SUBSYSTEM HAZARD ANALYSIS METHODOLOGY FOR THE ARES I UPPER STAGE SOURCE CONTROLLED ITEMS

Michael S. Mitchell, David R. Winner

The Boeing Company
499 Boeing Boulevard. MC JS-70
Huntsville, AL 35806 USA
michael.s.mitchell2@boeing.com; david.r.winner@boeing.com

ABSTRACT

This article describes processes involved in developing subsystem hazard analyses for Source Controlled Items (SCI), specific components, sub-assemblies, and / or piece parts, of the NASA ARES I Upper Stage (US) project. SCIs will be designed, developed and /or procured by Boeing as an end item or an off-the-shelf item. Objectives include explaining the methodology, tools, stakeholders and products involved in development of these hazard analyses. Progress made and further challenges in identifying potential subsystem hazards are also provided in an effort to assist the System Safety community in understanding one part of the ARES I Upper Stage project.

1.0 INTRODUCTION

This System Safety Hazard Analysis includes subsystem hazard reports (HRs) documenting the safety risks for the Upper Stage Production (USP) Source Control Items (SCI). Boeing System Safety is working with USP Integrated Product Team (IPT)/subsystem engineers and NASA Design Team (NDT) system safety to pro.vide SCI specific controls and verifications applicable to baselined USP Flight System Safety Hazard Analyses (HA).

2.0 SCOPE

This document provides the results of the system safety risk assessment performed to provide controls and verifications for the USP Source Control Items (SCIs):

- Structural and Thermal Pyro Separation Systems
- Main Propulsion System (MPS)
- Reaction Control System (ReCS)
- Roll Control System (RoCS)
- Thrust Vector Control (TVC) System
- Ullage Settling Motors (USM)

The affected hazard analysis will address specific SCI requirements and verifications applicable to their associated US Flight System Safety HA causes and controls. The location of the US within the Ares I vehicle is provided in Figure 2-0. General location of the listed subsystems is available in Figure 2-1.

3.0 SCI HAZARD METHODOLOGY

The identification of safety risks during the Preliminary Design Review (PDR), Interim Design Review (IDR) and Critical Design Review (CDR) design phases is used to eliminate or mitigate hazard risks early in the development phase and to clarify safety requirements. Figure 3.4 outlines the flow for performing the SCI Hazard Analysis (HA). Through data gathering and analysis, SCI specific requirements are reviewed to identify those SCI requirements which match up with baselined Phase I US Flight System Safety Hazard Report (HR) controls and verifications. Applicable requirements and related verifications necessary to control baselined US Flight System Safety hazards are then recorded in an US HR requirements matrices. The matrices are also used to identify “holes” where the analyst believes controls and / or verifications are missing. Each SCI HR verification is then updated for its respective US Flight System Safety HR control. Unique SCI hazard reports for each SCI subsystem are then developed to a level complementary to the level of the design following the requirements in CxP 70038, Hazard Analysis Methodology. The proposed SCI HR verifications will then be documented as part of a Safety Assessment Report (SAR), which will be provided to Ares I NASA Design Team (NDT) Safety and Mission Assurance (S&MA) group, which can be used to assist in updating applicable US Flight System Safety HRs prior to their assigned Critical Design Review (CDR) timeframe.

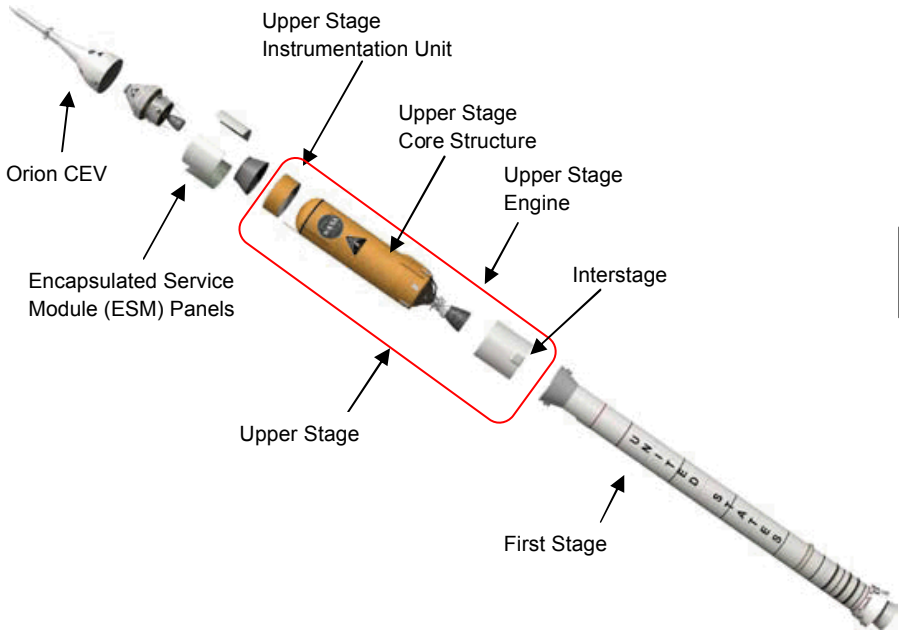


Figure 2.0.1 – Ares I Elements, Updated to Show Affected Upper Stage Area[1]

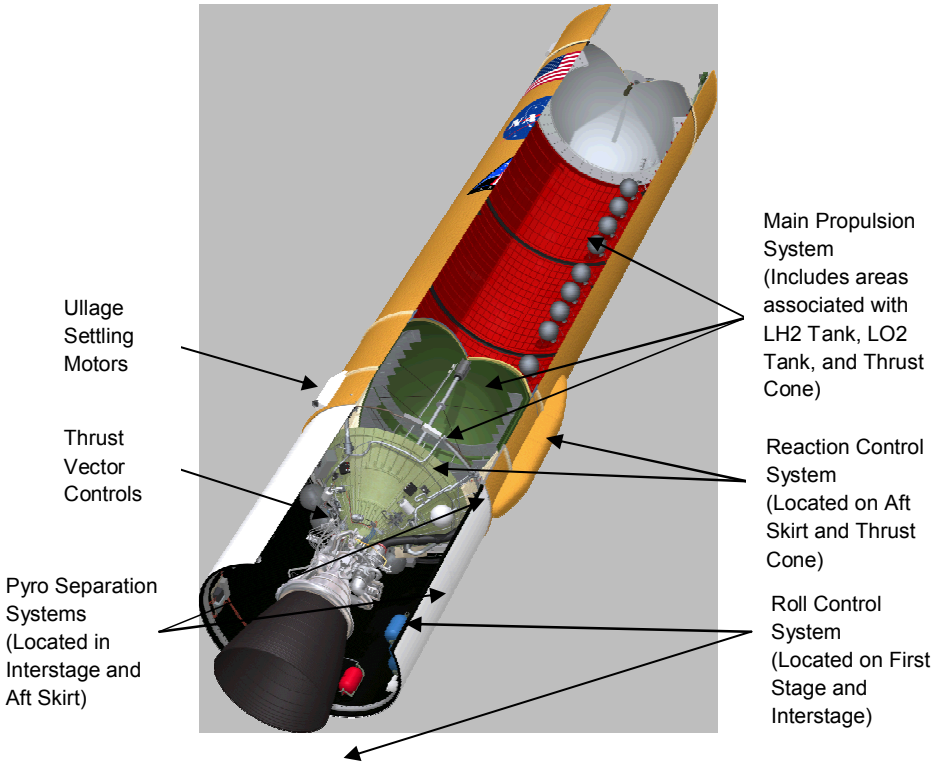


Figure 2.0.2 – General Location of USPC Subsystems[2]

3.1 System Safety Risk Reduction / Mitigation Precedence

The following system safety risk reduction / mitigation precedence sequence in the subsections below is consistent with CxP 70038, section 3.1. Verifications for Hazards identified in applicable US Flight System Safety HR utilize the following risk reduction order of preference [3]:

- Eliminate hazards
- Design to minimize hazards
- Incorporate Safety devices
- Provide Caution and Warning devices
- Develop and implement Special Procedures

Details addressing risk reduction are provided in the following subparagraphs.

3.1.1 Standard Risk Reduction Approach

Criteria used to select verifications that help reduce risk for applicable to USPC SCI components [4] include:

Eliminate hazards - Hazards will be eliminated from the design wherever feasible.

Design for minimum risk - If an identified hazard cannot be eliminated, it will be controlled through design selection. This can include designing in factors of safety and additional fault tolerance.

Incorporate Safety devices - Hazards that cannot be eliminated or controlled through design selection shall be controlled to an acceptable level through the use of fixed, automatic or other protective safety design features or devices.

Provide Warning devices - When neither design nor safety devices can effectively eliminate identified hazards, devices shall be used to detect the condition and to generate an adequate warning signal to alert personnel to the hazard.

Develop and Implement Procedural control - Where it is impossible to eliminate or adequately control a hazard through design selection or the use of safety and warning devices, procedures and training shall be used to control the hazard. Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the managing activity. Safety critical tasks and activities may require certification of personnel proficiency.

3.1.2 Upper Stage Risk Reduction Approach

Upper Stage S&MA currently employs a combination of Design for Minimum Risk (DFMR) and Fault Tolerance (FT) design philosophies [5] to control hazards identified in this safety analysis. Generic Upper Stage DFMR application areas include:
− Primary structures/interfaces
− Pressure vessels and pressurized lines and fittings
− Thermal Protection System (TPS)
− Pyrotechnic charges

Areas of Upper Stage design employing fault tolerance (FT) controls include:
− Electronic/electrical system
− Reaction control function
− TVC hydraulics
− MPS pressurization and pneumatic system function
− Pyrotechnic activation

Generally, DFMR and FT design requirements for hazard control are or will be cited in the individual US Flight System Safety hazard reports and will be expanded as each US Flight System Safety hazard analysis is updated.

3.2 Hazard Classification

All identified hazards are classified according to their severity (effects of the hazard) and likelihood (probability the effect will occur). Both parts of the classification process are qualitative in nature and determined by the amount of control in place to prevent occurrence. Once determined, they are combined to establish an overall risk classification.

3.2.1 Severity

Per CxP 70038, severity is defined as assessment of the most severe effect(s) of a hazard, assigned independently of the hazard controls [6]. Definitions for each severity type used in US Flight System Safety HRs receiving verifications from associated USPC CSI HRs are categorized per CxP 70038, Table 5.4-1. [7]

NOTE: Severities are not specifically included in USPC SCI HRs since these detailed verifications will assist in updates to their associated US Flight System Safety HRs. Based on new verifications and requirements from USPC CSI HRs, US Flight System Safety HR authors may be able to show reduced

severities based on updated "down-and-in" verifications and requirements submitted on a case-by-case basis.

3.2.2 Likelihood

Per CxP 70038, para 5.3, likelihood is defined as the probability of an identified hazard cause resulting in a mishap. Controls in each referenced US Flight System Safety HR are considered to be in place when performing the likelihood of occurrence assessment . Each likelihood description, referenced in CxP 70038, Table 5.4-1. [8]

NOTE: Likelihoods are also not specifically included in USPC SCI HRs since these detailed verifications will assist in updates to their associated US Flight System Safety HRs. Based on new verifications and requirements from USPC CSI HRs, US Flight System Safety HR authors may be able to show reduced likelihoods based on updated "down-and-in" verifications and requirements submitted on a case-by-case basis.

3.2.3 Overall Safety Risk

Overall safety risk is defined as the combination of (1) the probability (quantitative or qualitative) that a Project or Program will experience the undesired event and (2) the consequences, impact or severity of the undesired event were it to occur [7]. The new Risk Matrix defined in each of the US Flight Safety Hazard Reports uses a 5 x 5 matrix defined per CxP 70038, which is consistent with many industry standard 5 x 5 matrices used for risk assessments. A blank matrix from a US Flight System Safety HR using verifications and requirements from the USPC SCI SAR is available in CxP 70038, Figure 5.4-1[9].

Use of USPC SCI HRs and their associated verifications and requirements is expected to lower likelihoods (and maybe some severities) of many different Causes in their respective US Flight System Safety HRs.

3.3 USPC SCI Hazard Analysis Approach

Each USPC SCI Hazard Analysis provides verifications to its respective current US Flight System Safety Hazard Report. The approach used in developing each SCI HR is provided in the subsections below.

3.3.1 Data Accumulation

Each assessment is based on obtaining the best available data. Data sources include but are not limited to: US SCI element system description documents, system diagrams, mission descriptions, operational concepts, technical information from other engineering organizations (IPT teams), functional flow block diagrams, mishap data from similar systems and lessons learned from other projects. A SCI analysis process flow diagram overview is provided in Figure 3.3.1.

3.3.2 Analysis Process

After initial data accumulation, three major steps were taken to produce each USPC SCI HR section. This process includes selecting only those controls in the US Flight System Safety HR that will use "down-and-in" verifications. A graphical representation of this process is available in Figure 3.3.1, which includes the following overall steps:

1) Defining applicable SCI HR controls as baselined in the US Preliminary Design Review timeframe.

2) Development of USPC SCI HR worksheets applicable to affected USPC subsystems/components.

3) Development of the USPC SCI Safety Analysis Report (SAR), which includes use of the USPC SCI worksheets in organized appendices.

Information related to each major step of the analysis process is available in their respective subsections below.

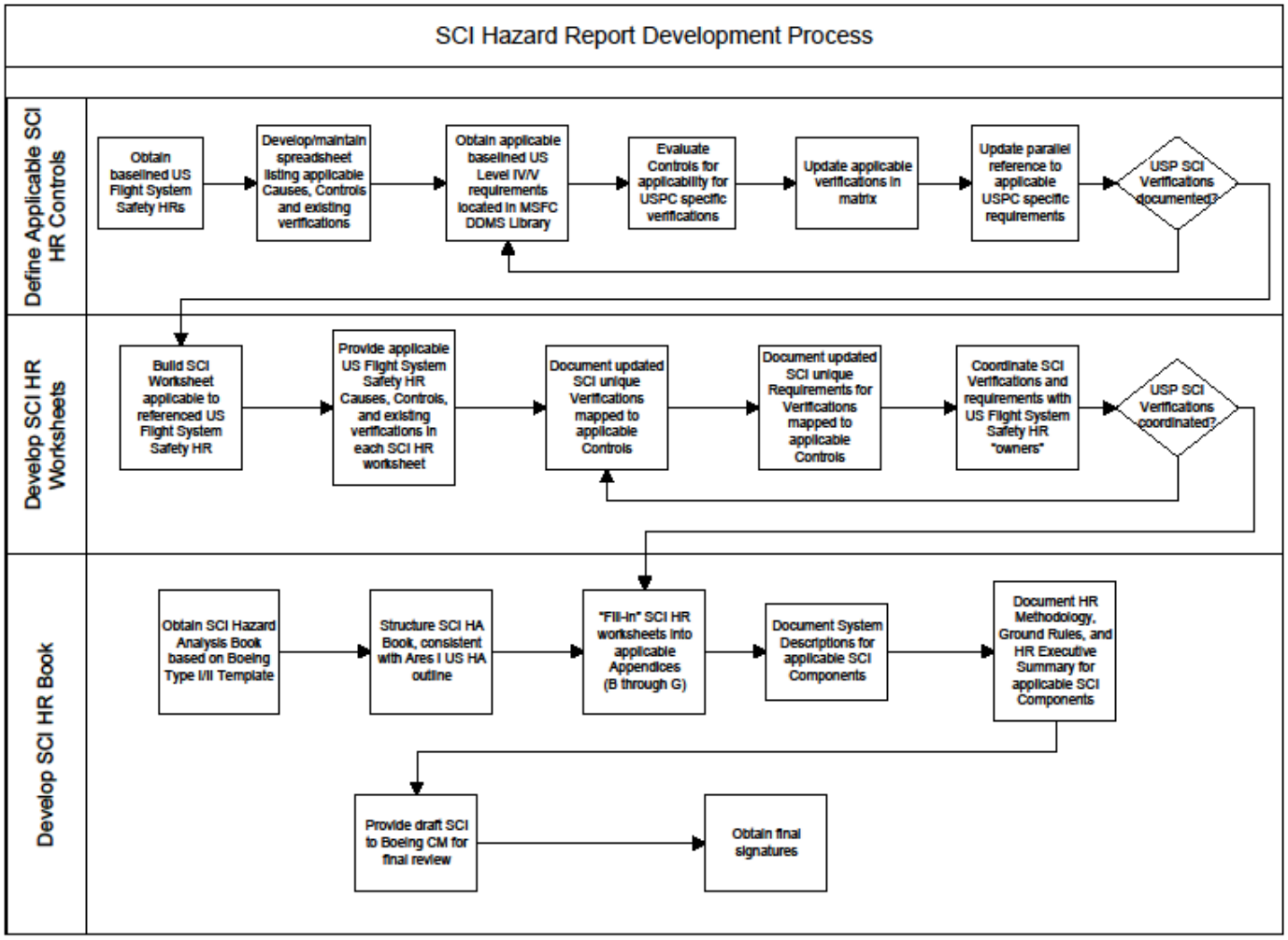


Figure 3.3.1 – SCI HR Analysis Flow Process

3.2.2.1 Selecting Applicable USPC SCI Controls

Step 1 involved reviewing controls and verifications from each baselined Phase 1 US Flight System Safety HR. An Excel spreadsheet listing all applicable US Flight System Safety HR Causes and controls to select applicable US Flight System Safety hazard report information related to USPC SCI verifications. Columns used for sorting included:

- US Flight System Safety Hazard numbers
- US Flight System Safety title
- Baselined US Flight System Safety Causes
- Baselined US Flight System Safety Controls
- Baselined US Flight System Safety Verifications

Other columns were available in this matrix to assist in mapping applicable USPC requirements related to US Flight System Safety HR Causes include:

- Boeing (USPC) applicable ??? (Yes/No)
- Related SCI documents ??? (Yes/No)
- (New) Related SCI Verifications
    - Detailed Verifications to replace those baselined shortly after the US Phase I PDR
- Related SCI Requirements (taken from applicable USPC Requirements Documents)
- Comments (used for notes and other suggestions as necessary

Upon completion of the SCI HR matrix, each baselined US Flight System Safety HR Cause and Control was evaluated for applicability to available USPC verifications. Baselined element requirement documents were reviewed for each SCI Item to "map" appropriate SCI requirements to applicable US Flight System Safety Controls and Verifications. Selected USPC SCI requirement verifications and requirements were then updated in the spreadsheet, using a "down-and-in" approach, to match the updated verifications with applicable US Flight System Safety HR Causes and Controls. Once applicable spreadsheet sections are completed per subsystem, development of specific USPC SCI HR worksheets could begin. An example matrix is provided in Appendix A.

3.2.2.2 Development of USPC SCI Hazard Report Worksheets

Upon completion of the requirements/verifications matrix referenced in section 3.3.2.1, applicable SCI HR worksheets are being developed to assist the Upper Stage NDT System Safety Team in updating their respective US Flight System Safety Causes and Controls. This process is illustrated in the "middle" section of Figure 3.3.1.Bulding the assigned USPC SCI HR worksheets included use of the following items from the completed verification / requirement matrices:

- Bulleted information from each affected US Flight System Safety HR, including:
    - Hazard Number
    - Hazard Title
    - Hazardous Description Condition
    - Acceptance rationale

- A table for each US Flight System Safety HR listing the following:
    - US Flight System Safety Controls selected to have "down-and-in" requirements and verifications
    - Updated verifications used to update those baselined during the Upper Stage PDR
    - Applicable Safety Requirements related to the updated USPC HR verifications

Changes in US Flight System Safety verifications and requirements, as identified in applicable USPC SCI HR worksheets will be discussed with US Flight System Safety HR "owners". Final updates will then be made to applicable sections of these worksheets to assist the US NDT Flight System Safety in providing applicable verifications and controls for "down-and-in" Controls.

An example USPC SCI worksheet is provided in Figure 3.2.2.2

3.2.2.3 Documentation of the USPC SCI Safety Analysis Report

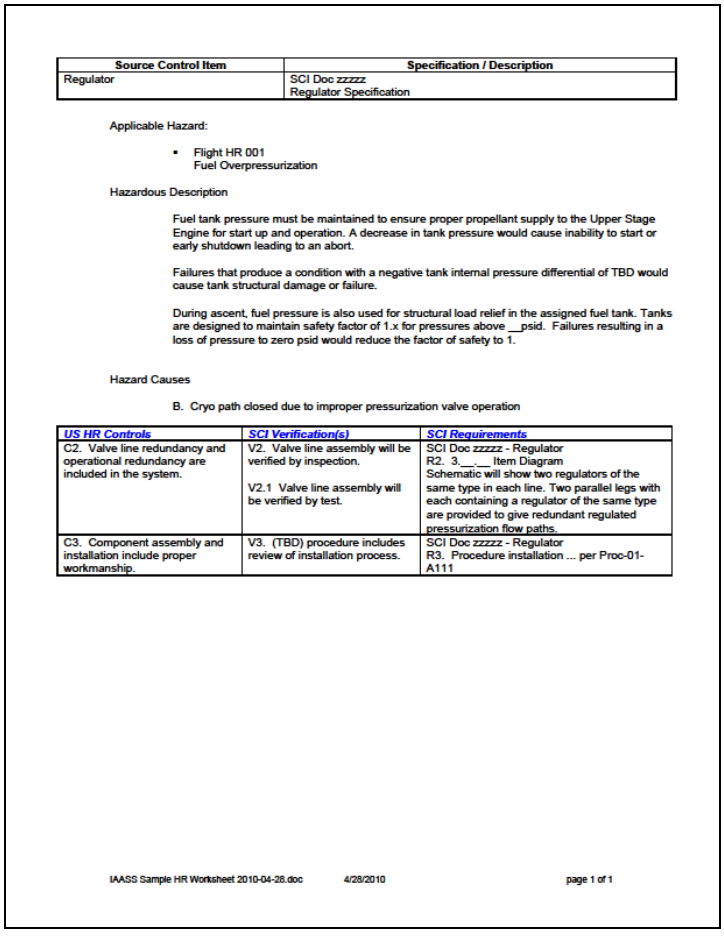
In an effort parallel to developing the USPC SCI HR worksheets, the overall USPC SCI Safety Analysis Report (SAR) is also being updated with applicable component descriptions. A flow illustration is provided in the "bottom" section of Figure 3.3.1.

Documentation of the USPC SCI SAR includes the following overall steps:

- Providing a standard Boeing document template to provide a structure for the overall SAR
- Structuring sections of the SAR which include areas such as title pages, Table of Contents, Lists of Figures and Tables, Introduction, System Descriptions, Methodology, Executive Summary, Conclusions, and Appendices for USPC SCI HRs listed by IPT.

Flight HR Number	Flight HR Title	HR Causes	HR Controls	Existing HR Verifications	SCI applicable ????	Related SCI Document(s)
FlightHR 001	HR Title 1 - Fuel Overpressurization	B. Cryo path closed due to improper pressurization valve operation	C2. Valve line redundancy, operational redundancy ...	V2. Operational testing	Yes	SCIDoc zzzzz
FlightHR 001	HR Title 1 - Fuel Overpressurization	B. Cryo path closed due to improper pressurization valve operation	C3. Component assembly / installation ...	V3. Inspection of procedure and as built hardware	Yes	SCIDoc zzzzz
FlightHR 002	HR Title 2 - Oxidizer Overpressurization	B. Cryo path closed due to improper pressurization valve operation	C4. Components designed to meet Natural Environments requirements ...	V4. Analysis, Qualification test/acceptance test	Yes	SCIDoc zazaz
FlightHR 002	HR Title 2 - Oxidizer Overpressurization	B. Cryo path closed due to improper pressurization valve operation	C5. Components are designed to meet requirements for Induced Environments	V5. Analysis, Qualification test/acceptance test	Yes	SCIDoc zazaz
FlightHR 003	HR Title 3 - Pressurization System - Operational Failure	B. Valve fails to open when pressurized	C6. Filters will be sized such that TBD amount of debris captured does not affect flow.	V6. Analysis	Yes	SCIDoc zazab

Figure 3.2.2.3 – Sample USPC SCI HR Matrix



Source Control Item	Specification / Description
Regulator	SCI Doc zzzzz Regulator Specification

Applicable Hazard:

- Flight HR 001
  Fuel Overpressurization

Hazardous Description

Fuel tank pressure must be maintained to ensure proper propellant supply to the Upper Stage Engine for start up and operation. A decrease in tank pressure would cause inability to start or early shutdown leading to an abort.

Failures that produce a condition with a negative tank internal pressure differential of TBD would cause tank structural damage or failure.

During ascent, fuel pressure is also used for structural load relief in the assigned fuel tank. Tanks are designed to maintain safety factor of 1.x for pressures above __psid. Failures resulting in a loss of pressure to zero psid would reduce the factor of safety to 1.

Hazard Causes

B. Cryo path closed due to improper pressurization valve operation

US HR Controls	SCI Verification(s)	SCI Requirements
C2. Valve line redundancy and operational redundancy are included in the system.	V2. Valve line assembly will be verified by inspection. V2.1 Valve line assembly will be verified by test.	SCI Doc zzzzz - Regulator R2. 3.__.__ Item Diagram Schematic will show two regulators of the same type in each line. Two parallel legs with each containing a regulator of the same type are provided to give redundant regulated pressurization flow paths.
C3. Component assembly and installation include proper workmanship.	V3. (TBD) procedure includes review of installation process.	SCI Doc zzzzz - Regulator R3. Procedure installation ... per Proc-01-A111

IAASS Sample HR Worksheet 2010-04-28.doc 4/28/2010 page 1 of 1

Figure 3.2.2.4 – Sample USPC Hazard Report Worksheet

- "Filling in" SCI subsystem information using available USPC SCI requirement documents
- Updating SCI HR worksheets and descriptions as such documents are baselined
- Presentation of an overall draft of the completed USPC SCI SAR through Boeing and NASA Design Team for final review and signatures

If necessary, presentation of the USPC SCI SAR and/or its associated US Flight System Safety Hazard Reports can be provided to the Upper Stage Constellation Safety Engineering Review Panel (CSERP) prior to incorporation of updates for the US Design Configuration Review (DCR).

3.4 SCI HR Review Process/Status

The SCI HR is a Boeing-provided document provided to assist in development of current US Flight System Safety Hazard Controls and Verifications. Informal reviews for each SCI section will be provided to the MSFC Safety and Mission Assurance (S&MA) Working Group prior to delivery. Internal delivery of this document, as a Boeing product per its assigned Data Requirements Document, will be carried out in response to the assigned Ares I Statement of Work (SOW) Request for Proposal. Agreements for changes necessary to complete applicable SCI verifications prior to the US PDR, after initial delivery, are documented in Appendix H of the SCI SAR.

4.0 RESULTS

Building any acceptable Safety Assessment Report requires teamwork from top to bottom. Cooperation from the NASA Design Team (NDT) and Boeing Integrated Product Team (IPT) engineers is a necessity in helping "root out" hazardous conditions during any and all design stages. Teamwork to date in building the USPC SCI SAR includes the following:

- Internal reviews of each section of the USPC SCI spreadsheet with responsible US Flight System Safety engineers
- Agreement on the overall USPC SCI HR development philosophy by the NASA Design Team and Boeing USPC System Safety at the 2010 Upper Stage Offsite meeting in Huntsville, AL (January 2010)
- Submittal and review of USPC SCI worksheets as delivered per the assigned schedule
- Updates in applicable USPC SCI HR worksheets and system descriptions
- Overall support in allowing updates to USPC SCI specifications when System Safety concerns are noted

A "matrix" containing 38 baselined Phase I US Flight Safety Hazard Reports with associated Causes, Controls, and Verifications was created in mid-2009 and completed for submittal to MSFC-S&MA (System Safety) in January 2010. Development of this matrix allowed in-depth research to select which controls/verifications can best use verifications in available US IPT requirements documents. Once the applicable requirements were reviewed, over 2000 detailed verifications were used to "map" applicable verifications with their associated requirements and verifications. This matrix also is useful in developing associated subsystem SCI hazard worksheets, which then allows easier updates of applicable US Flight System Safety HRs in preparation for their US CDR.

At this time, a total of 35 (TBR) draft subsystem HRs for the following subsystems have been provided to their respective Boeing and NASA design teams for internal review. SCI HR worksheets prepared for each Integrated Product Team (IPT) include:

- Pyrotechnic Separation System (15 HR worksheets)
- Reaction Control System (4 HR Worksheets)
- Roll Control System (8 HR Worksheets)
- Combined ReCS/RoCS (2 HR Worksheets)
- Main Propulsion System (6 HR Worksheets to date)

Creation of the Safety Analysis Report (SAR) containing detailed system descriptions, methodology, and an Executive Summary are in work and are expected to be completed for internal review within the next 6 months.

5.0 CONCLUSIONS

The proposed updates are expected to assist in defining necessary analyses and tests to be detailed for the referenced verifications prior to the US CDR. Future updates will be provided to complete verifications for applicable US SCI components prior to the US Design Certification Review (DCR).

Completion of the assigned SCI Safety Analysis Report (SAR) and specific HR worksheets will assist the Ares I US System Safety team in closing detailed verifications in their baselined US Flight System Safety Hazard Analyses. Each US Flight System Safety Engineer can use the enclosed SCI HR Worksheets related to their assigned US subsystems to help close applicable "down-and-in" verifications, as well as allowing Boeing and the NASA Design Team (NDT) Systems Engineering group in mapping applicable "down-and-in"

requirements to higher level requirements for traceability purposes.

6.0 ACRONYMS AND ABBREVIATIONS

CDR	Critical Design Review
CxP	Constellation Program
DFMR	Design for Minimum Risk
FT	Fault Tolerance
HA	Hazard Analysis
HR	Hazard Report
IDR	Interim Design Review
MPS	Main Propulsion System
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NDT	NASA Design Team
PDR	Preliminary Design Review
ReCS	Reaction Control System
RoCS	Roll Control System
S&MA	Safety and Mission Assurance
SAR	Safety Analysis Report
SCI	Source Control Item
SOW	Statement of Work
TPS	Thermal Protection System
TVC	Thrust Vector Control System
US	Upper Stage
USM	Ullage Settling Motors
USMS	Ullage Setting Motor System
USP	Upper Stage Production
USPC	Upper Stage Production Contract

7.0 REFERENCES

1. NASA Constellation Website, Ares Launch Vehicles; http://www.nasa.gov/pdf/231430main_UpperStage_FS_final.pdf; *NASA's Ares I Upper Stage*, page 2.

2. NASA Constellation Website, Ares Launch Vehicles; http://www.nasa.gov/pdf/231430main_UpperStage_FS_final.pdf; *NASA's Ares I Upper Stage*, page 2

3. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Rev. B, Change 001, section 3.1, page 12.

4. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, subsections 3.1.1 through 3.1.4, pages 12-13.

5. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, section 3.2, page 13.

6. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, section 5.3, page 29.

7. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, Table 5.4-1, page 32.

8. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, Table 5.4-1, page 32.

9. CxP 70038 (2009), *Constellation Program Hazard Analyses Methodology*, Revision B, Change 001, Figure 5.4-1, page 32.

8.0 BIOGRAPHY

Michael S. Mitchell

Mr. Mitchell is currently a System Safety engineer with The Boeing Company, working on the Ares I USPC Contract at MSFC. He earned his Chemical Engineering degree from Lamar University (Beaumont, TX) in 1983. Experience related to System Safety (starting in 1987) includes developing different types of hazard analyses for the Space Shuttle (Integration and Element), Space Station, Government-Furnished Equipment (GFE) and Ares I Upper Stage systems. Other aerospace safety experience includes work with Lockheed-Martin (1994 – 1997) in development of hazard analyses related to Hercules C-130-H and -J model aircraft. Recognition includes receipt of the Silver Snoopy award in September 2007 for development, monitoring, and updates of the Integration Debris Fault Tree used in identifying debris sources contributing to the 2003 STS-107 Columbia incident.

David R. Winner

Mr. Winner is currently a System Safety engineer with The Boeing Company, working on the Ares I USPC Contract at MSFC. He earned a Masters of Aeronautics and Aviation Science Degree from Embry Riddle University. System safety experience includes NASA/MIR, ISS, ESA, and Shuttle projects.