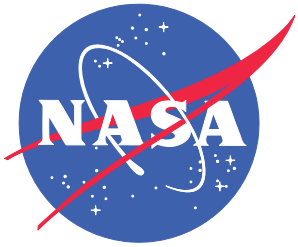
NASA/TM–2015-218676/Volume I
NESC-RP-14-00929



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

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:

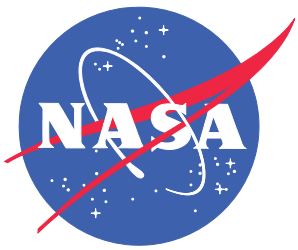
- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- 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 I
NESC-RP-14-00929



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

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 1

November 20, 2014

Report Approval and Revision History

NOTE: This document was approved at the November 20, 2014, NRB. This document was submitted to the NESC Director on December 15, 2014, for configuration control.

Approved:	*Original Signature on File*	12/15/14
	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Michael D. Smiles, NESC Chief Engineer, SSC	11/20/14

Table of Contents

Technical Assessment Report

List of Figures

Technical Assessment Report

1.0 Notification and Authorization

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). Any deficiencies, gaps, or improvements identified during this assessment could be incorporated into subsequent design or process changes.

The assessment plan was approved by the NESC Review Board (NRB) on February 20, 2014. Mr. Michael D. Smiles was selected to lead this assessment. The key stakeholders for this assessment were Mr. Paul McConnaughey, ESD Chief Engineer; Mr. Daniel Dumbacher, ESD Deputy Associate Administrator (DAA); Mr. William Hill, ESD Assistant DAA; Mr. Ralph Roe, NASA Chief Engineer; Mr. Terry Wilcutt, NASA Safety and Mission Assurance (S&MA) Chief; Mr. Timothy Wilson, NESC Director; Mr. Jeffrey Williams, ESD IHA Working Group (IHAWG) Lead; Mr. David Thelen, ESD Chief S&MA Officer (CSO); Mr. Jeffrey Hamilton, ESD Systems Safety Lead; Mr. Thomas Whitmeyer, ESD Assistant DAA; and Mr. George Deckert, Deputy ESD CSO.

2.0 Signature Page

Submitted by:

Team Signature Page on File - 1/12/15

Mr. Michael D. Smiles Date

Significant Contributors:

Mr. Michael P. Blythe Date

Mr. Bo Bejmuk Date

Dr. Nancy J. Currie Date

Mr. Robert C. Doremus Date

Ms. Jennifer C. Franzo Date

Mr. Mark W. Gordon Date

Ms. Tracy D. Johnson Date

Mr. Mark M. Kowaleski Date

Mr. Jeffrey R. Laube Date

Signatories declare the findings, observations, and NESC recommendations compiled in the report are factually based from data extracted from program/project documents, contractor reports, and open literature, and/or generated from independently conducted tests, analyses, and inspections.

3.0 Team List

Name	Discipline	Organization
Core Team		
Michael Smiles	NESC Lead; NESC Chief Engineer	SSC
Michael Blythe	Deputy Team Lead; NESC Deputy Director for Safety	JSC
Bo Bejmuk	Former Boeing SSP Orbiter and Systems Integration Program Manager	AMA
Nancy Currie	NESC Principal Engineer	JSC
Robert Doremus	Associate Director, JSC S&MA Directorate	JSC
Jennifer Franzo	MSFC S&MA Technical Interface to SSC	SSC
Mark Gordon	Chief, Payload Development and Processing Division, S&MA	KSC
James Harper	Systems Safety Expert	Ares Corporation
Tracy Johnson	SLS CSO Integration Engineer	MSFC
Mark Kowaleski	NASA Safety Center	GRC
Jeffrey Laube	Commercial Launch Projects Senior Project Engineer	Aerospace Corporation
Patricia Pahlavani	MTSO Program Analyst	LaRC
Consultants		
Jeff Hamilton	ESD Systems Safety Lead	MSFC
David Thelen	ESD CSO	JSC
Jeffrey Williams	ESD IHAWG Lead	JSC
Administrative Support		
Linda Burgess	Planning and Control Analyst	LaRC/AMA
Jonay Campbell	Technical Writer	LaRC/NG
Pamela Sparks	Project Coordinator	LaRC/AMA

4.0 Executive Summary

The Exploration Systems Development (ESD) Cross-Program Integrated Hazard (CPIH) process is unlike that of any other current or previous NASA human spaceflight (HSF) program. In fact, the overall integration approach chosen by the ESD, not just pertaining to integrated hazard analyses (IHAs), creates new challenges for a large, complex spaceflight program. The objective was to reduce costs, reduce enterprise-level management oversight, and drive decisions down to the programs, giving the programs a great deal of autonomy. However, this approach has the potential to foster inconsistencies between the programs and the ESD in the development/ approval of technical products and resolution of integrated problems. Concerns regarding the appropriate level of integration across all of the programs were raised by various insight groups such as the Aerospace Safety Advisory Panel (ASAP) and the ESD Standing Review Board (SRB).

The ESD Chief Engineer requested that the NASA Engineering and Safety Center (NESC) perform an independent assessment of the ESD CPIH process. The scope of this assessment was to gain an understanding of the ESD integrated hazard process, identify gaps (e.g., missed causes, cause tree incompleteness, or missed hazards), and suggest improvements to the process. The division of responsibilities between the ESD and the three programs was examined to properly evaluate the integrated hazard process. The assessment approach was two-fold: gain an understanding of the unique ESD integrated hazard process and identify any technical and process gaps.

The ESD Cross-Program Integration organizational concept consists of functional areas reporting to the Cross-Program Integration Team (CPIT) leadership. Each functional area consists of various integrated task teams (ITTs), which typically include just a few ESD-funded individuals. The products of each of those ITTs are developed by Engineering and/or Safety and Mission Assurance (S&MA) personnel that work for the three programs and deliver their assigned analyses to the ESD ITTs. The ESD IHA Working Group (IHAWG), which is supported by a single ESD-funded individual, is responsible for the development of the IHAs. The ESD IHAs are limited to areas where two or more of the three programs' hardware or software systems interact. Development of all other hazards unique to each program is the responsibility of the applicable program: the Space Launch System (SLS), the Orion Multi-Purpose Crew Vehicle (MPCV), or Ground Systems Development and Operations (GSDO). The approach taken by the IHAWG was to develop cause trees and cause reports in lieu of a higher-level integrated systems approach, often referred to as a "top-down" approach.

The NESC assessment team members were chosen for their familiarity with hazard development/ identification/mitigation policies and practices on critical flight programs, including HSF programs. The team included NASA and contractor experts from the NESC, the NASA Safety Center (NSC), past programs, the commercial launch arena, Goddard Space Flight Center (GSFC), and the three Centers where the SLS, MPCV, and GSDO Programs are stationed.

The NESC assessment team spent a considerable amount of time understanding the ESD integrated hazard process and the division of responsibilities between the ESD and the three

programs. The assessment team conducted a Technical Interchange Meeting (TIM) with the ESD personnel responsible for the integrated hazard process, interviewed a variety of key personnel, including all of the assessment's stakeholders, and reviewed documentation applicable to the hazard analysis processes. The IHAWG Chairman's and ESD Chief S&MA Officer's (CSO) cooperation and willingness to candidly share information and discuss the ESD methodology with the assessment team was outstanding.

To identify technical and process gaps, the NESC assessment team reviewed documents from the ESD and other HSF programs, conversed with people knowledgeable of previous HSF programs, and utilized the team members' expertise and collective experience of 268 years. The assessment team did not perform a comprehensive review of cause trees and cause records to identify all potential gaps. However, during the course of the assessment, team members reviewed selected cause trees and cause records to further understand ESD's IHA process. When gaps were identified, a deeper dive ensued and the results were documented as findings.

Organizational and procedural factors play a significant role in how risks of complex programs are identified, mitigated, and accepted. Because minimal Agency-level policy or guidance exists addressing the conduct of hazard analysis, the team chose to identify potential process gaps by comparing ESD's hazard analysis process approach with that of similar complex HSF programs.

The findings, observations, and NESC recommendations are organized into four categories: positive observations, process/approach issues, technical gaps, and risk acceptance issues. The following were key issues addressed in the findings and observations:

- A lack of uniformity exists in the hazard analysis processes between the enterprise and the programs, which could result in missed causes/controls during development and difficulties in evaluating the risk of technical issues during the operational phase.
- Because a higher-level integrated systems approach to IHA was not utilized, the potential exists to miss integrated hazardous causes and controls, thereby increasing risk.
- The level of management approval of hazard analyses and risk acceptance is insufficient for those hazards categorized as critical or catastrophic.
- ESD CPIHs do not include hazard effects across programs as one of the drivers for what comprises an integrated hazard, which could lead to missed hazard controls for causes such as engine stuck-throttle or interim cryogenic propulsion stage (ICPS) prevention of coupled structure propulsion instability (pogo).

The overriding issue is that the IHA baseline utilizing the current approach may not be sufficiently comprehensive. The assessment team evaluated the ESD integrated hazard process through familiarization with the CPIH methodology and understanding the organizational interactions between the programs and ESD. The NESC assessment team did not base its conclusions on the fact that the current process differed from previous HSF programs. After thorough discussion and debate, the NESC assessment team documented findings, observations, and NESC recommendations based on issues and concerns with risk acceptance, process gaps,

and technical gaps. Some technical gaps were identified by in-depth examination of selected cause trees and cause records. The NESC assessment team is confident the identified technical gaps will be addressed. However, if the CPIH process gaps identified in this report are not corrected, additional technical gaps may not be properly identified, assessed, and addressed. The NESC assessment team commends the ESD for increasing engineering engagement early in the IHA development process, and recognizes the amount of work accomplished in the CPIH development. By incorporating the NESC recommendations documented in this report, the existing products and knowledge can be leveraged into a more comprehensive hazard identification and mitigation process that will provide long-term benefit to the enterprise.

5.0 Assessment Plan

The scope of this assessment was to gain an understanding of the ESD integrated hazard process, identify any gaps (e.g., missed causes, cause tree incompleteness, or missed hazards), and suggest improvements to the process. The division of responsibilities between the ESD and the three programs was to be examined to properly evaluate the integrated hazard process. Additionally, the ESD IHAWG Lead requested real-time feedback from the NESC assessment team as the IHAWG evaluated top-down model methodologies to incorporate, such as fault trees.

The NESC assessment team members were chosen for their familiarity with hazard development/ identification/mitigation policies and practices on critical flight programs, including HSF programs. The team included NASA and contractor experts from the NESC, the NSC, past programs, the commercial launch arena, GSFC, and the three Centers where the SLS, Orion MPCV, and GSDO Programs are stationed (i.e., Marshall Space Flight Center (MSFC), Johnson Space Center (JSC), and Kennedy Space Center (KSC)).

The technical assessment focus was on the ESD integrated hazard development process and the division of responsibilities between the ESD and the three programs designing the next NASA HSF vehicle, and to identify any gaps/improvements in the process by accomplishing the following steps:

- Become familiar with the current ESD integrated hazard development process through participation in selected IHAWG weekly meetings and through review of IHAWG documentation, such as the Systems Safety Analysis Report and the Deep Dive presentation from the IHAWG chairman to ESD management during the GSDO Preliminary Design Review (PDR) timeframe.
- Conduct a TIM at JSC with the IHAWG and the IHA Architecture Team (IHAAT) to gain a more thorough understanding of the current process.
- Conduct interviews with concerned parties outside the ESD and the programs.
- Research and document the hazard development processes from previous HSF programs and utilize that information as a tool to aid in performing a gap analysis.
- Focus on deficiencies, gaps, and improvement opportunities for the overall process; missed causes; cause tree completeness; and missed hazards.
- Develop findings, observations, and NESC recommendations, to be presented as part of the stakeholder briefing at Headquarters prior to the IHAWG's Orion MPCV delta PDR data submittal deadline, in order to allow time for the stakeholder to consider and incorporate the NESC team's recommendations. Due to the complexity of the subject matter and the longer-term recommendations developed by the assessment team, the stakeholder briefing was not held until the conclusion of the delta PDR at JSC.

6.0 Problem Description, Background, and Assessment Approach

6.1 Problem Description

The ESD CPIH process is unlike that of any other current or previous NASA HSF program. In fact, the integration approach chosen by the ESD, not just pertaining to IHAs, creates new challenges for a large, complex spaceflight program. The objective of the approach was to reduce costs, reduce enterprise-level management oversight, and drive decisions down to the programs, giving the programs a great deal of autonomy. This approach has the potential to foster inconsistencies between the programs and ESD in the development/approval of technical products and resolution of integrated problems.

The ESD Cross-Program Integration organizational concept is shown in Figure 6.1-1. Each organizational functional "block" below the CPIT Leadership level is typically limited to a few ESD-funded individuals, and only one individual in the case of the Integrated Hazards block shown in green. The products of each of those functional teams, called ITTs, are developed by engineering and/or S&MA personnel that work for the three programs, who deliver their delegated analyses to the ESD ITTs.

Concerns that this approach may lack the appropriate level of integration across all the programs were raised by various insight groups such as the ASAP and the ESD SRB. The ESD Chief Engineer requested that the NESC perform an independent assessment of that process, which was the impetus for the creation of this assessment team.

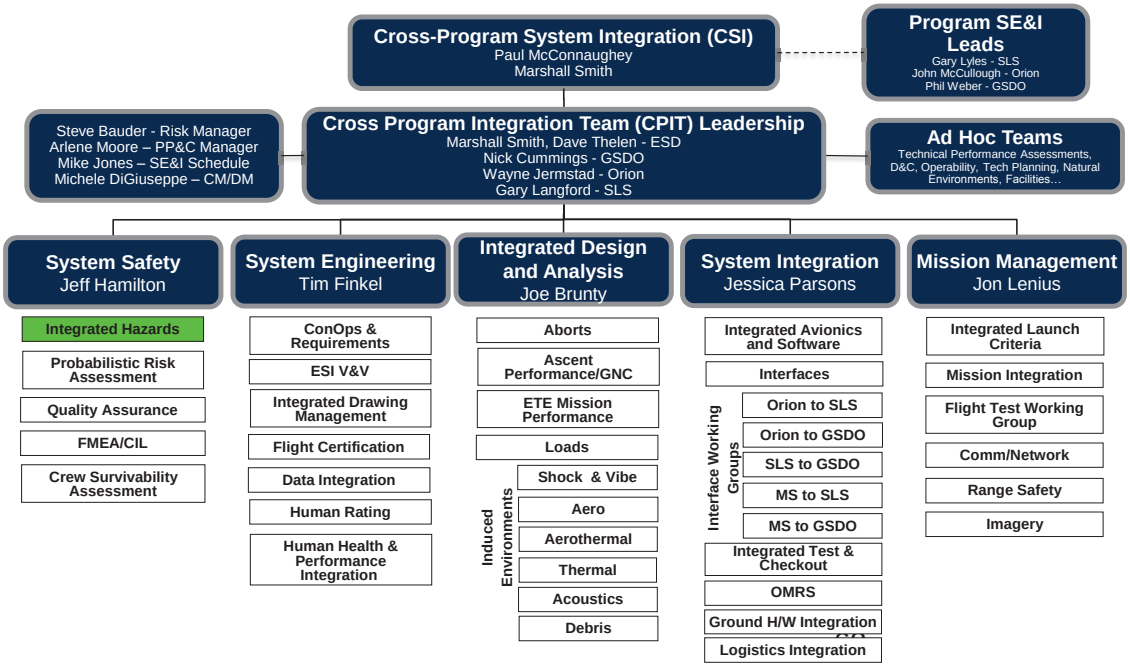


Figure 6.1-1. ESD ITT Organization

6.2 Background

For hazard analysis products, the ESD is responsible for the development of the IHA, limited to areas where two or more of the three programs' hardware or software systems interact. Responsibility to develop all other hazards unique to each program has been delegated to the applicable program: SLS, Orion MPCV, and GSDO.

The approach taken by the Integrated Hazard ITT was to develop cause trees and cause reports, as illustrated in Figure 6.2-1.

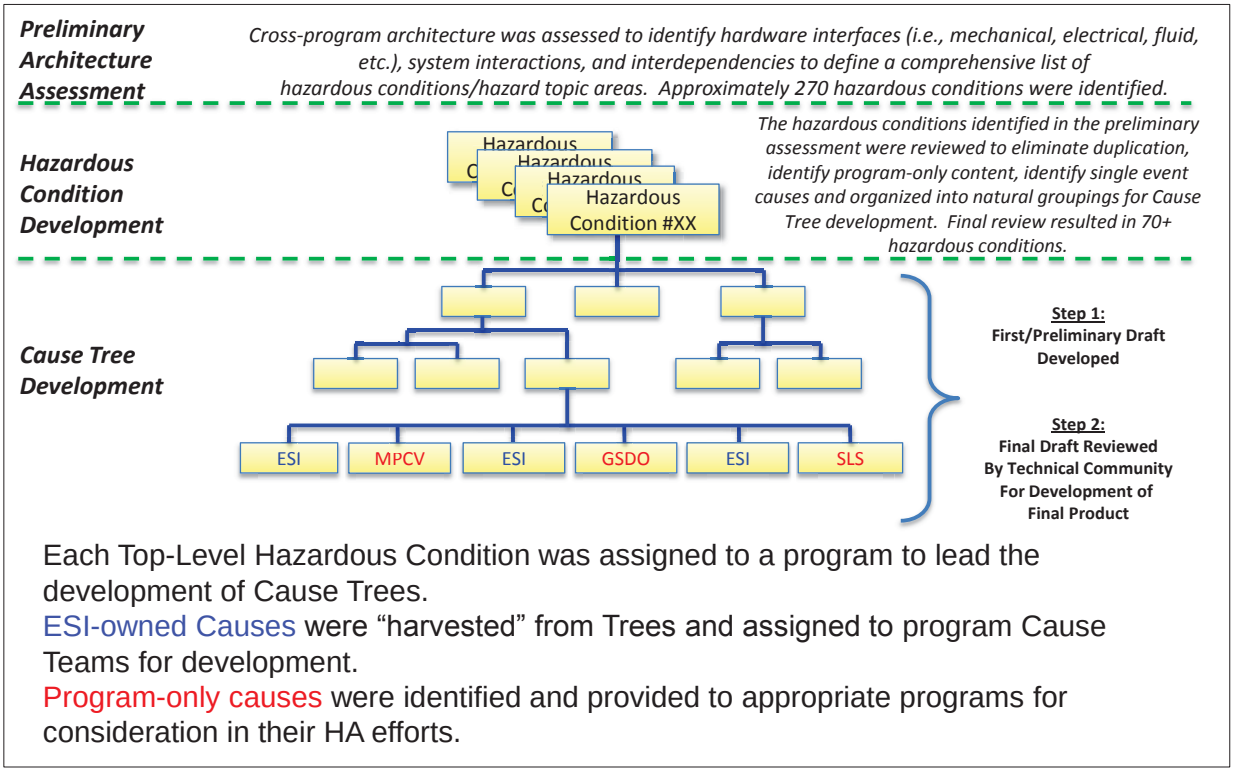


Figure 6.2-1. ESD IHA Methodology

According to the IHAWG, the advantages of the chosen approach include the following:

- Allows for a product with opportunity to influence design.
- Uses available cross-program products in the absence of a more detailed design definition.
- Implementable with limited resources, the vast majority of which are provided by the ESD programs.
- Easily adaptable; can add cause trees and causes as design changes (e.g., vehicle stabilization system).

According to the IHAWG, disadvantages and concerns of the chosen approach include the following:

- Potential to miss something due to lack of a more structured model.
- Potential lack of common understanding of approach by all those involved in IHA development and review (including stakeholders).
- Difficult to see the "big picture" regarding causes and the relationships between causes, which often results in scoping issues for these causes (e.g., fire/explosion causes are spread among multiple cause trees).
- Sustainability and maintainability of the model structure over the long term.

6.3 Assessment Approach

The scope of this assessment was to gain an understanding of the ESD integrated hazard process, identify gaps (e.g., missed causes, cause tree incompleteness, or missed hazards), and suggest improvements to the process. The division of responsibilities between the ESD and the three programs was examined to properly evaluate the integrated hazard process.

6.3.1 Understand the Process

To gain an understanding of the ESD integrated hazard process and the division of responsibilities between the ESD and the three programs, the assessment team conducted a TIM, interviewed a variety of key personnel, and reviewed documentation applicable to hazard analysis processes. The team also reviewed the NESC Director's integration white paper "Improving Exploration Systems Integration," dated January 29, 2014 [ref. 1].

A TIM was held early in the assessment with the IHAWG Chairman, the ESD CSO, and the ESD System Safety Team Lead to provide a face-to-face forum for explanation, questions, and discussion.

The team conducted interviews with most of the stakeholders to solicit background information and their expectations of the assessment results. Some of the stakeholders interviewed were the ESD Chief Engineer, the NASA Chief Engineer, the NASA S&MA Chief, the NESC Director, the ESD Deputy Associate Administrator (DAA), and the ESD Assistant DAA. A complete list of interviewees is given in Appendix A.

Pertinent ESD and program documentation was reviewed by the team to help understand the process and the interaction between ESD and the programs. The "Integrated Hazard Analysis Deep Dive" presentation (see Appendix B) to ESD management, compiled by the IHAWG Chairman, was reviewed and discussed in great detail at the TIM. Other key documents reviewed were the "Cross Program Safety and Mission Assurance Plan" (ESD 10010, Initial Baseline Release, dated September 20th, 2012; see Appendix C), the Programs' S&MA Plans, and the IHAWG Task Agreement. A complete list of the reviewed documents is given in Appendix A.

6.3.2 Identify Technical and Process Gaps

The NESC assessment team reviewed documents from ESD and other HSF programs, conversed with people knowledgeable of previous HSF programs, and utilized the team members' expertise and collective experience of 268 years. Key documents reviewed include the SLS Abort Triggers Definition Document (SLS-SPEC-197); Shuttle Integrated Hazard Report IPYR-01, Pyrotechnic System Malfunction; the ESD Systems Safety Analysis Report (ESD 10015, dated January 15th, 2014, released for GSDO PDR); the IHAWG Guidance for Analysis Causes; and selected cause trees and cause records (see Appendix A). The NESC assessment team did not perform a comprehensive review of cause trees and cause records to identify all potential gaps. However, during the course of the assessment, NESC assessment team members reviewed selected cause trees and cause records to further understand ESD's IHA process. When gaps were identified, further investigation was undertaken, and the results were documented as findings.

A key step in the NESC assessment team's approach to identifying process gaps was to compare ESD's hazard analysis process approach to that of similar complex HSF programs. Organizational and procedural factors play a significant role in how risks for complex programs are identified, mitigated, and accepted. The details of "who, what, when, where, why, and how" hazardous risks were managed by comparable HSF programs were consolidated in a comparison matrix developed by the NESC assessment team (see Appendix D).

The NESC assessment team researched and compared prior HSF program hazard analysis process approaches, including:

- Apollo original; post-Apollo 1
- Shuttle original; Shuttle post-*Challenger*; and Shuttle post-*Columbia*
- Constellation
- International Space Station (ISS)
- Accident/close calls findings

A sample of the comparison matrix is shown in Figure 6.3-1. The entire matrix is included in Appendix D.

Hazard Analysis Process	Exploration (ESD, SLS, MPCV, GSDO)		Apollo - Post-Apollo 1			Shuttle Post-Columbia		ISS
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	~	~	SSP Program Level II S&MA Office MX	~	Program Management
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	~	~	SE&I Prime Contractor - USA & Subcontractor Boeing - the HR was a contract Deliverable	~	ISS/Payload Contractor/Element developer
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	~	~	Integration Safety Review Panel (ISERP) Level II Safety Panel	~	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.
Approves/accepts it	Program Managers ~~(s)~~ (Joint PCB) and Level 1 (DAA for ESD ~~AA~~) depending on the residual risk level	~	SSEB & PCSSP	~	~	SSP Program Manager	~	Program Management

Figure 6.3-1. Hazard Comparison Analysis (see Appendix D for complete analysis)

The conclusions from the comparison confirmed that the ESD CPIH process is unlike that of any other current or previous NASA HSF program. Significant differences identified include:

- The starting point of the ESD analysis is the program-to-program interfaces in lieu of a suite of higher-level integrated system fault trees.
- ESD CPIHs are developed by NASA teams in lieu of a prime integration contractor.
- ESD and the programs utilize their own hazard analysis methodologies in lieu of a common methodology for the entire enterprise.

7.0 Data Analysis

The ESD IHA process is admittedly and purposely different from previous programs. Different, in and of itself, is not necessarily bad. *"It's different. So what? What are the potential dangers or undesired results of doing it this way?"* When something about the current process concerned the NESC assessment team, there was thorough discussion/debate to determine why it was or was not a concern or issue. The concerns or issues that remained after these team discussions were documented as findings and observations in the following subsections, with explanation.

The NESC assessment team was aware that terminology was key to properly communicate issues and proposed solutions. One of the terms that potentially derailed understanding between the team and the ESD systems safety personnel was "top-down approach." That terminology appears in many places in systems safety documentation and training, especially related to hazard analysis approaches. To some, "top-down approach" meant to start with the absolute worse-case hazardous event: loss of crew/loss of vehicle (LOC/LOV). To others, it meant one or two levels below the event—still very high-level in a fault-tree type analysis, but not *the* top-

level event. Therefore, to avoid any confusion with the stakeholders' possible preconception of the "top-down approach" and to help clarify the concerns/issues documented in the team's findings and observations, the NESC assessment team chose to use the terminology "higher-level integrated systems approach." This terminology is utilized in the findings, observations, and NESC recommendations discussed below.

The findings, observations, and NESC recommendations are offered with the intent of sharing the experienced assessment team's desire to improve the current ESD IHA process for the long-term safety and mission success of the next HSF enterprise. While similarity exists between some of the findings, each one is focused on a specific issue that could be resolved by implementing its unique recommendation. The findings and observations are presented as one-sentence statements of the issue, followed by additional explanation of the rationale for the statement. All recommendations are written as actions directed toward ESD management (unless otherwise stated) that could be implemented to resolve the issue. Not all observations have a corresponding recommendation.

The findings, observations, and NESC recommendations are organized into four categories:

- Positive observations
- Process/approach issues
- Technical gaps
- Risk acceptance issues

7.1 Positive Observations

7.1.1 Observation 1

Observation 1: The IHAWG Chairman and ESD CSO's cooperation and willingness to candidly share information and discuss the ESD methodology with the NESC assessment team was outstanding.

As the ESD process was challenged by the NESC assessment team, the IHAWG Chairman and ESD CSO drove to understand the concerns, working to clarify the ESD/IHAWG position and subsequently addressing the concerns in a productive manner. Although agreement was not reached on every point, they continued to willingly support the efforts of the NESC assessment team.

7.1.2 Observation 2

Observation 2: The assessment team commends the IHAWG for their initiative to analyze Space Shuttle Program (SSP) integrated hazards to help identify potential gaps in the current ESD analyses.

The NESC assessment team recognizes the efforts of the IHAWG for their decision to review the SSP technical documentation to compare and identify common integrated hazards that may be

missing in the IHAWG analyses. While this was a laborious effort, it was conducive to the development of an improved technical product.

7.1.3 Observation 3

Observation 3: The process of using Engineering/SMA cause teams to develop CPIH causes and the management focus on engagement by engineering personnel in CPIH activity have resulted in significant participation by engineering personnel in the IHAs.

Engaging engineering early in the process allows a better understanding of the ramifications of design/engineering choices as these choices are being made, and allows the CPIH process to influence design choices as well.

7.1.4 Observation 4

Observation 4: The interactive Cross-Program Hazard Database utilized by the IHAWG is flexible and searchable for trained users.

Initially, the NESC assessment team found the database to be cumbersome and confusing. Once an overview was provided on how to properly utilize the database, the NESC assessment team found the database to be accessible and user friendly.

7.2 Process/Approach Issues

7.2.1 Finding 1

Finding 1: The IHAWG is not using a higher-level integrated systems approach for CPIHs.

Instead, the current approach starts at an intermediate level (program-to-program interface) and applies controls and verifications only at the integrated cause level. Due to the nature of the enterprise being divided amongst three programs and given the current scope and approach of the ESD integrated hazards, there is no one team assigned to the task of mapping all possible causes from all three programs to a top-level event, such as "LOC," or to other intermediate integrated effects. Due to the lack of cause mapping to a top-level effect, it is possible there are missed opportunities to **apply controls to the integrated system effects**.

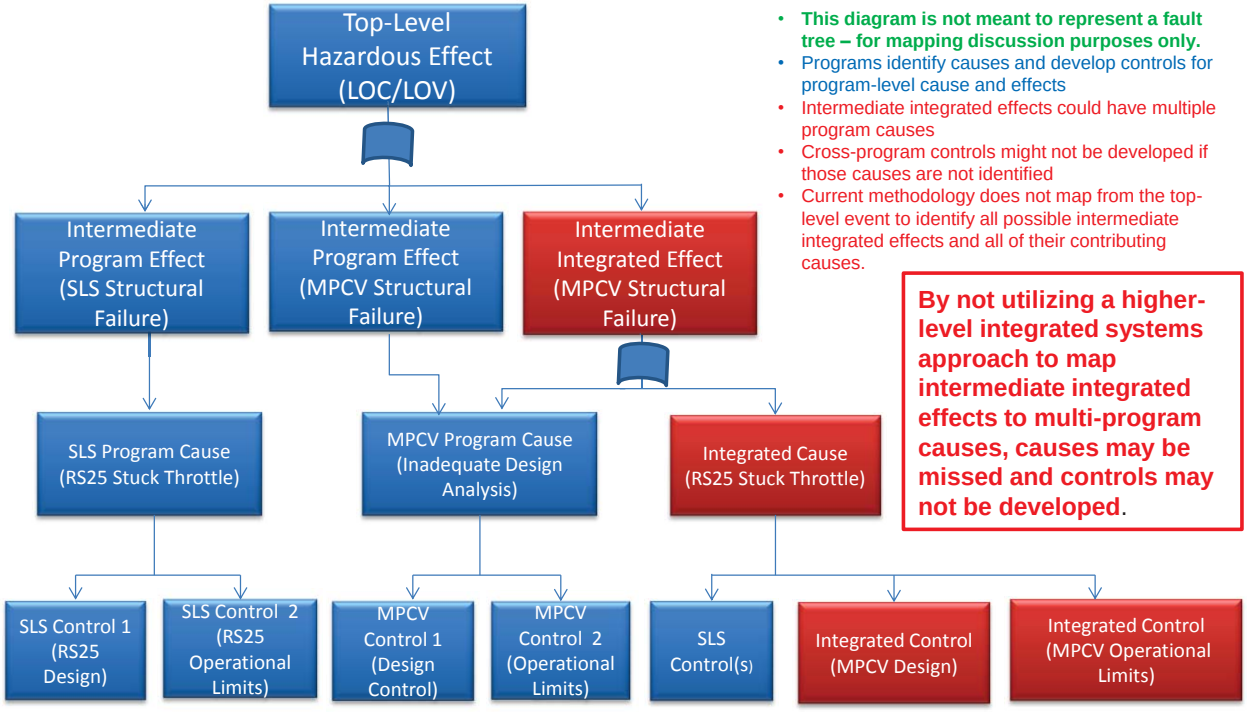
Two undesired results are possible from this approach:

1. Integrated causes could be missed because there is no systematic flow-down from the hazardous effects to their causes.

   Examples: Engine stuck throttle effect on MPCV (see Figure 7.2-1) and ICPS pogo.

2. Controls for the integrated system effects may not be developed.

   Examples: MPCV design control to mitigate engine struck throttle (Figure 7.2-1); systems tests/analyses following a lightning strike on the pad; system-level leak checks; crew procedures; wind placards; crew training; and personal protective equipment.



Note: Blue = current CPIH methodology; Red = potential missed causes.

Figure 7.2-1. RS25 Stuck Throttle Example of Process/Approach Issue

The NESC assessment team discovered that ESD program teams involved with the development of the new enterprise have been encouraged to or are transitioning to a higher-level approach:

- SLS elements and some of the programs already use the higher-level integrated systems effect approach.
- The IHAWG itself has chosen to analyze some (e.g., electromagnetic effects and natural environments) but not all integrated systems effects.
- During his interview with the NESC assessment team, the former ESD DAA stated that his long-range plan included transition to a more traditional IHA approach with a model that looked more like the SSP before the ESD design-to sync-point.
- SLS is now assembling the records into hazard records (HRs) and developing a fault tree for their program-level IHAs:

> *"The HRs (and fault trees) are a means of collecting the Cause Records into a cohesive story that shows the connectivity between the Cause Records. This was needed for two reasons: it helped us look for gaps in the analysis and it should help with the confusion of scope when reviewing the Cause Records. So it provides a "user's guide" to the Cause Records for the reviewers."* [ref. 2]

Recommendation 1: Develop a two-step approach:

1. **Map the existing cross-program hazard effects to all (Cross-Program Integrated, Program-Specific Integrated, and Program Element) potential hazard causes, and then identify any missed causes utilizing a team of subject matter experts. This is the more urgent concern and should be accomplished prior to the ESD design-to sync-point.**
2. **Transition to a higher-level integrated systems effect hazards approach to develop controls for integrated effects. This is a long-term concern and should be accomplished prior to the development of operational controls related to uncrewed flight prior to Exploration Mission (EM)-1 and related to crewed flight prior to EM-2.**

7.2.2 Finding 2

Finding 2: The ESD S&MA Plan (ESD 10010; see Appendix C) provides general guidelines but not uniform direction for hazard analysis for the programs, which has led to differing approaches throughout the programs, elements, and the ESD.

From ESD 10010, paragraph 4.1.1, "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)," but this only provides a description of hazard methodology for the CPIHs. Paragraph 4.1.2 allows program-unique requirements for hazard product format or content.

Previous programs provided a uniform methodology for hazard analysis across the program. For example, NSTS 22254 [ref. 3] required that for the SSP "Fault Tree Analyses (FTAs) or equivalent logic analyses…for evaluating the effects of individual and multiple hardware and software faults…on the system. The top-level fault tree will be based on the top undesired event, 'loss of vehicle/personnel.'"

The lack of uniform direction in ESD 10010 has led to elements performing "top-down" hazard analyses, while programs' IHAs vary in their approach, and the ESD is performing cause-focused IHAs.

This lack of uniformity poses several potential issues. For personnel working on programs that have utilized another hazard methodology, lack of uniformity can create difficulty in navigating between ESD CPIHs and programs' cause records/HRs. While a cause-focused approach may have been beneficial early in the system design cycle to affect design changes as early as possible, this approach was not used for hazard analysis at the program/element level. Rather, the cause-focused approach was used at the enterprise level, where a higher-level systems approach would be more appropriate.

This approach could also lead to missed causes and confusion in communication between the program, the ESD, stakeholders, and independent assessments. Varying approaches can also have the potential to lead to difficulties in assessing the impact of future design changes on the safety/risk baseline.

Recommendation 2: Require consistent hazard analysis methodology across all programs and the ESD.

7.2.3 Finding 3

Finding 3: ESD CPIHs do not include hazard effects across programs as one of the drivers for what comprises an integrated hazard.

The Cross-Program S&MA Plan (ESD 10010, in Appendix C) states, "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." However, this does not account for hazards that affect more than one program **based solely on the effect**.

One example is "Hydraulic lockup on the engine throttle valves." Currently, "Hydraulic lockup on the engine throttle valves" is considered an SLS Program hazard, not a CPIH. The IHAWG determined that the hazard cause does not meet the criteria of the first sentence of the CPIH definition since only SLS contributes to the cause, control, and verification. Therefore, it was ground-ruled out of the integrated hazard process. However, the hazardous effect clearly crosses program boundaries, requires inter-program analysis, and should be considered a CPIH. Although the SLS Program may apply controls to reduce the probability of occurrence of hydraulic lockup of the engine throttle valves, unless it is completely eliminated by design, there will be some probability of occurrence for a stuck throttle. In this case, the MPCV Program must analyze the loads under conditions of a stuck throttle during ascent and, if needed, apply appropriate controls to reduce the possibility of LOC/LOV.

In this example, SLS would inappropriately accept risk for MPCV. Both programs should analyze the effects to their systems, and both should accept the residual risk. By making this hazard a CPIH, the ESD would be assured that both programs analyze and accept the risks.

Another example is risk SLS-020 "Pogo instability during ICPS flight." This risk should be a CPIH due to the system effect between ICPS and MPCV.

Recommendation 3: Expand the CPIH definition to include integrated effect.

Change the definition to "A CPIH is defined as any hazard which meets either of the following criteria: (1) more than one program contributes to a cause, control, or verification for the hazard, or (2) more than one program contributes to the analysis of the system effect, the interactions/ interfaces, and interdependencies of the hazard."

7.2.4 Finding 4

Finding 4: No formal documented process exists for programs to identify to the IHAWG potential CPIHs that they discover in their program HA activities.

Due to the minimal personnel at the ESD level, ESD relies on program personnel to develop ESD hazard cause records. While many of the same individuals that are developing program-level hazards are also developing the ESD causes, there is currently no documented method of

informing the IHAWG of potential CPIHs discovered by the programs. This communication is essential to deriving a complete set of CPIHs. The utilization of program personnel to develop ESD cause records helps to minimize the possibility; however, a formal system should be defined to ensure that this informal communication does not lead to missing CPIH causes.

Recommendation 4: Define and document in the ESD and program S&MA plans a formal method of informing the IHAWG of potential CPIHs discovered by the programs.

7.2.5 Finding 5

Finding 5: No mandatory requirement exists to provide linkage between the CPIHs and failure modes and effects analysis (FMEA)/critical item lists (CILs).

Per ESD 10010 (Appendix C), paragraph 4.1.7, "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." Currently, no mandatory requirements exist to provide linkage between the CPIHs and FMEA/CILs. Linkage between the hazard analysis and the FMEA/CILs provides for a more detailed risk assessment and critical information for hazard controls in the CIL retention rationale. This linkage should be required to be provided when CIL information is applicable to the hazard cause. The NESC assessment team recognizes that there may not always be an applicable CIL for every cause record.

Recommendation 5: Require linkage or direct documentation of CIL retention rationale in applicable CPIHs.

7.2.6 Finding 6

Finding 6: Currently, there is no integrated plan to develop design controls to mitigate the risk of a bird strike during ascent.

The NESC assessment team did not find evidence of an investigation into design controls for a bird strike to the flight hardware. The possibility of a bird strike is currently shown as a 5×5 risk in CPIH 4302 and is carried in the ESD Risk Management System. A study has been initiated to investigate **operational** controls, but ESD is missing the opportunity to develop design controls. For this hazardous event, design controls could decrease the consequences of the hazard, while operational controls could decrease the probability of the hazard. The perception that design controls to the bird strike hazard are not practical to achieve originated during the Constellation Program (CxP). Since the elimination of Ares I, a lower SLS/Orion thrust-to-weight ratio and, therefore, its speed during early phase of ascent in comparison with Ares I/Orion warrants reexamining design controls for the bird strike hazard.

Recommendation 6: Develop integrated design controls as early in the design process as possible to reduce the 5×5 risk due to bird strike to an acceptable level.

7.2.7 Finding 7

Finding 7: The "Crew Survival Notes" section of many current cause reports is not "value added" information and, in some cases, is incorrect.

Many of the cause records utilize a boilerplate statement for this section without consideration of the particular hazard being addressed. For example, the cause record **"**Booster recontact with vehicle during separation due to improper booster trajectory" (CP Hazard 4342) utilizes the following crew survival methods statement:

> *"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). 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."*

Portions of this statement are not applicable to the hazard or mission phase addressed in Cause Record 4342.

The MPCV/SLS Abort Integration Team (MSAIT) ITT, which is the CPIT working group responsible for integrated aborts, is performing exceptional work to analyze crew egress and abort capabilities during all mission phases. These MSAIT products include integrated abort products, such as the SLS and abort conditions reports, emergency egress methodology, and the Cross-Program Integrated Abort Operations strategy. In addition to the MSAIT, the Crew Survivability Assessment ITT also generates products that interact with the integrated hazards. Currently, there is no formal link that cross-references products of other cross-program ITTs and the ESD cause reports. This information, while not a hazard control, could be utilized as acceptance rationale to ensure a complete risk story is conveyed in the cause records. In many cases, egress/abort capability will be used as acceptance rationale for hazards. It is imperative that these products are linked so that there is traceability if any conditions or capabilities change over the life of the program.

Recommendation 7: Rename the "Crew Survival Notes" section to "Crew Survival Hazard Mitigation" and include the applicable MSAIT integrated abort products and the Crew Survivability Assessment ITT products in the cause reports to provide an overall picture of the risk associated with hazards.

7.2.8 Observation 5

Observation 5: The current CPIH model (cause trees and cause records) will be difficult to maintain and sustain in the current form.

The cause trees are not logically linked together and, therefore, have no easily recognizable relationship to one another. Related causes are spread across multiple trees (e.g., fire/explosion,

software, and timing). Future owners and reviewers of the CPIH will need specific understanding of the unique methodology employed in order to maintain the model.

7.2.9 Observation 6

Observation 6: Communication between ITTs was very informal, counting heavily on common members.

The current architecture of the enterprise with three separate programs is utilizing a different approach for cross-program integration. This approach utilizes ITTs to address specific subjects for the cross-program integration for items that cross the boundaries of two or more of the programs. Various ITTs in the ESD contribute to the total risk management of the integrated flight vehicle. While this approach minimizes the bureaucracy involved with a top-heavy integration approach and aids in efficient resolution of issues, it also is highly dependent on diligent communication between the various ITTs. This communication is crucial for mission success and safety. Currently, the ITTs appear to rely heavily upon individuals that share common membership duties with multiple ITTs and on the communication skills of those individuals.

7.2.10 Observation 7

Observation 7: There is minimal NASA Agency-level policy or guidance currently addressing the conduct of hazard analysis, especially related to how they were implemented for past and present major programs, such as the SSP's NSTS 22254.

While evaluating the merits of the CPIH model and methodology utilized by the ESD, the NESC assessment team sought to compare it with NASA policy and guidance concerning the conduct of hazard analysis in order to determine whether there were any analytical gaps. The NESC assessment team found that there is only minimal NASA Agency-level policy or guidance currently addressing the conduct of hazard analysis. There is also minimal training available, and no tools are identified or offered to support the conduct of hazard analysis. This observation, while not specific to the ESD IHA methodology, identifies a lack of consistency across the Agency to ensure that programs are developing hazard analysis to a minimum level or standard that is needed to ensure mission success and safety.

Of concern is the NASA System Safety Handbook, Volume I (NASA/SP-2010-580), which states:

> *"…the handbook does not take a hazard-analysis-centric approach to system safety. Hazard analysis remains a useful tool to facilitate brainstorming but does not substitute for a more holistic approach geared to a comprehensive identification and understanding of individual risk issues and their contributions to aggregate safety risks."* [ref. 4]

Instead, the NASA System Safety Handbook focuses on scenarios and probabilistic methods and relegates hazard analysis to a mere supportive role of the safety analysis function. Two paragraphs referencing "Scenario-based Modeling for Hazard Analysis" are found in

NPD 8715.3C (General Safety Program Requirements) [ref. 5] in Section 2.3.6. The Fault Tree Handbook [ref. 6] dedicates a few pages to survey various hazard analysis and failure mode analysis techniques as they relate to FTA. The Probabilistic Risk Assessment (PRA) Procedures Guide [ref. 7] has one sentence in it concerning hazard analysis and implies that it is a primitive method. These limited views, as reflected in our safety policies, of the role of hazard analysis are inconsistent with how major NASA programs, including the ESD, have leveraged hazard analysis as a primary tool for the identification and control of technical risks.

NASA's past experience with proven hazard analysis methodology is drawn upon heavily from major programs such as the SSP, which relied extensively on its hazard analysis methodology to identify and control its risks. Most major programs have created their own hazard analysis guidance, such as the SSP's NSTS 22254 [ref. 3] and the CxP's 70038 [ref. 8] documents, likely due to the fact that no additional Agency policy or guidance exists.

Interestingly, current S&MA policy is completely devoid of any reference to a risk rank matrix (Probability × Severity), as found in most HRs. Further, the risk rank matrix is frequently used as a risk communications tool across NASA. The only reference to a risk rank matrix of any type is found in NASA-STD-7009, "Standard for Models and Simulations" [ref. 9].

There are only several instances of formal hazard analysis training found in the S&MA Technical Excellence Program courses, but these are very high level, amounting to a few hours of actual instruction. For example, the System Safety Fundamentals course (SMA-SS-WBT-0002) has approximately 4 hours of instruction in hazard analysis methodology, but the material is only offered at an introductory level (i.e., it does not address the system of hazard analysis management and control nor does it address the integration of hazard analyses). In addition, there are only two paragraphs that briefly describe hazard analysis in the NASA System Engineering Handbook (NASA/SP-2007-6105) [ref. 10].

In contrast, there are full, multiday courses taught on nearly every other major system safety topic, for example:

- Fault Tree Analysis offers 24 hours of training.
- PRA offers 48 hours of training (this also includes a course in the PRA tool SAPHIRE).
- Accident Precursor Analysis offers 24 hours of training.
- Bayesian Analysis offers 24 hours of training.

Recommendation 19: The Office of Safety and Mission Assurance (OSMA) should develop a rigorous hazard analysis policy and develop an associated hazard analysis handbook or procedural guide.

7.3 Technical Gaps

7.3.1 Finding 8

Finding 8: Although there are some software-related hazard causes in current CPIHs and in the programs' hazard analyses, there is no CPIH that comprehensively addresses the interactions between the programs' software for all mission phases.

This will make it difficult to identify integrated controls and could result in missed controls.

Two aspects of the inter-program software interactions should be considered in the CPIH analysis.

First, software errors originating from within a program can be causes of inter-program hazards. These causes have been considered to some extent in the current CPIH analysis. An example of such a cause resulting in inter-program hazardous conditions is a loss of control during ascent due to a software error. This is assessed in ESD-045, "Ascent Trajectory Anomaly." Causes of these inter-program hazards are contained within the programs, and the controls of these causes are developed by the programs. However, an overall assessment of software causes has not yet been performed in the CPIH.

The second aspect of software-related hazards is the causes that are attributable to the inter-program software interactions. A comprehensive treatment of the programs' software interaction problems resulting in inter-program hazardous conditions is not included in current CPIH analyses.

For example, during prelaunch propellant loading, a significant interaction between ground software and the integrated launch vehicle hardware and the programs' software occurs. Errors in implementation of inter-program interaction between the software applications, or inadequate verification of these interactions, can result in inter-program causes, leading to inter-program hazardous events.

Errors in these software interactions and their causes are not comprehensively treated in current CPIH analysis and, therefore, represent a gap. Improper treatments of the inter-program interaction requirements, documentation, implementation, and verification are the inter-program causes and should be treated in the CPIH analyses. The ESD would benefit greatly from expanding the current CPIH software analysis to include a comprehensive systems safety review of both software causes and causes due to interactions between the programs' software applications.

Recommendation 8: Expand the CPIH to include a comprehensive assessment of the hazards associated with the interaction of the programs' software hazards for all mission phases and develop appropriate integrated controls.

7.3.2 Finding 9

Finding 9: Cross-program hazard analysis does not take effect until cryogenic (cryo) loading at the launch pad.

ESD 10010 (Appendix C), paragraph 4.1.2, arbitrarily defines the bounds of the cross-program integrated hazard analysis (CPIHA) timeframe. "The CPIHA timeframe is bounded by Pre-launch Cryo-loading at the pad to post-flight crew egress." Integrated hazardous conditions could exist prior to this point in the process, and using this time frame omits a myriad of inter-program hazards.

Two examples of commonly recognized inter-program hazards are the rollout loads on the integrated vehicle and a lightning strike to the integrated system during the rollout.

During rollout operation, the integrated structure is subjected to a periodic forcing function, caused by the "slapping" of the track shoes on the ground. Frequency of this dynamic excitation is defined by the speed of the crawler during rollout. Dynamic response to this forcing function and the associated structural loads are based on the structural dynamics properties of the combined launch vehicle and the mobile launcher platform/crawler system.

Space Shuttle experience showed that either overload due to dynamic response or hardware fatigue failure can occur in the integrated stack during the rollout. This inter-program hazard mainly applies to the flight vehicle, although not exclusively. Control of this hazard requires dynamic analysis of the GSDO/SLS/MPCV system to determine safe crawler speed constraints. Final implementation of this hazard control would be implemented by GSDO.

Another cross-program hazard involves lightning strike to the integrated system during the rollout operation. GSDO will implement operational controls, minimizing the potential for a strike. However, if these operational controls fail and a lightning strike occurs during the rollout, an inter-program activity will follow to define and execute post-strike testing of the integrated system and each program's hardware to verify readiness to proceed with prelaunch and launch operations.

Due to the existence of significant inter-program hazards prior to cryo-loading, the NESC assessment team recommends extending the timeframe to include the inter-program hazards that exist prior to cryo-loading.

Recommendation 9: Expand the timeframe for the CPIH to include any operations that could have a hazardous effect on cross-program elements.

7.3.3 Finding 10

Finding 10: The IHAWG "Guidance for Analysis Causes" does not prompt the analysts to consider errors in integrated dynamic models due to lack of test verification as part of their "inadequate analysis" cause assessment.

This could result in inadequate development of hazard controls.

The IHAWG "Guidance for Analysis Causes" [ref. 11] provides many useful instructions on the approach to identify analysis causes and associated controls of the cross-program integrated hazards. The current "guidance" fails to prompt the analysts to consider hazard causes due to errors in the integrated dynamic models due to lack of test verification as part of their "inadequate analysis" cause assessment. This is significant because structural dynamic models are a key ingredient to many integrated analyses, including the following:

1. Loads on the ground and in flight.
2. Vehicle displacement relative to the ground systems before and during liftoff.
3. Flight control system in-flight stability analysis.
4. Core stage and ICPS pogo stability analysis.
5. Dynamic response and loads analysis due to buffet excitation.

Only scant dynamic model verification is planned by the ESD. "Piggyback" acquisition of dynamic properties during core stage hot fire test is currently planned. Additionally, limited verification of dynamic properties for the integrated launch vehicle on the ground will be available from the limited modal testing planned to occur in the Vehicle Assembly Building prior to flight.

Both tests occur late in the development cycle and provide limited controls of the hazards resulting from errors in the dynamic models. Therefore, the inter-program hazard controls should be implemented analytically early in development. Sensitivity analyses for each technical discipline could be performed to determine the effect of potential errors in mode shapes and modal frequencies on design margins. Based on this analysis, additional design margin may be required of each technical discipline to compensate for dynamic model error to a desired level of protection. These margins can be released as the maturity of dynamic models increases.

Implementing these analytically based controls will protect the ESD from the necessity to redesign in any of the five identified technical disciplines, when increased maturity of the dynamic models exposes errors in the models that were used in early design.

Based on the above, the "Guidance for Analysis Causes" should be revised to include specific guidance to analysts to identify hazard causes attributable to **insufficient verification by test** of structural dynamic models for the integrated SLS/MPCV/GSDO system. Furthermore, considering the current advanced development stage of the ESD, pursuing controls of these hazards via a currently unplanned ground vibration test program is impractical; therefore, analytically based controls for these inter-program hazards should be developed.

Recommendation 10: Revise IHAWG "Guidance for Analysis Causes" and expand existing and future CPIH analyses to include causes attributable to errors in unverified (by test) integrated dynamic models and develop appropriate controls.

7.3.4 Finding 11

Finding 11: Integrated vehicle and ground system structural failures, internal to the SLS/MPCV/GSDO hardware, caused by errors in the structural mathematical models of the integrated system or errors in the definition of environments are excluded from the CPIH.

Currently, only two inter-program structural failure hazards are identified. These hazards are Exploration Systems Integration (ESI)-060, "Addressing Structural Failure of the Vehicle Support Posts," and ESI-038, "Addressing Structural Failure of the MPCV Stage Adaptor." Structural failure due to cross-program causes can occur anywhere in the integrated system, not just at the two physical interfaces currently treated by the CPIH analysis.

Hazards of structural failure internal to SLS/MPCV/GSDO hardware prior to and during liftoff, and failures internal to SLS/MPCV hardware during ascent, must be identified and controls must be established.

Primary inter-program causes of the structural failures on the ground or in flight can be due to errors in the integrated structural models or errors in the definition of the integrated environments. Shuttle experience during Space Transportation System (STS)-1 provides a vivid example of these integrated hazards. An error in definition of the solid rocket booster ignition overpressure environment, to which the Space Shuttle was subjected during liftoff, resulted in a buckling failure of a nitrogen tetroxide tank support strut located in the forward fuselage of the orbiter, which was far away from any integrated vehicle interfaces.

Approximately 1 minute later, during flight through the maximum dynamic pressure, the incorrectly predicted integrated vehicle pressure distributions resulted in very significant negative structural margins on the orbiter's wings. Although no structural failure occurred, a 6-month stand-down was required to allow development of corrective actions prior to STS-2. This event, again, created a hazardous event far away from any integrated vehicle physical interface.

Both hazardous events in STS-1 clearly indicated that hazards of structural failure anywhere in the integrated system, either on the ground or in flight, should be treated by CPIH analysis and appropriate controls should be developed.

Recommendation 11: Expand the CPIH to include any structural failures due to cross-program causes.

7.3.5 Finding 12

Finding 12: CPIHs are not being generated for failure to abort and/or safely egress the crew.

The IHAWG has determined that the cause tree associated with "Failure to abort when needed" (ESI-062) is out of scope. Assessments of integrated abort scenarios and associated hardware/software are transferred to the MSAIT and the ESI Crew Survivability Assessment ITT due to the philosophy that the nominal mission phase hazard controls have failed and are,

therefore, outside the IHAWG's scope. The programs develop hazard analyses associated with their internal systems, but no CPIHs are developed by the ESD.

Examples of cross-program interfaces with no corresponding CPIH:

- Inability to abort when needed due to MPCV/GSDO/SLS/Mission Control Center (MCC) interface.
- Inability for crew to safely egress from Orion during launch abort due to MPCV/GSDO interface.

The NESC assessment team has repeatedly questioned the IHAWG position that once design controls over inter-program hazard causes fail, subsequent hazards and their controls are out of scope of the CPIH. The NESC assessment team strongly recommends that CPIH analysis consider hazards subsequent to initial failure of design controls and develop controls for those conditions, particularly operational controls and integrated controls.

As an outcome of this narrow definition of the CPIH domain, the IHAWG has determined that the cause tree associated with "Failure to abort when needed" (ESI-062) is out of scope of the CPIH analysis.

The NESC assessment team fully appreciates the roles of MSAIT and the ESI Crew Survivability Assessment ITT. These teams perform an important function in designing and implementing crew survival following an abort. Their role is not, however, a substitution for an independent safety identification of the inter-program hazards associated with a failure to abort when needed, due to cross-program interface problems, and developing appropriate integrated controls.

The NESC assessment team considers the absence of a CPIH for inability to abort when needed, due to MPCV/GSDO/SLS/MCC interface problems, to be a gap in the CPIH analysis. Similarly, the inability for the crew to safely egress Orion following launch abort due to an MPCV/GSDO interface problem should also be treated in the CPIH analysis. Currently, it is not a CPIH and, therefore, constitutes a CPIH analysis gap.

Recommendation 12: Expand the scope of the IHAWG to include CPIHs of failure to abort or safely egress when needed due to cross-program interfaces.

7.3.6 Finding 13

Finding 13: Other than the specific ones addressed in the previous findings, there may be additional technical gaps in the CPIH that need to be analyzed and addressed.

Five specific technical gaps have been identified (see sections 7.3.1 through 7.3.5). These gaps were a result of the NESC assessment team's analysis of current ESD documentation, the programs' safety-related documentation, and materials provided by the IHAWG.

Two additional gaps were called out as examples for Findings 1and 3 (see Sections 7.2.1 and 7.2.3) to indicate shortfalls in the IHAWG approach to define the bounds of the CPIH analysis.

These shortfalls resulted in the exclusion of the stuck throttle during ascent and ICPS pogo from the CPIH analysis.

The NESC assessment team identified additional potential gaps and recommends that the IHAWG perform further analysis.

The first potential gap is the absence of CPIH for micrometeoroid and orbital debris (MMOD) impact to the Orion/ICPS system. In the final stage of Orion/ICPS flight, the combined system can be exposed to the MMOD environment and, therefore, should be subject to CPIH analysis.

The second potential gap is the absence of CPIH for timing synchronization between all ground and flight systems during flight. SLS, MPCV, and GSDO participate in multiple integrated activities that require all programs to be chronologically synchronized to support distinct integrated events. Liftoff, staging, main engine cutoff, and trans-lunar injection are examples of these events. Each program needs to maintain the same "time" so that interdependent activities are conducted at the correct times and in the correct sequence. There is no single master timing unit or similar device for the entire enterprise to utilize to maintain event timing synchronization. It is, therefore, necessary for hazards related to a lack of event timing synchronization between programs to be analyzed to determine the effectiveness of the controls for maintaining synchronization. The CPIH does address this issue in some cause trees (e.g., ESI-035 and ESI-045 both address timing and sequencing of events); however, a thorough assessment of all potential timing and synchronization hazards for all integrated events across the programs would be of great value to the enterprise.

In examining hazards associated with transition from a nominal mission to an aborted mission, the NESC assessment team observed the absence of an abort trigger for solid rocket booster failure to separate. All other SLS failures requiring mission termination followed by MPCV crew escape had an associated abort trigger. These abort triggers are sent to MPCV to initiate crew escape. The absence of a solid rocket booster failure to separate trigger is likely to be an MSAIT or CPIH gap.

To address the above and potentially other additional gaps, the NESC assessment team recommends that the IHAWG develop flowcharts of the ESD and each program's hazard analysis processes. Comparison of ESD CPIH development process flowchart with flowcharts representing hazard analysis process of the programs may reveal additional weaknesses in the CPIH process and lead to identification of additional gaps. The NESC assessment team also encourages the IHAWG to complete the ongoing comparison of the ESD and SSP hazard analyses in order to identify potential gaps in the ESD CPIH. This effort should be expanded to compare the ESD CPIH hazard analysis with other HSF and large military programs. The NESC assessment team found references to Apollo-era risk assessments but was not able to locate individual safety analyses or hazard reports.

Recommendation 13a: Roadmap or flow chart the entire ESD and the programs' hazard analysis processes.

Recommendation 13b: Compare the CPIH process to other HSF programs (e.g., SSP, CxP, Apollo, large military launch systems, etc.).

7.4 Risk Acceptance Issues

7.4.1 Finding 14

Finding 14: Program-centric design solutions are possible with current CPIH methodology.

Due to resource limitations at the enterprise level (ESD), all cause trees (composed of a hazardous condition in the top box followed by all causes that can lead to that hazardous condition) are assigned to a program S&MA engineer, who facilitates the development of the tree in collaboration with engineering and S&MA personnel from impacted or contributing programs. ESD-owned integrated hazard causes are harvested from cause trees and assigned to a program for development, as opposed to having a program-independent Systems Engineering and Integration (SE&I) type function perform the development. Not only can this lead to a non-optimal solution at the enterprise level for integrated cause and effect elimination/mitigation, but this approach can also promote competition for program resources between the programs and the ESD since the same people are doing both. Though not the ideal solution of an enterprise level program-independent SE&I type function, assigning a representative from the ESD CSO organization and the Chief Engineer organization, independently funded from the program, is achievable and a step in the right direction to provide greater independence in risk decisions.

Recommendation 14: Assign full-time ESD CSO and Chief Engineer representatives funded independently from the programs as core IHAWG members, and change the Crew Office representative from an ad-hoc member to a core member.

7.4.2 Finding 15

Finding 15: CPIHs are not required to be independently reviewed like the Program/ Element Hazard Analyses.

The IHAWG is not only responsible for generating CPIHs but also reviews and approves the CPIHs. ESD 10010 (Appendix C) requires per Section 4.1.9, "Hazard Analysis Review," that "The safety review activity will include an evaluation by safety and subject matter experts that were not responsible for developing the hazard products" for program and element hazards. This approach follows the policy of "Don't grade your own homework." However, ESD 10010 does not specify that an independent review process will be performed by an entity that is not responsible for developing the hazard product for the CPIHs. In addition, according to the IHAWG Task Agreement dated August 2012, "The primary objective of the IHAWG is to develop and manage an affordable cross-program IHA effort that improves the safety of the vehicle by early identification of potential design solutions" [ref. 12].

Recommendation 15: Require the same independent review activity of the CPIHs so that it is consistent with the requirements and membership for Program/Element Hazard Analysis independent review, as outlined in Section 4.1.9 of ESD 10010.

7.4.3 Finding 16

Finding 16: All catastrophic hazards are not approved by the ESD Control Board (ESDCB) that is chaired by the ESD DAA.

Only moderate- and high-probability catastrophic hazards are elevated to the ESDCB for approval (see Figure 7.4.3-1).

Likelihood	Minor	Moderate	Severe	Critical	Catastrophic
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
			Consequence		

Figure 7.4.3-1. Hazard Risk Acceptance Strategy from Cross-Program S&MA Plan (reprinted from ESD 10010)

There were several cases of accidents and close calls in other NASA HSF programs in which the probability of occurrence for a catastrophic hazard was underestimated. LOC/LOV due to Space Shuttle debris impact, extravehicular activity drowning, and ISS ammonia leak due to interface heat exchanger damage are all examples of catastrophic hazards in which the probability of occurrence was either significantly underestimated or determined to be not credible (see below for more detail on these examples). Elevating all catastrophic risks to the ESD Program Manager provides additional scrutiny for hazards that can result in the LOC and/or loss of essential flight/ground assets. During the operational phase, in-flight anomalies or problem reports related to hazards with catastrophic consequences should also be reviewed by the ESDCB to determine if hazard controls have been compromised or have greater uncertainties than originally estimated.

Prior to STS-107, the risk of LOC/LOV due to debris strikes was characterized as "remote-catastrophic." The SSP used a 3×4 hazard matrix, while ESD uses a 5×5 matrix. The ESD definitions for consequence and probability are shown in Figures 7.4.3-2 and 7.4.3-3. The SSP "Remote" probability was defined in NSTS 22254 [ref. 3] as "Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties." ESD "Low" definition states, "Not expected to happen. Controls have minor limitations or uncertainties ($\sim 1/100{,}000 < P \leq 1/10{,}000$)." If mapped to the ESD's risk matrix, the debris hazard would be characterized as "Low-Catastrophic." Given that, a hazard such as LOC/LOV due to debris impact would not be required to be accepted by the ESD Program Manager under the current ESD S&MA Plan.

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 7.4.3-2. Hazard Consequence Definitions (reprinted from ESD 10010)

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 7.4.3-3. Hazard Likelihood Definitions (reprinted from ESD 10010)

Post STS-107, the "Space Shuttle Integrated Debris Hazard Report," IDBR-01 [ref. 13], listed all of the expected debris sources categorized into one of 42 distinct debris causes. IDBR-01

documented the risk for each of these causes, including the likelihood of catastrophic impact to the Space Shuttle vehicle, the justification for that likelihood, and the program's acceptance rationale for accepting that risk. This hazard report was frequently updated. Between return to flight in July 2005 and March 2011, just three months prior to the final Space Shuttle mission, the hazard report was updated 15 times. Many of the revisions involved updates to the likelihood justification and acceptance rationale based on continuous review of the controls and verifications for debris causes.

Each time the hazard report was revised, there was substantial discussion and debate at the SSP Control Board (SSPCB) regarding test and analysis results of potential transport mechanisms and impact capability of the vehicle, as well as demonstrated strength of controls to limit debris liberation. PRAs, which were used in many cases to justify the likelihood estimates, were reviewed in detail at the SSPCB. This intense scrutiny of integrated debris hazard causes and review by the highest levels of program management were essential to ensure that the risk of LOC/LOV due to debris impact was properly characterized during the final years of the SSP.

Recommendation 16: Require all catastrophic hazards, for both ESD and the programs, to be approved by the ESDCB.

7.4.4 Finding 17

Finding 17: The only signature blocks on the current CPIH cause records are those of the IHAWG and the author.

Each cause record should be endorsed by the parties/organizations responsible for the technical accuracy of the content. This establishes accountability for the technical content and traceability. For the SSP, the first signature on the integrated hazard report was that of the responsible engineer.

Recommendation 17: Establish appropriate signatories for CPIH cause records.

7.4.5 Finding 18

Finding 18: The ESD S&MA Plan allows the (undefined) developer to accept minor, moderate, and severe consequence risks. (See Figure 7.4.5-1.)

Severe consequence can be injury/illness requiring medical treatment or damage to significant flight/ground assets. NPR 7120.5E, "NASA Space Flight Program and Project Management Requirements," Section 3.3.2.2, states:

> "*On decisions related to technical and operational matters involving safety and mission success residual risk, formal concurrence by the responsible technical authorities (TAs) (Engineering, Safety and Mission Assurance, and/or Health and Medical) is required. This concurrence is to be based on the technical merits of the case. For residual risks to personnel or high-value hardware, the cognizant safety organization needs to agree that the risk is acceptable. For matters involving human safety risk, the actual risk taker(s) (or official spokesperson(s) and their supervisory chain) need to formally consent to taking*

the risk and the responsible program, project, or operations manager needs to formally accept the risk." [ref. 14]

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 7.4.5-1. Hazard Risk Acceptance Strategy from Cross-Program Safety and Mission Assurance Plan (reprinted from ESD 10010)

Recommendation 18: Revise the approval level for higher likelihood, severe-consequence hazards to a management level independent of the developer. As a minimum, the high and very high likelihood, severe-consequence hazards should be approved by the Joint Program Control Board (JPCB)/Program Control Board (PCB).

8.0 Summary of Findings, Observations, and NESC Recommendations

8.1 Findings

The following findings were identified:

Process/Approach Issues

F-1. The IHAWG is not using a higher-level integrated systems approach for CPIHs.

F-2. The ESD S&MA Plan (ESD 10010; see Appendix C) provides general guidelines but not uniform direction for hazard analysis for the programs, which has led to differing approaches throughout the programs, elements, and the ESD.

F-3. ESD CPIHs do not include hazard effects across programs as one of the drivers for what comprises an integrated hazard.

F-4. No formal documented process exists for programs to identify to the IHAWG potential CPIHs that they discover in their program hazard analysis activities.

F-5. No mandatory requirement exists to provide linkage between the CPIHs and FMEA/CILs.

F-6. Currently, there is no integrated plan to develop design controls to mitigate the risk of a bird strike during ascent.

F-7. The "Crew Survival Notes" section of many current cause reports is not "value added" information and, in some cases, is incorrect.

Technical Gaps

F-8. Although there are some software-related hazard causes in current CPIHs and in the programs' hazard analyses, there is no CPIH that comprehensively addresses the interactions between the programs' software for all mission phases.

F-9. Cross-program hazard analysis does not take effect until cryo-loading at the launch pad.

F-10. The IHAWG "Guidance for Analysis Causes" does not prompt the analysts to consider errors in integrated dynamic models due to lack of test verification as part of their "inadequate analysis" cause assessment.

F-11. Integrated vehicle and ground system structural failures, internal to the SLS/MPCV/GSDO hardware, caused by errors in the structural mathematical models of the integrated system or errors in the definition of environments are excluded from the CPIH.

F-12. CPIHs are not being generated for failure to abort and/or safely egress the crew.

F-13. Other than the specific ones addressed in the previous findings, there may be additional technical gaps in the CPIH that need to be analyzed and addressed.

Risk Acceptance Issues

F-14. Program-centric design solutions are possible with current CPIH methodology.

F-15. CPIHs are not required to be independently reviewed like the Program/Element Hazard Analyses.

F-16. All catastrophic hazards are not approved by the ESDCB that is chaired by the ESD DAA.

F-17. The only signature blocks on the current CPIH cause records are those of the IHAWG and the author.

F-18. The ESD S&MA Plan allows the (undefined) developer to accept minor, moderate, and severe consequence risks.

8.2 Observations

O-1. The IHAWG Chairman and ESD CSO's cooperation and willingness to candidly share information and discuss the ESD methodology with the NESC assessment team was outstanding.

O-2. The assessment team commends the IHAWG for their initiative to analyze SSP integrated hazards to help identify potential gaps in the current ESD analyses.

O-3. The process of using Engineering/SMA cause teams to develop CPIH causes and the management focus on engagement by engineering personnel in CPIH activity have resulted in significant participation by engineering personnel in the IHAs.

O-4. Observation 4: The interactive Cross-Program Hazard Database utilized by the IHAWG is flexible and searchable for trained users.

O-5. The current CPIH model (cause trees and cause records) will be difficult to maintain and sustain in the current form.

O-6. Communication between ITTs was very informal, counting heavily on common members.

O-7. There is minimal NASA Agency-level policy or guidance currently addressing the conduct of hazard analysis, especially related to how they were implemented for past and present major programs, such as the SSP's NSTS 22254.

8.3 NESC Recommendations

The following NESC recommendations are directed to ESD Management unless otherwise noted.

Process/Approach Issues

R-1. Develop a two-step approach to resolve the issue of not using a higher-level integrated systems approach for CPIHs. ***(F-1)***

R-2. Require consistent hazard analysis methodology across all programs and the ESD. ***(F-2)***

R-3. Expand the CPIH definition to include integrated effect. ***(F-3)***

R-4. Define and document in the ESD and program S&MA plans a formal method of informing the IHAWG of potential CPIHs discovered by the programs. ***(F-4)***

R-5. Require linkage or direct documentation of CIL retention rationale in applicable CPIHs. ***(F-5)***

R-6. Develop integrated design controls as early in the design process as possible to reduce the 5×5 risk due to bird strike to an acceptable level. ***(F-6)***

R-7. Rename the "Crew Survival Notes" section to "Crew Survival Hazard Mitigation" and include the applicable MSAIT integrated abort products and the Crew Survivability Assessment ITT products in the cause reports to provide an overall picture of the risk associated with hazards. ***(F-7)***

Technical Gaps

R-8. Expand the CPIH to include a comprehensive assessment of the hazards associated with the interaction of the programs' software hazards for all mission phases and develop appropriate integrated controls. ***(F-8)***

R-9. Expand the timeframe for the CPIH to include any operations that could have a hazardous effect on cross-program elements. ***(F-9)***

R-10. Revise IHAWG "Guidance for Analysis Causes" and expand existing and future CPIH analyses to include causes attributable to errors in unverified (by test) integrated dynamic models and develop appropriate controls. ***(F-10)***

R-11. Expand the CPIH to include any structural failures due to cross-program causes. ***(F-11)***

R-12. Expand the scope of the IHAWG to include CPIHs of failure to abort or safely egress when needed due to cross-program interfaces. ***(F-12)***

R-13. (a) Roadmap or flow chart the entire ESD and the programs' hazard analysis processes. ***(F-13)***

(b) Compare the CPIH process to other HSF programs (e.g., SSP, CxP, Apollo, large military launch systems, etc.). ***(F-13)***

Risk Acceptance Issues

R-14. Assign full-time ESD CSO and Chief Engineer representatives funded independently from the programs as core IHAWG members, and change the Crew Office representative from an ad-hoc member to a core member. ***(F-14)***

R-15. Require the same independent review activity of the CPIHs so that it is consistent with the requirements and membership for Program/Element Hazard Analysis independent review, as outlined in Section 4.1.9 of ESD 10010. ***(F-15)***

R-16. Require all catastrophic hazards, for both the ESD and the programs, to be approved by the ESDCB. ***(F-16)***

R-17. Establish appropriate signatories for CPIH cause records. ***(F-17)***

R-18. Revise the approval level for higher likelihood, severe-consequence hazards to a management level independent of the developer. As a minimum, the high and very high likelihood, severe-consequence hazards should be approved by the JPCB/PCB. ***(F-18)***

R-19. The OSMA should develop a rigorous hazard analysis policy and develop an associated hazard analysis handbook or procedural guide. ***(O-7)***

9.0 Alternate Viewpoint

There were no alternate viewpoints identified during the course of this assessment by the NESC team or the NRB quorum.

10.0 Other Deliverables

No unique hardware, software, or data packages, outside those contained in this report, were disseminated to other parties outside this assessment.

11.0 Lessons Learned

No applicable lessons learned were identified for entry into the NASA Lessons Learned Information System (LLIS) as a result of this assessment.

12.0 Recommendations for NASA Standards and Specifications

Per recommendation 19, the following NASA standards and specifications should be developed/ updated by the OSMA:

- Develop a more rigorous hazard analysis policy.
- Develop a hazard analysis handbook and/or procedure guide.
- Develop formal training in hazard analysis.

13.0 Definition of Terms

Finding	A relevant factual conclusion and/or issue that is within the assessment scope and that the team has rigorously based on data from their independent analyses, tests, inspections, and/or reviews of technical documentation.
Lessons Learned	Knowledge, understanding, or conclusive insight gained by experience that may benefit other current or future NASA programs and projects. The experience may be positive, as in a successful test or mission, or negative, as in a mishap or failure.
Observation	A noteworthy fact, issue, and/or risk, which may not be directly within the assessment scope, but could generate a separate issue or concern if not addressed. Alternatively, an observation can be a positive acknowledgement of a Center/Program/Project/Organization's operational structure, tools, and/or support provided.
Problem	The subject of the independent technical assessment.
Recommendation	A proposed measurable stakeholder action directly supported by specific Finding(s) and/or Observation(s) that will correct or mitigate an identified issue or risk.
Supporting Narrative	A paragraph, or section, in an NESC final report that provides the detailed explanation of a succinctly worded finding or observation. For example, the logical deduction that led to a finding or observation; descriptions of assumptions, exceptions, clarifications, and boundary conditions.

14.0 Acronym List

PDR	Preliminary Design Review
AMA	Analytical Mechanics Associates
ASAP	Aerospace Safety Advisory Panel
CIL	Critical Item List
CPIH	Cross-Program Integrated Hazard
CPIHA	Cross-Program Integrated Hazard Analysis

CPIT	Cross-Program Integration Team
CSO	Chief S&MA Officer
CxP	Constellation Program
DAA	Deputy Associate Administrator
EM	Exploration Mission
ESD	Exploration Systems Development
ESDCB	ESD Control Board
ESI	Exploration Systems Integration
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GRC	Glenn Research Center
GSDO	Ground Systems Development and Operations
GSFC	Goddard Space Flight Center
HR	Hazard Records
HSF	Human Spaceflight
ICPS	Interim Cryogenic Propulsion Stage
IHA	Integrated Hazard Analysis
IHAAT	Integrated Hazard Analysis Architecture Team
IHAWG	Integrated Hazard Analysis Working Group
ISS	International Space Station
ITT	Integrated Task Team
JPCB	Joint Program Control Board
JSC	Johnson Space Center
KSC	Kennedy Space Center
LaRC	Langley Research Center
LOC	Loss of Crew
LOV	Loss of Vehicle
MCC	Mission Control Center
MMOD	Micrometeoroid and Orbital Debris
MPCV	Multi-Purpose Crew Vehicle
MSAIT	MPCV/SLS Abort Integration Team
MSFC	Marshall Space Flight Center
NESC	NASA Engineering and Safety Center
NG	Northrop Grumman
NPR	NASA Procedural Requirement
NSC	NASA Safety Center
OSMA	Office of Safety and Mission Assurance
PCB	Program Control Board
PDR	Preliminary Design Review
Pogo	Prevention of Coupled Structure Propulsion Instability
PRA	Probabilistic Risk Assessment
S&MA	Safety and Mission Assurance

SE&I	Systems Engineering and Integration
SLS	Space Launch System
SRB	Standing Review Board
SSC	Stennis Space Center
SSP	Space Shuttle Program
SSPCB	Space Shuttle Program Control Board
STS	Space Transportation System
TIM	Technical Interchange Meeting

15.0 References

1. Wilson, T.: "Improving Exploration Systems Integration," NESC White Paper, January 29, 2014.
2. Quote from SLS S&MA personnel performing SLS Integrated Hazards to assessment team member via August 12, 2014, email.
3. "Methodology for Conduct of Space Shuttle Program Hazard Analyses," Revision B, NSTS 22254, December 30, 1993.
4. "NASA System Safety Handbook, Volume I: System Safety Framework and Concepts for Implementation," NASA/SP-2010-580, Version 1, November 2011.
5. "NASA General Safety Program Requirements," NPD 8715.3C, March 12, 2008.
6. "Fault Tree Handbook with Aerospace Applications," Version 1.1, NASA Office of Safety and Mission Assurance, August 2002.
7. "Probabilistic Risk Assessment Procedures Guide For NASA Managers and Practitioners," NASA/SP-2011-3421, 2nd Edition, December 2011.
8. "Constellation Program Hazard Analyses Methodology," CxP 70038, Revision B, 2009.
9. "Standard for Models and Simulations," NASA-STD-7009, July 11, 2008.
10. "NASA System Engineering Handbook," NASA/SP-2007-6105, Revision 1, December 2007.
11. "Guidance for Analysis Causes," IHAWG presentation, September 3, 2013.
12. "Task Agreement: Integrated Hazard Analysis Working Group (IHAWG)," NASA, August 2012.
13. "Space Shuttle Integrated Debris Hazard Report," IDBR-01.
14. "NASA Space Flight Program and Project Management Requirements," NPR 7120.5E, August 14, 2012.

16.0 List of Appendices (separate volume)

Appendix A. Interviews Conducted and Documents Reviewed
Appendix B. "Integrated Hazard Analysis Deep Dive" Presentation to ESD Management
Appendix C. "Cross-Program Safety and Mission Assurance Plan" (ESD 10010)
Appendix D. Hazard Analysis Comparison

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

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-20522 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 I

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	49	(443) 757-5802