Integrated Safety Analysis Tiers

Carla Shackelford, Co-author, Bastion Technologies Inc., Marshall Space Flight Center, Huntsville, Alabama, USA
Lisa McNairy, Co-author, Bastion Technologies Inc., Marshall Space Flight Center, Huntsville, Alabama, USA
Jon Wetherholt, Co-author, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: Integrated Safety Analysis, Safety Analysis Processes

Abstract

Commercial partnerships and organizational constraints, combined with complex systems, may lead to division of hazard analysis across organizations. This division could cause important hazards to be overlooked, causes to be missed, controls for a hazard to be incomplete, or verifications to be inefficient. Each organization's team must understand at least one level beyond the interface sufficiently enough to comprehend integrated hazards. This paper will discuss various ways to properly divide analysis among organizations. The Ares I launch vehicle integrated safety analyses effort will be utilized to illustrate an approach that addresses the key issues and concerns arising from multiple analysis responsibilities.

Introduction

There are several considerations when attempting to determine the best place to divide analysis between a major system and its elements or subsystems. Politics, funding, expertise, responsibility/ownership, and clarity all contribute to the decision of how to perform this task. Misjudgment in any one of these factors can cause the effort to fail due to confusion when performing the work, lack of ownership by an engineering group, or inability to present a cohesive analysis to the safety authority. Failure constitutes missing hazards, missing hazard causes, lack of hazard control, inadequate verification of controls, or an inefficient effort costing valuable resources.

NASA typically writes hazard reports to document the outcome of a hazard analysis. The reports themselves are not the analysis, but must represent the analysis and must be divided in a logical fashion. Hazard reports include a description of the hazard, a list of causes, controls for each cause, and verifications for the controls. Fault Trees, Failure Modes Effects Analysis, Probabilistic Risk Assessment, and other distinct analysis types are inputs to the overall hazard analysis.

In order to understand how safety analysis is divided, one must understand how a Program is broken down. NASA typically organizes safety for a given program. The Space Shuttle Program, the Apollo Program, and the Constellation Program are examples. Each Program consists of projects; for example, within the Constellation Program, there is the Ares Project (the launch propulsion vehicle), the Orion Project (the

spacecraft), and the Ground Systems Project. There are other projects in the Constellation Program; however, the Ares I project will be the main focus of this paper.

Division of Analysis

The Ares Project is divided organizationally into four elements: First Stage, Upper Stage Engine (J-2X), Upper Stage, and Vehicle Integration (Fig. 1 and Fig 2). The Ares I First Stage is a single five-segment solid rocket booster which is a derivative of the space shuttle's solid rocket booster. The Upper Stage Engine is a liquid oxygen/liquid hydrogen J-2X Engine derived from the J-2 Engine used on Apollo's second stage. The J-2X Engine will power the launch propulsion vehicle's second stage into low Earth orbit. The Upper Stage is the core structure that houses the avionics for the launch propulsion vehicle. The Upper Stage interfaces with the Orion spacecraft and the First Stage as well as the J-2X engine. Vehicle Integration performs many of the integrated vehicle analyses necessary to ensure an overall safe, robust, and properly functioning launch vehicle. The Ares I will lift more than 55,000 pounds of payload to low Earth orbit.

There are several structural interfaces as well as avionics and electrical interfaces between the elements. The Upper Stage, the brains of the launch vehicle, contains the software that controls the first stage and interfaces with the Upper Stage Engine controller and Orion crew module. The complexity of these interfaces is where the true ownership of the hazard analysis is not apparent and has been the root of much discussion. The First Stage and Upper Stage Engine being designed by contractors adds another level of complexity in the hazard analysis division. Contractual considerations, part of the ownership/responsibility factor, are a major driver. The Upper Stage is being designed in-house as well as the integration analysis of the Ares Vehicle. The Vehicle Integration Team has the advantage of the Upper Stage Safety Team being easily accessible, as well as reduced contractual interfaces in data exchange. Working with the Upper Stage Element safety engineers has always had a positive effect of performing well.

The initial division of the analysis was not performed using a defined set of ground rules agreed upon by the various teams. The analysis by each element including vehicle integration progressed to a point that allowed some differentiation to be seen. This was not by design, but by necessity. The engineering boundaries, especially in the area of avionics and vehicle control, were not defined in the beginning. Initially vehicle integration using fault tree analysis drove deep into the elements. This was essential since vehicle integration was the first element to start developing their safety analysis. This initial effort of driving deep into the elements was necessary for Vehicle Integration as an “independent” assessment for identifying hazards for the Ares vehicle. Although this effort was done early on in the development cycle, it allowed for Vehicle Integration to set the ground work for ensuring a comprehensive hazard analysis. Once the other elements started developing their own fault trees and boundaries started to become clearer, Vehicle Integration began transferring many of their lower level fault tree blocks to the elements. Throughout this process there were certain areas that consistently continued to have overlaps between Vehicle Integration and the other Ares elements.

These were pointed out during some of the Safety Reviews with the Constellation Safety and Engineering Review Panel. The areas that were subject to much discussion were avionics, the Upper Stage main propulsion system, and separation. This was due to the nature of how the Upper Stage and Vehicle Integration hazard analyses were performed.

Vehicle Integration in the Ares I project is considered an element and does not have any real authority over the hardware elements other than the ability to derive requirements from integrated analysis. Since Vehicle Integration does not own any hardware, it made logical sense to break out the safety analysis by hazards. Using a top down system level approach, Vehicle Integration was able to tell the whole story for the Ares Vehicle. This allowed the analysis to be truly integrated, which helped identify any gaps in the hazard analysis. Upper Stage broke out the hazard analysis by subsystems. These subsystems lined-up with the Integrated Product Teams (IPT) therefore each IPT only had to sign off on the controls for which they had ownership. This resulted in Upper Stage deciding to create integrated hazard reports to complete the story for Upper Stage. The Upper Stage Team, having integration hazard reports of its own, resulted in duplicating some of the same work that Vehicle Integration had performed. As the analysis and documentation efforts continued and presentations to the safety panel were made by the teams, it became evident that it was time to create stricter ground rules so that the teams, safety panel, and future users of the documentation could better understand how to navigate the complex analysis that was being created.

The overlap eventually diminished once preliminary documentation of the hazard analysis was established. Communication was initiated to set ground rules and divide responsibility across both teams. Unwritten agreements were made which helped narrow the scope, but not eliminate all overlap in order to ensure all hazards had been captured. The division was clear for the element contractors since they had little integration responsibility and had ownership of the control for a hazard that did not cross element lines. For example, a failure of the Auxiliary Power Unit in the first stage leading to a fire or explosion would be controlled and owned by First Stage. However, the failure of the structural interface of first stage to Upper Stage would be an integrated hazard because Vehicle Integration would own the design interface.

During this process of identifying integrated hazards, Vehicle Integration came across an issue with the First Stage-Upper Stage structural interface. This risk was raised to Ares Project. As a result, a design team was coordinated by Vehicle Integration to analyze the interface post Preliminary Design Review of the Ares vehicle. At the beginning, First Stage and Upper Stage each had a baseline design for their element Preliminary Design Reviews, but the two element designs were not compatible at the interface. Vehicle Integration started with a hybrid design taken from the two elements as well as a couple of other options to trade. Vehicle Integration reviewed and chose the best options and now owns the design and stress analysis at the interface. The elements own the design and hardware up to the interface. The integrated hazard report captures the causes and controls across this interface boundary.

Upper Stage was not so clear with ownership of hazards. The Upper Stage provides propellants, liquid hydrogen fuel, and liquid oxygen to the J-2X engine. If this propellant is not provided in the correct condition, the J-2X engine could cavitate resulting in possible fire/explosion of the engine. This shows a perfect example of why the role of vehicle integration is necessary. Strictly speaking, Upper Stage would have no need to incorporate any of the controls to provide the correct propellant conditions to the engine because it is not a hazard to the Upper Stage. The actual hazard resides in the engine; however most of the controls need to be on the Upper Stage side to mitigate the hazard from actually manifesting itself in an engine failure. During discussions with the other elements, a few concepts were proposed on the best way to document the analysis and minimize the duplication of effort between the elements.

There were two prevailing concepts in dividing the documentation with the understanding that the analysis must overlap. The first approach was for integration to analyze and document all integrated hazards and for the elements to only cover hazards within their element. The problem with this approach was that the integrated hazard reports would have to incorporate element controls. This meant that the elements, particularly Upper Stage, would have to sign off on the integrated hazard reports that housed some of the controls owned by Upper Stage, the elements would have one place to check for integration issues. Since Upper Stage would not have ownership of the hardware controls in the first concept, this was deemed unacceptable by Upper Stage.

The second concept was oriented toward control ownership. In this second concept, since integration did not own any hardware, many integrated hazards would be owned by Upper Stage because they owned the controls. However, Vehicle Integration owned much of the analysis for the integrated hazards. This was true for the first stage and Upper Stage Engine. This process would be challenging for Vehicle Integration due to the difficulty in implementing a hardware control that would be owned by another element. Another interesting point was that the Upper Stage safety engineers were already engaged in the product development teams analyzing the integrated hardware and software, not the integration safety engineers. This meant that the ability of understanding of the hazard as well as the relationship to work out the best control lay in the hands of the element safety engineers.

A third approach discussed was a combination of the first two approaches. This third approach would result in the Vehicle Integration reports duplicating parts of the Upper Stage reports while allowing Upper Stage to continue with a parallel report. The Upper Stage report would contain the controls allowing that element ownership of the controls. Vehicle Integration would duplicate the controls and be able to “tell the story” for the hazard. However this effort would have been a configuration management issue keeping track of hazard report changes and would have caused confusion and increased work load.

Control ownership, the second concept, was the final consideration that drove the choice for the division of the analysis among the Ares elements. This meant that integration would write a report that would describe the hazard and point to the Upper Stage reports

for the controls. This would allow Upper Stage to document the controls for which they had ownership, while Vehicle Integration maintained the integrated controls. Control ownership was the only concept that a majority of both parties could agree on. As previously stated the other two concepts would have resulted in more conflict and struggle due to the layout of the Ares Project. This outcome may not always be the case in all systems. A project with a strong central integration team, that owns interface hardware and the authority, might have chosen to have all the integrated hazard reports written by the integration safety team.

Another layer of complexity in the division of integrated hazard analysis was the Program Hazard Analysis. This was the integration of Ares, Orion, and Ground Systems Projects. Part of this analysis was delegated to the Ares project. This division was owned by the Program, which did have some authority over the other projects. Fortunately the Orion –Ares interfaces are more limited than the Ares element interfaces, and the Ground interfaces have similar traits as the Shuttle to Ground interfaces. These have yet to be completely divided.

Conclusion

There are several factors to consider in dividing hazard analysis responsibility among organizations in a large program. The deciding factor in the case of Ares I was control ownership due to the organizational structure. A certain amount of overlap in the beginning was necessary for two reasons. First, it forced both Upper Stage and Vehicle Integration to understand what was beyond what would later be the boundary. Second, this helped ensure that there were not any gaps in the analysis. There are exceptions that need to be considered when breaking out analyses among multiple divisions. It takes hard work and long deliberation to separate the hazard reports in a manner that makes sense. Ares I's decision to break out the analysis along control ownership is still in the process of being fully incorporated. Much thought has gone into this decision and kinks will be worked out as the process matures.

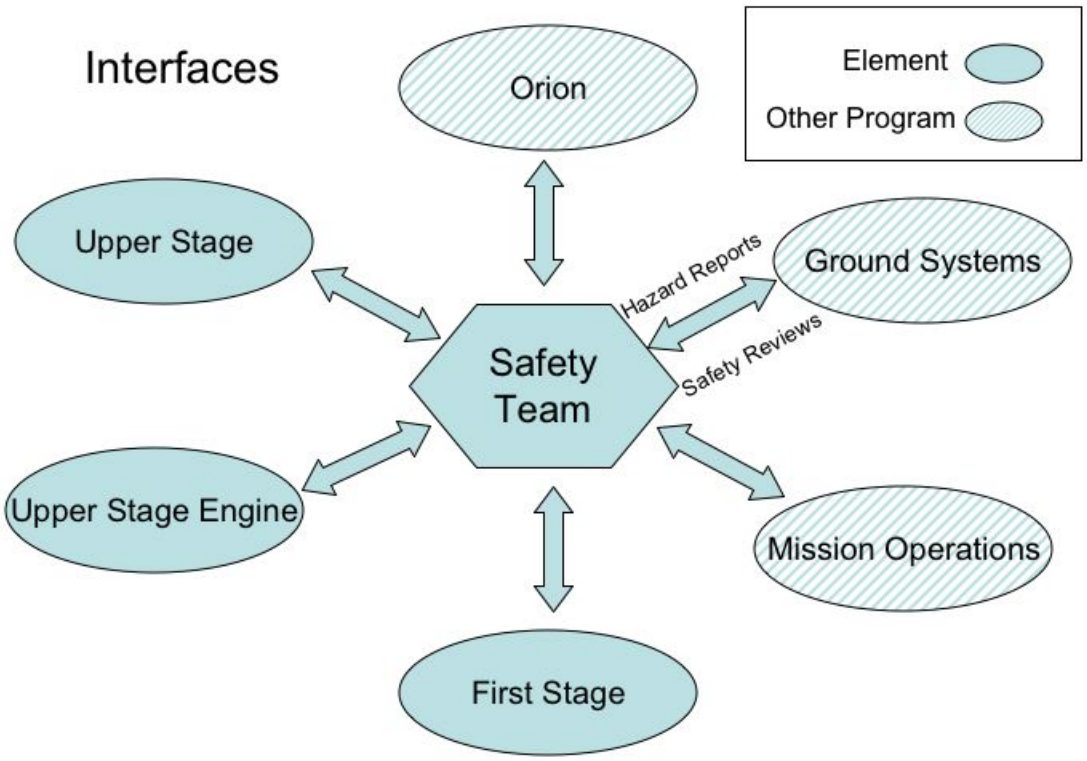
Interfaces
Orion
Element
Other Program
Upper Stage
Ground Systems
Hazard Reports
Safety Reviews
Safety Team
Upper Stage Engine
Mission Operations
First Stage

Figure 1

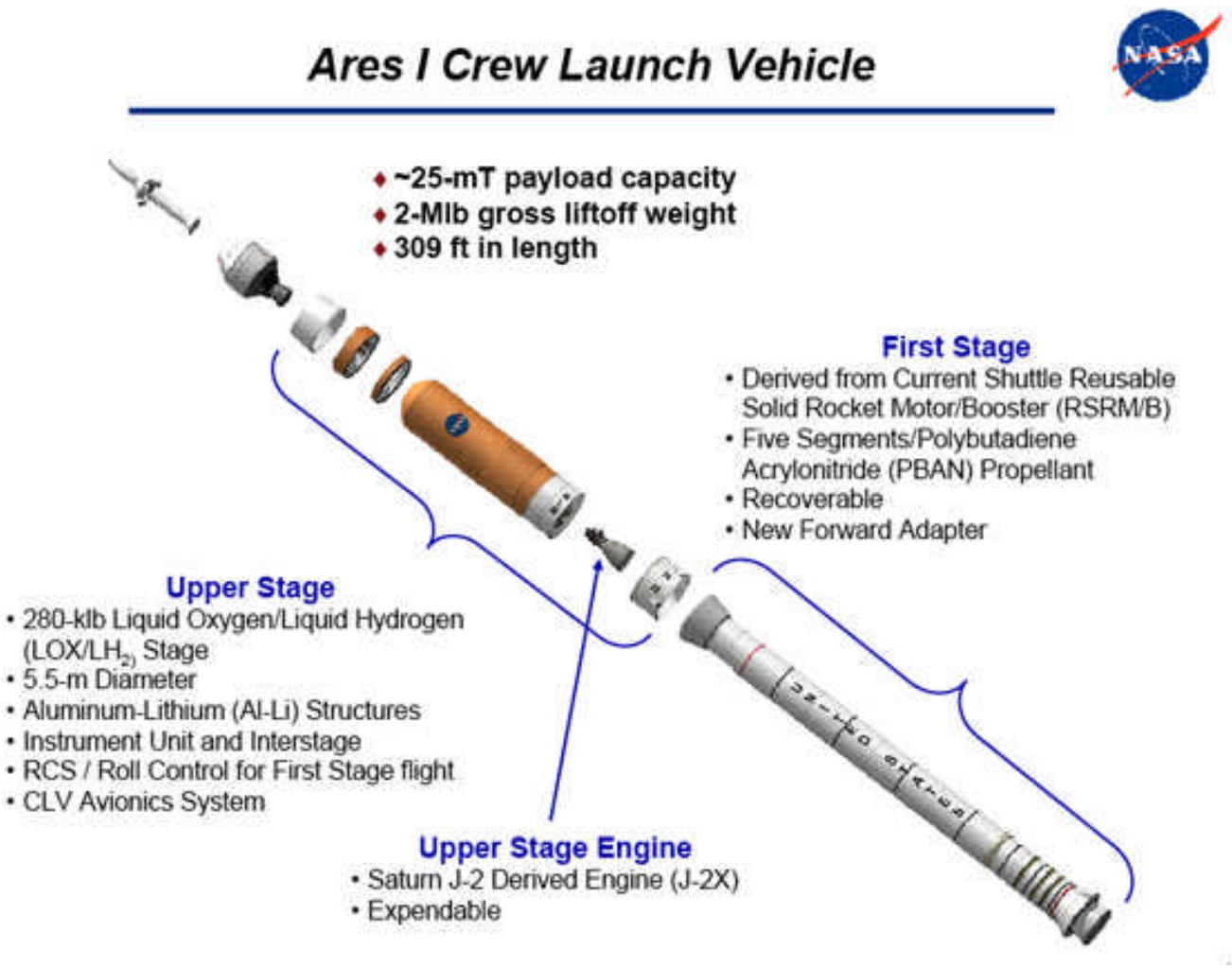
Ares I Crew Launch Vehicle
♦ ~25-mT payload capacity
♦ 2-Mlb gross liftoff weight
♦ 309 ft in length
First Stage
• Derived from Current Shuttle Reusable Solid Rocket Motor/Booster (RSRM/B)
• Five Segments/Polybutadiene Acrylonitride (PBAN) Propellant
• Recoverable
• New Forward Adapter
Upper Stage
• 280-klb Liquid Oxygen/Liquid Hydrogen (LOX/LH2) Stage
• 5.5-m Diameter
• Aluminum-Lithium (Al-Li) Structures
• Instrument Unit and Interstage
• RCS / Roll Control for First Stage flight
• CLV Avionics System
Upper Stage Engine
• Saturn J-2 Derived Engine (J-2X)
• Expendable

Figure 2

CxP Hierarchy of Systems and Elements

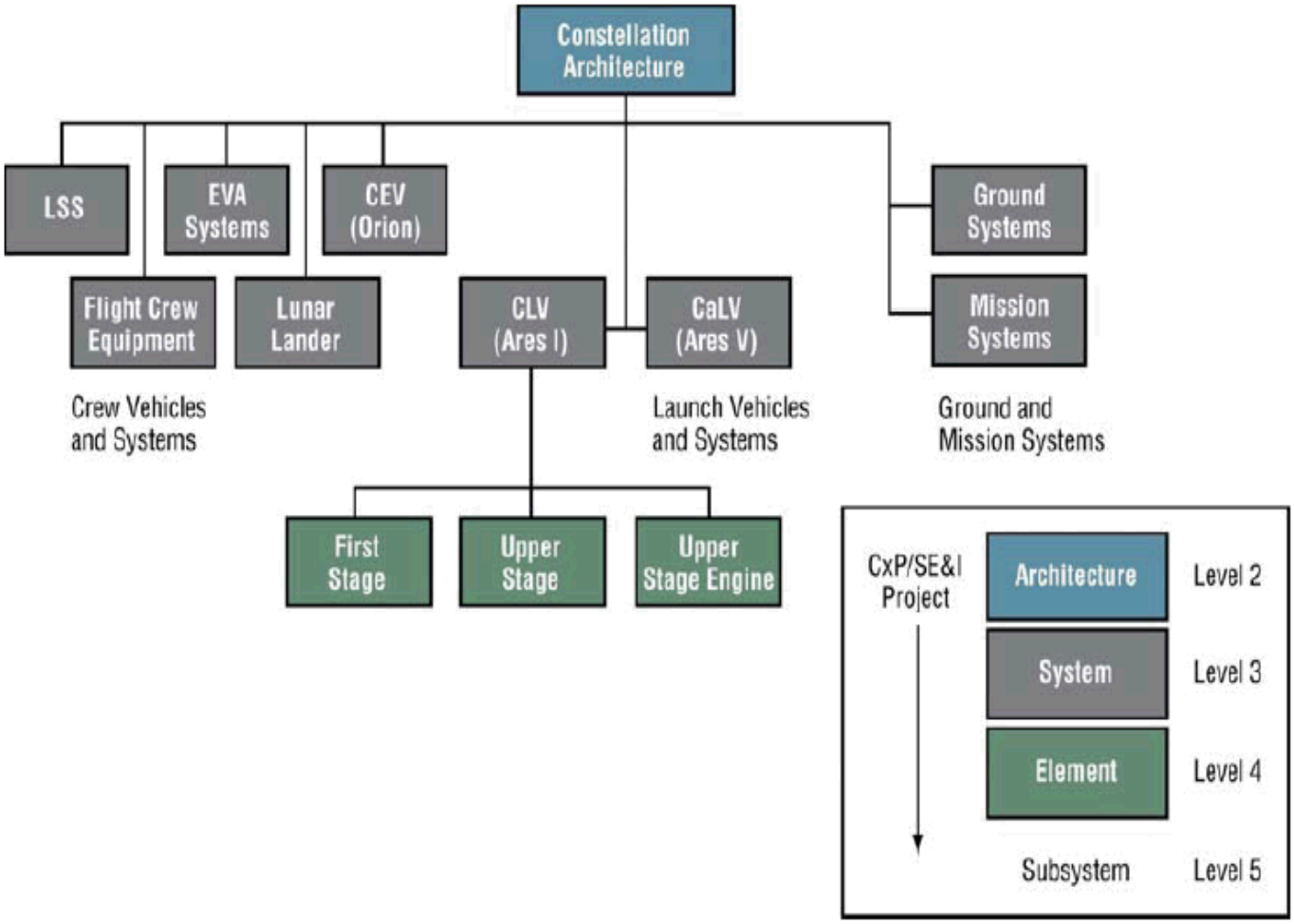

Figure 3