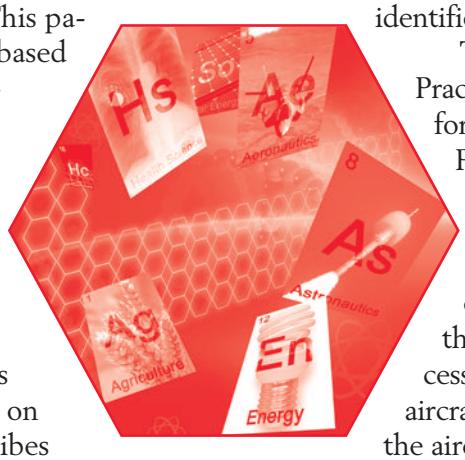
A Structured Scenario-Based Approach for Performing Functional Hazard Identification Analyses

by Tom Woodbridge
Satellite Beach, Florida

Several industry standards call for performing a functional hazard analysis as an early step in the overall hazard analysis process. This paper describes the structured, scenario-based approach for a functional hazard identification analysis used by the NASA Constellation Program's Level 2 Ground Integration Hazard Analysis Team. The team used this method to determine system functions and identify the hazards associated with the Constellation Ares I rocket while on the launch pad. This paper provides examples from the analysis performed on the Ares I Crew Launch Vehicle, describes the method and offers a summary of the hazards uncovered by the method per vehicle stage. This method is applicable for identifying hazards in all types of systems and system integration scenarios. Lastly, while this functional hazard identification analysis approach has its advantages and should be in the safety engineer's analytical toolbox, this paper also touches on the approach's limitations.



Introduction

The desire and goal in conducting a system safety hazard analysis is to identify all hazards associated with the functions of a system. When the system becomes increasingly complex — as in aerospace vehicles, aircraft and naval ships, as well as chemical and petroleum plants — achieving this goal becomes difficult.

Traditionally, safety analysts obtain what information they can about the system via available drawings and operations concept documents, and then use a hazard checklist to help identify hazards to assess in a Preliminary Hazard Analysis (PHA). However, this approach is rather unstructured and can lead to grave omissions in identifying all hazards associated with a complex system. Wilkinson and Kelly [Ref. 1] characterize the use of hazard checklists as reactive, rather than a proactive approach to identifying hazards.

The Constellation Program Hazard Analyses Methodology document CxP 70038 requires performing a functional hazard analysis (FHA) for each design reference mission (DRM) for the NASA Constellation Program and lists ARP4761 as a reference document for performing hazard analyses [Ref. 2]. It requires the analysis of the integrated vehicle to use the integrated hazards identified in the program's FHA.

The SAE Aerospace Recommended Practice, ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, states that a functional hazard assessment or FHA "is conducted at the beginning of the aircraft/system development cycle" and "is the first step in a safety assessment process that is performed on new or modified aircraft programs" [Ref. 3]. It is performed at the aircraft systems level during the concept development and preliminary design phase. The FHA identifies the failure conditions and hence the hazards associated with the aircraft functions. Per guidance in ARP4761 and EUROCONTROL, the FHA provides the first step in the safety process and offers input for conducting the preliminary system safety assessment (PSSA) [Refs. 3 & 4].

The use of the functional hazard assessment as required by the FAA has been around since the early 1980s or earlier [Refs. 5 & 6]. There are two approaches for conducting an FHA: One is a brainstorming method and the other is a systematic method [Ref. 7]. ARP4761 and ANSI/GEIA-STD-0010 outline systematic processes for performing a functional hazard analysis [Ref. 8]. The general process is to identify all functions of the system under analysis, identify failure conditions associated with the functions, assess the effects of the failure condition, classify the failure condition effects and develop the appropriate safety requirements and verifications.

This author performed system assurance analysis (SAA) on many space shuttle ground support equipment (GSE) systems over a 15-year period. The SAA combines the FMEA, fault tree and hazard analysis into a single document. Per NSTS 22206, prior to performing failure mode and effect analysis (FMEA) on a system or subsystem, the analyst is to perform a criticality assessment (CA) [Ref. 9]. The CA identifies all of the inputs and outputs of the interfaces a system or subsystem has, determines their function, and performs an analysis of the worst-case effect of a functional failure or malfunction. The CA calls for the analyst to consider "failure to

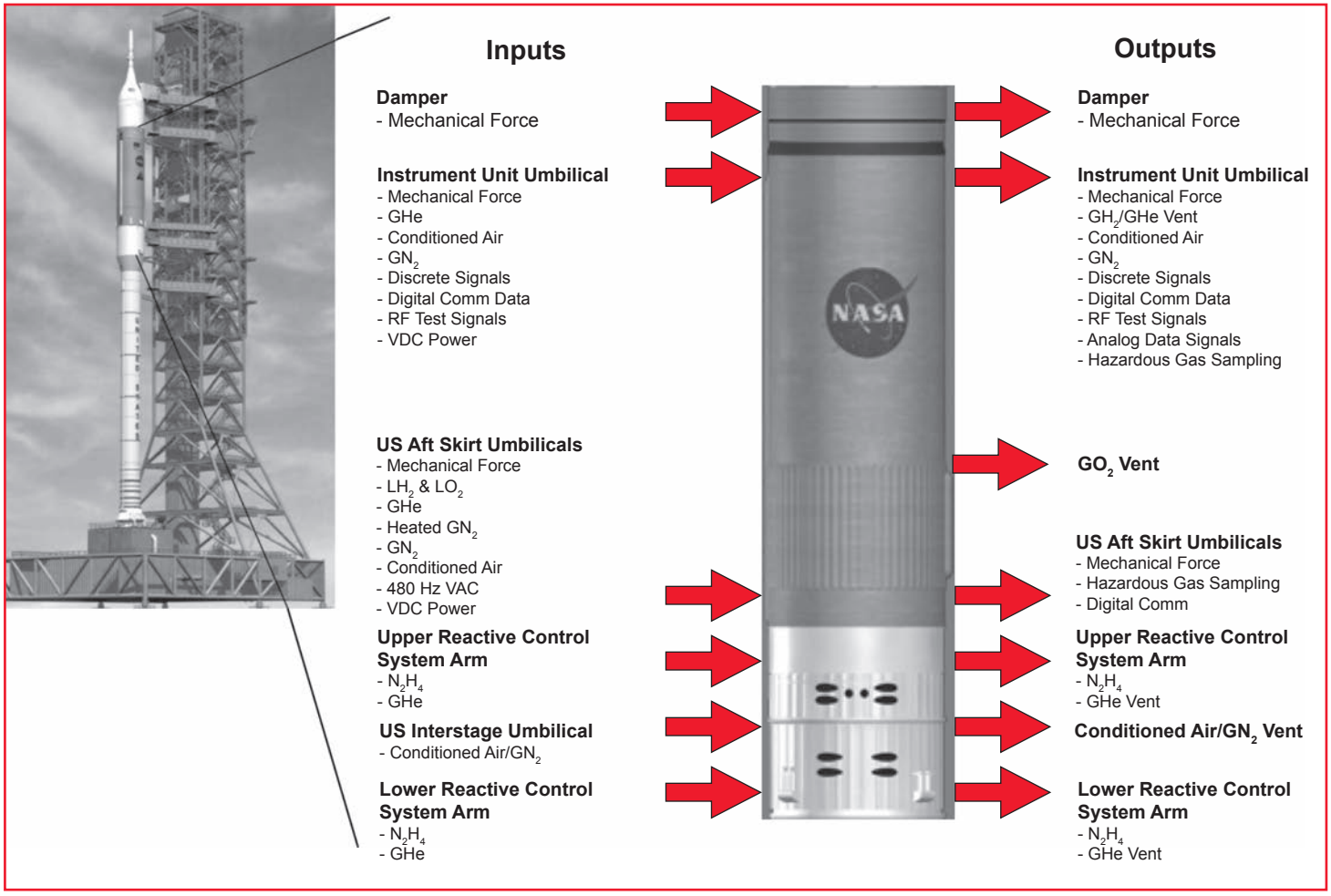


Figure 1 — Inputs/Outputs Integrated Ares Upper Stage and Launch Pad Ground Systems.

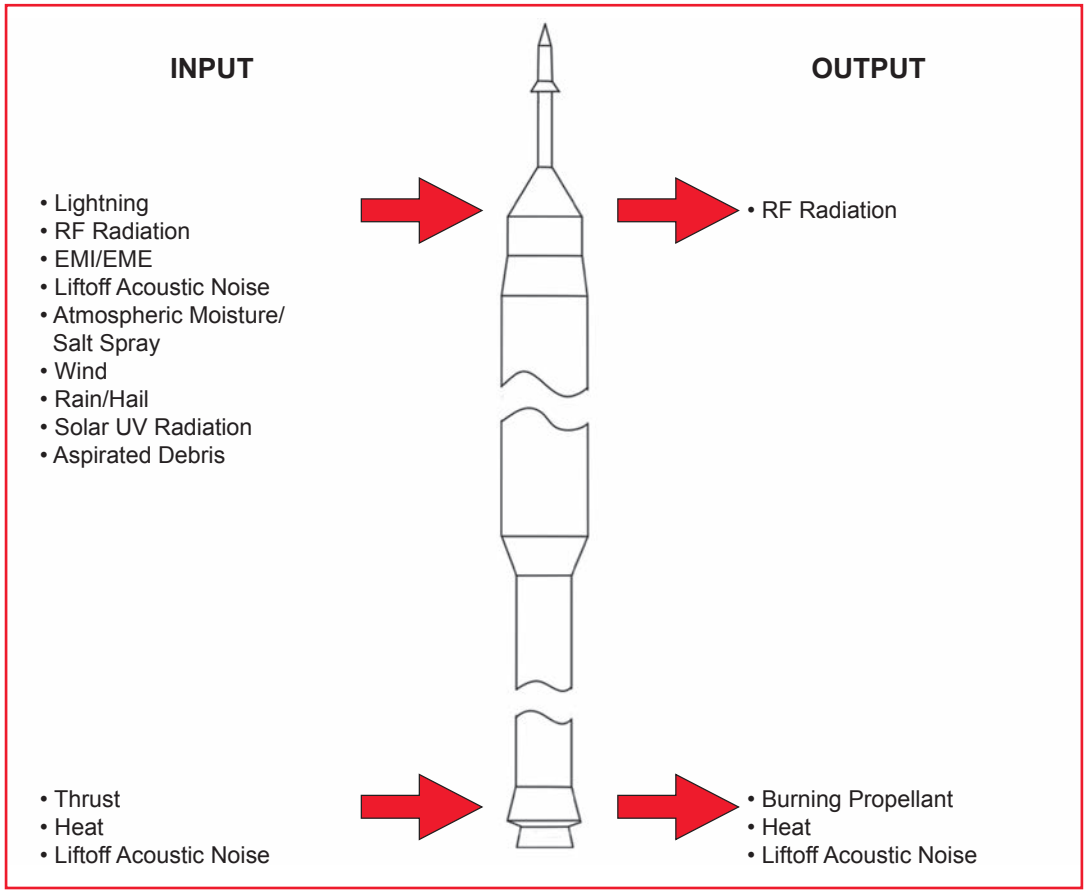


Figure 2 — Inputs/Outputs Natural and Induced Environments on the Launch Pad.

operate on time, failure to cease operation on time, failure during operation, and premature operation" in determining a specific loss statement for each output function. The CA also assigns a classification (critical or non-critical) for each failure or malfunction's consequence.

In September of 2009, a new Level 2 Ground IHA Team formed. Its task was to be responsible for the hazards associated with the integration of the launch pad ground systems and the Ares/Orion crew launch vehicle (CLV). Although an overall program-level functional hazard analysis was performed about a year earlier by the Constellation Program, the Level 2 Ground IHA Team did not include anyone that participated in that earlier FHA effort, and all members were new to the Ares/Orion CLV design. The team decided to perform a new FHA, concentrating only on the interfaces between launch pad ground systems (GS) and the Ares/Orion CLV.

The Level 2 Ground IHA Team used a structured, scenario-based functional hazard analysis approach, which was derived from the functional hazard analysis direction given in ARP4761 and the criticality assessment methodology per NSTS 22206 that was used in the space shuttle ground operations SAAs. Because this method identifies only potential hazards and does not include other parts of traditional hazard analyses, such as hazard controls or verifications, it is dubbed a functional hazard identification analysis (FHIA). There are two goals for this approach: Provide a structured method for each team member to learn their assigned portion of the GS - Ares/Orion CLV integrated functions and identify top-level integration hazards associated with these functions. With this method, and using brainstorming, the team was able to find a number of hazards not identified by the previous FHA that was conducted.

As covered by Ericson in his book *Hazard Analysis Techniques for System Safety*, the FHA identifies system hazards by evaluating the safety impact of functional failures [Ref. 10].

FHIA: Identifying System Inputs and Outputs

The first step in almost all problem-solving efforts is to draw some form of a picture or diagram to help in understanding the problem. Therefore, the first step in the FHIA is to create a diagram that identifies the system/subsystem boundaries and input/output commodities/functions that cross each boundary. It is important to note that while the FHIA may resemble a failure modes and effects analysis/failure modes, effects, and criticality analysis (FMEA/FMECA), this method addresses functions and not necessarily specific hardware failure modes.

The FHIA that the Level 2 Ground Integration hazard analysis team performed was specifically looking for hazards associated with the umbilical interfaces between the ground and launch vehicle and spacecraft. However, this method is applicable to any system or integration of systems, and is not limited to launch vehicle and the launch pad hazard identification. Figure 1 shows an example of an input/output block diagram of all the interfaces between the launch pad ground systems and the Ares Upper Stage.

Input/output diagrams can also help address hazards occurring from surrounding natural and induced environments (e.g., radiation, launch vibrations, launch acoustics, lightning, electromagnetic, etc.), as Figure 2 shows.

The structured, scenario-based functional hazard identification analysis consists of the following considerations. Practitioners should assess each individual commodity and physical interface to identify its function.

- Determine the function for each time the commodity changes state. The same commodity/interface can have different functions for different times during its use
- Using the function statement should also answer questions such as, "Why is it needed?" "Why is it being turned on/off at this time?" "Why is speed increased or reduced?"

For each function and timeframe, assess the effect of each of the following six scenarios:

- Starts operating prematurely
- Stops operating prematurely
- Does not start operating at the prescribed time
- Does not stop operating at the prescribed time
- Does not operate within specification (i.e., operates at incorrect speed, temperature, pressure, purity, voltage, etc.)
- Does not contain or store energy or fluids

A similar set of scenarios is:

- Starts operating prematurely
- Starts operating late
- Stops operating prematurely
- Stops operating late
- Does not operate within specification (i.e., operates at incorrect speed, temperature, pressure, purity, voltage, etc.)
- If applicable, does not contain or store energy or fluids

Note that a system which does not operate at the prescribed time or stops operating prematurely encompasses the scenario of not transmitting energy or fluids.

It is important to keep in mind that the assessment is on the interface functions and is not concerned with

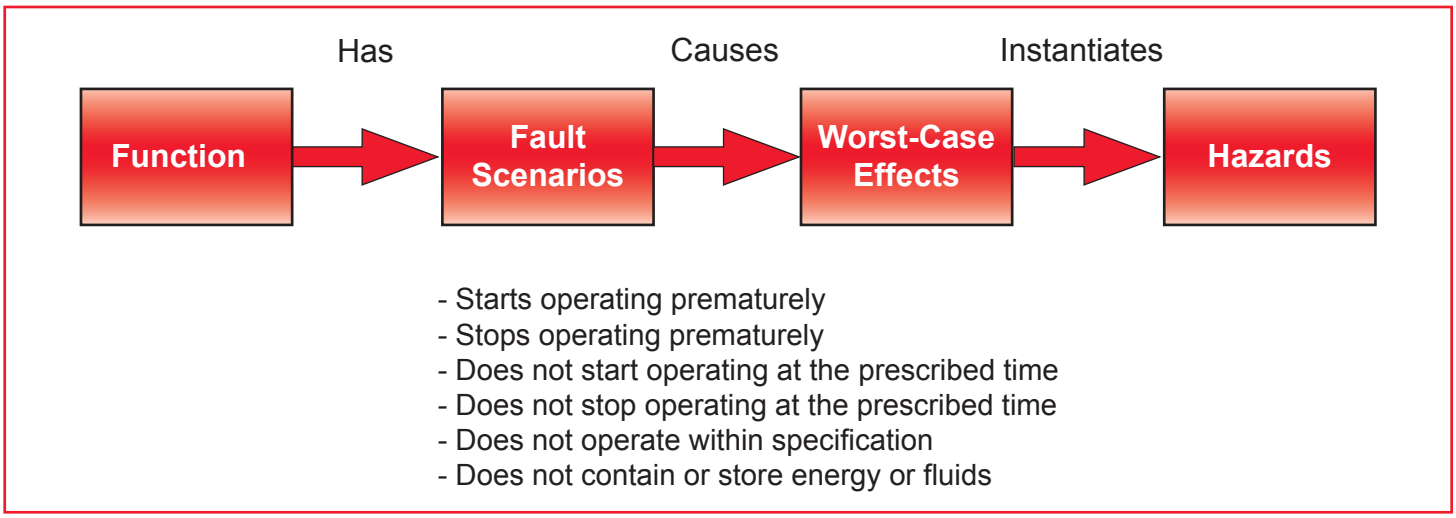


Figure 3 — Functional Hazard Identification Analysis Process Diagram.

Table 1 — Functional Hazard Identification Analysis Table Format Example.

Functional Hazard Identification Analysis Table					
Input/ Output	Time Period	Function	Effect of Failure/Hazard if Function a. Starts operating prematurely b. Stops operating prematurely c. Does not start operating at the prescribed time d. Does not stop operating at the prescribed time e. Does not operate within specification (incorrect speed, temperature, pressure, purity, voltage, etc.) f. Does not contain or store energy or fluids	Hazard Statement	Hazard Severity Level

specific component failure modes. Also, these scenarios do not require a fault or failure to occur.

The FHIA should perform a separate set of scenario assessments for each timeframe in which the function operates or changes state, as well as during times when the function must not inadvertently operate. The assessment of each scenario determines the potential worst-case effect, assuming that no redundancy is in place and no detection/correcting action occurs.

The description of the effect of each scenario should provide the chain of events, as applicable, that could lead to the potential worst-case effect. The description of the effect could be a hazard condition that, with no detection or correcting action, could allow a critical mishap or accident to occur. The analyst should describe how the hazardous condition could lead to a mishap or accident.

Review of a hazard checklist may be helpful in determining the worst-case effect. It is acceptable to combine operational timeframes if the function and the worst-case failure effect is the same.

The next step is to create a Hazard Statement for each scenario that results in a critical or catastrophic effect. The hazard statement should include a short description of the hazard, including the consequence, so that the statement makes sense on its own without requiring additional information to explain it. A generic hazard statement is a summary of multiple, but similar, scenario effects — it can be in the suggested form of, "The (system) (does what? What requires control?), resulting in (consequence(s)." This suggested hazard statement format comes from the hazard title format used in the NASA CxP 70038 hazard analyses methodology document [Ref. 11].

Note that not all interfaces will be associated with a potential hazard cause; some may be associated with hazard controls. An interface that provides hazardous gas leak detection is an example of this. Lastly, the FHIA should assign a hazard severity rating for each hazard statement, based on the worst-case effect.

Figure 3 gives a graphic depiction of this hazard identification process.

The analyst can also use a table format similar to that shown in Table 1 or some other suitable format to perform the analysis.

Table 2 — Example of FHIA Output.

Top Level Hazard Statement	Intermediate Hazard Event Statement	Functional Faults/ Hazard Cause-Event
Ignition of flammable vapors and atmospheric oxygen in or near the vehicle results in a potential for an explosion and loss of crew and vehicle	Ignition of possible explosive environment inside the US Instrument Unit results in loss of life and/or vehicle	Excessive ground supplied voltage to a vehicle component can create an electric short.
	Improper GN_2 flow to the First Stage aft skirt area negates effectiveness of purge, allowing the hazardous accumulation of hydrazine vapors in the nozzle area and a possible explosion upon motor ignition and loss of crew and vehicle.	The purge to the FS aft skirt does not start at the required time, stops flowing prematurely, or flow at an insufficient rate.
	Loss of or insufficient GN_2 to provide an inert environment for the Orion SM/SA may allow an explosive atmosphere to form in a shared compartment and a potential for fire explosion.	The purge to the Orion SM/SA does not start at the required time, stops flowing prematurely, or flows at an insufficient rate.
	Loss of crew and vehicle from inadequate ECS purge, allowing an explosive atmosphere to form in the Service Module area	A damaged umbilical plate allows the ECS purge to leak between the ground and flight plates at levels that exceed specification.
		Premature loss of the force holding the ECS ground and flight halves tightly in place will allow the ECS to leak between the ground and flight plates at levels that exceed specification.
	Loss of life and vehicle from ignition of hazardous GH_2 environment created by a GH_2 leak into the Instrumentation Unit Umbilical Plate cavity	Premature loss of or improper operation (binding) of the Instrument Unit (IU) Umbilical arm compliance ability to track the wind-induced swaying of the vehicle, causing damage to the GH_2 Vent interface between the ground and flight plates.
		A failure causing the GHe IU Umbilical Plate Purge to stop operating prematurely, not start at the prescribed time, or flow at an insufficient rate.
		Improper connection of the LH_2 Tank Vent QD ground and flight halves.
	Loss of life and vehicle from ignition of hazardous GH_2 environment created by a GH_2/LH_2 leak into the LH_2 Umbilical Plate cavity	Premature loss of or improper operation (binding) of the LH_2 Umbilical arm compliance ability to track the wind, induced swaying of the vehicle, causing damage to the LH_2 Fill/Drain interface between the ground and flight plates.

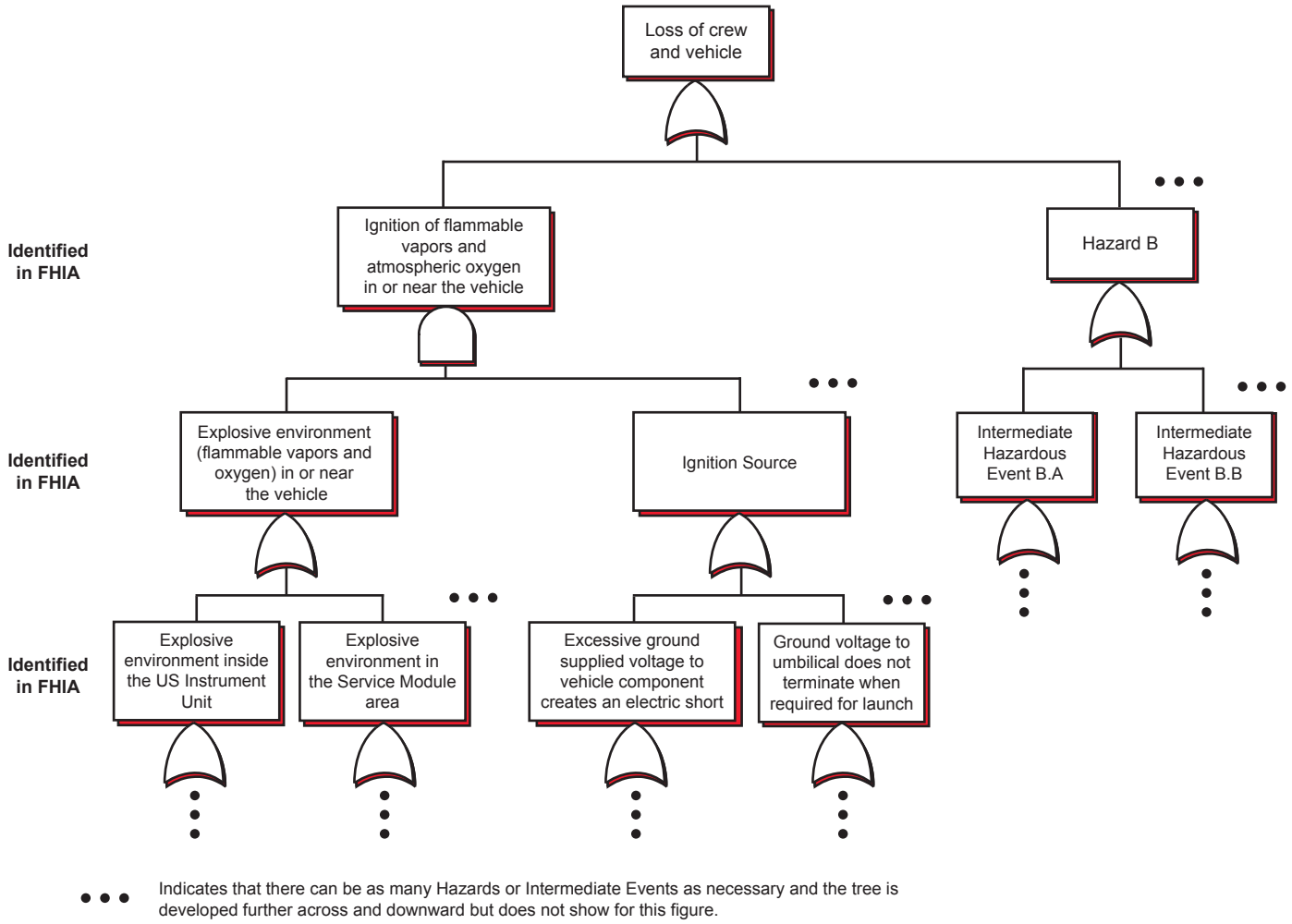


Figure 4 – Example of FHIA Input to Fault Tree.

FHIA Output

When the FHIA table is complete, it provides a raw list of hazard statements and their integration or system/subsystem-level causes. The analyst can then combine similar hazard statements to reach a more generic or higher-level hazard statement if deemed necessary. As Dr. Nancy Leveson states in her book, *Engineering a Safer World*: "Even the most complex system seldom has more than a dozen high-level hazards, and usually less than this" [Ref. 12]

Table 2 shows an example from the Ares I FHIA of how the individual functional faults in the FHIA "tree" up to intermediate hazard statements, and then up to a common top system-level hazard. These hazard statements and intermediate causes provide the input for the fault tree and the rest of the hazard analysis process. Because the FHIA assumes no interrelation between the hazardous events, the fault tree also provides logic between the individual intermediate hazardous events not addressed in the FHIA. Figure 4 shows an example of a fault tree using the FHIA hazard statements and the associated functional faults to help start building the top levels of the fault tree.

The outputs of the FHIA also help identify where more detailed analyses, such as subsystem hazard analyses or FMECAs, are necessary and, for scenarios that do not lead to a hazardous condition, where deeper analysis is not necessary.

When continuing with the fault tree and further hazard analyses, keep in mind that a cause or intermediate event, which could make one of the six scenarios occur, does not have to be from one of the scenarios in the FHIA. A cause of intermediate event could result from other circumstances the FHIA does not cover. This is explored a bit more in the "Limitations and Drawbacks to the FHIA Method" section.

The FHIA is a living document and should be continually updated as new information becomes available,

Table 3 — Ares I – Ground Integration FHIA - By the Numbers Summary.

Summary Description	Number
Total individual raw Functional Failure/Hazard Statements Associated with GS-Veh Umbilical Integration at the Pad	386
Unique Hazard Statements Associated with GS-Orion Umbilicals at the Pad	27
Unique Hazard Statements Associated with GS-Upper Stage Umbilicals at the Pad	100
Unique Hazard Statements Associated with GS-First Stage Umbilicals at the Pad	21
Unique Functional Failure/Hazard Statements Associated with Umbilicals for the GS and integrated Veh at the Pad	138*
Hazards Associated with GS-Veh Umbilical Integration at the Pad	66

* There are a number of hazard statements, such as premature release of umbilicals, that are common for all of the vehicle elements, which is why the sum of the unique hazard statements for each vehicle element (147) is not the same as the number of unique statements associated with the ground system and integrated vehicle at the launch pad (138).

as the design matures or for design modifications. Table 2 shows an example from a portion of the Ares I FHIA, of how the individual raw hazardous events roll up to a more generic hazard statement.

The purpose of the Ground Integration Hazard Analysis Team's fault trees was to identify potential hazard causes at each side of the interface. These became transfer events to the Ground System and Flight Vehicle elements (crew/service module, upper stage, first stage), and provided the Level 2 Integration's team mechanism for ensuring linkage coverage between the ground system and flight vehicle elements.

NASA used a hazard report format for verification that the interfacing ground and vehicle project had coverage of the hazards in their analyses. For each hazard cause the integration fault tree identifies, the Level 2 Hazard Report's mitigating control field identified the appropriate ground or flight vehicle hazard report, thus providing a link from the integration analyses to the lower-level analyses. For each hazard cause, the Level 2 Integration Hazard Reports also identify the safety requirements and, where applicable, mitigating controls owned by NASA's Level 2 organization.

Summary of Constellation Program Level 2 Ground Integration FHIA Results

Using this method, the Level 2 Ground Integration Hazard Analysis Team identified 386 individual functional hazard statements associated with the integration of the ground systems and vehicle systems across the umbilical connections at the launch pad. Because a number of the individual raw hazard statements are similar, as shown in the previous section we grouped the similar hazard statements under an appropriate unique functional hazard statement, and then grouped the unique hazard statements under a more generic hazard.

The upper stage, with its cryogenic and high-pressure pneumatic tanks that require servicing via umbilical connection with ground systems, contains the most hazards. The FHIA identified 100 unique hazard statements associated with the upper stage/ground system umbilical connections.

The Orion capsule and service module receive minimal servicing at the launch pad and were the next most hazardous part of the overall vehicle, with 27 unique hazard statements. Although the Orion capsule and service module contain hypergolic and high-pressure pneumatic tanks, the vehicle arrives at the launch pad with these already filled and pressurized. Therefore, the umbilical between the service module and the launch pad does not contain connections for servicing these commodities and the corresponding hazards occur at the processing facility, rather than at the launch pad.

The first stage contained the fewest hazards associated with the launch pad umbilical connections, with 21 unique hazard statements resulting from the FHIA. For the integrated vehicle, the individual hazard statements from the vehicle elements join and condense down to 138 unique hazard statements covering 66 hazards.

For reporting purposes, the 66 hazards were grouped into a smaller number of hazard reports covering common effects and time periods, such as "pressurization or fill errors during cryo tank load/drain operations causes vehicle structural damage and catastrophic failure leading to loss of life and/or vehicle." These hazard reports can also include inherent hazards that the FHIA method may not identify.

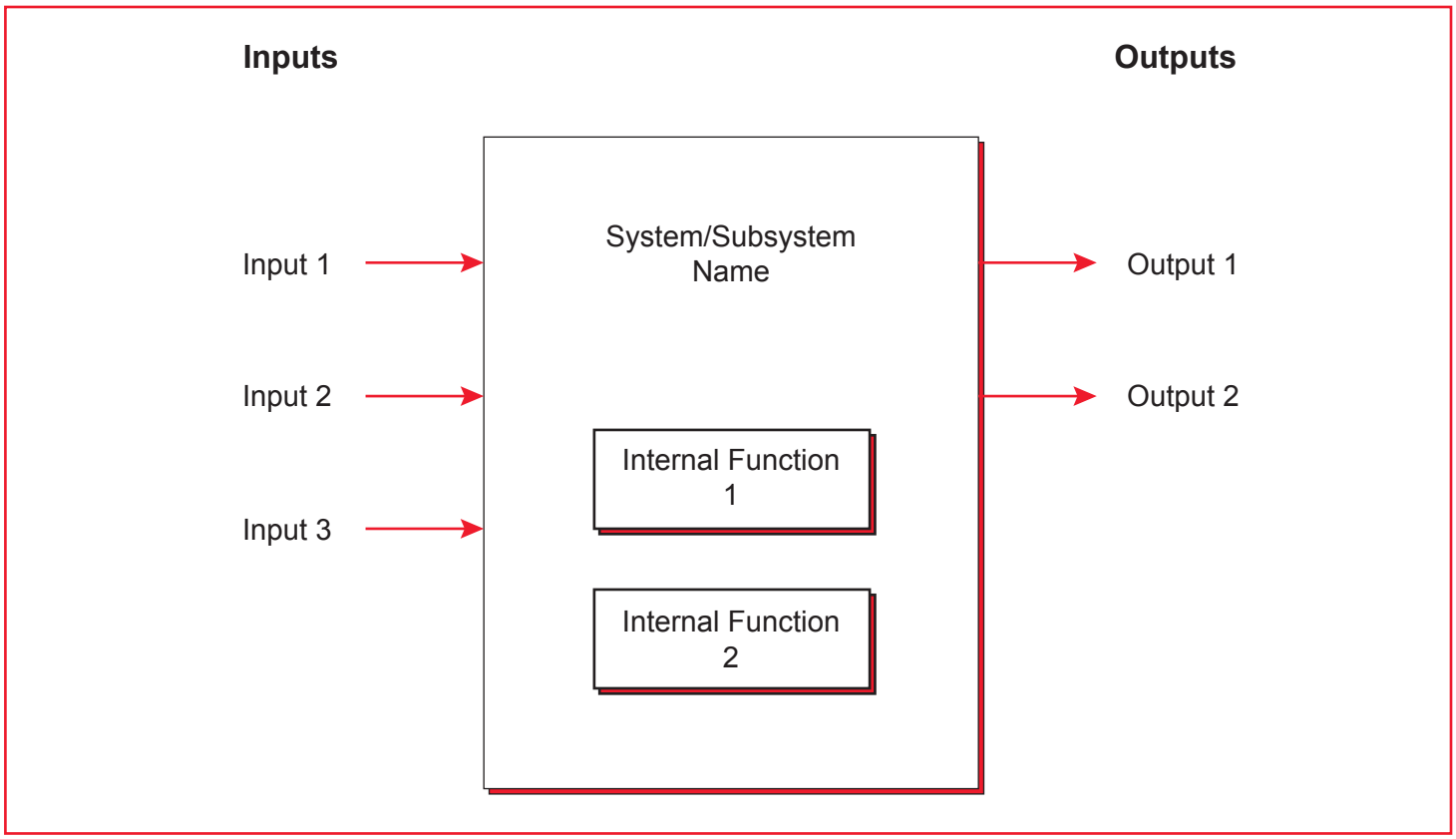


Figure 5 – Inputs/Outputs Diagram with Internal Functions.

Limitations and Drawbacks to the FHIA Method

The program-level hazard analysis efforts to identify integration hazards also used other traditional preliminary hazard analysis methods to identify other hazards related to the launch vehicle and not necessarily associated with the interface between the ground umbilicals and the vehicle. Examples of such hazards with the Ares I Crew Launch Vehicle are:

- Uncontained failure of the first stage auxiliary power unit (APU)
- Cabin fire
- Liquefaction of N_2 in the instrumentation unit (IU)/LH2 tank crotch can cause insulation foam on outside of IU to come off in flight
- Inadvertent operation of the launch abort system

Therefore, this method has limitations in that it does not necessarily uncover hazards outside of the realm of functions at the chosen interface, or those that may be inherent in normal operations.

A drawback to the FHIA method is that it takes dedicated effort and time to meticulously evaluate each item in the interface to determine its functions for the different times or phases of system operation, and then assess the potential faults and resulting effects.

Expand FHIA Coverage When Possible

To help address the limitation of looking only at the system/subsystem interface boundaries when performing an FHIA, if the system or subsystem under analysis is not overly complex, the analyst can expand the coverage of the analysis to add a section for internal functions in the FHIA analysis. Figure 5 shows internal functions blocks in the input/output diagram.

Conclusion

The FHIA method provides systematic, comprehensive examination of a chosen system's interface to determine system functions, and then to identify and classify the hazardous effect of improper operation of those functions according to their severity. It is important to note that the improper operation of a function does not need to be caused by a failure in the system and that the main purpose of the functional hazard identification analysis is to identify hazards. Although it identifies top-level function faults and hazardous events, the FHIA does not identify basic hazard cause events; it does, however, provide excellent starting points for further fault tree and hazard analyses.

Advantages of this FHIA method include:

- A structured systematic approach makes the analyst go through each individual interface to determine its functions and hazards. Doing so means the analyst is less likely to overlook less obvious hazards.

- The process gives the analyst a better understanding of how the systems under analysis work than simply studying drawings and operating documents would.

The FHIA method does have drawbacks and limitations, including:

- It does not reveal hazards not necessarily associated with the chosen interface, or that may result from normal operations
- It can require a substantial amount of time and effort to complete

The structured, scenario-based functional hazard identification analysis method presented provides a systematic technique based on a scenario approach for identifying integrated system functions, and finding the obvious hazards, as well as those obscured in the complexity of system integration. It is applicable for use in uncovering hazards in all types of simple and complex systems; however, because it does not necessarily identify potential internal or inherent system hazards, the analyst should combine this method with other hazard identification methods to ensure they identify all hazards. Other new hazard analysis methods to consider are systems-theoretic accident model and processes (STAMP) [Ref. 13] and system theoretical process analysis (STPA) [Refs. 14-16].

Acknowledgments

The author thanks the following individuals for their peer review:

- Terry Osborn, Booz Allen Hamilton, Level 2 Ground Integration Hazard Analysis Team
- Patrick O'Malley, Booz Allen Hamilton, Level 2 Ground Integration Hazard Analysis Team
- Brian Balu, NASA JSC, Constellation Program, SR&QA Safety Manager
- Dr. Bill Vesely, NASA HQ, Probabilistic Risk Assessments Directives, Tools and Capability Development

References

1. Wilkinson, P.J. and T. P. Kelly. "Functional Hazard Analysis For Highly Integrated Aerospace Systems," *Certification of Ground/Air Systems Seminar (Ref. No. 1998/255)*, IEE, London, U.K., February 17, 1998, pp. 4/1 - 4/6.
2. NASA, "Constellation Program Hazard Analyses Methodology", CxP 70038 Rev C, pp. 11, 70.
3. Aerospace Recommended Practice. "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", SAE ARP4761, Society of Automotive Engineers, Inc, 1996. pp. 16-17, Appendix A.
4. EUROCONTROL Experimental Centre, "Review of Techniques to Support the EATMP Safety Assessment Methodology," EEC Note No. 01/04 - Volume I, M. Everdij (NLR), January 2004, p. 5.
5. FAA, Advisory Circular, "System Design and Analysis", 25.1309-1A, June 21, 1988, p. 9.
6. Everdij, Mariken H.C. (NLR), Henk A.P. Blom (NLR), "Safety Methods Database," Version 1.0, March 2013, Id 289.
7. EUROCONTROL, "Guidance Material A: The Process in Practice: Planning and Conducting FHA Sessions," SAF.ET1.ST03.1000-MAN-01-03-A, Edition 2.0.
8. "Standard Best Practices for System Safety Program Development and Execution," ANSI/GEIA-STD-0010, TechAmerica, 2009, pp. 93 – 95.
9. NASA, "Requirements for Preparation and Approval of Failure Modes and Effects Analysis and Critical Item Lists," NSTS 22206 Rev D Change No. 41, pp. 4-4, 4-17.
10. Ericson, Clifton A., *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Inc., Hoboken NJ, 2005, p. 271.
11. NASA, "Constellation Program Hazard Analyses Methodology", CxP 70038 Rev C, p 87.
12. Leveson, Nancy G. *Engineering a Safer World: Systems Thinking Applied to Safety*, The MIT Press, Cambridge, Massachuetts, 2011, p. 187.
13. Leveson, Nancy, Mirna Daouk, Nicolas Dulac and Karen Marais. "A Systems Theoretic Approach to Safety Engineering," The MIT Press, October 30, 2003.
14. Leveson, Nancy G. *Engineering a Safer World: Systems Thinking Applied to Safety*, The MIT Press, Cambridge, Massachuetts, 2011, Chp. 8.
15. Nakao, Haruka, Masa Katahira, Yuko Miyamoto and Nancy Leveson. "Safety Guided Design of Crew Return Vehicle in Concept Design Phase Using STAMP/STPA", 6th IAASS Conference Procedings, May 5, 2013.
16. Asplund, Fredrik, Jad El-khoury and Martin Törngren. "Safety-Guided Design through System-Theoretic Process Analysis, Benefits and Difficulties", *30th International System Safety Conference Proceedings, 2012*.