Integrated Safety Analysis Teams

Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: Integrated Team, Safety Analysis Processes

Abstract

Today's complex systems require understanding beyond one person's capability to comprehend. Each system requires a team to divide the system into understandable sub-systems which can then be analyzed with an Integrated Hazard Analysis. The team must have both specific experiences and diversity of experience. Safety experience and system understanding are not always manifested in one individual. Group dynamics make the difference between success and failure as well as the difference between a difficult task and a rewarding experience. There are examples in the news which demonstrate the need to connect the pieces of a system into a complete picture. The Columbia disaster is now a standard example of a low consequence hazard in one part of the system; the External Tank is a catastrophic hazard cause for a companion subsystem, the Space Shuttle Orbiter. The interaction between the hardware, the manufacturing process, the handling, and the operations contributed to the problem. Each of these had analysis performed, but who constituted the team which integrated this analysis together? This paper will explore some of the methods used for dividing up a complex system; and how one integration team has analyzed the parts. How this analysis has been documented in one particular launch space vehicle case will also be discussed.

Introduction

This paper draws on examples from National Aeronautics and Space Administration (NASA) programs and is applicable to forming teams in other industries.

The safety team discussed in this paper describes the team that the safety organization is responsibile for. It is recognized that the complete safety effort includes the design engineers and systems engineers that work diligently with safety to analyze the system. While working on a payload for the European Space Agency (ESA), the chief engineer was my greatest ally on the project and provided me a much greater understanding of electrical safety. Building this bond can be as important as organizing the safety engineers that make up the team discussed in this paper.

After the accident it is generally easier to see the integrated failure mechanism. Finding the interaction before hand is difficult. A number of cases are presented in the book "Normal Accidents," by Charles Perrow (Ref. 1), where many of today's high risk technologies are discussed. There are times when engineers have identified the integrated hazard, but the hazard is not considered realistic by management. This was evident in the Challenger accident where part of the engineering team was concerned with the conditions of the Solid Rocket Booster O-ring before the flight (Ref. 2), and the Columbia accident where some were concerned enough with the foam loss to investigate

means of determining if damage had occurred (Ref. 3). Having a well-respected team is important as well as being positively coupled with the engineering team.

Integrated Safety Analysis Team Disciplines

Complex systems involve electrical systems, mechanical systems, fluids, software, and human systems (operations). Each system must be understood individually, as well as its part in the system as a whole. One difficulty is finding safety engineers to fill the team ranks who have backgrounds in each of these areas. This difficulty is due to a number of reasons. One reason is engineering graduates generally desire to perform design work. A second reason is that the increase in the number of large government projects has diminished the available pool of safety engineers. Another reason is that in the past the need for a separate safety discipline was not well understood nor supported by the engineering community and academia. This means the safety discipline path was not available for engineers to pursue. This fact affects the constituency of the team. Where one might ideally prefer an even mix of disciplines, reality dictates that this is not possible. This leads to choosing flexible people who have an eager desire to learn and an interest in the product. This also requires that a mentoring situation be provided as well as an open team arrangement where discovering the hazards is a joint experience. Although most of the engineers on the design side of the projects are eager to teach and explain, they are often inundated with work and do not have the time to go into basics. In addition, the safety team is supposed to contribute to the design which is difficult with out basic experience in that field. With the shortage of safety engineers, the team will have to be populated with a large number of either non-safety experienced discipline engineers, or safety engineers without discipline experience. This requires that the team have a mix of experienced safety engineers, discipline engineers, a willingness to share the workload, and a spirit of camaraderie.

Integrated Safety Analysis Process

In order to understand how safety analysis is divided, one must understand how a Program is broken down. NASA typically organizes safety in terms of a Program; for example, the Space Shuttle Program, the Apollo Program, and the Constellation Program. The Programs are considered Level II. Each Program consists of projects; for example, within the Constellation Program, there is the Ares project (the launch vehicle), and the Orion project (the crewed portion). These projects are considered Level III. There are other projects as well in the Constellation Program. The Ares project is also divided organizationally into three elements: Upper Stage, Upper Stage Engine, and First Stage (Fig. 1). Level I is Headquarters (HQ) where the top level NASA requirements are kept.

In the past NASA has taken two basic approaches to the Shuttle and Payload/Station safety process. Each approach organized differently to respond to the requirements, but each having a separate safety organization working in conjunction with the design team. The Shuttle approach is a System Based approach added by engineering after the Columbia accident. The Payload/Station approach is chaired by program integration with discipline membership (engineering, safety, and operations). The Constellation project

uses a safety panel, the Constellation Safety Engineering Review Panel (CSERP). CSERP originally reported to program management, but is now under the auspices of Safety, Reliability and Quality Assurance. The safety team presents the hazard analysis to the CSERP in phased reviews which are in proximity to the project milestone reviews. This ensures the support and participation engineering. engineering.engineering. At each level there are multiple independent lines of communication to NASA upper management (e.g., Center Directors, HQ S&MA Director) by various means of Chief Safety Officers and the Directors of the safety organizations.

Each of these processes has a commonality in that they require hazard reports to be generated. A hazard report contains a top level hazard, the list of causes for that hazard, a list of controls for each cause, verification for each control, and other supporting data; such as, pertinent portions of fault trees, retention rationale, references to the Failure Modes and Effect Analysis/Critical Item List, and indication of risk. These reports, when taken together, should reflect the entire set of hazards to the vehicle. The analysis process is not only to document the controls that are in place, but also to help drive the design by discovering hazards that are not controlled and by providing feedback to the design organization. This process also provides management information on how much risk they are accepting and where the areas of open work are.

Integrated Safety Team Responsibilities

One consideration in delineation of responsibility is division of labor between the parts of the task. For Ares, the team has a division of labor. There is a lead/facilitator, one graphical analyst that is responsible for leading the fault tree effort, several design interface/analysts, a report champion, and an engineering interface. Although each of the team members must have these skills, at least one member must excel in each of these tasks. Knowing what is needed and where the short fall is will help to shore up any weak areas.

The lead/facilitator is generally one person, but sometimes the facilitator role is passed to another while other aspects of the safety organization are considered; such as, changes to requirements, special studies, Level II schedule, and management. For the Ares program, the lead monitors the overall health of the safety team and performs the task of obtaining resources to support the team as well as acting as an interface with management to work out the problems encountered. The facilitator works with the team day-to-day on hazard analysis to solve the technical issues, work out consistency, and integrate the findings of the other team members. The whole team must be looking for the cross element integrated hazards, but this role of facilitator is particularly important in understanding past failures as well as having a certain “paranoia” towards complex system interactions.

The graphical analyst role in the team is crucial. There are many methods of performing graphical analysis, fault trees, fish bone diagrams, and event trees. It is important to have someone willing and capable of performing this sometimes tedious work. The person must be consistent and able to see across element lines. For Ares, there is one person who keeps the fault tree and works with all safety analysts so that the fault tree supports

the analysis activity. The fault tree provides consistency in documentation, an understanding of the hazard, and is an aid in explaining the hazard to those who must review the analysis. The fault tree is also useful in finding connections and similarities across the hazard reports.

The design interface/analysts works with the project on trade studies, supports meetings, provides input to design, and performs the safety analysis with supporting fault trees. This part of the team has the most members and those fulfilling the facilitator role have also performed this task as well. The analysts work with the element safety engineers as well as the design engineers. Since hazard reports cut across element lines, they interface with all the elements. In order to keep the team from being inundated with the element safety reviews, one analyst will be assigned to an element to attend the review, to provide feedback to the team, and inform integrated hazard report owners when a subject of interest is coming up in the review. In addition to the element reviews, there are other reviews such as Ground Operation Systems and Orion reviews that are covered in similar fashion.

The report champion ensures the safety effort is properly documented and provides the risk insight to those who make the decisions. Every safety team has an oversight organization which reviews risk and is one of the customers for the documentation. For the Ares Vehicle, it is the CSERP and the project manager. The CSERP requires an integrated data package to be delivered with fault trees, design discussions, safety analysis, and hazard reports. A report and a presentation have to be created for the CSERP.

The Engineering interface is a person provided by engineering to work with the team and provides the link to the engineering personnel needed to perform the work. This person provides engineering information and perspective to the safety team as well as the safety products to engineering. They also present briefings at Technical Interchange Meetings and reviews.

Analysis Approach

Dividing up the hazard analysis and subsequent hazard reports consists of choosing between a discipline (electrical, mechanical, etc.) approach, an element (Upper Stage, Upper Stage Engine, First Stage) approach, or a hazard category approach. Division by discipline and element is a common engineering issue found in all organizations, which typically leads to the matrix approach where either the discipline manager or the element (or product) manager has control of the budget. In this case, we were free to choose which approach was the best with out the budget issue bydividing the team by hazard using a hazard checklist, explosion, loss of control, loss of structural integrity, loss of function, etc. (Fig 2).

The Ares Integration Safety team breaks up the hazard reports by hazard category. The reason for breaking up the hazard reports by hazard category is because the element hazard reports, which the team is integrating, are based more on hazard category than

discipline. The Ares team itself could have been divided several ways: by discipline, by element, by hazards, or by some combination, each having its own advantage. Each of the elements of the Ares vehicle has a team with safety engineers broken up in different manners. Part of this element team breakup that affected the team interface and analysis was that fact that contractors are designing the First Stage and Upper Stage Engine. The Upper Stage is being designed in-house. The integration of the Ares Vehicle is also being done in-house. Interface with the Upper Stage safety team has the advantage of the team being easily accessible, as well as reduced contractual interfaces in data exchange Dividing the integration team by element has been easy in terms of interface, but major element issues that need to be identified could be missed. Dividing the team strictly by discipline could have lead to difficulties in integration of the findings into hazard categories. The past two manned space flight failures were cross disciple hazards which fit into hazard categories. Challenger was fire/explosion of one element caused by leakage of a separate element. Columbia was a structural failure caused by debris from a different element. Lack of full coverage of each discipline also made the disciple approach less viable. The Failure Modes and Effects Analysis, which is being done by the reliability group, tends to be element oriented. Therefore, breaking up the hazard analysis by hazard category is a view which would have been lost if the element division approach would have been used. Another driving factor came from the way the hazard reports were broken up. Having multiple members responsible for any one hazard report would have led to the need to perform an additional integration activity.

Training is essential since several of the engineers have not worked NASA safety programs before. The team meets most mornings to work through issues and specific hazard reports as they are created or updated This provides the opportunity for questions to be raised and general information or instruction to be passed on to the team.

Conclusions

When assembling a safety team there are times when the choice of team members is limited. Therefore, creativity is needed to work within the constraints. Selecting people that are motivated and eager to learn, combined with an open team atmosphere that allows training, is one answer to the problem. Choosing how the work is divided, both functionally as well as how the hazards are broken up, can limit confusion and reduce the number of interfaces to a workable level. In any case, integrated hazard analysis is an essential part of any complex system.

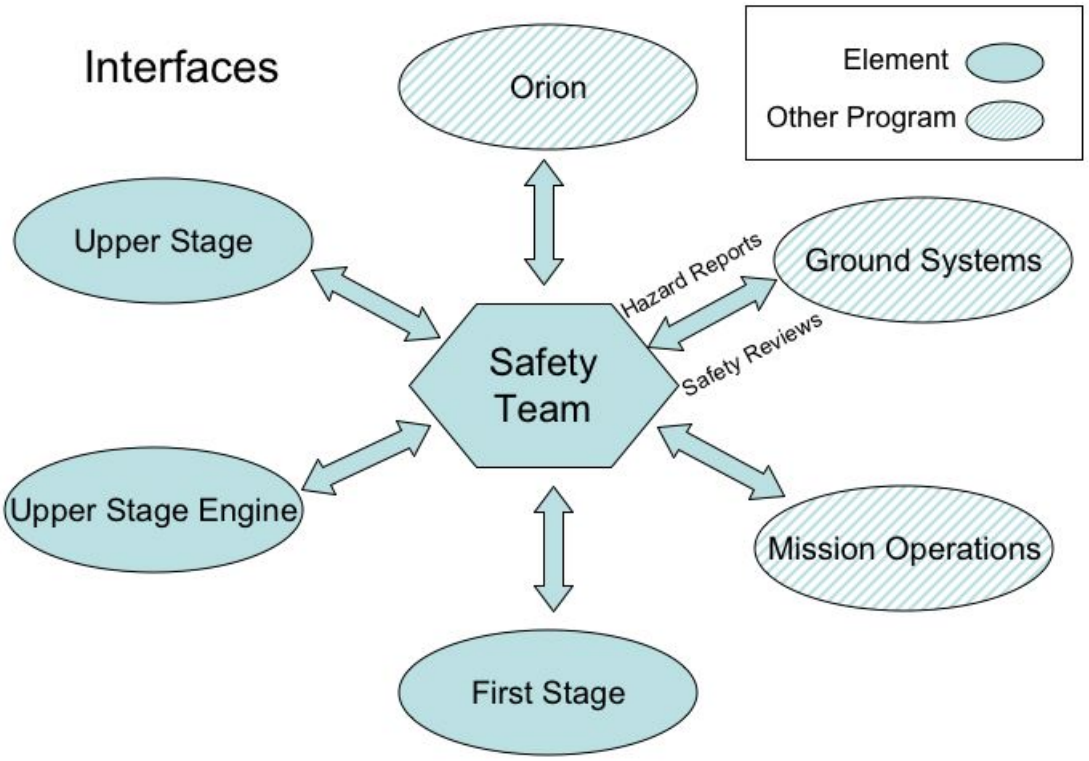

Figure 1 – Integrated Analysis Interfaces

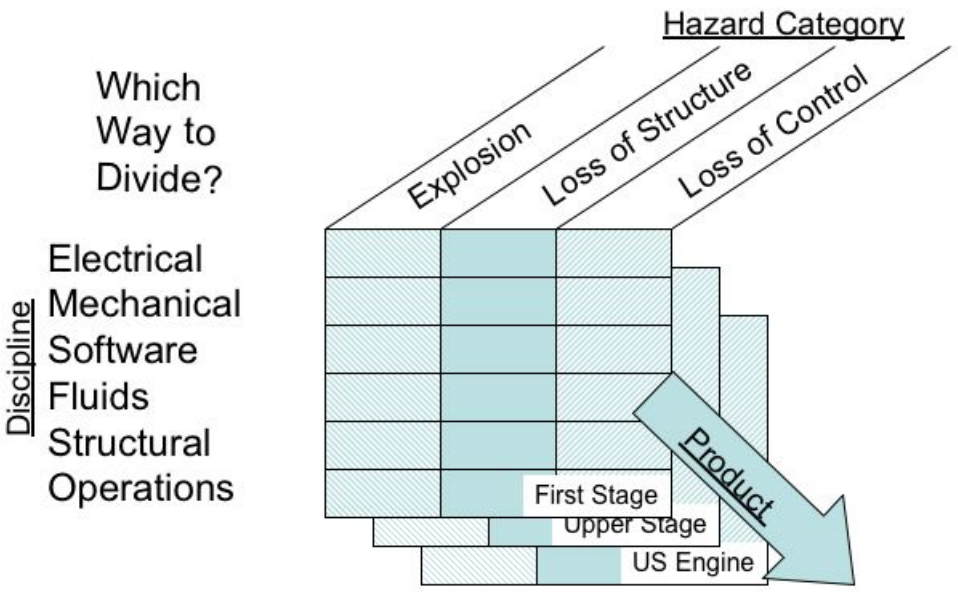

Figure 2 – Dividing Hazard Analysis

References

Reference 1: Charles Perrow, "Normal Accidents"

Reference 2: pg 303, chapter 37, Claus Jensen "No Down Link"

Reference 3: Columbia Accident Investigation Report (CAIB) Paragraph 6.3 pg 140

Biography

Jon Wetherholt Building 4203, QD 34, George C. Marshall Space Flight Center, Marshall Space Flight Center, Alabama, 35812. Phone Number 256-544-4847. Email jonathan.c.wetherholt@nasa.gov.

Jon Wetherholt started working at NASA Lewis Research Center in 1983, on the Shuttle/Centaur Project and the Space Station Power System for SR & QA. He left NASA to work for the European Space Agency for two years on Spacelab payload safety analysis. He returned to NASA Lewis as a Systems Engineer and safety engineer on various payloads flown on the Shuttle and the International Space Station. During this time he led several teams in performing safety analysis. In 2005 Jon moved to Huntsville, Alabama, to support the Marshall Space Flight Center Constellation Program as a Safety Engineer.