HAZARD ANALYSIS OF COMPLEX SYSTEMS: A NEW METHOD FOR HAZARD ANALYSIS OF ROCKET VEHICLES

Jay T. Naphas

Federal Aviation Administration, Office of Commercial Space Transportation, 800 Independence Ave SW, Washington, DC, 20910, U.S.A., Email: Jay.Naphas@faa.gov

ABSTRACT

As systems become more complex, system analyses must adapt in order to handle the increase in complexity. The human mind can accommodate a certain number of discrete pieces of information in working memory simultaneously, and as modern systems involve volumes of information well in excess of this number, modern system analysis tools must supplement the mind's capacity and adequately organize the information so that it does not exceed cognitively manageable proportions while preserving information integrity.

Humans are purpose-driven, and as such are particularly adept at organizing information according to its purpose. People also provide different answers based on the way in which a question is asked. This hazard analysis technique utilizes the human propensity for purpose and asks the proper questions to drive a more effective hazard identification and mitigation process.

The product of this reexamination of the hazard identification process is a hazard analysis method that explicitly guides the analyst to the critical hazards of a system, effectively increasing the analytical power of all subsequent hazard analyses. The result is a hazard analysis method that improves hazard identification by structuring the search for hazards in a form that complements the natural abilities of the human mind.

1. INTRODUCTION

This paper presents a description of the form and use of a new hazard analysis method. Based upon the STAMP [1] model of accident causality, this method is designed to reduce the perceived complexity of preliminary hazard analysis of complex systems to a cognitively manageable degree while preserving the integrity of the system information itself. The reduction in apparent complexity is achieved by designing the hazard analysis method in a way that facilitates the natural inquisitiveness of the analyst. By acting as an extension of the mind while guiding the hazard identification process, this method reduces the perceived complexity of the hazard analysis of complex systems.

The new analysis method also provides input to a variety of system safety analyses and operational documentation, including the construction of fault trees, operational checklists, test programs, and even regulatory compliance documentation. It will be shown that this new analysis method ties not only individual component tests to the relevant hazards, but also connects the most common hazard analysis techniques to a cognitively manageable, centralized reference point. This interconnectivity encourages cross-checking between hazard analysis methods to further enhance the hazard analysis process.

The analytical architecture of this method facilitates comprehensive hazard analysis of a relatively complex system, and does so without the need for specialized software or statistical analyses. This method is thus ideally suited for experimental systems, where detailed component reliability data is not available and the system configuration is rapidly changing.

2. METHOD DEFINITION

The Nominal Aggregate Program Hazard Analysis (NAPHA) is based on a simple spreadsheet, shown in Tab. 1; "nominal" as it is focused solely on identifying hazards, "aggregate" as it includes all categories of subsystems (mechanical, digital, and social), and "program" as it includes the whole system life cycle in the analysis by facilitating tracking of the system's evolution over time. Though similar to the Preliminary Hazard Analysis (PHA) in function, this method elicits different system information by changing the form of the information request. This spreadsheet will now be examined, column by column, from left to right, to demonstrate the NAPHA process.

Table 1: NAPHA Spreadsheet Format

System Intent	Sub-Intents	Involved Systems	Involved Subsystems	Control Actions	Intent Failures	Mitigation Measures	Verification Evidence

The many purposes for which the system is built and rules by which it must operate are listed in the first column, labeled "System Intent." If desired, columns of "Sub-Intents" or "Constituent Intents" can be used to refine and further organize the analysis. The goals of a system are well understood before the hazard analysis would begin, and the NAPHA method uses these known system goals as the starting point for the hazard identification process. By first enumerating the goals that the system must achieve and the constraints within which it must operate, the analyst is directed to examine the system's operation as a whole at the outset of the hazard analysis process. This process of enumerating system goals results in a shift in focus from component or subsystem specialization to interaction prediction and integrated multi-disciplinary analysis. Further, when performance measures are derived from regulations and placed in the system intent columns, the NAPHA spreadsheet becomes a regulatory compliance tracking checklist as well as a hazard analysis system.

The next column lists the system components or subsystems that are involved in achieving each of the stated intents, with one list for each of the intents; this is the "Involved Systems" column. Similarly, the system components can be refined in subsequent columns (i.e. "Involved Subsystems" or "Involved Components") to provide the desired level of detail. System components and subsystems will be repeated as the conceptualization of their roles progresses; this repetition provokes renewed conceptualization of the potential system interactions at each instance of a subsystem, and checking these iterations of conceptualization against each other provides a more complete model of the safety-critical roles of each component and characteristics of the whole system. This effectively causes the safety professional to revisit their analysis from many different angles, as each different mental context in which each of the components is analyzed increases the thoroughness of the hazard identification and mitigation process.

The next column is "Control Actions." In this column, the analyst decomposes the actions of each system or component into individual control actions. This process invites a detailed inspection of the steps involved in achieving each goal and satisfying each constraint, ultimately leading to a thorough understanding of the system as a whole.

After the control actions column is the "Intent Failures" column. This column lists each of the means by which an individual subsystem or component could fail to meet the intent listed in the "System Intents" column, or fail to conduct the control action specified in the "Control Actions" column. The failure mechanisms can later be accumulated for each component, by means of a simple sorting of spreadsheet data, to derive a full list of any component's failure modes, the types of mishaps each mode can cause, and the measures in place to mitigate the effects of the failures.

The final two columns are "Mitigation Measures" and "Verification Evidence" respectively. These columns are filled with all of the mitigation measures in place for each of the hazards identified in the prior column, and the means by which each of the mitigation measures is proven to be in place and functioning correctly. If no mitigation is deemed necessary, the verification evidence must show proof that the hazard circumstance is either implausible or mitigated by the nature of the system. Engineering judgment is relied upon to determine when a hazard is sufficiently mitigated. The degree of system understanding gained by using a structured system for hazard identification allows engineering judgment to be relied upon for the design of mitigation measures and verification tests by keeping the system intellectually manageable.

3. THEORETICAL BASIS

This hazard analysis system is based on systems theory and human information processing models. These models imply that the form of a question strongly influences its answer. The NAPHA method asks questions that are designed to elicit responses based on system interactions as opposed to component reliabilities. By answering these questions, the safety analyst implicitly considers the interactions between components on a deeper level, not as "if subsystem X fails, how does the system respond?" but as "how could subsystem X prevent the achievement of goal A?"

The focus on intent achievement differentiates this method from similar forms of hazard analysis. Asking "how could the system fall short of its goals?" elicits different responses than "how could the components of the system break?" For a demonstration of this effect, ask yourself how your computer could break. Now ask yourself how you will generate a report that's due tomorrow and how that effort might fall short. The difference between your responses represents the shift in perspective generated by asking not how each component can fail, but how the system relies on each component to achieve its goals. In this example, the first question only considers the computer, while the second includes electricity, food, water, and distractions, thus providing a more complete analysis of the system as a whole. Goals are achieved by whole systems, and analyzing goal achievement (as opposed to component failure) provides the component interaction perspective so vital to the analysis of complex systems.

By focusing on the goals of a system, the human mind automatically reduces the scope of the hazard identification process to focus on the system goal in the analyst's working memory. It is difficult, if not impossible, for a person to hold all of the goals of a complex, modern system in their working memory simultaneously, so the spreadsheet allows the analyst to examine a system goal-by-goal. The safety analyst's mind is superb at the task of analyzing an individual goal, as humans are goal-driven themselves.

Using the innate goal analysis processes, this method allows the hazard analyst to focus on each subsystem from the perspective of achievement of a particular goal. The NAPHA method works as a supplement to the analyst's working memory; the spreadsheet combines these perspectives to provide a view of the full system. In essence, dividing subsystem hazard identification by goal creates a hazard analysis process that invites multiple inquiries into system traits, effectively increasing the number of "eyes" looking at the system. Further, by focusing on goals instead of subsystems, the safety analyst is invited to examine both the details of subsystem fault modes and the attributes of the system design, rather than focusing on one or the other.

The NAPHA method uses its form to ask these improved questions at each level of the analysis. Listing the goals of the system is the basis of conceptual design; it enumerates the regulations by which the system is constrained and the tasks it must accomplish in a central location. Enumerating the purposes of the system asks what the system must do, where traditional methods ask only what components are involved. This process, when conducted with input from experts in all of the constituent systems, provides early resolution of conflicts that could be set up by the system's basic design approaches.

Organizing constituent systems by the goals they support asks what must work to achieve each goal. This will naturally lead to repeated entries for different constituents, and this replication is desirable. Its desirability is the result of the same human information processing concepts that drive the method itself; the analyst is asked how each constituent can fail to achieve each goal, resulting in a different perspective on a given constituent for each of the intents that constituent supports.

This array of questions increases the thoroughness of "what does it need to do" by repeating that question in slightly different forms; a problem seen from one angle may be invisible from any other. In spreadsheet form, the analyst can sort by constituent system to cross-check the intent failures. This check improves the cognitive manageability of hazard identification by asking a question in a number of ways, storing the answers, and later comparing the results. Should a hazard be seen from one perspective and no other, its implications for all of the relevant system goals can be analyzed without excessive mental load.

The analyst can derive a list of critical components and procedures from the mitigation measures column. Everything in this column is implicitly goal-critical, as the contents are means by which goal achievement is assured. During any change to the program, this column provides a central source for analysis of the impact of the change on the goals of the program. Tests and performance measures for acceptance of a given change are quickly found in the verification evidence cells that correspond to the change.

4. METHOD UTILIZATION AND LIMITATIONS

This method is essentially a structured notepad. It is also an initial step in a full systems theoretic hazard analysis. The NAPHA method is best applied in the hazard identification phase of a system safety program or as a verification of the completeness of another hazard analysis method. Judicious use of the capabilities of spreadsheet software facilitates a variety of well-known hazard analyses based on each of several columns from the spreadsheet. For example, the "Intent Failures" column can be organized into a fault tree, and the "Verification Evidence" column can be organized into operational checklists. Deriving other analytical methods from a central reference method, such as a NAPHA spreadsheet, encourages the analyst to check each derivative method against the central reference method. By extension, each improvement derived from each subsequent method improves the core method and the system safety process as a whole.

The NAPHA method is applicable to any system of any scope. However, it does not elegantly handle systems of high complexity, such as multiple-vehicle launch systems or large organizations. When the complexity of a system exceeds the degree common for experimental rocket vehicles, a spreadsheet is not an adequate supplement to the analyst's mental capacity, and there is a corresponding decrement in the quality of NAPHA analyses of such highly complex systems.

For systems of very high complexity, the subsystem interactions can be too complex to understand with only a spreadsheet to supplement the analyst's comprehension of the system; the underlying structure of the system is no longer adequately represented in the spreadsheet. Such complex systems are better understood by using a hazard analysis method such as STPA [1], where specialized software enables the analyst to comprehend all of the potential actions of a vast system.

5. METHOD RESULTS

The NAPHA method has been applied to several rocket vehicle hazard analysis projects. In general, the use of the NAPHA method expands the hazard identification process to include a greater variety of system interaction hazards than comparable methods, such as the PHA. Further, fewer "trivial" hazards are identified, as the NAPHA method is designed to identify only those hazards that could potentially violate identified safety constraints.

6. REFERENCES

1. Leveson, Nancy G. (2002). *System Safety Engineering: Back To The Future*, last retrieved 10/17/08 from http://sunnyday.mit.edu/book2.pdf.