

Background:
The ML shall provide a Vehicle Stabilizer to support the SLS vehicle during roll-out and pre-launch pad operations.

Vehicle Stabilizer malfunctions due to other causes are addressed in the hazard records listed below:
- CR TBR, Malfunction of the Vehicle Stabilizer due to Improper Configuration (including procedural errors)
- CR TBR, Improper Vehicle Stabilizer Separation due to Improper Release Signal
- CR TBR, Malfunction of the Vehicle Stabilizer due to electrical arcing
- CR TBR, Vehicle Stabilizer Recontact with Integrated Vehicle
- CR 4943, Erroneous Vehicle/Tower Excursion Analysis
- CR 4993, Excessive Vehicle Excursion

Below is a complete list of the functions supported by the Vehicle Stabilizer and worst case effects for loss of those functions:
1. Provide T-0 Vehicle Stabilization
- TBD
2. De-mate Stabilizer for Liftoff
- TBD

Program/Element Control References

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version — Page 7 of 9

61

Example of Analysis Cause Sheet

CP-Hazard: 4964 **Cause #:** No information listed	**Program:** Exploration Systems Integrated Causes	**Milestone Review:** GSDO PDR **Closure Status:** Final for GSDO PDR
Title: Malfunction of the Vehicle Stabilizer during Operations including Separation due to Inadequate Analysis, Design Definition, or Operational Procedures		

NOTE: Related Watch Item # 5118 - Control Methodology Needed for Requirements Resulting from Integrated Analyses

Trade Studies

SLS-TRADE-0050: SLS On Pad Tie-Down Trade

During the SLS DAC2 loads analyses, it was predicted that gapping would occur between the booster aft skirt and vehicle support posts (VSP) during the liftoff sequence after RS-25 ignition, but before booster ignition. Any gapping or slippage between the booster aft skirt and VSP results in non-linear behavior of the joint. Non-linear behavior of the joint invalidates the vehicle design loads and design load indicators as well as increases the risk of vehicle on-pad instability. Midway through the trade, the mitigation of high ICPS and MPCV load exceedances were identified as additional trade goals.

Due to the added complexity of the MPCV and ICPS liftoff loads, not all possible solutions have been run to ground. Our top three solutions have been presented in detail. The Hard To and Non-T0 with Wind Placarding options satisfy all but one of the trade goals: mitigation of the ICPS loads. The Hard T0 is more effective than the wind placarding that has been studied to date. The Soft T0 option only satisfies the gapping criteria and would need to be combined with wind placarding and possibly Mandrel/Expansion Tube concept. All options carry foward work and some degree of programmatic and technical risk. Solving gapping is easy, solving ICPS liftoff load issues is hard (I'll take this out of the final version). Trade resulted in the opening of SLS-TRADE-0055: T-0 Stay Design.

SLS-TRADE-0055: T-0 Stay Design

Trade Scope - Compare options and recommend the conceptual design for the Vehicle Stabilizer System (VSS) T-0 release.
Recommendation - GSDO to proceed with parallel design on frangible nut and split spool concepts for ~3 months to ~30% design.

Program/Element Control References

Cause Report #

Report Generated: Jan 13, 2014 based on Current Version

Page 8 of 9

62

Slices of the IHA

CAUSE SPECIAL TOPICS – DEBRIS HAZARDS

63

Top-Level View of the ESI IHA: IHA Cause Categories

Debris Hazards

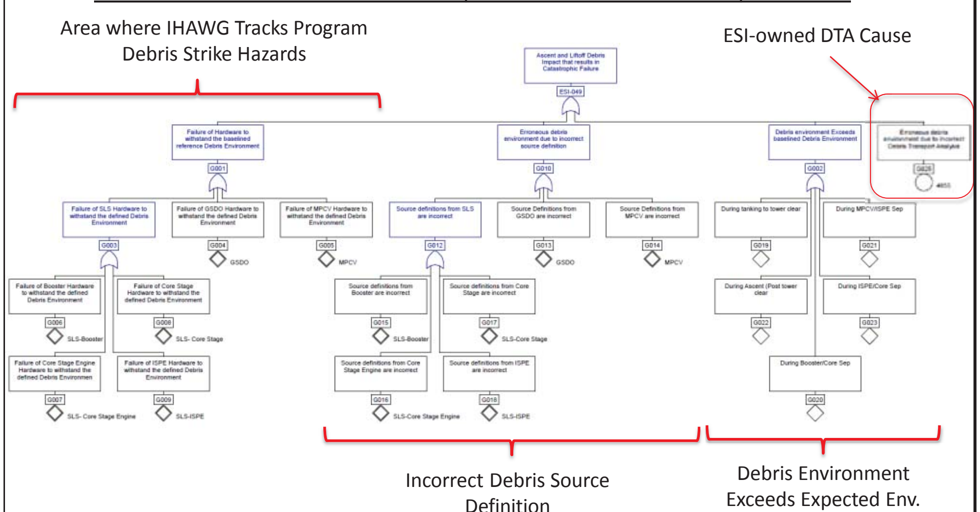
- Generally, debris impacts do not constitute integrated hazards from the strictest sense of the IHA definition.
  - ESD Programs are not required to tolerate strikes from debris liberated by other programs.
- However, assessment of cross-program risks from debris is a highly integrated activity.
  - Debris Transport Analysis needed to estimate likelihood of debris strikes to critical areas of flight and ground systems.
- Approach to debris hazards:
  - Programs identify their debris sources.
  - Cross-Program Debris Team (sub-team under Loads ITT) performs DTA using inputs from Programs. Results (debris environment) will be documented for Program assessment.
  - Programs assess potential damage from debris environment.
  - Results documented in program-owned hazard reports.
  - IHAWG will own cause(s) associated with integrated analysis (DTA).
  - IHAWG will capture/track program-owned debris hazards as events in Cause Tree ESI-049 (Debris Impacts that Result in Catastrophic Failure).

64

Top-Level View of the ESI IHA: IHA Cause Categories

Debris Hazards

ESI-049 – Ascent and Liftoff Debris Impact that Results in Catastrophic Failure



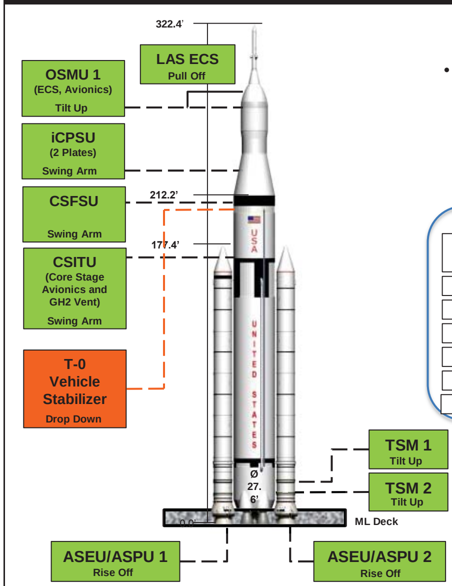
65

Slices of the IHA

CAUSE SPECIAL TOPICS – T-0/UMBILICAL CAUSES

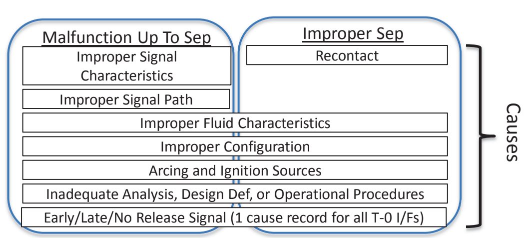
66

Top-Level View of the ESI IHA: IHA Cause Categories



T-0 Interfaces (GSDO-Flight)

- 2 cause trees developed for each T-0 interface:
  - Malfunction of interface up to separation
  - Improper separation
    - Premature separation
    - Failure to properly separate
    - Recontact with flight vehicle



TSMs are both on South side of ML

NOTIONAL

Courtesy of GSDO
Eric Bissonnette LX-S1

67

Top-Level View of the ESI IHA: IHA Cause Categories

- There are 66 IHA Causes related to T-0 Interfaces (Umbilicals and Vehicle Stabilization System)
  - 35% of all Causes (190)
  - 44% of Causes applicable to GSDO PDR (149)
- Cause categorization helped promote commonality and consistency in these causes.
- Special TIMs were convened to address certain T-0 related Cause categories.

68

Slices of the IHA

DISCUSSION OF HIGH-RISK CAUSES

69

Slices of the IHA: High-Risk Causes

- Per ESD S&MA Plan, any hazards with 3x5 LxS or higher are elevated to ESD (ECB) for final acceptance. This would occur later in the life cycle once hazards are finalized (prior to FRR or equivalent).
- At each major program and integrated milestone, the SSAR will contain a brief discussion of each hazard cause that meet the elevation criteria.
  - Discussion is for visibility. Idea is to provide risk acceptor with current risk picture before affordable options for mitigation are lost.
  - SSAR for any given Program milestone will only include high-risk causes applicable to that Program.
- Likelihoods will fluctuate over time with changes in uncertainty, design and design definition, operational definition, etc.
  - Initial likelihoods of IHA causes reflect best understanding of identified controls informed by experience.
- With exception of single watch item associated with one of these causes that was elevated to CPIT, IHAWG does believe any additional management attention is required at this time.

70

Slices of the IHA: High-Risk Causes

- Following charts summarize High-Risk Causes that are depicted in the GSDO PDR version of the SSAR.
  - All high-risk causes will be included in the SSAR at ESD Design Sync

Record	Title	LxS
4302	Bird Strikes During Ascent (to be discussed as Watch Item)	5x5
4424	External H2 due to failure to dilute/inert Lag RS-25 H2	3x5
4426	H2 external to the vehicle due to unburned H2 from core stage APU exhaust	3x5
4428	External H2 due to failure to dilute/inert Lead RS-25 H2	3x5
4610	Loss of SLS to GSDO hardline communication due to improper system characteristics	3x5
4983	Improper load of the ICPS LO2 tank due to Propellant Under fill / Overfill	3x5
4981	Improper load of the ICPS LH2 tank due to Propellant Under fill / Overfill	3x5

71

Record	Title	LxS
4302	Bird Strikes During Ascent (to be discussed as Watch tem)	5x5
4424	External H2 due to failure to dilute/inert Lag RS-25 H2	3x5

- Fuel-rich mixture during on-pad shutdown. Potential for hazard environment external to vehicle if H2 not burned off or diluted.
  - Hydrogen Burn-Off Igniters (HBOIs) placement and analysis in-work so effectiveness is uncertain.
  - Preliminary Rain Bird flow rates and timing for acoustics potentially negate HBOI effectiveness.
  - FireEx activation also affects HBOI operation.
- Cause Likelihood is Moderate: "May occur. Controls exist with some uncertainty.
- SLS PDR RID SLSP-0059:
  - HBOI output will be modeled and HBOIs will be aligned to provide max coverage.
  - Diverter plate on ML to protect HBOIs being modeled.
  - FireEx analysis in work.
- Risk will be reassessed as part of RID closure.
- Cause record likelihood is expected to be categorized as low upon completion of the analysis.

72

Record	Title	LxS
4426	H2 external to the vehicle due to unburned H2 from core stage APU exhaust	3x5

- Core Stage CAPU vents GH2 below the Engine Section. Failure to burn-off the CAPU GH2 as it emerges from the Core Stage exhaust vents could result in hazardous concentrations of hydrogen external to the vehicle.
- Hydrogen Burn-Off Igniters (HBOIs) placement and analysis in-work so effectiveness is uncertain.
- Cause Likelihood is Moderate: "May occur. Controls exist with some uncertainty.
- SLS PDR RID SLSP-0059, HBOI Effectiveness:
  - HBOI output will be modeled and HBOIs will be aligned to provide max coverage for CAPU H2.
- Risk will be reassessed as part of RID closure.
- Cause record likelihood is expected to be categorized as low upon completion of the analysis.

73

Record	Title	LxS
4428	External H2 due to failure to dilute/inert Lead RS-25 H2	3x5

- Fuel-rich mixture during RS-25 start. Potential for hazard environment external to vehicle if H2 not burned off or diluted.
  - Hydrogen Burn-Off Igniters (HBOIs) placement and analysis in-work so effectiveness is uncertain.
- Cause Likelihood is Moderate: "May occur. Controls exist with some uncertainty.
- SLS PDR RID SLSP-0059:
  - HBOI output will be modeled and HBOIs will be aligned to provide max coverage.
- Risk will be reassessed as part of RID closure.
- Cause record likelihood is expected to be categorized as low upon completion of the analysis.

74

Record	Title	LxS
4610	Loss of SLS to GSDO hardline communication due to improper system characteristics	3x5

- Loss of hardline communication could occur if the redundant Ethernet cables, which run in close proximity to each other, were compromised/destroyed, possibly due to a common cause issue.
- Loss of hardline communication could result in:
  - Inability to execute critical functions/commands.
  - Inability to monitor the state of a system, for example the pressure and temperature of a tank or the voltage of a battery.
- Loss could result in catastrophic events such as over stressing structures (over filling, wrong sequence, etc.)
- IHAWG will work with cross-program safing team to capture operational responses to loss of comm events.

75

Record	Title	LxS
4981	Improper load of the ICPS LH2 tank due to Propellant Under fill / Overfill	3x5
4983	Improper load of the ICPS LO2 tank due to Propellant Under fill / Overfill	3x5

- Prop under fill of propellants leads to premature engine shutdown/abort.
- Overfill could cause:
  - Wetting of pressurization diffuser to with potential pressurization control issues.
  - Propellant mass exceeds the mission needs (loss of payload delivery performance).
  - Prop flowing through vent/relief valve possibly causing a fire/explosion.
  - Icing and blockage at the vent relief valve, possibly resulting in an over pressurization and structural failure of the tank.
- Currently many unknowns, TBDs, and TBRs.
  - The number and extent of what analyses to be done.
  - Wet dress rehearsal is the only procedural testing that will be done for verifying the loading requirements of the ICPS.
  - Differential pressure transducer for monitoring the propellant fill level is zero fault tolerant. (SPIO reports that the pressure transducer is only critical during loading, and could be replaced on the pad assuming adequate access . There is currently a trade study underway in regards to the removal of the ICPS access arm.)
- Engineering working the TBD/TBRs and should be matured in the coming months.
  - Once analyses completed and relevant documents are released, the risk should be lowered.

76

Slices of The IHA

ELEVATED IHAWG WATCH ITEMS

77

Slices of the IHA: Elevated Watch Items

- IHA Cause Record #4302, "Bird strikes during ascent"
  - LxS: 5x5
  - Lead Program: GSDO
- Summary:
  - No controls for catastrophic hazard resulting from a bird strike have been identified.
  - Likelihood based on lack of controls and Shuttle experience of 1 strike in
  - Cross-Program Design Specification for Natural Environments (DSNE) defines bird environment (2.2 kg commonly found up to an altitude of 0.5 km above MLP).
    - SLS Program Vehicle Design Environments does not allocate launch/ascent flora/fauna environments to SLS elements as a design requirement.
      - The risk of exposure to this environment to be assessed as part of the hazard analysis
    - Orion System Requirements Document requires Orion to meet its requirements during and after exposure to the environments defined in the Cross-Program DSNE.
      - Actual design capability is uncertain but not expected to meet DSNE based on CxP history*.
    - GSDO has no requirement to provide operational controls for bird strike.
  - WI elevated to CPIT on 12/9/13
    - Action to IHAWG to reassess likelihood using other applicable launch history from KSC & CCAFS.

* In waning days of CxP, Program was moving away from augmenting designs to withstand bird strikes towards using operational controls similar to Shuttle (avian radar, bird abatement, etc.). (reference Orion Change Directive #CEV-00254 and CxP directive C000432)

78

Slices of the IHA

DEEP DIVE WHERE DAN WANTS TO GO

79

Success Stories

AREAS WHERE IHA IMPACTED DESIGN

80

Success Stories: Where IHA Impacted Design

- The development and review of the IHA adds another level of cross-program integration:
  - Cause Tree development and review
  - Cause Development
  - Cause Review
- The IHA team has been identifying issues as the analysis has matured, then passing them on to the design teams through the engineering representatives who then work them as part of their design cycles.
  - With this "as they pop up" approach, the team has not tried to document them unless they remain an issue and end up on the Watch Item List.
  - The next chart contains some examples that have been recalled by members.
- IHAWG has CSI action to track instances where IHA has impacted design or operations.

81

Success Stories: Where IHA Impacted Design

IHA Process Finding	Results
Identified a potential failure tolerance deficiency during umbilical cause tree development that needed further interface work between JSC and KSC.	Design issue was identified and solution being worked in engineering
Requirements for limiting vehicle charging were deemed insufficient for controlling static build-up.	Cross-Program E3 requirements were updated (MPCV 70080).
Identified integrated analyses needed to characterize potential hazards or hazard controls: e.g., MSA hazardous gas analysis; SLS/Orion separation analysis; combined external leakage flammability analysis; core stage pressurization analysis given H2 bleed for APUs.	New analyses are in work.
Identification of LVSA diaphragm as a potential for several hazards which may reduce its intended advantage	Part of trade study to keep/remove diaphragm.
Identified Hydraulic lock up on the engine throttle valve.	Identified integrated cause that needs analysis to determine consequence before working failure tolerance.

82

Success Stories: IHA Status for GSDO PDR

- IHA Team delivered SSAR for GSDO PDR.
  - 70 of 75 Cause Trees
  - 139 of 149 Causes
    - 10 Causes not approved for release (forward work):
      - 7 Inadequate Analysis Causes on umbilicals and CAA
      - 2 causes regarding inadvertent abort while on pad
      - 1 Aft Skirt Purge umbilical configuration
  - SSAR also includes 27 of 33 Causes updated since SLS PDR in response to pre-declared RID:
    - 6 Causes not approved for release:
      - 1 on-hold pending SM/ICPS diaphragm trade study
      - 3 Orion H/W jettison d/t SLS notification
      - 1 RS-25/Booster plume analysis
      - 1 Orion S-Band comm
- Other forward work includes updated program cause accountability matrix.

83

Forward Work for IHA

84

Forward Work: IHA Model Completeness & Sustainability

- As acknowledged prior to adoption of the ESI IHA methodology, the lack of a comprehensive model could result in gaps in the analysis.
- In addition, the current IHA model (Cause Trees) may not be easily maintainable or sustainable in the long run.
  - The Cause Trees are not logically linked together and therefore have no easily recognizable relationship to each other.
  - Related causes are spread across multiple trees (e.g., fire/explosion).
  - Future owners and reviewers of the IHA will need specific understanding of the unique methodology employed in order to maintain the model.
- The IHAWG will evaluate options for evolving the current cause tree structure with the goal to have a comprehensive and sustainable model by the ESI Design-To Sync point.
- Planned completion: ESI Design Sync

85

Forward Work: Vehicle Safing in Response to Failures

- The IHA addresses conditions that may lead to realization of a critical or catastrophic outcome. However, not all of these conditions are imminently critical or catastrophic depending on time of occurrence and/or responses to initiating conditions.
- Loss of comm and loss of power between GSDO and flight systems (as examples) are assessed with a catastrophic severity. However, mitigations may be implemented such as safing responses (automated on flight systems) and operational work-arounds.
- The IHAWG is participating in the ad hoc cross-program team looking at potential responses to such initiating events.
  - IHAWG will provide hazardous scenarios from the IHA.
  - Proposed safing operations will be assessed as part of the IHA.
- Planned completion: Orion Δ-PDR

86

Forward Work: MM/OD

- MM/OD is not currently included in the IHA.
- IHAWG will assess need for inclusion of MMOD in new or existing cause tree(s).
- Planned completion: Orion Δ-PDR

87

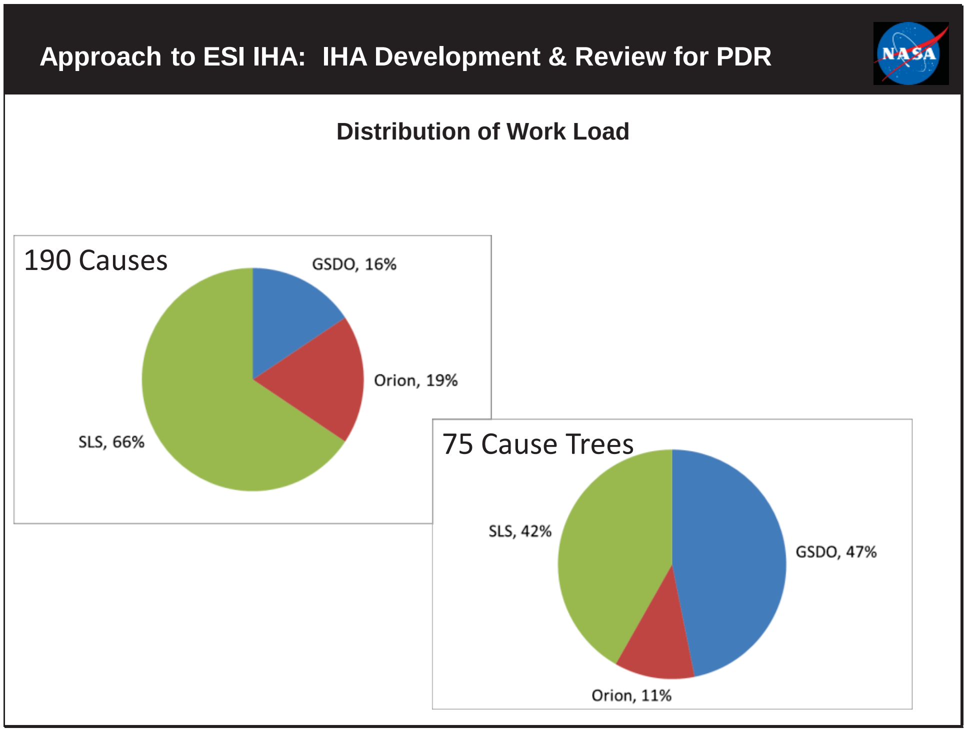
Forward Work: Road to Orion Delta-PDR and ESI Sync Point

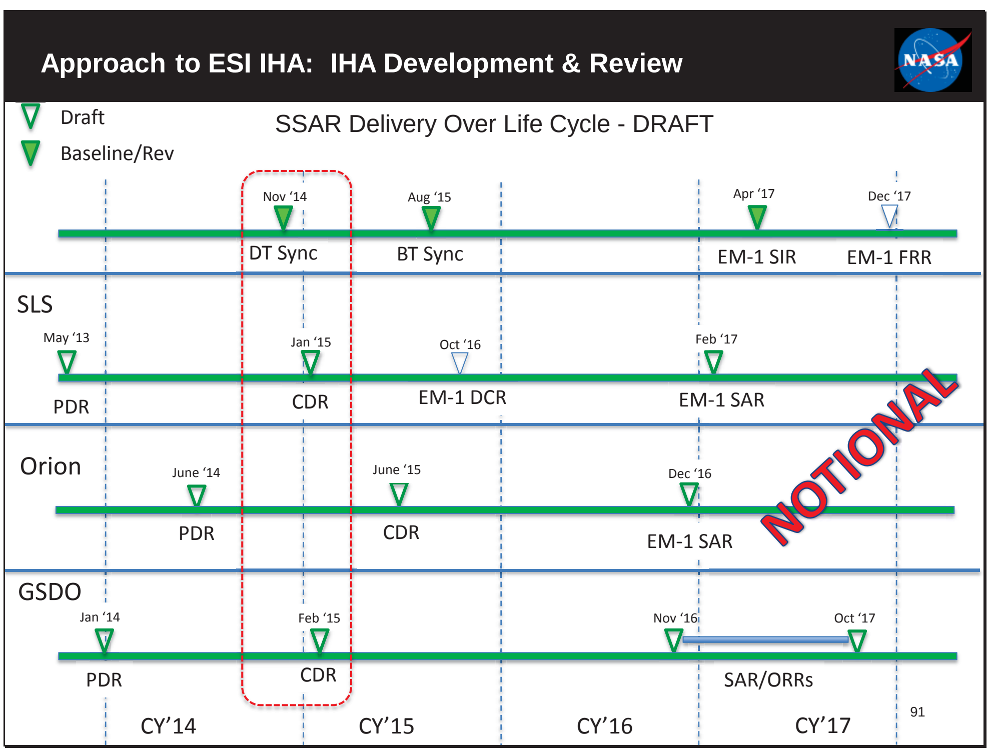
- Beyond forward work already discussed, IHAWG at a minimum will:
  - Update causes and cause trees as needed
  - Improve commonality and consistency across IHA content
  - Improve cohesiveness between causes and cause trees (or future model)

88

Backup

89


Approach to ESI IHA: IHA Development & Review for PDR
Distribution of Work Load
190 Causes
GSDO, 16%
Orion, 19%
SLS, 66%
75 Cause Trees
SLS, 42%
GSDO, 47%
Orion, 11%


Approach to ESI IHA: IHA Development & Review
Draft
Baseline/Rev
SSAR Delivery Over Life Cycle - DRAFT
Nov '14
DT Sync
Aug '15
BT Sync
Apr '17
EM-1 SIR
Dec '17
EM-1 FRR
SLS
May '13
PDR
Jan '15
CDR
Oct '16
EM-1 DCR
Feb '17
EM-1 SAR
NOTIONAL
Orion
June '14
PDR
June '15
CDR
Dec '16
EM-1 SAR
GSDO
Jan '14
PDR
Feb '15
CDR
Nov '16
Oct '17
SAR/ORRs
CY'14
CY'15
CY'16
CY'17
91

3x5 Cause Records

- Cause record number 4408 – Structural Failure of the MPCVP to SLSP Interface due to Improper Loads Analysis or Definition during Ascent up to SM Separation
  - **Engineering Lead: Rumaasha Maasha** **S&MA Lead: Cody Hawes**
  - **Potential Consequences** – Improper loads definition leads to load exceedances during ascent due to unknowns/uncertainties within the analysis leads to structural failure of the interface and/or vehicle.
  - **Current Control Strategy** – To ensure analysis has adequate margin and conservatism or low uncertainty. Engineering will acquire modal data from a planned series of tests that include element static structural tests, element modal tests, a modal survey of the integrated vehicle in the VAB, and an instrumented roll-out. Engineering expects these test to provide sufficient data to confirm/validate the integrated vehicle model.
  - **Current Verification Strategy** – Review and approval of the analysis and methodology by the Joint Loads Task Team (JLTT). Validation of models via the rollout and modal test. Engineering will review data from the modal survey and compare it to the model; any significant outliers could potentially delay the launch until the correlation between the model and the test is better understood.
  - **Likelihood Justification** – The likelihood of structural failure due to an improper loads analysis/definition is currently ranked as moderate due to the uncertainty within the design; however, the uncertainty factors applied during the analysis/model and the FoS used during hardware design help mitigate the risk of loads exceeding the structural capability. The modal survey test should drive out potential discrepancies within the model.
  - **Recommendations** – Based on the better understanding of the application of uncertainty factors and FoS, recommend lowering likelihood to 2x5 (Low). Although it is possible to have errors within the loads definition process the uncertainty factors applied to the analysis and FoS applied to hardware design make the possibility of structural failure due to an improper loads definition low. Likelihood may be lowered more as the design matures and as the uncertainty within the analysis decreases.

92

3x5 Cause Records

- Cause record number 4424 - External H2 due to failure to dilute/inert Lag RS-25 H2
  - **Engineering Lead: Louise Strutzenberg** **S&MA Lead: Janette May**
  - **Potential Consequences** - Following an on-the-pad engine shutdown, the engine is designed to shutdown with a hydrogen lag which provides a fuel-rich environment to prevent LOX-rich combustion and hardware burn-through. Failure to burn-off the Lag GH2 as it emerges from the Core Stage Engine (CSE) nozzle could result in hazardous concentrations of hydrogen external to the vehicle, which could lead to a fire/explosion.
  - **Current Controls:**
    - Design: HBOI System function for lag H2 is identified in ICD-052-01
    - Design: The HBOIs shall be configured with sufficient directional redundancy to prevent accumulation of H2 for all applicable environmental conditions and redundancy in the event of HBOI failure to operate. Configuration of the HBOI system will be documented in SLS-ICD-052-03
    - Operational: A complete ground checkout of the HBOI will be performed prior to launch.
    - *Placeholder Control: Firex water system may improve or worsen dilution of Lag H2 depending timing, location, etc. Will consider all aspects of the pad configuration including Firex timing and location in the analysis*.
  - **Current Control Strategy** – Hydrogen Burn-Off Igniters (HBOIs) or "sparklers" are used to burn-off the vented GH2 by ejecting hot particulates. The HBOI system is mounted on the mobile launcher near the SLS core stage engine nozzles and is comprised of 6 pairs of HBOIs to provide redundant coverage for the 4 SLS CSEs and the 2 CAPU exhaust vents.
  - **Current Verification Strategy** – TBD analysis will be performed to verify HBOIs will be adequate to ignite Lag GH2 based on engine-provided allowable leak rates. . Analysis will be documented in SLS-HDBK-033, SLSP Vehicle Acoustic Data Book. HBOI alignment will be performed to ensure adequate coverage of all four engines.
  - **Likelihood Justification** – HBOI placement and analysis are currently in-work and therefore the effectiveness of the HBOIs are uncertain. Also, preliminary Rain Bird water flow rates and timing requirements for mitigating the acoustic environments hazard, compromises, or completely removes the HBOIs to effectively mitigate unburned Lag GH2 by potentially deflecting or quenching the HBOI output (hot particulates). Firex water (used to cool the surrounding surfaces to prevent re-ignition/explosion events during on-the-pad engine shutdown) may also worsen (or improve) HBOI effectiveness. Per SLS-RQMT-015, Moderate definition: *May occur. Controls exist with some uncertainties.*

National Aeronautics and Space Administration

93

3x5 Cause Records

- Cause record number 4424 - External H2 due to failure to dilute/inert Lag RS-25 H2 (continued)
  - **Recommendation** – The HBOI output will be modeled and then aligned to provide maximum coverage with both systems operating across the modeled Main Engine Nozzle exit plane. A diverter plate on the ML to cascade rain bird water around HBOIs is currently being modeled. Firex water analysis on Lag GH2 during pad abort is in-work. Analysis supports PDR RID SLSP-0059, *HBOI Effectiveness*. Re-assessment of the risk level will be a part of its closure. This cause record is expected to be categorized as low upon completion of the analysis.

National Aeronautics and Space Administration

94

3x5 Cause Records

- Cause record number 4426 – H2 external to the vehicle due to unburned H2 from Core Auxiliary Power Units (CAPU) exhaust
  - **Engineering Lead: Louise Strutzenberg** **S&MA Lead: Janette May**
  - **Potential Consequences** – Core Stage CAPU system has been designed to vent GH2 below the Engine Section. Failure to burn-off the CAPU GH2 as it emerges from the Core Stage exhaust vents at engine start could result in hazardous concentrations of hydrogen external to the vehicle, which could lead to a fire/explosion.
  - **Current Controls:**
    - Design: The HBOIs shall be configured with sufficient directional redundancy to prevent accumulation of H2 for all applicable environmental conditions and redundancy in the event of HBOI failure to operate. Configuration of the HBOI system will be documented in SLS-ICD-052-03
    - Operational: A complete ground checkout of the HBOI will be performed prior to launch.
  - **Current Control Strategy** – Hydrogen Burn-Off Igniters (HBOIs) or “sparklers” are used to burn-off the vented GH2 by ejecting hot particulates. The HBOI system is mounted on the mobile launcher near the SLS core stage engine nozzles and is comprised of 6 pairs of HBOIs to provide redundant coverage for the 4 SLS CSEs and the 2 CAPU exhaust vents.
  - **Current Verification Strategy** – TBD analysis will be performed to verify HBOIs will be adequate to ignite CAPU H2 based on Core-provided allowable leak rates. . Analysis will be documented in SLS-HDBK-033, SLSP Vehicle Acoustic Data Book. HBOI alignment will be performed to ensure adequate coverage of both CAPU exhaust vents.
  - **Likelihood Justification** – HBOI placement and analysis are currently in-work and therefore the effectiveness of the HBOIs are uncertain. Per SLS-RQMT-015, Moderate definition: *May occur. Controls exist with some uncertainties.*
  - **Recommendations** – The HBOI output will be modeled and then aligned to provide maximum coverage with both systems operating across the modeled CAPU exhaust vents. Analysis supports PDR RID SLSP-0059, *HBOI Effectiveness*. Re-assessment of the risk level will be a part of its closure. This cause record is expected to be categorized as low upon completion of the analysis.

95

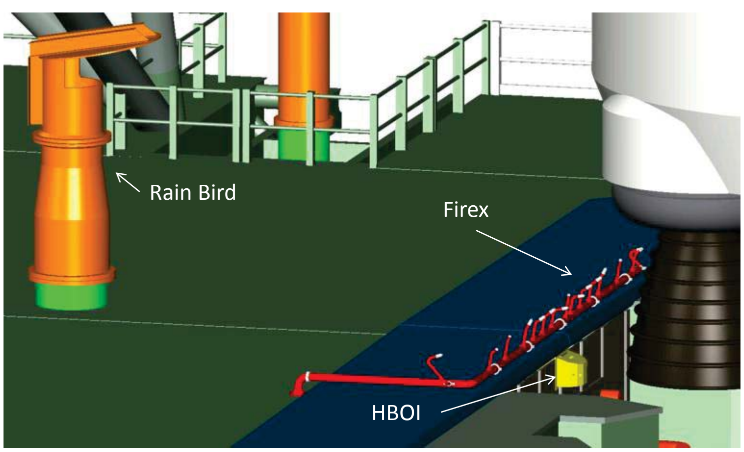
3x5 Cause Records

- Cause record number 4428 – External H2 due to failure to dilute/inert Lead RS-25 H2
  - **Engineering Lead: Louise Strutzenberg** **S&MA Lead: Janette May**
  - **Potential Consequences** – The engine is designed to start with a hydrogen lead which provides a fuel-rich environment to prevent LOX-rich combustion and hardware burn-through. Failure to burn-off the Lead GH2 as it emerges from the Core Stage Engine (CSE) nozzle prior to engine start could result in hazardous concentrations of hydrogen external to the vehicle, which could lead to a fire/explosion.
  - **Current Controls:**
    - Design: HBOI System function for Lead H2 is identified in ICD-052-01
    - Design: The HBOIs shall be configured with sufficient directional redundancy to prevent accumulation of H2 for all applicable environmental conditions and redundancy in the event of HBOI failure to operate. Configuration of the HBOI system will be documented in SLS-ICD-052-03
    - Operational: A complete ground checkout of the HBOI will be performed prior to launch.
  - **Current Control Strategy** – Hydrogen Burn-Off Igniters (HBOIs) or "sparklers" are used to burn-off the vented GH2 by ejecting hot particulates. The HBOI system is mounted on the mobile launcher near the SLS core stage engine nozzles and is comprised of 6 pairs of HBOIs to provide redundant coverage for the 4 SLS CSEs and the 2 Core Auxiliary Power Units (CAPU) exhaust vents.
  - **Current Verification Strategy** – TBD analysis will be performed to verify HBOIs will be adequate to ignite Lead H2 based on engine-provided allowable leak rates. Analysis will be documented in SLS-HDBK-033, SLSP Vehicle Acoustic Data Book. HBOI alignment will be performed to ensure adequate coverage of all four engines.
  - **Likelihood Justification** – HBOI placement and analysis are currently in-work and therefore the effectiveness of the HBOIs are uncertain. Per SLS-RQMT-015, Moderate definition: *May occur. Controls exist with some uncertainties.*
  - **Recommendations** – The HBOI output will be modeled and then aligned to provide maximum coverage with both systems operating across the modeled Main Engine Nozzle exit plane. Analysis supports PDR RID SLSP-0059, *HBOI Effectiveness*. Re-assessment of the risk level will be a part of its closure. This cause record is expected to be categorized as low upon completion of the analysis.

96

3x5 Cause Records

- Background



National Aeronautics and Space Administration

97

3x5 Cause Records

- Background

4.1.7 Hydrogen Burn off Igniter (CL-8000)

The purple shaded cones shown in Figures 4-52, 4-53, and 4-54 notionally depict the coverage of the Hydrogen Burn Off Igniters (HBOI) for the Core Stage Engines exhaust and TVC CAPU exhaust. The HBOI system will be comprised of 2 sets of 6 each HBOIs (12 total per launch attempt) to provide redundant coverage for the 4 SLS Core Stage Engines and the 2 pairs of Core Auxiliary Power Unit exhaust vents. They will be directed at the SLS Core Stage Main Engines and CAPU exhaust vent pairs. The HBOI output is specified for a 15' minimum throw with a 20° cone pattern. The cone angle pattern will be modeled and then aligned to provide maximum coverage with both systems operating across the modeled Main Engine Nozzle exit plane. CAPU Exhaust Vent HBOIs will be directed at the each of the modeled exhaust vent locations. HBOIs will provide a minimum of 22 seconds burn duration and ignited prior to Core Stage Main Engine start (~ T-10 seconds).

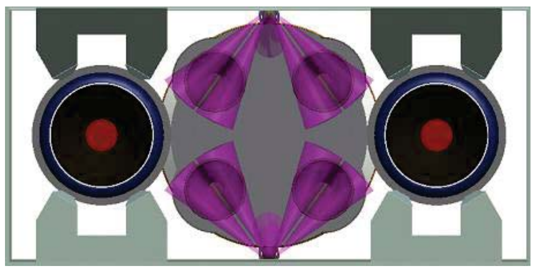


Figure 4-52. HBOI Coverage Bottom View

National Aeronautics and Space Administration 98

3x5 Cause Records

- Cause record number 4582 – Ascent Trajectory Anomaly due to Unexpected Dynamic Response
    - **Engineering Lead: Rumaasha Maasha** **S&MA Lead: Cody Hawes**
    - **Potential Consequence** – Inability to correctly define or characterize the vehicle dynamic modes and responses causes load exceedances and leads to structural failure of the vehicle.
    - **Current Control Strategy** – To ensure analysis has adequate margin and conservatism or low uncertainty. Engineering will acquire modal data from a planned series of tests that include element static structural tests, element modal tests, a modal survey of the integrated vehicle in the VAB, and an instrumented roll-out. Engineering expects these test to provide sufficient data to confirm/validate the integrated vehicle model. Control algorithms are validated through rigorous testing in multiple dynamic situations.
    - **Current Verification Strategy** – Review and inspection of MAVERIC and Monte Carlo models to ensure compliance with the model and simulation plan. Models shall also be validated via the rollout and modal test.
    - **Likelihood Justification** – The likelihood of structural failure due to load exceedances caused by an unexpected dynamic response is currently ranked as moderate due to the uncertainty within the design; however, uncertainty factors applied to the G&NC algorithms used in the analysis and the FoS used during hardware design help mitigate the risk of loads exceeding the structural capability. The margin/uncertainty factors used in the analysis account for uncertainty and errors. The modal survey test should drive out potential discrepancies within the model and it is very unlikely to launch without proper correlation of the model to the test.
    - **Recommendations** – Based on the better understanding of the application of uncertainty factors to the G&NC algorithms and FoS used during hardware design, recommend lowering likelihood to 2x5 (Low). Likelihood may be lowered more as the design matures and as the uncertainty within the analysis decreases.

National Aeronautics and Space Administration 99

3x5 Cause Records

- Cause Record number 4610 – Loss of SLS to GSDO hardline communication due to improper system characteristics
  - **Engineering Leads: Jon Patterson, John Ormsby, and Bob Trapnell S&MA Lead: Early McKnight**
  - **Hazard Cause** – Loss of command/data path communication between Ground Support Design Organization (GSDO) and Space Launch System (SLS) interface during critical operations in the preflight phase of launch resulting in inability to execute functions like opening or closing valves or switches; and inability to monitor the state of a system, for example temperature and pressure of a tank or voltage of a battery.
  - **Potential Consequences** – Potential consequences include over/under filling tanks resulting in structural failure or inability to reach target, inability to safely remove cryogens if required, loss of vehicle power due to under charged/damaged batteries, and failure to process commands. All of which potentially resulting in Loss of Mission (LOM), or Loss of Crew (LOC).
  - **Current Control Strategy** – Currently, controls to ensure a viable communication path with fault tolerance are not ensured. The existence of redundant paths and separation of those redundant paths has been demonstrated to some extent, but common cause potential still exist.
  - **Likelihood Justification** – The likelihood applied to this cause is moderate because of the uncertainty resulting from immaturity of analysis
  - **Recommendations** –
    - GSDO to provide capability to detect loss of communication sufficient to prevent catastrophic failure of vehicle or GSDO
    - SLS to provide capability to detect loss of communication sufficient to prevent catastrophic failure of vehicle system
    - Upon detection of loss of communication, switch to backup communication
    - Upon detection of loss of Safety-critical communication link, SLS and GSDO to provide capability to safe vehicle and/or ground systems as expeditiously as possible in order to minimize risk to crew, vehicle and facilities

100

3x5 Cause Records

- Cause record number 4981 – Improper load of the ICPS LH2 tank due to Propellant Under fill / Overfill
  - **Engineering Lead: Jay Russell S&MA Lead: Dustin Drake**
  - **Potential Consequences** – Under fill of propellants will lead to premature engine shutdown causing loss of vehicle thrust resulting in a mission abort. Overfill could cause the pressurization diffuser to become wetted which could result in potential pressurization control issues. Excessive overfill could result in LH2 flowing through vent/relief valve possibly causing a fire/explosion. Excessive overfill could also cause icing and blockage at the vent relief valve, possibly resulting in an over pressurization and structural failure of the tank. These effects or combination of effects may potentially result in loss of mission, loss of vehicle, or loss of crew.
  - **Current Control Strategy** – The propellant fill level sensor system in conjunction with GSDO control software will allow proper control of propellant flow rates to reach the nominal propellant load per the requirements defined in the ICDs. Operational procedures based on heritage loading information TBD.
  - **Current Verification Strategy** – Testing at the wet dress rehearsal to ensure operational procedures lead to a proper propellant fill level as well as inspection of the ICDs to ensure proper propellant requirements are documented.
  - **Likelihood Justification** – Currently there are many TBDs and TBRs which cause uncertainties in the controls and overall mitigation strategy. The number and extent of what analyses are going to be done is unknown at this time. The wet dress rehearsal is the only procedural testing that will be done for verifying the loading requirements of the ICPS. The differential pressure transducer for monitoring the propellant fill level is zero fault tolerant. Failure of the differential pressure transducer would likely require a de-tanking and roll back to the VAB. SPIO reports claim that the pressure transducer is only critical during loading, and could be replaced on the pad. This assumes there will be adequate access to the ICPS. There is currently a trade study underway in regards to the removal of the ICPS access arm.
  - **Recommendations** – Engineering is working the TBD/TBRs and should be matured in the coming months. Once relevant documents are baseline and the analyses are released, the risk should be lowered. Additionally, perform sensor and software testing to ensure that overfill can be properly detected and that the software will provide the correct response to the situation. Add redundancy to fill level sensor system or accept risk of a de-tanking and roll back assuming access to the ICPS is not available.
- Cause record number 4983 – Improper load of the ICPS LO2 tank due to Propellant Under fill / Overfill
  - **4983 is identical to 4981**

101

Appendix C. ESD Cross Program Safety and Mission Assurance Plan (ESD 10010)

National Aeronautics and Space Administration

ESD - 10010
INITIAL RELEASE - BASELINE
RELEASE DATE: 09/20/2012

CROSS PROGRAM
SAFETY AND MISSION ASSURANCE PLAN

Publicly Available: Release to Public Websites Requires Approval of Chief, Office of Primary Responsibility

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 2 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

REVISION AND HISTORY PAGE

Revision No.	Change No.	Description	Release Date
-	ESD CR-0009	Initial Release (Reference ESD CR-0009) - Establish Baseline – CR Version	07/17/12
-	ESD CR-0009	Initial Baseline Release – Approved Outside of Exploration Systems Development Control Board	09/20/12

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 3 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

TABLE OF CONTENTS

APPENDIX

TABLE

FIGURE

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this plan is to define the approach to integrating the safety, reliability, and quality assurance activities throughout the programs within the Exploration Systems Development (ESD) Division. It explains the integration of Safety and Mission Assurance (S&MA) analyses and activities among the programs to assure the safety and success of integrated missions.

Each program is expected to establish policies and requirements to fulfill the responsibilities agreed upon and documented in this plan. If any program is unable to fulfill its agreed upon responsibilities, changes to the multi-program agreements will be reflected as changes to this plan. This plan does not create the requirement for a program to perform an activity, but this plan is the documentation of the agreements.

This plan defines the S&MA interfaces between the programs, as well as between the programs and Headquarters Office of Safety and Mission Assurance (OSMA) and ESD. This plan, together with the individual program plans listed in section 2.2, responds to the National Aeronautics and Space Administration (NASA) requirement for a Program S&MA Plan identified in NPR 8715.3C, NASA General Safety Program Requirements (paragraph 1.5), and NM 7120-81, NASA Requirements for Program and Project Management (paragraph 4.1.2).

This is a living plan that will be modified as needed to reflect the direction of exploration systems development as part of the capability-driven framework. With the recognition that the development of exploration capabilities is based on a flexible path to multiple destinations, S&MA's approach to integration will need to be flexible as well. The focus of initial S&MA planning is to address the needs of the tactical capability. Although many aspects of the S&MA plan are extensible to future missions and strategic paths, the plan will be updated to adjust to changing strategic directions.

1.2 SCOPE

This plan addresses integrated Safety and Mission Assurance for Space Launch System (SLS) Program, Multi-Purpose Crew Vehicle (MPCV) Program and the Ground Systems Development & Operations (GSDO) Program. Only integrated activities are addressed. Each ESD program is required to have a separate S&MA Plan to address stand-alone activities. Program S&MA Plans are identified in section 2.2. Program S&MA Plans are a necessary component of the total S&MA planning for integrated missions and should be considered as technically linked with this integration plan. The scope of this plan is limited to activities associated with the current ESD Flight Manifest. As Flight Manifest changes this plan will be revised and updated as required to support.

It is the responsibility of the programs to ensure their individual program S&MA activities address the integrated Cross Program S&MA activities identified in this plan.

1.3 CHANGE AUTHORITY/RESPONSIBILITY

Proposed changes to this document will be submitted via a Change Request (CR) to the appropriate ESD Board or Panel for consideration and disposition.

All such requests will adhere to the ESD Configuration Management Change Process.

This plan is maintained by the ESD Safety & Mission Assurance Panel (ESMAP). The appropriate NASA Office of Primary Responsibility (OPR) identified for this document is Johnson Space Center (JSC) Safety and Mission Assurance (S&MA).

Program S&MA Plans are maintained by the cognizant programs, who retain change authority for those plans.

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. The documents listed in this paragraph are applicable to the extent specified herein.

Document Number	Document Revision	Document Title
ESD 10011		Cross Program Probabilistic Risk Assessment Methodology

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document.

Document Number	Document Revision	Document Title
NPD 8700.1E		NASA Policy for Safety and Mission Success
NPR 8715.3C		NASA General Safety Program Requirements
NM 7120-81		NASA Space Flight Program and Project Management Requirements
NASA-STD- 8709.20		Management of Safety and Mission Assurance Technical Authority (S&MA TA) Requirements
NPR 8715.5A		Range Flight Safety Program
NPR 8705.2B		Human-Rating Requirements for Space Systems

Document Number	Document Revision	Document Title
NPR 8000.4		Agency Risk Management Procedural Requirements
NASA/SP-2010-576		NASA Risk-informed Decision Making Handbook
NASA/SP-2011-XXX		NASA Risk Management Handbook
NPR 8705.5A		Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
NPR 8705.6		Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments
NPR 8715.6A		NASA Procedural Requirements for Limiting Orbital Debris
NASA-HDBK-8719.14		Handbook for Limiting Orbital Debris
CxP 75081		Crew Survival Analysis Report for Cx PDR
ESD 10012		ESD Concept of Operations
ESD 10001		Explorations Systems Development Implementation Plan
MPCV 72008		Multi-Purpose Crew Vehicle Program Plan
SLS-PLAN-001		Space Launch System Program Plan
GSDO-PLN-1000		GSDO Program Plan
MPCV 72094		Multi-Purpose Crew Vehicle Safety and Mission Assurance Plan
SLS-PLAN-013		Space Launch System Safety and Mission Assurance Plan
GSDO-PLN-1036		Ground Systems Development & Operations Safety and Mission Assurance Plan
MPCV 72223		MPCV Mishap Response and Contingency Action Plan
<TBD-001>		Space Launch System Mishap Response and Contingency Action Plan
ESD 10002		Exploration Systems Development (ESD) Requirements
ESD 10003		ESD Risk Management Plan
SAE ARP4761		Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
MIL-STD-882		System Safety Program Requirements
NASA Reference Publication 1358		System Engineering "Toolbox" for Design-Oriented Engineers
NPD 1000.1		NASA Strategic Management Handbook
NPD 7120.5		NASA Requirements for Program and Project Management
NPR 8621.1		NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping

3.0 MANAGEMENT AND ADMINISTRATION

3.1 SAFETY AND MISSION ASSURANCE TECHNICAL AUTHORITY

In accordance with NPD 1000.1, NASA Strategic Management Handbook, and NPR 7120.5 NASA Requirements for Program and Project Management, NASA has implemented the S&MA Technical Authority governance strategy for ESD programs. The Chief of NASA Headquarters Office of Safety and Mission Assurance (OSMA) delegates program S&MA technical authority to the Center Director for the program's host center, who has further delegated authority to the Center S&MA Director. Each Center S&MA Director has in turn, identified a Chief S&MA Officer (CSO) for each program. In addition, the NASA Headquarters OSMA requires an Integration Chief S&MA Officer whose responsibilities include assuring that S&MA integrated tasks and integrated risks are properly identified and addressed.

3.2 SAFETY AND MISSION ASSURANCE ORGANIZATION

Organization of S&MA within each ESD program is defined in program S&MA plans identified in section 2.2. This plan will address the organization of integrated S&MA teams and the relationship to joint program engineering and program management groups.

Each program has a responsibility to identify the individual who has responsibility for safety, reliability, and quality engineering and assurance functions within the program. Each program has delegated this responsibility to the Center S&MA organization, who in turn has identified the Program CSO and the program's manager of S&MA functions. The Center's S&MA Director determines how the CSO and program's manager of S&MA functions is implemented (dual or separate roles). The Integration CSO, together with the program CSOs, form the management nucleus which manages all S&MA functions in the ESD programs. There is no single S&MA person with authority over all ESD S&MA functions. Program CSOs have authority over program S&MA functions and risks. The Integration CSO has authority over integrated S&MA functions and risks. The Integration CSO and the Program CSOs are voting members of the ESD and Program Boards and Panels as defined in their respective charters.

Because each Center S&MA organization and Program CSO has dual accountability for Technical Authority and program S&MA functions, the Program CSO also has a dual reporting path as depicted in Figure 3.2-1. Similarly, the Integration CSO has a dual reporting path to both Center S&MA and the Program Director. General S&MA Program and Technical Authority responsibilities are depicted in Table 3.2-1. Responsibilities for the individual CSOs are shown in Table 3.2-2.

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 10 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

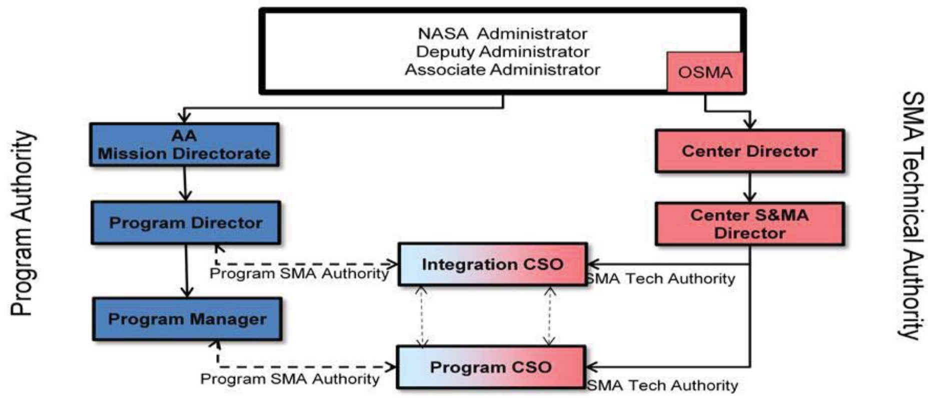


FIGURE 3.2-1 S&MA DUAL MANAGEMENT FRAMEWORK

SEPARATION OF PROGRAM AND S&MA TECHNICAL AUTHORITY

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 11 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

TABLE 3.2-1 S&MA PROGRAM AND TECHNICAL AUTHORITY RESPONSIBILITIES

Program S&MA Authority	S&MA Technical Authority
• Directing and controlling the S&MA elements of the program • Program/project S&MA requirement development • Prime contract Statement of Work (SOW)/Data Requirements development and performance evaluation • S&MA budget/resource management (cost authority) • Management/oversight of S&MA product development (schedule authority) • Management of program/project Quality Management System (QMS) • Status reports, metrics, and risk reports for S&MA Work Breakdown Structure (WBS)	• Serving as member of program or project control boards, change boards, and internal review boards to assure compliance with S&MA Technical Authority requirements and concur on the acceptability of residual safety risk. • Provide concurrence on the technical suitability of S&MA products provided for program/project approval. • Assuring proper flowdown and application of S&MA Technical Authority requirements, and providing interpretation of such requirements as needed. • Assuring that requests for waivers or deviations from Technical Authority requirements are submitted to and acted upon by the appropriate level of Technical Authority. • Assuring proper disposition of Dissenting Opinions.

TABLE 3.2-2 S&MA PROGRAM MANAGEMENT

Position	Responsibilities	Primary Customers
Integration CSO	• S&MA rep to Exploration Systems Development Control Board (ESDCB) • Ensures all S&MA integration tasks are planned and accomplished • Ensures integrated S&MA risks are identified, characterized, and resolved appropriately • Leads the ESD S&MA Panel	• JSC S&MA Director • NASA Chief of S&MA • ESD Program Director • ESD Chief Systems Engineer
SLS CSO	• Program's S&MA management • S&MA rep to SLS Program Control	• Marshall Spaceflight Center (MSFC) S&MA

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 12 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

	Board (PCB) • SLS rep to ESD S&MA Panel • Ensure program's integration tasks and products are accomplished per agreed-to technical scope and schedule	Director • SLS Program Manager • Integration CSO • SLS Chief Engineer
MPCV CSO	• Program's S&MA management • S&MA rep to MPCV PCB • MPCV rep to ESD S&MA Panel • Ensure program's integration tasks and products are accomplished per agreed-to technical scope and schedule	• JSC S&MA Director • MPCV Program Manager • Integration CSO • MPCV Chief Engineer
GSDO CSO	• Program's S&MA management • S&MA rep to GSDO PCB • GSDO S&MA rep to ESD S&MA Panel • Ensure program's integration tasks and products are accomplished per agreed-to technical scope and schedule	• Kennedy Space Flight Center (KSC) S&MA Director • GSDO Program Manager • Integration CSO • GSDO Chief Engineer

3.3 ESD S&MA PANEL (ESMAP)

The ESD S&MA Panel was created as a forum for ESD program S&MA representatives to discuss integrated S&MA activities and products, and collaborate on planning for accomplishment of these integrated activities. The charter for the ESD S&MA Panel is detailed in ESD Management Directive 12006. It describes the scope, purpose, responsibilities, authority, and membership of the ESD S&MA Panel. The relationship of the ESD S&MA Panel to other ESD boards, panels, and forums is represented in ESD 10001, ESD Implementation Plan.

In order to accomplish some integrated S&MA activities, the ESD S&MA Panel will create Integration Working Groups (IWGs) comprised of subject matter experts from each affected program. The IWG's collaborate on specific integrated products and processes to determine the need for commonality of products or processes, the appropriate governing requirements/agreements, data exchange requirements, and program responsibilities. The IWGs manage the execution of the integrated activities and the development of the integrated products. The ESMAP will document and maintain task agreements that describe S&MA IWG scope, tasks, products, membership, and relevant schedules. Generally, these task agreements are approved by the ESMAP chair and the CSOs from the participating programs. Where IWGs include membership from organizations outside of S&MA, the ESMAP will obtain the appropriate concurrence of the affected organizations.

The current S&MA integrated working groups are identified below.

TABLE 3.3-1 S&MA INTEGRATED WORKING GROUPS

IWG	Responsibilities	Lead
Integrated Hazard Analysis Working Group (IHAWG)	• Define Integrated Hazard Analysis (IHA) process • Develop the IHA • Manage the IHA approval and risk acceptance process • Integrate with Integrated Probabilistic Risk Assessment (IPRA)	SLS
Cross Program PRA Team (XPRAT)	• Support Level 1 requirement development • Establish Probabilistic Risk Assessment (PRA) methodology • Develop the IPRA • Manage the IPRA reporting and risk mitigation process • Integrate with IHA • Cross Program Loss of Crew (LOC)/Loss Of Mission (LOM) Verification	MPCV
Quality Assurance IWG	• Determine Quality Assurance (QA) requirements for Hardware (HW)/Software (SW) handover and manage related QA processes • Develop and manage closed-loop process for SLS/MPCV Government Mandatory Inspection Points (GMIPs) in GSDO • Develop and manage inter-program Problem Reporting and Corrective Action System (PRACA) process • Develop and manage an integrated audit strategy	SLS

3.4 S&MA REQUIREMENTS

NASA Headquarters Office of Safety and Mission Assurance levies NASA safety and mission assurance policies, requirements, and standards on each program. Refer to

NPR 8709.20, Management of Safety and Mission Assurance Technical Authority (S&MA TA) Requirements, for more information on the process by which S&MA TA requirements are levied, assessed for applicability, and reconciled for each program. Each program, through an agreed upon process, will evaluate the OSMA applied S&MA TA requirements and resolve applicability, tailoring, or exceptions/deviations with program management, Center S&MA, and OSMA. The Program CSO is responsible for assuring the appropriate S&MA TA requirements are determined, applied on the program, and traceable to program requirements and contracts, and any exceptions or deviations have been appropriately resolved.

Each program will have S&MA requirements documented in program-controlled documentation. There will not be an integrated S&MA requirements document applied on all three programs.

The Integration CSO reviews each program's S&MA requirements applicability and traceability reports and concurs (for visibility) on each product. In the event of disagreements between a program and OSMA regarding applicability or implementation of OSMA requirements, the Integration CSO determines the final disposition. Programs may appeal to the Chief, NASA OSMA if required.

3.5 BUDGET AND RESOURCES

Each program budgets for S&MA resources, as well as the associated engineering and institutional resources, to fulfill its responsibilities as defined by this plan. Some resources, such as databases, may be shared among the programs and funding is arranged on a case-by-case basis.

3.6 S&MA IN THE CAPABILITY-DRIVEN FRAMEWORK

The capability-driven framework creates an expectation of systems development to support multiple possible future missions. As such, the S&MA processes must support current systems development activities, while also being flexible to adjust to strategic changes in the future as decisions are made. Current S&MA planning is limited to the ESD Flight Manifest (currently EM1 and EM2, which have documented design reference missions). S&MA design analysis work (hazard analysis, Failure Modes and Effects Analysis (FMEA), PRA on initial ESD systems for the tactical capability will assume the EM1 and EM2 Design Reference Missions (DRMs).

The majority of hazard analysis and FMEA work identifies failures and consequences of hardware/software systems and such scenarios are not dependent on the mission. The ability of the hazard analysis and FMEA to influence the design is still possible even without a confirmed mission or missions. This is particularly true for SLS and GSDO where systems and operations are largely common across multiple missions.

FMEAs are performed on system and component designs. The failure effects are described at multiple levels, including the effects on the mission and crew. FMEAs may require updates over time to incorporate new or different missions and mission effects. These updates may or may not change the risk or acceptability of critical items for the chosen missions, but re-evaluation of critical items by program management will be conducted when such risk changes occur.

While specific missions and operations can introduce new hazards, a portion of the hazard analysis is based on identifying system failures as hazard causes. The hazard analysis can still influence system design for these causes as part of the capability-driven framework. As specific missions are defined, the hazard analysis will be updated for each flight to reflect flight-specific hazards that may arise.

4.0 SAFETY

4.1 FLIGHT SYSTEM SAFETY

4.1.1 System Safety/Hazard Analysis Process

Each ESD program is required to establish a system safety analysis and engineering process, which includes hazard analysis requirements in compliance with Agency NASA Procedural Requirements (NPRs). This process should be documented in individual program S&MA plans and be consistent with the hazard risk acceptance matrix in Figure 4.1.3-1. Establishing a safety review panel is not required; however, each program will ensure that the required stakeholders are included in the review and approval of the system safety analysis as shown in section 4.1.9.

4.1.2 Cross Program Integrated Hazard Analysis Approach and Methodology

The Cross Program Integrated Hazard Analysis (CPIHA) is a coordinated effort by more than one program to analyze the hardware interfaces, system interactions, and interdependencies to identify the Cross Program Integrated Hazards (CPIHs), causes and effects. The CPIHA timeframe is bounded by Pre-launch Cryo-loading at the pad to post-flight crew egress. A CPIH is defined as any hazard in which more than one program is a contributing cause, control, or verification for the hazard. CPIHs require more than one program to contribute to the analysis of the system effect, the interactions/interfaces, and interdependencies of the hazard. The CPIHA will provide the controls necessary to manage or mitigate the risk crossing the interface and assess the impact or effects of the residual risk between programs. CPIH causes are causes for which controls are outside any one program or controls that involve Cross Program Integrated Hazard Analysis.

The CPIHA process is owned by the Integrated Hazard Analysis Working Group (IHAWG). (See IHAWG Task Agreement for membership and other details.) All stakeholders are provided access to meetings and any information maintained by the

IHAWG for full visibility of the IHA process and results. If any stakeholder disagrees with IHAWG decisions or results, the concern can be addressed with the IHAWG or elevated to higher forums (e.g. ESMAP, JPCB, ESD CB) as required for resolution.

Information sources which aid identification of CPIHs include (but are not limited to): concept of operations; integrated mission and functional analyses; generic/standardized hazard identification checklists; prior failure history; DRMs; mission timelines; flight test objectives; hardware/Ground Support Equipment (GSE) designs; individual program hazard reports; Interface Control Documents (ICDs); Space Shuttle or Constellation fault trees, hazard analyses, FMEAs; and PRA models. The CPIHA will only be performed for baselined missions (EM-1 and EM-2) rather than all design reference missions.

Hazard Analysis will be performed at the Program and Cross Program Level, and will address design and operational hazards associated with flight and ground hardware, software, operations, training, maintenance, and environments (including facilities) used in the successful execution of all design reference missions. Ground systems (GSE and Government Furnished Equipment (GFE) delivered to the GSDO Program) that are owned by SLS or MPCV, and used during ground processing, will have the hazard analysis performed by the owning Program. MPCV and SLS will deliver such hazards to GSDO for review and incorporation into GSDO safety and operations products as needed. MPCV and SLS will support hazard analysis development activities by providing data or analysis results as required by IRDs or other bilateral agreements for pre-flight activities associated with the respective Program system. Emergency systems will be analyzed for hazards potentially occurring during otherwise nominal operations that are associated with the existence of the emergency system (e.g., Launch Abort System (LAS) failure to jettison, inadvertent operation). Hazard analysis will not be performed on emergency equipment in emergency or crew survival operations.

The CPIHA, performed with participation from all Programs' engineering and safety organizations, will determine a preliminary list of CPIH topics. Other stakeholders including flight crew, mission operations, and health and medical also provide input to the CPIHA. The list of CPIH topics will be updated as necessary due to design maturity or design/operational concept changes. Cause trees will be developed from the list of hazard topics. The cause trees are used to identify the CPIH causes and the program only causes for each hazard topic. CPIH causes will be assigned to the accountable program to be developed with engineering and safety technical authority representatives (or their designees) from the affected programs to define controls and verifications. Any causes determined to be program-only will be passed to the identified program for further evaluation. Individual programs will be responsible for verification that program-only hazard causes have been properly mitigated

The IHAWG will oversee the development of the Cross-Program Integrated Hazard Analysis and is responsible for tracking the schedule and status of the CPIH causes. The IHAWG will assign an S&MA and Engineering representative to be responsible for the collaborative effort to generate and develop each CPIH cause. Engineering is accountable for the cause effect and design mitigation strategy which includes controls and verification. S&MA will provide the process expertise and will ensure completeness by assuring all the controls, verifications, consequences and likelihood have been addressed. In addition, S&MA will coordinate with the other program stakeholders (Crew, Operations, Health & Medical) as required concerning other risk mitigation strategies (crew survival or operations options). Mission operations, as well as crew and Health and medical are accountable for working with S&MA and engineering to ensure any operations controls are credible and can be implemented.

The CPIHA will identify CPIH causes throughout the life cycle of the programs. The ESD Programs will be responsible for verification that the risk associated with Program only causes identified during the integrated hazard analysis have be properly mitigated. Each CPIH cause will be assigned a severity and likelihood level using the severity and likelihood definitions in Figure 4.1.3-2 and Figure 4.1.3-3, respectively. Classification of risk will be based upon controls and verifications (as expected to be implemented); acceptance rationale will be developed at the cause level. CPIH causes and a top risk list with CPIHA issues will be developed and made available for review as part of individual program Preliminary Design Reviews (PDRs) and Critical Design Reviews (CDRs).

While each program may have program-unique requirements for hazard product format or content, CPIHA products (hazard causes and risk sheets) will be developed based on the common set of requirements described in this plan. CPIHA products will be documented using a common set of hazard database fields. The CPIHA product content will be housed and maintained in a configuration controlled hazard analysis database. This database is required for sharing CPIHA product information between programs. The database is not required for program-unique hazard product development, although it may be used for such by any program.

4.1.3 Hazard Risk Acceptance

Consistent with the NPD 1000, NASA Governance Model; NPD 8700.1, NASA Policy for Safety and Mission Success; and the NASA Interim Directive for NPD 7120.5D, the NASA Programmatic Authority has the responsibility to formally accept residual safety risks with the concurrence of the program Technical Authorities. Hazard products are used as a mechanism to fulfill this responsibility, and will be presented to Program Management, Cross Program Management, and the Technical Authorities for formal risks acceptance. The level of management required to approve the hazard risk products and accept residual risk is determined by the risk level of the hazard. ESD owns the integrated risk acceptance products which the IHAWG manages. The Cross Program hazard risk acceptance strategy is depicted in the Figure 4.1.3-1, with hazard severity and likelihood definitions defined in Figure 4.1.3-2 and Figure 4.1.3-3, respectively.

MPCV or SLS ground hazard analyses which identify critical and catastrophic hazards are provided to GSDO for integration and completion of the GSDO program hazard analysis. These analyses only consider hazards potentially occurring after transfer of ownership to the Government (i.e., post-DD250) and are not subject to risk acceptance per Figure 4.1.3-1. The GSDO ground hazard analysis is subject to the risk acceptance of Figure 4.1.3-1.

Severe hazards do not apply to flight after T-0. Injuries to or occupational illness of crew in flight which are more severe than "first aid" are considered loss of mission. Injuries to crew in flight which result in permanent disability are considered catastrophic. Damage to flight systems which is considered, in the worst case, to have no effect on mission completion (i.e. not loss of mission) will be considered minor.

Waivers to failure tolerance requirements require Program Manager and S&MA Technical Authority approval and may require Associate Administrator approval if deemed a violation of NPR 8705.2 Human-Rating Requirements for Space Systems. Program/S&MA TA-approved exceptions to failure tolerance do not constitute a waiverable condition.

The programs will initiate hazard analysis during the conceptual phases and continue to mature the analyses throughout the life cycle of their respective programs. Programs will establish a formal, closed-loop, risk acceptance process to identify and track hazards with residual risk, and communicate those risks for acceptance at each milestone review to assure that all hazards and risks identified in the CPIHA hazard analysis are either eliminated or controlled to acceptable levels. The other programs will be a part of the milestone review process to ensure complete identification of hazards, as well as correct controls and verifications related to those programs.

The CPIHA effort will support each program's milestones including design reviews and ESD Cross Program reviews as required. Each program milestone will include a briefing of program-only hazard products and any CPIHA products delivered for review summarizing the analysis effort, review process, open work or issues, and identifying any issues/risks as well as recommendations. The focused safety review of the hazard analysis presented to the Program Milestone Review Board (not a separate S&MA board but rather a programmatic board established to oversee a major review such as PDR, CDR, etc.) may be limited to hazard products which identify the high risk levels. The presentation will include the control and verification strategy for the causes, the resulting safety risk, and the identified level of failure tolerance (including identification of any waivers that are required).

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 19 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

Likelihood					
Very High	Developer	Developer	Developer	ESDCB	Administrator
High	Developer	Developer	Developer	ESDCB	ESDCB
Moderate	Developer	Developer	Developer	JPCB/PCB	ESDCB
Low	Developer	Developer	Developer	JPCB/PCB	JPCB/PCB
Very Low	Developer	Developer	Developer	JPCB/PCB	JPCB/PCB
	Minor	Moderate	Severe	Critical	Catastrophic
			Consequence		

FIGURE 4.1.3-1 HAZARD RISK ACCEPTANCE STRATEGY

PER MISSION	LIKELIHOOD	
	VERY HIGH	QUALITATIVE: VERY LIKELY TO HAPPEN. CONTROLS ARE INSUFFICIENT. QUANTITATIVE: ~1/200 <P
	HIGH	QUALITATIVE: LIKELY TO HAPPEN. CONTROLS HAVE SIGNIFICANT LIMITATIONS OR UNCERTAINTIES. QUANTITATIVE: ~ 1/1,000 <P≤ 1/200
	MODERATE	QUALITATIVE: NOT LIKELY TO HAPPEN. CONTROLS EXIST, WITH SOME LIMITATIONS OR UNCERTAINTIES. QUANTITATIVE: ~ 1/10,000 <P≤ 1/1,000
	LOW	QUALITATIVE: NOT EXPECTED TO HAPPEN. CONTROLS HAVE MINOR LIMITATIONS OR UNCERTAINTIES. QUANTITATIVE: ~1/100,000 <P≤ 1/10,000
	VERY LOW	QUALITATIVE: EXTREMELY REMOTE POSSIBILITY THAT IT WILL HAPPEN. STRONG CONTROLS IN PLACE. QUANTITATIVE: ~ P≤ 1/100,000

FIGURE 4.1.3-2 HAZARD LIKELIHOOD DEFINITIONS

CONSEQUENCES	
CATASTROPHIC	PERSONNEL: LOSS OF LIFE OR PERMANENTLY DISABLING INJURY. FACILITIES, EQUIPMENT, ASSETS: LOSS OF VEHICLE PRIOR TO COMPLETING ITS MISSION, OR LOSS OF ESSENTIAL FLIGHT/GROUND ASSETS
CRITICAL	PERSONNEL: INJURY OR OCCUPATIONAL ILLNESS REQUIRING DEFINITIVE/SPECIALTY HOSPITAL/MEDICAL TREATMENT RESULTING IN LOSS OF MISSION. FACILITIES, EQUIPMENT, ASSETS: LOSS OF MISSION, CONDITION THAT REQUIRES SAFE-HAVEN, OR MAJOR DAMAGE TO ESSENTIAL FLIGHT/GROUND ASSETS
SEVERE	PERSONNEL: INJURY OR OCCUPATIONAL ILLNESS REQUIRING MEDICAL TREATMENT. FACILITIES, EQUIPMENT, ASSETS: DAMAGE TO SIGNIFICANT FLIGHT/GROUND ASSETS.
MODERATE	PERSONNEL: INJURY REQUIRING FIRST-AID TREATMENT, MODERATE CREW DISCOMFORT. FACILITIES, EQUIPMENT, ASSETS: DAMAGE TO NON-ESSENTIAL FLIGHT/GROUND ASSETS.
MINOR	PERSONNEL: MINOR INJURY NOT REQUIRING FIRST-AID TREATMENT, MINOR CREW DISCOMFORT. FACILITIES, EQUIPMENT, ASSETS: MINOR DAMAGE TO NON-ESSENTIAL FLIGHT/GROUND ASSETS.

FIGURE 4.1.3-3 HAZARD SEVERITY DEFINITIONS

4.1.4 Hazard Controls

Hazard cause controls will be identified for each cause to address the associated hazard. In many cases existing ICD or Interface Requirements Document (IRD) requirements will contain the necessary controls, however, new requirements will be added to ICDs, IRDs, or program design specifications as necessary to implement the required hazard controls. Hazard analyses will maintain traceability to controls documented in requirements and design specifications.

4.1.5 Hazard Control Verification

Each cause will identify preliminary hazard control verification plans at PDR, with final verification plans at CDR. For hazard verifications that are not complete by System Acceptance Review (SAR) or equivalent, each program maintains a Safety Verification Tracking Log (SVTL) or equivalent for those verifications for which it is responsible. Prior to integrated ground or flight operations, the IHAWG ensures closure of all applicable control verifications through audit and review of the SVTLs (or equivalent).

Hazard analyses will maintain traceability to the verification of controls documented in requirements, specifications, and ground/flight operational documentation..

Programs will verify successful hazard control implementation through Inspection, Test, Demonstration, and/or Analysis. Verification activities will demonstrate that risk mitigation and hazard controls have been implemented. Hazard control verifications will be addressed through each program's Test and Verification planning and processes.

A closed-loop system to track hazard controls and verifications both within a program and across multiple programs will be implemented. The system at a minimum should include a "hazard control" identifier in program documentation, and be traceable to the hazard product and the cause of the supporting program (a transfer in and a transfer out).

4.1.6 Analysis Of Program Change

All Program and ESD change requests will be assessed for impact to the hazard analysis as part of the program's change evaluation process. This is to assure that potential hazards or hazard causes are not introduced or controls weakened without program approval. As part of the change package, an impact to baselined hazard causes will be identified along with acceptance rationale. Any potential increases or decreases in the baselined cause risk will be identified. A change will be considered to involve an increase in baselined risk if any of the following is true:

a. The change introduces a new hazard or new cause(s).

b. The change eliminates or adversely affects a previously defined hazard control or hazard control verification.

c. The change increases probability of a hazard or critical failure mode manifesting itself. This could include supporting probabilistic risk analysis, where reasonable and available, in order to provide an assessment of impact on Loss Of Crew (LOC) risk.

d. The change increases the consequences of a previously identified hazard, hazard cause, failure mode, or failure cause.

4.1.7 Cross Program Hazard Analysis Inter-Relationship With The FMEA/CIL

The safety hazard analysis and FMEA/CIL are complementary analyses that by themselves have unique limitations, but together provide a comprehensive means to identify, understand, and eliminate or control the safety and reliability risks present in the design and intended operations. Proper coordination between these analyses is important to reduce duplication and ensure their maximum effectiveness.

The FMEA/CIL will provide data to support the hazard analysis in the assessment of compliance with failure tolerance requirements, and the identification, control and/or verification of hazard causes. At the discretion of the hardware developer, controls and verifications for hardware failure modes may be documented either directly in the applicable hazard products or through linkage to specific CIL retention rationale.

4.1.8 Cross Program Integrated Hazard Analysis Inter-Relationship With The Cross Program IPRA

Previous programs have experienced inconsistencies between S&MA products and have proposed lessons learned to help bridge those gaps. One such gap is between hazard analyses and PRA. Hazard analyses help identify the initiating events that a PRA assesses with Event Sequence Diagrams (ESDs) and event trees developed to a specific end state, and then quantifies the likelihood of that scenario. The hazard analyses also assess the likelihood of each hazard cause. Therefore, to minimize gaps, the two S&MA disciplines will work together to produce a more consistent set of S&MA products. The XPRAT team members will be part of the cause tree development. The interim products from each team will be compared to identify inconsistencies or gaps between the products. The IHAWG and XPRAT will collectively address any inconsistencies that may require updates to the analyses to properly document the risks. Where hazards have the potential for significant risk, the XPRAT will work with program and integrated hazard developers to provide likelihood levels for selected hazard causes, consistent with the Cross Program IPRA. The two teams will continue to share data through sharing and reviewing each other's maturing analyses.

4.1.9 Hazard Analysis Review

In accordance with NPR 8715.3, NASA General Safety Program Requirements, a safety review process will be used to assist each program in assuring that the safety analyses are compliant with applicable requirements, comprehensive, technically accurate and that residual risks are at acceptable levels. The ESMAP will ensure that each program has a safety review activity that ensures the accuracy and adequacy of HA product prior to approval at the appropriate board. Each program will determine the type of safety review activity that will be performed. The review process description will reside in the respective Program's S&MA plan. The safety review activity will include an evaluation by safety and subject matter experts that were not responsible for developing the hazard products. To assure that safety risk is communicated to the appropriate stakeholders, the safety review process should consider, at a minimum, a representative from the following organizations:

- ESD
- S&MA Technical Authority
- Engineering Technical Authority
- Health & Medical Technical Authority
- Risk-takers (Crew Office and/or ground operators)
- Multi-Purpose Crew Vehicle (MPCV) Program
- Ground Systems Development & Operations (GSDO) Program
- Space Launch System (SLS) Program
- Mission Operations Directorate

4.1.10 Cross Program Integrated Hazard Analysis Review

<TBD-006>

4.1.11 Crew Survival Analysis

Per NPR 8705.2B, Human-Rating Requirements for Space Systems, ESD programs will describe the crew survival strategies through all phases of the reference mission. The descriptions will include identification of the system capabilities required for the crew survival methods. ESD programs are not required to provide a crew survival capability for all failure scenarios, but are expected to provide survival capabilities to the extent practical within other constraints on the program (e.g. cost, schedule, performance, risk).

As with all aspects of human-rating, crew survival must be addressed as an integrated space system. Therefore, ESD programs will collaborate to produce the Crew Survival Analysis Report (CSAR) at major milestones and as a deliverable to support the Human-Rating Certification Package. The MPCV Program will lead the development of the CSAR.

Crew survival requirements in NPR 8705.2B were analyzed by the Cross-Program Human Rating Team to determine requirements for each ESD program. Each ESD program will incorporate these responsibilities into program requirement documents, or elevate disagreements to the Joint Program Control Board (JPCB) for resolution.

The approach for crew survival analysis will be based on the approach used for Constellation PDR (refer to CxP 75081, Crew Survival Analysis Report for Cx PDR). Each program hazard and Cross Program integrated hazard cause, as well as the Cross Program IPRA, will be assessed for available crew survival methods should all hazard controls fail and the hazardous condition occur. Initially, prior to PDR, all potential survival methods will be inventoried, with qualitative descriptions of effectiveness and likelihood of success. At each successive review of the hazard products, crew survival methods will be re-assessed for validity, level of implementation and verification in the program(s), and updated characterization of effectiveness and likelihood of success. Where possible and reasonable, the effectiveness and likelihood of success will be quantified. (Note: Aborts and other crew survival methods are not considered as hazard controls. See section 4.1.11 for more detail on crew survival analysis.)

The CSAR compiles all crew survival methods and identifies applicability across the mission phases. The crew survival capabilities are also in the LOC IPRA. Crew survival analysts determine if there are any gaps in crew survival coverage (i.e. hazards without a survival method), or where the survival capabilities have a low likelihood of success. The results of the crew survival analysis are briefed to applicable program systems engineering forums in timely a fashion to permit program mitigation of gaps or risks as much as possible.

The CSAR is concurred on by the ESD S&MA Panel and will be approved via cross-program change request. At each program milestone review, the program will address compliance with required crew survival capabilities. The CSAR is delivered as part of the Human-Rating Certification Package

4.2 RANGE SAFETY

ESD programs are required to comply with NPR 8715.5, NASA Range Safety Requirements.

ESD has chartered the Human Exploration Range Safety Panel (HERSP) to integrate and define the approach for ascent and entry range safety, including negotiation of requirements and deliveries with the Air Force Range Safety offices. Refer to the HERSP Task Agreement for more details.

4.3 ORBITAL DEBRIS ASSESSMENT

ESD programs are required to comply with NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris, and NASA-HDBK-8719.14, Handbook for Limiting Orbital Debris.

The MPCV Program is responsible for producing the integrated Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP) as required. SLS will provide data required to support the ODAR development.

4.4 GROUND OPERATIONS SAFETY

Each program will address ground safety and hazard analysis requirements as part of its Program S&MA Plan for operations pre-DD250, pre-turnover to GSDO.

Ground safety requirements for integrated operations (post-turnover) will be established in ICDs and IRDs.

GSDO will lead and develop a ground hazard analysis (which will integrate the inputs from SLS and MPCV) to address hazards and hazard mitigation strategies for all ground operations hazards beginning with hardware turnover to GSDO until the space system clears the launch tower on ascent. GSDO will also lead the hazard analysis activities for recovery operations post-flight until hardware disposal or turnover to the appropriate program or contractor. SLS and MPCV are required to provide ground hazard analysis and supporting data to the GSDO.

The GSDO Program S&MA Plan will address the methodology for the ground hazard analysis and the process for acceptance of residual ground safety risks, including risks to the SLS and MPCV systems.

4.5 INDUSTRIAL SAFETY

NASA Centers and contractors are required to comply with federal, state, and local safety regulations. NASA industrial safety requirements do apply to NASA Centers and each Center establishes local policies and procedures which comply with NASA requirements as well as state and local regulations. NASA contractors are required to comply with NASA Center requirements for all activities on a NASA Center (except in Industrial Operations Zones (IOZs). NASA industrial safety requirements do not apply to NASA contractor operations located off NASA sites.

4.6 MISHAP RESPONSE AND CONTINGENCY ACTION PLAN

Each ESD program is required to have a Mishap Response and Contingency Action Plan (MRCAP) for stand-alone operations (pre-DD250, pre-turnover to GSDO) that complies with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping. Program MRCAPs are identified in section 2.2. (NOTE: The development of an integrated MRCAP is forward work. **<TBD-002>**)

For integrated ground and flight operations, the ESD MRCAP takes precedence and serves as the integrated plan.

5.0 RELIABILITY

5.1 FMEA/CIL

Each program will establish requirements and methodology for conducting Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL). As part of producing the program FMEA/CIL, each program is responsible for identifying failure effects or CIL Retention Rationale that may cross program boundaries and affect another program. In addition each program is responsible for proper coordination with affected programs. In such cases, reliability engineering representatives from each affected program will collaborate through technical interchange meetings to review such failure cases, determine planned mitigation strategies and retention rationale, agree on documentation responsibilities, and agree on CIL verification requirements. The FMEA/CIL for integrated failure scenarios is ultimately the responsibility of the program that owns the item that causes the propagated failure effects. Program FMEA/CILs are shared among all programs to ensure integrated failure causes or effects are properly identified and resolved. Integrated FMEAs and CILs are approved at the responsible program's appropriate control board (e.g. PCB), with representation from the other affected programs. CIL design, test, and inspection controls which are imposed on another program are documented in ICDs or IRDs, or other bilaterally agreed upon processes. Verification of these imposed CIL controls is the responsibility of the performing program. A common global FMEA/CIL methodology is not required; however, some data fields and definitions need to be common to allow for proper integration. These common areas are addressed in the following sections.

The MPCV, SLS, and GSDO FMEA leads will provide status of FMEA/CIL integration activities to the ESD S&MA Panel on a regular basis. In the event that the program FMEA leads are not able to reach consensus on FMEA/CIL issues affecting multiple programs, the issue will be elevated to the ESD S&MA Panel for resolution.

5.1.1 Criticality Definitions

To ensure consistency of FMEA/CIL analysis among the programs, the following definitions for criticality are established.

TABLE 5.1.1-1 CRITICALITY DEFINITIONS

Criticality	Definition
1	**Single failure that could result in loss of life or vehicle.**
1R#	**Redundant hardware that, if all failed, would result in loss of life or vehicle. A number (#) is used to indicate the number of failures that must occur before the criticality 1 effect is manifested.**
1S	**Single failure of a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition, potentially resulting in loss of life or vehicle.** Note: The SLS Program will not use the 1S criticality definition. Critical items whose failure causes an emergency system to fail to detect, mitigate, or operate when needed during an emergency condition will be classified as Criticality 1 or 1R#, depending on the associated degree of failure tolerance.
2	**Single failure that could result in loss of mission**
2R	**Redundant hardware item that, if all failed, could cause loss of mission.**
3	**All other failures.**

5.1.2 Failure Effect Levels

For each failure mode, the FMEA will describe the worst-case credible failure effects. The failure effect descriptions must be sufficiently detailed to clearly describe impacts on item/element/vehicle required functionality and interfaces. For redundant systems, the analysis will address the loss of all redundancy. The failure effects will be described at the following indenture levels:

a. Immediate Effect – Failure effect on the item under analysis, the assembly it is associated with (if appropriate), and its interfaces.

b. Next Effect – Failure effect at the next higher assembly level, typically the subsystem/system, and ultimately at the SLS/MPCV/GSDO element level.

c. End Effect – Failure effect at the integrated vehicle level, including effects on the MPCV/payload, mission, and crew.

5.1.3 Interfaces

Each program's FMEA will include assessment of system/subsystem interfaces within the element, between elements, and with the Interfacing Programs. The analysis of a component whose failure may propagate across an interface will not end at the interface with other elements/systems/programs, but must be communicated to the impacted entities and analyzed across the interface to determine effects on the interfacing element and ultimately on the vehicle, MPCV/payload, crew, and mission.

5.2 SYSTEM RELIABILITY PREDICTIONS

Reliability predictions for flight hardware and flight critical GSE are developed and controlled by each ESD program as described in their respective Program S&MA Plan. Flight critical GSE is defined as Ground Support Equipment that physically or functionally interfaces with flight hardware during the integrated timeline (Cryo loading to post-flight crew egress). Reliability engineering representatives share reliability prediction data across the programs to ensure the most appropriate reliability data is available and used in each program. Each program supplies reliability estimates (i.e., failure rates) for use in launch availability analyses, probabilistic risk assessments, system trade studies, and other purposes as required.

6.0 QUALITY ASSURANCE

6.1 PROBLEM REPORTING AND DISPOSITION

6.1.1 Nonconformances

Each program will establish nonconformance reporting systems for its pre-DD250, pre-turnover operations and document such approach in its Program S&MA Plan.

During post-turnover operations to GSDO, nonconformances with SLS or MPCV hardware/software detected by GSDO will initially be entered into the GSDO nonconformance system. The GSDO system will be used to document the discrepancy, its resolution, as well as the remedial action and verification of preventive/recurrence control actions. Post turnover, GSDO will make nonconformances visible to the respective design centers in the Cross Program Problem Assessment System (CP PAS).

6.1.2 Integrated Material Review Boards

GSDO will coordinate the disposition and final closure of any nonconformances with the design centers. The process will be defined in the GSDO-PLN-1036, GSDO S&MA Plan with MPCV and SLS concurrence. Until the disposition is approved by the design center, the design attributes of the nonconforming material will not be further processed.

Material Review Board (MRB) final summary containing the technical and flight safety rationale require formal concurrence from the design center.

6.1.3 Cross Program Reportable Issues and Anomalies

Pre-turnover to GSDO, significant MPVC and SLS nonconformances, issues and anomalies (e.g. Crit 1/1R functional failures) that meet the elevation criteria defined in their program S&MA requirements are to be made available electronically via CP PAS. Post-turnover, KSC will make all MPCV and SLS nonconformances available to the design centers in CP PAS.

6.2 DATA REQUIREMENTS FOR HARDWARE HAND-OVER

When contractually required by the procuring agency, Acceptance Data Packages (ADP's) for flight hardware/material, GSE, and ground hardware will be made available to GSDO. Where GSDO will be performing sustaining engineering activities, ADP's will be turned over to GSDO for configuration control. Content and format will be determined by the procuring agency, as provided in their respective S&MA Plans.

The flight hardware ADP data requirements for MPCV and SLS are defined in MPCV 70146, MPCV ADP Requirements, and SLS **<TBD-003>**, respectively. For GSE and ground hardware, the Cross Program ADP data requirements are defined in GSDO-PLN-1027, Cross Program Ground Hardware/Software Acceptance Data Package. This data may be provided as part of an ADP or as a separate data request by GSDO.

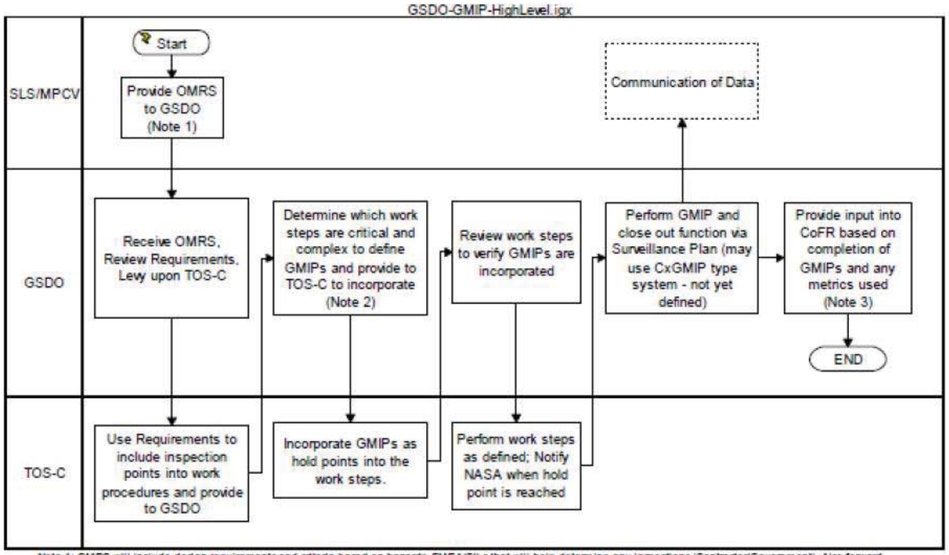
6.3 SUPPLIER AUDITS

Each program will conduct audits of supplier policies, procedures, and operations which implement the quality program. These audit processes will be documented in their Program S&MA Plan. Where multiple programs need to audit a single supplier for multiple contracts, the programs will coordinate and integrate audit efforts to minimize the burden on the supplier. The Quality Assurance Integrated Working Group (QAIWG) will ensure that the proper supplier audit coordination is accomplished. Information pertaining to these type audits will be captured in an electronic database **<TBD-004>**. For audits of sub-tier suppliers, each Program will accompany their Prime Contractors as applicable. These audits will be documented in that contractor's system.

6.4 GOVERNMENT MANDATORY INSPECTION POINTS (GMIPS)

Each program will establish GMIP criteria and processes for its pre-DD250, pre-turnover operations and document the approach in its Program S&MA Plan. Post-turnover, SLS and MPCV will provide requirements criteria to GSDO including but not limited to hazards, FMEA/CILs that will help to determine mandatory inspections. MPCV and SLS will also communicate to GSDO those "critical" process inspections (i.e. inspections of processes where an attribute of the hardware cannot be verified). See Figure 6.4-1.

GSDO-GMIP-HighLevel.igx



Note 1: OMRS will include design requirements and criteria based on hazards, FMEA/CILs that will help determine any inspections (Contractor/Government). Also forward work can include open "GMIPs" which will be trasferred to GSDO to implement. Completion of these can be fed back to the originating program if needed, but will be controlled by GSDO.

Note 2: This will be part of the surveillance planning process. GMIP definition is based on NPR 8735.2A, but other surveillance techniques will be performed for "high risk" items.

Note 3: Any forward work GMIPs that were performed could be communicated back to the originating program.

General Note: Any nonstandard work stemming from nonconformance dispositions will include GMIPs as necessary.

FIGURE 6.4-1 GSDO-GMIP PROCESS

6.5 QUALITY ASSURANCE IWG

The QAIWG is a Cross Program forum to facilitate quality assurance issues and concerns across the Programs/Elements. In particular, sharing of quality assurance information that could potentially affect other Programs, Elements, or the Integrated vehicle should be brought for discussion.

The QAIWG will identify cross program issues and information that are candidates for elevation to integrated management forums within ESD. Such candidates may include trends in significant nonconformances or quality issues (e.g. process escapes), cross-program quality initiatives, etc. For each candidate, an assessment of likelihood and severity will be performed. Those items that are assessed with significant risk will be carried forward to the ESD S&MA Panel for discussion. The QAIWG will coordinate these items with the ESD S&MA Panel prior to elevation. Each program will document its approach to communicating quality topics to program management in its Program S&MA Plan.

7.0 RISK

7.1 INTEGRATED PROBABILISTIC RISK ASSESSMENT (IPRA)

7.1.1 Objectives

IPRA has three specific objectives to facilitate risk-informed decisions by ESD program during the design, development, and operation phases:

a. **Quantitative Risk Requirements Establishment**: Establishing quantitative risk requirements, or removing the "To Be Resolved" designations, is performed using analysis early in the program life cycle and again as the design matures. NASA's preferred approach to this process is PRA, as specified in Agency NASA Procedural Requirements (NPRs) and standards. The PRA should be supplemented with available deterministic analyses and other data to make it a best-estimate of achievable risk levels for a given reference mission.

b. **Quantitative Risk-Informed Design Trade Studies**: Quantitative risk informed design trade studies use the "current" PRA of the vehicle and/or mission to assess design options offered as a means of reducing risk or assessing the risk impact of improving other performance measures. The "current" PRA is a product of a "living PRA" approach that is maintained and updated throughout the program's life cycle. It would be the best-estimate risk assessment at any point in time. The PRA must be supplemented with current and relevant deterministic analyses and other data to make it a legitimate trade study.

c. **Quantitative Risk Requirements Verification**: Verification of quantitative risk requirements is also performed using analysis. NASA's preferred approach to this verification is PRA, as specified in Agency NPRs and standards. The PRA must be supplemented with deterministic analyses and other data to make it a legitimate assessment.

7.1.2 Integration

The complex and interactive nature of NASA's exploration architectures requires an integrated effort in order to understand the interaction of systems and to account for failure scenarios initiated in one mission phase that manifest in later phases. Two very notable examples are ascent aborts and debris strikes to re-entry Thermal Protection System (TPS).

Stand-alone probabilistic models by themselves are insufficient for capturing and quantifying the effects of integrated system interactions. The overall model design should allow for integration, much like the elements themselves are eventually integrated into a functioning space system. This requires that all sides involved collaborate in the planning of the integrated model structure, the definition of the interfaces between models, and the assignment of responsibilities and associated timelines for building the pieces of the model.

The Cross Program PRA Team (XPRAT) was formed to provide a forum for PRA representatives from each program to collaborate to fulfill the ESD PRA objectives. In addition, the XPRAT will:

a. Develop, establish, and maintain the standard methodology by which the SLS, MPCV, and GSDO programs will perform an integrated, consistent PRA for the Cross Program (XP). This ESD 10011, Cross Program Probabilistic Risk Assessment Methodology document will be shared across the XPRAT.

b. Establish a Cross Program working group to build, maintain, and apply the integrated PRA. This includes documentation of the Cross Program IPRA at all levels to capture the system description, assumptions, data analysis, engineering inputs, and results in order to preserve the basis of the analysis for internal and external peer reviews.

c. Identify and incorporate partnership considerations and opportunities between outside organizations, such as the crew office, mission operations, engineering, and human health and performance.

d. Perform architecture risk analysis and key trade studies across all elements, including DRMs, manifests, launch campaigns, and phased development plans.

e. Establish, maintain, and report technical performance measures in response to ESD reporting requirements for quantitative risk. This will be done through coordination with the program PRA team members, the ESD and program CSOs, and reported on an agreed upon frequency.

f. Provide and maintain schedules including points at which the integrated model will be drafted and updated in support of integrated milestones and Human Rating Certification Package (HRCP) delivery/endorsement.

g. Identify primary interface points between system models and integrated models among the XPRAT.

h. Recommend quantitative risk requirement values, Technical Performance Measurements (TPMs) and mission phases allocations for ESD and program-level requirements documents.

i. Document roles and responsibilities for all organizations involved in building and maintaining the integrated PRA.

j. Support the Agency in the development of loss of crew thresholds and goals.

7.1.3 Requirements

Quantitative risk requirements are defined in ESD 10002, Explorations Systems Development (ESD) Requirements. The Level 1 risk requirements are expected to be imposed for specific DRMs as the mission Concepts of Operation (ConOps) are developed. The SLS, MPCV, and GSDO programs will collaborate in further allocation, flowdown, analysis, and verification of the LOC requirements as needed. As required, the XPRAT will support the ESD S&MA Panel in assisting the Agency's determination of loss of crew thresholds/goals and ESD efforts to determine appropriate Level 1 requirements for future missions through preliminary PRA and achievability assessments.

Using agreed upon methodologies and data, the XPRAT will develop a preliminary PRA model of each DRM and determine appropriate risk allocations for each ESD program in order to achieve the Level 1 requirements. If the program agrees with the allocation, the program will formalize the allocation as a requirement in its System Requirements Document, or equivalent program specification. If there is disagreement over allocations, the issue can be elevated through program and ESD management forums in accordance with ESD 10001, ESD Implementation Plan.

To integrate PRAs performed by multiple, geographically dispersed organizations, some degree of commonality of approach is required to assure that such PRAs can indeed be integrated and provide confidence in using the results as a decision making aid. As with any other resource (e.g., money), balancing risk across multiple systems can be hampered without a common accounting methodology and could even result in making the wrong decision if program methodologies are too disparate. ESD programs will provide PRA models and data which comply with ESD 10011 Cross Program Probabilistic Risk Assessment Methodology.

The XPRAT will report status of analysis progress and requirement compliance to the ESD S&MA Panel and higher forums as required. Prior to reporting the results, the XPRAT will review those results of the Integrated PRA to ensure that the risk drivers, methodology, and data are credible. Once it has been determined that the model and data are acceptable, the XPRAT may assign actions to its program representatives to report and discuss the results of the analysis with their program prior to presenting the results outside of the XPRAT. The XPRAT will then bring the results forward to the ESD S&MA Panel. The PRA results may require further communication to higher level ESD forums, particularly if there are technical issues that require ESD decisions or deficiencies indicating potential noncompliances with ESD risk requirements. The ESMAP will determine the forward reporting path following the governance structure described in ESD 10001, ESD Implementation Plan.

7.1.4 Risk-Informed Design

Each program is required to establish a systems engineering process which considers safety, reliability, and risk in system design processes. Each program defines this process in their respective program documentation.

The Integrated PRA also needs to inform the program system engineering process. The integrated PRA will be compiled from program inputs, and results of the integrated PRA will be shared with the program representatives on a continual basis informally to help inform the programs of risk drivers and Level 1 risk requirements compliance status. For risk drivers that are wholly caused and controlled by a single program, the XPRAT will expect that the owning program will address those risk drivers internally for mitigation/reduction as needed to meet their risk allocations. For risk drivers that are truly integrated in nature (i.e. require actions from multiple programs to mitigate), then such risk drivers will be discussed with the ESD S&MA with recommendations for risk mitigation or acceptance. The ESMAP will elevate issues and recommendations for visibility or decision as needed.

If a program is within allocation, and the integrated PRA indicates compliance with Level 1 requirements, then residual risk for that program can be proposed for acceptance by the ESDCB. However, even when compliance is achieved, NASA policy requires that ESD programs pursue continuing efforts to further reduce risks by on-going financial investments in technology development, testing, and new design. Each ESD program will define a strategy for continuous risk improvement as part of their respective program documentation.

The most critical aspect of informing the design is the timing that allows PRA results to be a part of design decisions at the time they are being made. Again, consistency between IHA Cross Program Hazard Analysis and IPRA will help during these discussions. Building a PRA requires design input for the PRA models to be constructed. The systems engineering process must take this into account by incorporating iterative analysis cycles to assess design concepts for safety, reliability, and risk, while optimizing the design against all performance parameters until the design trades have resulted in an optimum balance of risk, performance, cost, and schedule that can be accepted by the program stakeholders. Clearly, integrated PRA results will lag program analysis and design efforts, which presents some risk that IPRA results will not be timely inputs for program-level decisions. However, the majority of IPRA risk drivers will be unique to a single program and program-level analysis will identify those and work them to resolution. The number of integrated risks requiring multi-program actions to mitigate will be somewhat limited and are identified in advance by the XPRAT and are areas of high focus to address early. The XPRAT will participate in aborts planning and other working teams to address these integrated risks so that PRA results can help inform and focus the team. With the XPRAT focused on these integrated risks, and the programs focused on uniquely-owned risks, the PRA efforts can inform the design activities in a reasonable time. Agreements reached between programs on multi-program risk mitigation strategies will be documented in ICDs and IRDs.

In the program phases prior to verification closure, there will be points at which the integrated model will need to be formally updated. The IPRA will be updated prior to ESD integrated milestone reviews and also for each major milestone where the HRCP is endorsed. However, for PRA to be an effective design and decision-making aid, informal or preliminary results will be sought at points between planned updates. Any PRA model, integrated or not, should have a quick-response capability that supports decisions at any time during the life cycle. All parties building pieces of the integrated PRA must be aware of this and embrace model designs that facilitate quick-turnaround estimates, even if they are rough order of magnitude.

7.1.5 Products and Quality Assurance

MPCV is responsible for the generation of XPRAT products and maintaining the supporting data. SLS and GSDO are responsible for providing specific inputs to those products, review and concurrence of XPRAT products, and supporting the presentation of XPRAT products to external parties to help explain their program content.

MPCV will generate the integrated PRA model in accordance with ESD 10011 Cross Program Probabilistic Risk Assessment Methodology, and retaining all supporting analysis, reliability, and design data necessary to establish verification of the Level 1 risk requirements.

SLS, MPCV, and GSDO are responsible for providing models, data, and supporting information requirements in accordance with data exchange requirements as necessary to produce the integrated PRA. Programs are responsible for the quality assurance of their products and information, as well as responding to any questions or actions from external parties on their analysis work.

The XPRAT will generate analysis plans, status reports, and metrics as required and agreed upon with ESD S&MA Panel.

The XPRAT will establish a process for independent quality assurance of the integrated PRA. This assurance will determine compliance of the IPRA to ESD 10011, Cross Program Probabilistic Risk Assessment Methodology, and NASA NPR 8705.5, Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, as well as assurance that the model is accurate and complete. NASA policy requires an independent peer review of the PRA to assess methodology and policy compliance; the frequency and proposed level of model maturity required to conduct a peer review will be set forth in the ESD 10011, Cross Program Probabilistic Risk Assessment Methodology document. The XPRAT and all member programs will support the NASA Independent Peer Review (IPR) process, or alternative verification as approved by NASA Office of Safety and Mission Assurance.

7.2 PROGRAM RISK MANAGEMENT

ESD programs are required to comply with NPR 8000.4, Agency Risk Management Procedural Requirements. The ESD Programmatic and Strategy Integration (PSI) team defines the process for integrating program risk management processes and dispositioning integrated risk topics. The process is documented in ESD 10003, ESD Risk Management Plan.

8.0 OTHER INTEGRATED TOPICS

8.3 HUMAN-RATING

ESD programs are required to achieve human rating certification of the integrated space system per NPR 8705.2B. S&MA supports the integrated human rating efforts through the development of products required to achieve a human rating certification. These include PRA, IHA, and crew survival analysis. Also, as technical authorities, the CSOs assess the progress of the programs' individual and integrated efforts towards achieving human rating certification and provide recommendations to the programs to facilitate certification. Also, the CSOs will provide recommendations to the Agency (OSMA Chief) regarding the worthiness of the integrated capabilities with respect to human rating certification.

Revision: Initial Release Baseline	Document No: ESD 10010
Release Date: 09/20/2012	Page: 37 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

8.4 CERTIFICATION OF FLIGHT READINESS (CoFR)

ESD will establish an integrated CoFR plan and certification process, which will define S&MA endorsement responsibilities. The ESD S&MA Panel will define the tasks, products, and processes required to fulfill each S&MA endorsement and assign responsibility for each task/product to the appropriate program or IWG. Where S&MA shares task or product responsibilities with other disciplines (such as Engineering for the IHAs), S&MA will coordinate with the appropriate organizations on CoFR endorsement responsibilities. ESD programs are required to comply with the requirements for Safety and Mission Success Reviews (SMSR) defined in NPR 8705.6, Safety and Mission Assurance (S&MA) Audits, Reviews, and Assessments. Each program S&MA organization may define separate CoFR plans to further define processes and responsibilities to fulfill its endorsement responsibilities to its program manager, institution, and for integrated CoFR endorsements.

The Integration CSO will lead development and maintenance of the S&MA CoFR Integrated Implementation Plan.

Revision: Initial Release (Draft)	Document No: ESD 10010
Release Date: TBD	Page: 38 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

APPENDIX A
ACRONYMS AND ABBREVIATIONS AND GLOSSARY OF TERMS

A1.0 ACRONYMS AND ABBREVIATIONS

ADP	Acceptance Data Package
CDR	Critical Design Review
CIL	Critical Item List
CoFR	Critical Item List
ConOps	Concepts of Operation
CP PAS	Cross Program Problem Assessment System
CPIH	Cross Program Integrated Hazard
CPIHA	Cross Program Integrated Hazard Analysis
CR	Change Request
CSAR	Crew Survival Analysis Report
CSI	Cross Program System Integration
CSIP	Cross Program Integration Panel
CSO	Chief S&MA Officer
CSM	Crew Survival Method
DCR	Design Certification Review
DFMR	Design for Minimum Risk
DRM	Design Reference Mission
ECB	ESD Control Board
EM1	Exploration Mission 1
EM2	Exploration Mission 2
EOMP	End of Mission Plan
ESD	Exploration Systems Development, NASA Headquarters

ESD	Event Sequence Diagram
ESD CB	Exploration Systems Development Control Board
ESMAP	ESD Safety & Mission Assurance Panel
FFBD	Functional Flow Block Diagram
FHA	Functional Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FT	Fault Tree
GFE	Government Furnished Equipment
GMIP	Government Mandatory Inspection Point
GO	Ground Operations
GSDO	Ground Systems Development & Operations
GSE	Ground Support Equipment
HA	Hazard Analysis
HERSP	Human Exploration Range Safety Panel
HW	Hardware
HR	Hazard Report
HRCP	Human Rating Certification Package
ICD	Interface Control Document
IHA	Integrated Hazard Analysis
IHAWG	Integrated Hazard Analysis Working Group
IHR	Integrated Hazard Report
IOZ	Industrial Operations Zones
IPR	Independent Peer Review
IPRA	Integrated Probabilistic Risk Assessment
IRD	Interface Requirements Document
IWGs	Integration Working Groups

JPCB	Joint Program Control Board
JSC	Johnson Space Center
KSC	Kennedy Space Center
LAS	Launch Abort System
LEO	Low Earth Orbit
LOC	Loss of Crew
LOM	Loss of Mission
LOV	Loss of Vehicle
MPCV	Multi-Purpose Crew Vehicle
MRB	Material Review Board
MRCAP	Mishap Response and Contingency Action Plan
MSFC	Marshall Spaceflight Center
NASA	National Aeronautics and Space Administration
NPRs	NASA Procedural Requirements
ODAR	Orbital Debris Assessment Report
OMRS	Operations and Maintenance Requirements and Specifications
OPR	Office of Primary Responsibility
OSMA	Office of Safety and Mission Assurance
PCB	Program Control Board
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PIB	Program Integration Board
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action System
PSI	Programmatic and Strategy Integration

QA	Quality Assurance
QAIWG	Quality Assurance Working Group
QMS	Quality Management System
SAARIS	Surveys, Audits, and Reviews, Information System
RID	Review Item Disposition
S&MA	Safety and Mission Assurance
SLS	Space Launch System
SMAP	Safety and Mission Assurance Panel
SDR	System Design Review
SE&I	Systems Engineering and Integration
SLS	Space Launch System
SMSR	Safety and Mission Success Reviews
SOW	Statement of Work
SR&QA	Safety, Reliability, and Quality Assurance
SRR	System Requirements Review
SSAR	System Safety Analysis Report
SVTL	Safety Vehicle Tracking Log
SW	Software
TA	Technical Authority
TIM	Technical Interchange Meeting
TA	Technical Authority
TLI	Trans-Lunar Injection
TOSC	Test and Operation Support Contract
TPM	Technical Performance Measurement
WBS	Work Breakdown Structure
XP	Cross Program

XPRAT	Cross-Program PRA Team
QMS	Quality Management System

A2.0 GLOSSARY OF TERMS

Term	Description

APPENDIX B
OPEN WORK

B1.0 TO BE DETERMINED

The table To Be Determined Items lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within carets. The TBD item is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBD-XXXXXX-001>** is the first undetermined item assigned in the document). As each TBD is resolved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBDs will not be renumbered.

TABLE B1-1 TO BE DETERMINED ITEMS

TBD	Section	Description
<TBD-001>	2.2	Space Launch System Mishap Response and Contingency Action Plan
<TBD-002>	4.6	Develop an integrated Mishap Response and Contingency Action Plan held by NASA Headquarters
<TBD-003>	6.1.1	SLS ADP Requirements
<TBD-004>	6.3	Supplier audit database
<**TBD-005>**	Section 4.X	CSAR Maturity Expectations need to be defined
<TBD-006>	4.1.10	Cross Program Integrated Hazard Review Process – IHAWG/ESMAP to determine process for independent review of integrated hazard products.
N/A	6.1.3	Definition of criteria for elevating pre-DD250 discrepancies/MRBs where performance of program-to-program interfaces is potentially impacted.
N/A	4.0	Add guidelines for hazard maturity needed to meet review/milestone success criteria.

B2.0 TO BE RESOLVED

The table To Be Resolved Issues lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within carets. The TBR issue is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBR-XXXXX-001>** is the first unresolved issue assigned in the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBRs will not be renumbered.

TABLE B2-1 TO BE RESOLVED ISSUES

TBR	Section	Description

APPENDIX C
SAFETY TOPICS

SECTION 1: HAZARD RISK REDUCTION ORDER OF PRECEDENCE

The primary method for minimizing hazards/risks is through a control strategy that will prevent the occurrence of the hazard/risk or reduce the residual risk to an acceptable level by either reducing the likelihood of occurrence or reducing the severity of the hazard.
To eliminate or control hazards, the Programs will use the following hazard reduction precedence sequence:

a. Eliminate hazards by design: Hazards will be eliminated by design where possible.

b. Design for minimum hazards: The major goal throughout the design phase will be to ensure inherent safety through the selection of appropriate design features such as fail-operational/fail-safe combinations and appropriate safety factors. Damage control, containment, and isolation of potential hazards will be included in design considerations.

c. Incorporate Safety Devices: Known hazard risks, which cannot be eliminated through design selection, will be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.

d. Provide Caution and Warning Devices: Where it is not possible to preclude the existence or occurrence of a known hazard, devices will be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application will be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

e. Develop and Implement Special Procedures: Where it is not possible to reduce the magnitude of existing or potential hazard risks through design, or the use of safety and warning devices, special procedures will be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations will be standardized. The need for hazard detection and safing by the flight crew will be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available. With Program approval, real-time monitoring and hazard detection and safing may be utilized to support control of hazardous functions provided that adequate crew response time is available and acceptable safing procedures are developed.

f. Provide personal protective clothing and equipment.

Revision: Initial Release (Draft)	Document No: ESD 10010
Release Date: TBD	Page: 46 of 50
Title: CROSS-PROGRAM SAFETY AND MISSION ASSURANCE PLAN	

SECTION 2: HAZARD REPORT DATA ELEMENTS

HAZARD REPORT DATA ELEMENTS

The following data elements are documented at the report level for each hazard.	
Hazard Number	Identification of the Hazard Report unique within the program/element/subsystem. This unique identification is assigned to each specific Hazard Report and is never reassigned or reused. The hazard report number will be traceable from the initial identification of the hazard through its resolution and any updates. (EXAMPLE CSHR-05.B.PDR where CSHR-05 = Core Stage Hazard Report number 5, B = revision, and PDR = the traceable delivery)
Hazard Title	Provide a descriptive title of the hazard to give insight into the scope of the Hazard Report. The title should include the hazard and any major defining cause and effect.
Mission Phase(s)	Identify and document the applicable mission phase(s) in which the hazard could manifest. Note that this may not necessarily be the same as the mission phase(s) in which the hazard causes occur. The hazard analysis will use the following mission phases (as applicable): a. <u>Pad Operations and Launch</u>:– Hazard analysis begins at start of cryogenic tanking to T-0 umbilical separation. b. <u>Ascent</u>: T-0 umbilical separation through placement of MPCV in stable Earth orbit c. <u>LEO and TLI Operations</u>: Placement of MPCV in stable Earth orbit through trans-lunar propulsion stage disposal d. <u>SLS Post-Ascent Operations</u> (Recovery/Disposal) Program/Element hazard reports may utilize different mission phase descriptions as long as they are inclusive of and can be mapped to the mission phases specified above and are consistent with ESD 10012, Concept of Operations.
Hazardous Condition Description	The description of the hazardous condition defines the event or condition, fully describes the scenario and hazardous events that must be controlled, and identifies the local effect(s), intermediate effects (e.g., damage to XYZ assembly, subsystem becomes

	inoperable, etc.) and the worst case effects or results of the hazardous event. Include a description in terms of one or more generic hazards (i.e., fire/explosion, impact, toxicity, etc.). The description should be made explicit to specify the equipment involved. If the hazard is for off-nominal conditions, note the assumptions that were made.
Acceptance Rationale	Provide a summary of the rationale for accepting the risk associated with the Hazard Report commiserate with the maturity level of hazard analysis performed. Summary should include an overview of the control strategy utilized.
Likelihood Justification	Provide rationale for the likelihood level provided based on control level.
Risk of each cause identified in 5X5 risk matrix	A risk matrix will be completed for each Hazard Report by entering each of the causes (or number of causes if too numerous) into the matrix shown in Figure 4.1.3-1, thereby documenting each hazard cause severity and likelihood of occurrence. Only causes identified in the Cause Summary will be entered into the matrix.
Hazard Cause Title	The title should briefly describe the root or symptomatic reason for the occurrence of a hazardous condition.
Hazard Cause Description	Provide a description of Hazard causes down to the level at which controls are to be applied. Consider environments, software errors, hardware failures, secondary failures/conditions, procedural errors, operationally induced external and internal failures, FMEA/CIL failure causes, and human errors/limitations when developing the description. Include a description of the cause effects.
Likelihood of Occurrence	Hazard likelihood is the probability that an identified hazard cause will occur and result in the hazardous effect in a single mission. The controls are considered to be in place when performing the likelihood of occurrence assessment. Classify the likelihood for each cause by assessing the controls that are in place and documenting the likelihood as very high, high, moderate, low, or very low as defined in Table 4.1.3-1
Likelihood Justification	Provide a summary of the rationale for classification of the likelihood. Include assumptions, any empirical data, a qualitative summary of the failure history, and any uncertainties, confidence factors, or limitations (including applicable waivers) in the controls identified in the report that provide the basis for establishing the likelihood or probability of the hazardous event occurring. When a certain cause(s) is classified with a higher likelihood relative to the

	other causes within the Hazard Report, additional rationale will be necessary to support that classification. PRACA data should be consulted for qualitative failure history when determining the likelihood. The time parameter for assessing the likelihood is for the mission under analysis. Update the rationale and classification at each design milestone review based upon the evaluation of the successful implementation of the control and verification strategy.
Severity	The severity level is an assessment of the worst case effects of the hazard, assuming no controls are in place. Complete for each cause by assessing the most severe effect and documenting it as catastrophic, critical, severe, moderate, or minor (defined in Table 4.1.3-2). FMEA/CIL criticality should be consulted when determining the severity.
Control(s)	Document or reference all controls that prevent the occurrence of a hazard cause or reduces the residual risk to an acceptable level. A valid control used to meet failure tolerance requirements must exist such that no single event or common cause failure can result in a potentially hazardous event. Design controls include those attributes of the robustness of the design. Operational controls include both operational constraints as well as crew and support personnel training to prevent a hazard, lessen the likelihood or severity of a hazardous occurrence, or to mitigate its effects once it has occurred. Provide a summary statement of any actual operational constraint, when applicable. Include a description of all the necessary design/operational controls for this hazard cause, including existing technical requirements (e.g., factors of safety, design standards, etc.), including documentation references, if applicable. To the extent practical, the Hazard Report should include pointers with unique identification(s) to specific test and inspection controls documented in the retention rationale for the applicable CILs in order to minimize duplication. The hazard controls will be numbered (indexed) to provide direct linkages with the appropriate cause and verification(s) within the hazard report as well as with any other hazard report causes that utilize the control(s). For element hazards controlled by other programs and/or elements; provide a direct linkage of each Hazard Report cause with all control(s) relevant to controlling that cause documented in the integrated hazard report.
Verifications	Provide a summary with sufficient detail/explanation of the verification methods (testing, inspection, analysis, etc) which

	assure the identified controls are present, adequate, and effective, and support hazard closure or risk acceptance rationale. CIL retention rationale verifications will be identified where appropriate to assure consistency between the hazards and the CILs. CILs may be referenced by unique identification number to avoid duplicating information. Verifications will be performed by the contractor, government, or both. Identify and document specific verification types including analyses, tests, inspections, and\or demonstration for each verification activity. Each verification type will be indexed with its corresponding hazard cause (PDR), and control (CDR, DCR). When more than one type of verification is listed for a control, the verification types and status will be listed with a unique identifier. Traceability to the specific control information is required. The required documentation of verification activities progresses with the maturity of the design as follows: • PDR – Identify and document the specific verification type (i.e., test, analysis, inspection, or demonstration) applicable to each hazard cause as well as a description of the planned verification activities which outline the overall verification strategy providing enough detail to facilitate classification of the likelihood of the hazard. • CDR - Completion of document number or completion plan with ECD of verification activities to assure the effectiveness of each hazard control is identified and required for the CDR Delivery. • DCR – Design Certification Review, document completed hazard control verifications, including reference to specific documents (test reports, analysis reports, etc) where control verification is demonstrated. A verification tracking log or other traceability tool will reference each verification to an approved Element / Program document to ensure effective implementation of the controls.
Crew Survival Methods	Program integrated hazard analyses must identify Crew Survival Methods (CSMs) that will increase the probability of crew survival in the event that all hazard controls have failed and the catastrophic event is imminent. Within the program integrated hazard analysis, the planned CSMs (Abort, Escape, Emergency Egress, Safe Haven, Rescue, Emergency Medical, Other, or None) should be identified, a description provided if not evident by the survival

	method identified, and reference provided to documentation or analysis that verifies the adequacy of the survival method identified.

Appendix D. Hazard Analysis Comparison

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
Who:									
Owns the overall HA requirement	Enterprise System Development (ESD) Level I - As defined in ESD 10010 Enterprise System Development Safety and Mission Assurance Plan.	SSEB & PCSSP	SSEB & PCSSP	Shuttle Program, documented in NSTS-07700 Requirement Documents	SSP Program Level II	SSP Program Level II S&MA Office MX	Constellation Program owned the HA requirements. Maintained by program SR&QA.	Program Management	STS-1 two close calls: SRB Ignition Overpressure- non-catastrophic failure of Orbiter hardware. Aerodynamic anomaly - non catastrphic negative margins during ascent. Both owned by Level II System Integration. NEITHER WAS IDENTIFIED AS A HAZARD.
Generates the IHA	NASA - The IHAWG (as a CSI ITT) oversees the development of the Cross-Program Integrated Hazard Analysis and is responsible for tracking the schedule and status of the CPIH causes and compiling/delivering the System Safety Analysis Report. The IHAWG assigns Program S&MA and Engineering representatives to be responsible for the collaborative effort to generate and develop each CPIH cause and cause tree.	SSEB & PCSSP	SSEB & PCSSP	System Contractor (Rockwell International)	Since all waivers and CILs were cancelled, Rockwell and NASA re-generated and expanded all IHA	SE&I Prime Contractor - USA & Subcontractor Boeing - the HR was a contract Deliverable	CxP SE&I led the development with Program and Project S&MA personnel - MOA from SE&I SMA identified responsibilities for specific IHAs. In-flight IHAs between Orion and Ares only were developed by Ares Project under delegation from CxP SE&I.	ISS/Payload Contractor/Element developer	Hazards were not identified
Reviews it	Integrated Hazard Analysis Working Group (IHAWG). Drafts are delivered for review during major program milestones. Also undergoes cross-program review via change request prior to delivery for major cross-program milestones.	SSEB & PCSSP	SSEB & PCSSP	Rockwell Engineering and JSC S&MA	Space Shuttle Safety Review Panel (SSRP)	Integration Safety Review Panel (ISERP) Level II Safety Panel	Constellation Safety and Engineering Review Panel (CSERP)	Reveiwed and approved by the Flight SRP and/or GSRP (dependent on the nature of the hazard) per SSP 30599. Accepted by Program Management via CoFR process.	N/A
Approves/accepts it	Program Managers ~~(s)~~ (Joint PCB) and Level 1 (DAA for ESD ~~AA~~) depending on the residual risk level	SSEB & PCSSP	SSEB & PCSSP	JSC S&MA Director, NASA Integration Manager and finally NASA Shuttle Program Manager	Same as Shuttle - Original. In adition all Criticality 1 items were required to be reviewed and accepted by NASA HQ. Involvement by crew and JSC engineering mandated. Additionally, NRC formed a post Challenger review of Controlled Hazards and Accepted Risk Hazards with Retention Rationale.	SSP Program Manager	Approval of 1x5 , 2x4, 1x4, and all marginal, minor, and negligible hazards were approved by the CSERP. All other critical and catastrophic hazards, except those ranked 5x5, were approved by the CxCB. 5x5 hazards approved at the agency level - revisions after base lining reviewed and approved by CSERP (program cancelled prior to this)	Program Management	N/A
Baselines it	Enterprise System Development Control Board (ECB)	SSEB & PCSSP	SSEB & PCSSP	SSP Program Control Board	SSP Program Control Board	SSP Program Control Board	See above	?	N/A

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
Implements controls and verifications (i.e., who makes it happen)	Programs	SSEB & PCSSP	SSEB & PCSSP	Projects, as directed by the Shuttle Program Manager	Projects, as directed by the Shuttle Program Manager	Projects, as directed by the Shuttle Program Manager	Projects	?	N/A
Monitors/reviews systems changes for their effect on accepted risk level	S&MA personnel	SSEB & PCSSP	SSEB & PCSSP	System Contractor and NASA S&MA, report chages at FRR	Monitoring elevated to newly appointed Associate Administrator for Safety & Reliability	SSP Level II SE&I MS and S&MA	Integration S&MA personnel - Change approved by CSERP	?	N/A
Generates the element-level HA	Prime Contractor - CFE NASA - GFE NASA - SLS Integrated Hazards	SSEB & PCSSP	SSEB & PCSSP	Element Contractor S&MA	SSP Element Prime Contractors with oversight from NASA/ crew office	SSP Element Prime Contractors with oversight from NASA/ crew office	Prime Contractor	Element Provider	N/A
Reviews them	Varies between programs: NASA Safety & Engineering Reviews at minimum	SSEB & PCSSP	SSEB & PCSSP	Element Contractor Engineering and NASA S&MA	SSRP	Center Safety Engineering Review Panels (KSERP, MSERP, JSERP) and SE&I (to check for integrated effects)	CSERP	SRP/GSRP	N/A
Approves them	Program Manager(s) and Level 1 (DAA for ESD AA) depending on the residual risk level	SSEB & PCSSP	SSEB & PCSSP	NASA Program Manager	SSP Program Manager	SSP Program Manager	Approval of 1x5 , 2x4, 1x4, hazards were approved by the CSERP. All other critical and catastrophic hazards, except those ranked 5x5, were approved by the CxCB. 5x5 hazards approved at the agency level. All marginal, minor and negligible hazards approved at project level. - revisions after base lining reviewed and approved by CSERP (program cancelled prior to this)	SRP/GSRP	N/A
Baselines them	Program control Board (PCB)	SSEB & PCSSP	SSEB & PCSSP	NASA Element Project Control Board	NASA Element Project Control Board	NASA Element Project Control Board	See above	?	N/A
Implements controls and verifications (i.e., who makes it happen)	Programs	SSEB & PCSSP	SSEB & PCSSP	NASA & Contractor S&MA and Engineering as directed by NASA Element Project Mgr	NASA & Contractor S&MA and Engineering as directed by NASA Element Project Mgr	NASA & Contractor S&MA and Engineering as directed by NASA Element Project Mgr	Element	?	N/A
Monitors/reviews systems changes for their effect on accepted risk level	S&MA personnel	SSEB & PCSSP	SSEB & PCSSP	NASA and Contractor S&MA, report changes at FRR	NASA and Contractor S&MA, report changes at FRR, Additioal oversite from AA for Safety and Reliability at FRRs	NASA and Contractor S&MA, report changes at FRR, Additioal oversite from AA for Safety and Reliability at FRRs	Prime Contractor and Element S&MA Personnel - changes approved by CSERP	?	N/A

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
What:									
Is the IHA starting point	Interfaces, operations concepts, and Shuttle and CxP hazards were used to derive potentially hazardous conditions. IHA is defined as any hazard in which more than one program is a contributing cause, control, or verification for the hazard. CPIHs require more than one program to contribute to the analysis of the system effect, the interactions/interfaces, and interdependencies of the hazard.	Varies by element and subsystem	Varies by element and subsystem	Elements' FMEA/CILs, Element Hazard Analysis, and EEFA (Element Interface Functional Analysis), and definition of top level generic hazards	Elements' FMEA/CILs, Element Hazard Analysis, and EEFA (Element Interface Functional Analysis), and definition of top level generic hazards	Level II Fault Tree created by SSP SE&I	Program level Fault Tree Analysis. Development begun at the Concept Development Phase	Element-to-Element	
Is the process/flow	As defined in ESD 10010 Enterprise System Development Safety and Mission Assurance Plan. With 3 Programs - The cause trees are used to identify the IHA causes and the program-only causes for each hazard topic. IHA causes are assigned to the accountable program to be developed with engineering and safety representatives from the affected programs to define controls and verifications. Any causes determined to be program-only will be passed to the identified program for further evaluation. Individual programs are responsible for verification that program-only hazard causes have been properly mitigated.	MIL-S-38130 (then 882)	MIL-S-38130 (then 882)	Contractor S&MA develops IHA, table top review with contractor engineering, engineering performs analysis, results of analysis assists in clsification of hazard - controlled hazard or accepted risk, or recommendation of design change	Hazard Reports were not emphasized by the program, the focus was on FMEA/CIL Aditional crew involement and JSC Engineering sign off on FMEA/CIL and HA	Fault Tree Items --> Hazardous Events --> causes --> Hazard Reports Hazard Reports were submitted via SSP Change Request	Fault Tree developed. Causes identified and Hazard Reports developed. Product matures throughout life cycle review process	Safety review process, keyed to design maturity	

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
Is included in the IHA (Condition, Cause, Effect, Mitigation, Control, Verification, Risk Classification, etc.)	Mission Effectively, Mission Phase, Cause Description, Mitigation Strategy, Acceptance Rationale, Failure Tolerance, Likelihood Justification, Risk Matrix, Cause Tree Reference, Effects, Transfers Out, Controls, Control Verifications, Verification Status, Severity, Likelihood, FEMA/CIL number, Program/Element Control References, Crew Survival Notes, Background	Mostly included but not clear	Mostly included but not clear	Description of hazard, causes, controls, verification of controls, and clasification - controlled or accepted risk	Description of hazard, causes, controls, verification of controls, and clasification - controlled or accepted risk	Yes to all, along with Acceptance Rationale	Mission Effectively, Mission Phase, Hazardous Condition Description, Cause Summary, Acceptance Rationale, Likelihood Justification, Hazard Risk Matrix, Cause, Fault Tree Reference, Effects, Transfers Out, Controls, Transfers In, Verifications, Verification Status, Severity, Likelihood, Safety Requirements, Interfaces, FEMA/CIL number, operations Related Documentation, Detection and Warning Method, CSM, Operational Implementation of CSM, Verification of CSM, Background	All	
Is not included in the IHA	Hazards caused and controlled by a single program. Hazards during crew surivial ops (e.g., aborts).	no RAC	no RAC	Hazards created by a single element and controlled by that element	Hazards created by a single element and controlled by that element	Hazards created by a single element and controlled by that element	Hazards created by a single project/element and controlled by that project/element	n/a	
Is the format	Narrative SSAR submitted at milestone reviews - ESI System Safety Analysis Report (ESD 10015). Hazard Tables in SSAR include top-level hazardous condition description and integrated (cross-program) causes contributing to that condition.	Unknown	Unknown	Narrative report	Narrative report	Narrative report	Narrative SSAR submitted at milestone reviews include a.The relevant information on the Project/element/subsystem being analyzed b. Descriptions and background data c. Reference(s) to milestone review data necessary to understand the analyzed system d. The ground rules for the analysis, hazards evaluated and excluded from further detail in hazard reports e. The hazard reports	Safety Data Package/Hazard Reports	

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
When:									
Are the products delivered	Milestone Reviews	Milestone Reviews	Milestone Reviews	Initial delivery conurent with Design Reviews. All IHAs closed fefore each flight	HRs must be Submitted via CR Prior to FRR - 30 Days	HRs must be Submitted via CR Prior to FRR - 30 Days	Final approval at SAR	Consistent with design and I&T maturity	
Does the Crew Office get involved	Yes. Member of IHAWG,	Yes	Yes	Individual interested crew members were involved in selected areas of interest	Yes, at SSRP and PRCB	Yes, at ISERP and PRCB	Member of CSERP that reviews the SSAR (hazard reports, fault trees) throughout the process	Yes	
Where:									
Are controls focused (Ops, Design, etc.)	Yes, as applicable. Fault tolerance for catastrophic hazards/DFMR per Human-Rating Requirements for Space Systems NPR 8705.2B. Controls for engineering processes driving integrated analysis and design definition. Ops controls such as constraints and OMRS.	Controls are spread out across the system by what was deemed important to cover	Controls are spread out across the system by what was deemed important to cover	First focus was on design(strongest controls), followed by Safety Systems, followed by notifications (alarms), followed by operational controls (weakest controls)	Design - preventing the hazardous event	Design - preventing the hazardous event	Design	Yes, as applicable. Two-fault tolerance for Catastrophic Hazards/DFMR. SPP 50021, Safety Policy and Requirements	
Are the safety design requirements defined	Human-Rating Requirements for Space Systems NPR 8705.2B and NPR 8715.3C NASA General Safety Program Requirements	Yes, but loosely by today's standards	Yes, but loosely by today's standards	Vol X of NSTS - 07700 doccumented all design requirements, including safety related requrements such as safety factors and safety margins, redundancy requirements and requirements for analysis and test. NHB-5300.4 was an SR&QA Process Requirement Doccument for Shuttle Program.	After Challanger accident, System Integrity Assurance Program Plan (SIAPP) was developed and imposed on the Shuttle Program,to elevate level of discipline of all activities from design, test, manufacturing, and operations. NSTS 22254 and NSTS 5300.5	NSTS 22254 and NSTS 5300.5	Constellation Architectural Requirements	SSP 50021, 5002, 5004, KHB 1700.7B	
Are the verification requirements defined	Program Verification Plans	Yes - but loosely by today's standards	Yes - but loosely by today's standards	Yes, in the same documments as design requirements	NSTS 22254	NSTS 22254	Program Verification Plan - clarifications for verifications in hazards listed in Appendix of CxP 70038	SSP 50021, and applicable referenced documents.	

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
Why:									
Was this approach taken	To influence design earlier than possible with a top-down fault tree approach. To take maximum advantage of program resources given light-touch intgration approach.	Safety Program; "learn as you go" philosophy	Safety Program	Shuttle development was challenging, with new technologies required and perception of no room for safety shortcuts. Therefore conventional top-down hazard analysis, with hierarchical controlls were used to provide safety net under untried design	Challenger accident resulted in increased focus on SSP Critical Items, FMEA, and CILs - Full review of all Program CILs	Columbia accident resulted in increased focus on SSP hazard reports and Program Integration - IHRs were rebaselined	Consistency from each project/element at each design phase - Consistency in formatting from project to project and element to element - Looked at Shuttle, Payload Safety, Space Station for guidance on use of fault tree methodology and hazard reports	Consensus standard, utilized by other NASA programs, DOD, industry.	
How:									
Are hazards identified	Mixture of sources - Interface requirements; con ops; engineering interview/brainstoarming; experiences of past programs (Shuttle, CxP), cause trees.	HA & FMECA	HA & FMECA	Mixture of sources - top level generic hazards, Element FMEA, Element Hazard Analysis, and EEFAs	Mixture of sources - top level generic hazards, Element FMEA, Element Hazard Analysis, and EEFAs	Fault Tree	Fault tree analysis approach	Based on unmitigated credible worst case results.	
Are the IHA controls implemented	Primarily through cross-program documentation (environments def, IRD/ICDs, etc.). Through program-owned documentation for engineering process controls.	Yes but no clearly	Yes but no clearly	Following was preferred priority- design features/margins, safety features, warning systems, operational controls	Following was preferred priority- design features/margins, safety features, warning systems, operational controls	Following was preferred priority- design features/margins, safety features, warning systems, operational controls	A closed loop tracking system utilized for closing verifications - Hazard Precedence - a. Eliminate the Hazard b. Design to Minimize Hazards c. Incorporate Safety Devices d. Provide Caution and Warning Devices e. Develop and Implement Special Procedures	Consistant with fault tolerance and other design requirements.	

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)	Apollo - Pre-Apollo 1	Apollo - Post-Apollo 1	Shuttle - Original	Shuttle Post-Challenger	Shuttle Post-Columbia	Constellation	ISS	Accidents/Close Calls Findings
Are the element HA controls implemented	Through program- and element-owned documentation, drawings, etc.	Yes but not clearly	Yes but not clearly	Same priority as in IHAs	Same as in IHAs	Same as in IHAs	Same as above	Same	
Are the controls verified	Test, Analysis, Inspection	Not sure but likely in CM	Not sure but likely in CM	Analysis and test during design, OMRS during operations	Analysis and test during design, OMRS during operations	Analysis and test during design, OMRS during operations	Test, Analysis, Inspection, Demonstration	As required by reference requirements.	
Is configuration control implemented	Yes	Yes	Yes	Math models under configuration control, configuration control of OMRSD, PCASS System - closed loop verification of satisfaction of the OMRS requirements	Submitted via CR and Under SSP Program CM	Submitted via CR and Under SSP Program CM	CxP hazard database was required to be under configuration control - SSAR delivered at each milestone review placed under program configuration control	?	
Are likelihood and consequence assessed (numerically, subjectively)	Both qualitatively and quantitatively but matrix for likelihood only shows qualitative assessment.	No RAC or probability calculations	No RAC or probability calculations	Only by engineering judgment	Subjectively - done to preclude people "gaming the numbers" in lieu of focusing on HR controls	Subjectively - done to preclude people "gaming the numbers" in lieu of focusing on HR controls	Methodology states both qualitatively and quantitatively but matrix for likelihood only shows qualitative assessment.	Subjectively.	
Are other risk identification/control processes integrated with the HAs (FMEA/CIL, PRA, etc.)	Linked to the CILs and program-owned hazards/controls.	Does not appear that way	Does not appear that way	System Integration S&MA integrated IHA with FMEA/CIL, Element Hazards, EEFA (but not PRA) to create a safety net for the Space Shuttle System	NoFMEA/CILs had priority over HRs	No not for IHRs	yes - linked to the fault trees and hazard reports - maintained in separate systems	Not specified.	
Are LOC and LOV risks marked: separately or combined on (5x5) risk matrix	No	No data	No data	No	No	No	separately *(JAW: I don't think CxP logged these seperately in the risk matrix. Considered worst case.)*	Not specified.	

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01- 01 - 2015	Technical Memorandum	February 2014 - November 2014

4. TITLE AND SUBTITLE
Review of Exploration Systems Development (ESD) Integrated Hazard Development Process
Appendices

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Smiles, Michael D.; Blythe, Michael P.; Bejmuk, Bo; Currie, Nancy J.; Doremus, Robert C.; Franzo, Jennifer C.; Gordon, Mark W.; Johnson, Tracy D.; Kowaleski, Mark M.; Laube, Jeffrey R.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
869021.05.07.09.49

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L-20523 NESC-RP-14-00929

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM-2015-218676/Volume II

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 16 Space Transportation and Safety
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Chief Engineer of the Exploration Systems Development (ESD) Office requested that the NASA Engineering and Safety Center (NESC) perform an independent assessment of the ESD's integrated hazard development process. The focus of the assessment was to review the integrated hazard analysis (IHA) process and identify any gaps/improvements in the process (e.g., missed causes, cause tree completeness, missed hazards). This document contains the outcome of the NESC assessment.

15. SUBJECT TERMS
Exploration Systems Development; Cross-Program Integrated Hazard Process; NASA Engineering and Safety Center; Integrated Hazard Analysis Process

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER ***(Include area code)***
U	U	U	UU	117	(443) 757-5802