System safety assessments combining first principles and model based safety assessment methodologies

M. A. Dvorack
Assessment Technologies Department, Sandia National Laboratories, Albuquerque, New Mexico 87185-0405 USA

T. R. Jones
Assessment Technologies Department, Sandia National Laboratories, Albuquerque, New Mexico 87185-0405 USA

D. D. Carlson
Manager, Assessment Technologies Department, Sandia National Laboratories, Albuquerque, New Mexico 87185-0405 USA

J. F. Wolcott
System Surety Assessment Department, Sandia National Laboratories, Albuquerque, New Mexico 87185-0405 USA

G. A. Sanders
System Surety Assessment Department, Sandia National Laboratories, Albuquerque, New Mexico 87185-0405 USA

ABSTRACT: In performing assessments of low probability, high consequence systems, it is often preferable to use more than one methodology in order to assure that such systems undergo a thorough assessment. Hence, employing two methodologies in a complementary manner allows the analyst to bring the strongest features of each approach to bear upon the problem. The results of one methodology can be used to crosscheck or better characterize the results of another methodology, with the results being synergized in providing a comprehensive assessment of the system. This paper will briefly describe both the first principles and model based safety assessment methodologies, and will illustrate how both methods are used in a complementary manner in order to perform overall safety assessments of low probability, high consequence engineered systems at Sandia National Laboratories.

INTRODUCTION

Safety assessments of low probability, high consequence systems at Sandia National Laboratories are performed by utilizing a "first principles" qualitative methodology in combination with a quantitative model based safety assessment (MBSA) in order to provide throrough, technically defendable assessments. This paper describes both the first principles and MBSA methodologies, as well as discusses how they are used together in performing a system assessment. An example illustrating the application of these two methodologies in a synergistic manner is also provided.

FIRST PRINCIPLES METHODOLOGY DESCRIPTION

The first principles design approach makes use of the fundamental characteristics inherent in the physics and/or chemistry of a material in order to provide a predictable response of a component when subjected to specific environmental stimuli. A passive material response or property (such as electrical isolation or diversion) is sought, while designs that rely on a chain of events or active "sensing" in order to achieve a predictable response are avoided. An example of a first principles design approach is the use of a material having a well-defined melting point in the design of a component that is required to fail safe if a certain undesired threshold temperature is exceeded. Rather than utilize an active heat sensor in order to detect and then send a signal to some safing circuit, the material will instead inherently melt and fail safe.

A first principles assessment evaluates the material, component, or system against the design requirements in order to assure that the device provides the required predictable response. Furthermore, the adequacy of these requirements is also evaluated. During the performance of this assessment, all test/validation data, as well as production controls for safety critical design features, are reviewed in order to ensure compliance with the requirements. Hence, the assessment also ensures that there is a controllable and traceable design and production path to the safety requirements, as well as a change control process in order to ensure that the safety critical features are not inadvertently degraded by design changes or material substitutes.

There may also be a safety theme associated with the component. The safety theme is a plan of how safety requirements will be satisfied. The safety theme serves as a description of the safety design methodology, as well as a means of identifying safety requirements for individual components. An example of a safety theme may be the isolation of unintended electrical energy from safety critical electrical circuits in both normal environments (i.e., the operational environments in which the system is expected to perform without degradation in operational reliability) and abnormal environments (i.e., thos environments in which full operational reliability is not expected but for which safety must still be assured). In a first principles design approach, the system would be designed such that the system itself would fail in a safe manner prior to the loss of electrical isolation. Safe system failure would be based on the fundamental characteristics of the materials used, such as melting points in the case of severe thermal environments. Safety themes are evaluated

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

DISCLAIMER

with respect to their adequacy, as well as how well they are implemented with the various individual components. The chain, or system, is no stronger than its weakest link, or component.

The output from a first principles assessment consists of the evaluation of the safety requirements and identification of potential vulnerabilities, often referred to as "softspots," which may compromise the safety of the system. In addition, potential areas for additional testing, modeling, controls, and component characterization are identified. However, the first principles assessment cannot easily prioritize these vulnerabilities, nor can it quantify the risks associated with these vulnerabilities. Furthermore, the first principles assessment cannot quantify the potential benefits of production controls and design changes.

MODEL BASED SAFETY ASSESSMENT DESCRIPTION

Model Based Safety Assessment (MBSA) is a term that refers to a systems analysis methodology in which the possibilities of experiencing defined sets of undesirable consequences are determined and assessed. MBSA also identifies the probabilistically significant risk contributors which may lead to undesirable consequences. The MBSA methodology utilizes thermal and structural finite element models in order to evaluate system responses to different environments such as temperature. Hence, this assessment becomes a search for specific abnormal environments in which the safety of the system may be compromised and, once these environments have been identified, makes a quantitative estimate of how likely these environments are and how probable it is that potential pathways may lead to an undesired event.

MBSA incorporates three analytical tools: event trees, fault trees (which are also used in the first principles methodology), and physical response models. Event trees are used in order to determine accident frequencies associated with abnormal environments, fault trees are used to determine the necessary and sufficient conditions, as well as the probability of pathways, leading to the undesired top event, and the physical response models are used to determine the environmental conditions that will cause the system to exceed it physical thresholds. These physical response models consist of finite element thermal and structural models.

SYNERGISM OF THE FIRST PRINCIPLES AND MODEL BASED SAFETY ASSESSMENTS

The outputs from a first principles assessment, such as a list of potential vulnerabilities and desired modeling inputs, are used as inputs to the MBSA. MBSA then uses these inputs in order to provide various forms of information, such as the modeling of specific responses and the quantification of the timing of thermal "races" (e. g., identifying the times at which each critical component reaches its temperature threshold) in order to determine whether safe inoperability is achieved before electrical isolation fails. Furthermore, the models can be used to further prioritize those dominant risk contributors which were initially identified in the first principles assessment. The benefits of potential design changes identified in the first principles assessment can also be assessed and quantified.

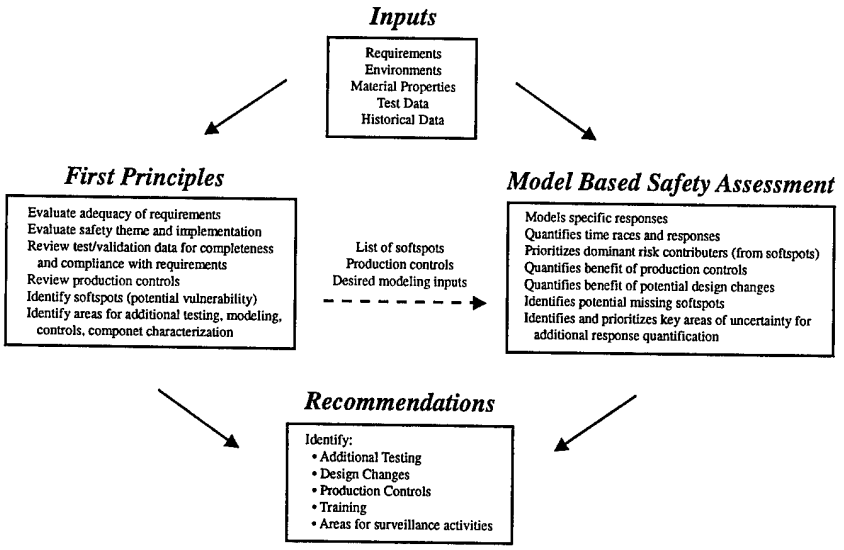

Figure 1. Illustration of the relationship between first principles and model based safety assessments.

In addition, the MBSA methodology may identify potential vulnerabilities that were not identified in the first principles assessment. The MBSA can also identify important areas of uncertainty that require additional response quantification. An illustration of the synergism between the first principles and MBSA assessments is shown in Figure 1.

EXAMPLE

1. Definition of sample safety theme and problem

Consider the hypothetical circuit illustrated in Figure 2. The safety theme for this circuit is the prevention of potentially damaging undesired electrical energy from reaching the load, L, such as a flash lamp. The circuit is designed so that upon receipt of an initial signal, switch S1 closes, enabling the capacitor to be charged to a voltage V while switch S2 remains open. A second signal then opens S1 and closes S2, enabling capacitor C to act as a short- term power source to the load. Hence, the two switches perform an isolation function with respect to preventing undesired voltage from reaching the capacitor and the load. Furthermore, this circuit is to fail safe in an environment where overheating is possible. Therefore, as a safety feature, the capacitor is designed to safely fail to hold an electric charge when the external environment exceeds a certain threshold temperature. The capacitor is also to fail safe in such a thermal environment before any of the other components fail, especially the two switches which may fail in a closed position if the thermal environment is too high, thereby creating a potential electrical path for an undesired voltage. Finally, as a further safety feature designed to help prevent undesired electrical energy from reaching the load, the circuit is placed in a protective enclosure such as a steel container. Numerical design criteria, such as the required failure temperatures for the capacitor and the switches, would also be established in the design process.

2. First principles assessment

The first principles assessment of this circuit would consist of evaluating the materials that comprise the components against the design requirements in order to determine if the circuit would behave as intended. For example, the materials comprising the capacitor would be evaluated in order to determine if the capacitor would indeed fail safe beyond the design failure threshold temperature. Hence, this evaluation would entail the determination of the melting temperature of the dielectric material. In addition, the adequacy of the design requirements themselves would also be evaluated. For example, the threshold temperature and tolerances at which the capacitor is to fail would be evaluated. Validation test data would be reviewed in order to determine if the capacitor's behavior is well within the design requirements for such parameters as, for example, various heating rates and directions, and material aging characteristics, as opposed to marginally meeting these requirements. Areas where testing is inadequate or lacking in order to ensure a comprehensive characterization of the capacitor, as well as the other components, would also be identified. The adequacy of production controls with regard to the quality of the materials used in production builds would be evaluated in order to ensure intended product functionality and minimal production lot-to-lot variability.

One possible outcome of this assessment would be a list of potential vulnerabilities. Examples of such vulnerabilities may be the relatively wide variability in the capacitor's dielectric thickness, an ill-defined failure temperature threshold, or variability in response for differing heating rates. Another vulnerability may be the relatively poor location of the capacitor in the physical configuration of the electrical circuit which may cause one or more of the other components, such as the switches, to be preferentially exposed to an abnormal thermal environment rather than the capacitor itself. As stated earlier, a switch failure may result in an undesired voltage overcharging the capacitor and/or being directly applied to the load. Still other vulnerabilities may include the relative lack of understanding of the potential failure mechanisms for the switches and the relative non-uniqueness of the electrical signals sent to the two switches.

3. Model Based Safety Assessment

The MBSA methodology would entail several activities. These activities would entail fault tree analysis, event tree analysis, and physical response modeling,

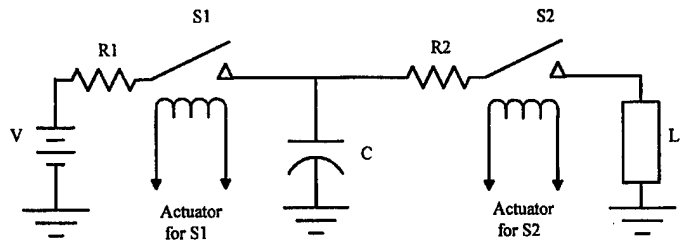

Figure 2. Sample circuit to be assessed using a combination of first principles and model based safety assessments.

all of which are described below.

Fault tree analysis of the circuit would consist of creating a fault tree having the loss of circuit predictability, for example, as the top event. In other words, if performance of a particular component is considered to be unpredictable, it is assumed to function in a manner that will cause an unintended voltage across the load. Analysis would then be performed in order to identify and determine potential combinations of events leading to the undesired top event of this tree. The fault tree itself would be solved three times: before switch S1 is closed, after S1 is closed, and after S1 is re-opened and S2 is closed. Historical and reliability data would be used to quantify the various pathways obtained during the analysis. The results of the fault tree analysis would then be compared against the numerical design requirements stated for the circuit and its components. The fault tree analysis also identifies potential vulnerabilities which can be compared to those identified in the first principles analysis.

Event tree analysis would consist of developing scenarios, depicting potential consequences, from various initiating events. An example of an event tree for this example may be based on an initiating event consisting of an electrical short which occurs in a nearby electrical circuit. This electrical short causes a component or subassembly to melt and cause a fire. Using available data, frequencies of occurrence of the resulting consequences can be estimated. The results of the event tree analysis would also be used to provide boundary conditions for performing thermal physical response analysis and in prioritizing vulnerabilities based on the likelihoods of occurrence.

While the fault and event tree analyses are under way, finite element physical response thermal models of the components in the circuit would be created and benchmarked against existing data. Hence, the time response of the components under various thermal conditions can be estimated. Time versus temperature histories would be generated while exercising these models under the different conditions. As a result, this analysis might indicate that, in certain thermal environments, one or both of the switches may actually marginally "fail" (i.e., become unpredictable) before the capacitor itself fails, causing unintended voltage to be applied across the load. The thermal models may also indicate undesired component degradation in other thermal environments, a vulnerability that was not identified from the first principles analysis.

4. Results

During the assessment of the system (i.e., circuit), it is important that those analysts performing the first principles assessment and those performing the MBSA communicate openly and frequently with each other. For example, since the MBSA emphasizes the overall system response rather than concentrating on individual components, the first principles assessment provides material properties and potential failure mechanisms of these system components that the MBSA incorporates into the system models. Conversely, the MBSA results may identify potential vulnerabilities that were overlooked during the first principles assessment. In addition, the MBSA results may help those performing the first principles assessment to recommend potential design and/or production control changes which, in turn, would require another MBSA in order to determine the effectiveness of such changes.

For the given example, the combined first principles/MBSA results may identify the following:

- There are no problems, or -
- Potential failure of the switches before that of the capacitor under certain thermal environments ("loss of a thermal race")
- Inadequate testing/validation of the capacitor's behavior in certain thermal environments
- Lack of adequate characterization of the capacitor's material properties
- Lack of adequate characterization of the material properties of the switches
- Unpredictable behavior of the capacitor and the switches in certain defined thermal environments
- Production controls for the capacitor not well-defined in some areas (e.g., too much variability in the dielectric thickness)
- Design criteria too vague in some areas

SUMMARY

The combination of first principles and MBSA has been used successfully at Sandia National Laboratories in performing thorough, technically defendable assessments of low probability, high consequence engineered systems. However, much work remains in improving the methodology. For example, the lack of adequate component characterization can hinder the development and benchmarking of structural and thermal physical response models. In addition, more detailed fault trees of actual components need to be developed in order to enhance production controls and field surveillance. Furthermore, adequate electrical models which complement the structural and thermal models need to be developed. These electrical models would need to have the capability to respond to thermal and structural abnormal environments.

Another important area in performing combined first principles/MBSA analyses is in regard to the cross-training of analysts. MBSA incorporates quantification tools and models that are used in conventional probabilistic risk assessment (PRA) and which are often not familiar to analysts who are steeped in first principles analytic methods. Likewise, PRA approaches usually use active, reliability data and, as

such, analysts who are performing MBSA often do not understand the passive material and physics approaches that first principles analysts demand. Cross-training of such analysts enables the strengths of both methodologies to be brought to bear on a particular assessment.

As stated above, the combined first principles/MBSA approach has shown a great deal of promise in performing assessments of complex, low probability, high consequence engineered systems. It is hoped that this approach may ultimately be applied to a wide range of safety assessment activities in a variety of commercial applications.

Report Number (14) SAND--98-0162C
CONF--980621--

Publ. Date (11) [19801]
Sponsor Code (18) DOE/DP, XF
UC Category (19) UC-705, DOE/ER

DOE