Model-Based Safety Assessments

David D. Carlson
Sr. Manager
(505) 844-8497
Ddcarls@sandia.gov

Todd R. Jones
Department Manager
(505) 844-2622
Trijones@sandia.gov

Sandia National Labs
Surety Assessment Center
Surety Engineering Programs
Albuquerque NM

Abstract
Sandia National Laboratories performs systems analysis of high risk, high consequence systems. In particular, Sandia is responsible for the engineering of nuclear weapons, exclusive of the explosive physics package. In meeting this responsibility, Sandia has developed fundamental approaches to safety and a process for evaluating safety based on modeling and simulation. These approaches provide confidence in the safety of our nuclear weapons. Similar concepts may be applied to improve the safety of other high consequence systems.

Introduction
Sandia National Laboratories is responsible for the design of nuclear weapons, exclusive of the explosive physics package. Nuclear safety is of utmost importance. Sandia has developed fundamental design principles to ensure predictably safe response under accident conditions. As part of the Independent Assessment performed by Sandia’s Surety Assessment Center, we have developed a model-based safety assessment process to give us deeper insight into weapon safety. This paper briefly describes weapon safety design principles...
DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.
and then summarizes the model-based safety process and insights from its application to nuclear weapons. Similar approaches may prove beneficial to other high consequence operations.

**Nuclear Weapon Design Principles**

To ensure that improper electrical signals cannot be generated in nuclear weapons, Sandia designs the warhead electrical system according to the following principles:

1. **Isolation** – enclosing critical safety components inside a barrier, known as the “exclusion region,” to protect them from the accident environment and to keep out undesired electrical energy.
2. **Incompatibility** – since the operation requires electrical energy, openings in the exclusion region are required. These electrical pathways are provided by specially designed switches, known as “strong links,” which open only upon receipt of uniquely engineered signals incompatible with signal generated by nature.
3. **Inoperability** – recognizing that situations could arise, in which the strong links fail, additional components, known as “weak links,” are incorporated within the exclusion region in the path of the electrical energy. These components, located as near to the strong links as possible, are designed to predictably fail in accident environments before failure of the strong links, thus ensuring inoperability.

These principles of design are incorporated into all modern nuclear weapon systems to ensure safety. The elements of the design deemed critical to safety by the designers are known as the “safety theme.” The intent is to limit the number of safety design feature to an absolute minimum which bounds the analysis required for safety assessment.

An assessment of the design is performed by an organization within Sandia, which is independent of the designers. These independent assessors, possessing a deep understanding of weapon design, carefully review the safety theme and its implementation to ensure adherence to the design principles. This in-depth review is now supplemented with insights from a newly developed model-based safety assessment process described below. Insights from the independent assessment are provided to the designers and independently to executive management at the laboratories.

**Model-Based Safety Assessment Process**

Weapons operations are highly controlled and carefully performed. Nevertheless, the potential exists for accidents to occur. Such accidents may occur, for example, during transportation, handling for maintenance, or under extreme natural conditions such as lightning or tornadoes. If an accident occurs, the weapon may be exposed to abnormal environments, challenging the safety of the design. The model-based safety assessment process evaluates weapon
performance under these abnormal environment conditions to assure safe response. Should conditions be identified in which the safety theme no longer can be assured to remain intact, improvements in design or limitations to operations may be considered to preclude such conditions from occurring.

The model-based safety assessment process consists of four elements:
1. Environment definition
2. System modeling
3. Physical response modeling
4. Evaluation.
Each is discussed briefly below.

Environment Definition
As part of the weapon design process, normal and abnormal environments that the weapon is expected to experience over its lifetime are specified. These specifications, citing parameters such as temperature ranges, vibrations, shock loading, and radiation fields, provide a representative set of conditions for which the designer must certify that the weapon will be safe.

Recent methodological developments have applied event tree models to delineate potential weapon accident scenarios and associated abnormal environments. Each weapon operation from first delivery to the military until retirement is examined to ascertain potential initiating events. These initiating events include events such as transportation accidents, exposure to lightning, or dropping of the weapon during handling. Following the initiating event, other events may transpire such as a fire, impact, or application of unintended electrical energy. Together, the initiating event and the subsequent events constitute an accident scenario. The event tree provides a structured process for delineating these scenarios and, given the data on the initiating event frequency and conditional probabilities on the subsequent events, a basis for quantifying the likelihood of the scenario. Further diagnosis of the results can provide estimates of the frequency and severity of the associated abnormal environments. The SETAC/SANET software programs contained within Sandia’s ARRAMIS code suite can be used for event tree construction and solution.

System Modeling
We use system fault trees to develop the set of conditions necessary and sufficient to cause the undesired top event. For modern nuclear weapons with well developed and implemented safety themes, this is a rather straightforward exercise. The number of safety critical components is generally less than a dozen, and the resultant cut set expressions number in the 10s.

The resultant set of events – component performance which may cause energy to propagate through the systems (such as closure of the strong links) or which
may cause energy flow to be terminated (such as assured failure of the weak links) — are defined with the Boolean solution of the fault tree. The SABLE software, also contained with the ARRAME code suite, is used for fault tree analysis.

**Physical Response Modeling**

Given the range of environments that the weapon may see and the definition of events of interest from the fault tree, the challenge is to perform an evaluation of whether these events can occur under any of the environmental conditions. We perform this analysis using finite element physical response models.

Three dimensional structural and thermal finite element models are constructed for the weapon. These models are generally quite complex, with thermal models often having 5000-15000 mesh elements and structural models often having three to four times as many elements. The models are benchmarked against test data obtained during weapon development. Solution of the models relies upon workstations.

Parameters are selected from the environment ranges specified in the environment definition process. These time dependent boundary conditions are applied to the physical response models and the environmental conditions are transmitted through the warhead to the components buried within. Time dependent stresses experienced by the components are calculated.

**Evaluation**

The evaluation process takes the results of the physical response modeling — mechanical loadings and time dependent temperature histories of the safety critical components — together with the fault tree cut sets to determine whether, in fact, predictable safe performance may be in question. With an understanding of the environments experienced by the components together with knowledge of the conditions under which components can fail, we predict the time dependent state of each of the safety critical components. Various potential undesired results are sought.

In thermal environments, we evaluate the time at which the strong link temperature reaches a value that exceeds the threshold to which the component has been certified. We similarly calculate the time at which the weak link temperature reaches the value at which it has been certified to be inoperable. If the strong link reaches its critical temperature before the weak link is predicted to be assuredly safe, the safety theme has been compromised.

Similarly, for mechanical environments, we evaluate whether the strong link has experienced loadings that exceed the design threshold and whether, at the same
time, the weak link may remain operable. Should such conditions be satisfied, again the safety theme is viewed as compromised.

We examine the performance of the exclusion region barrier particularly closely to ascertain whether the environment has caused breakdown of the isolation of the critical components. Should this occur, unintended electrical energy might be introduced into the region containing the safety critical components, potentially bypassing the safety built into the fireset.

**Iterations**

We began the evaluation with a selection of parameters from the environment range that the weapon may experience. The results of the evaluation are a determination of the integrity of the safety theme and the associated margins of safety. As might be expected, careful design of the weapons precludes compromise of the safety theme under essentially all postulated conditions. The results of the initial evaluations are examined to identify regions of the environment parameter space for which the potential exists for compromise of the safety theme.

From these insights, additional iterations are performed, successively selecting more challenging conditions from the range of environments to ascertain whether any conditions can be identified in which assured safety may be lost. Recent advances in optimization theory and computational intelligence aid the analyst in their search for such regions of vulnerability. Should any vulnerability be found, the results are carefully reevaluated using the highest fidelity tools available. Potential design improvements are sought to preclude such potential vulnerabilities from the design; operational changes may also warrant consideration to preclude the environment from occurring.

The model-based safety assessment process is summarized below.
Results

The model based safety assessment process has been applied to most of the systems in the nation's nuclear stockpile. Some general observations resulting from this process may be presented.

We have successfully applied this process to evaluate the margins of safety for the weapons in the stockpile. We have found almost no environmental conditions under which the warhead electrical system safety theme may be compromised. The conditions leading to loss of assured safety require highly specialized environments that are predicted to be extremely unlikely.

In relative terms, conditions which could breach the exclusion region, possibly permitting energy to enter the system bypassing the safety components in the firing set, are more likely to occur than conditions which could compromised the warhead electrical system safety theme.

Experience collected from the performance of the safety critical components over the life of the stockpile substantiate that we meet the safety specifications set forth by the military for normal environments. As such, the potential for an undesired response under normal environments conditions is less than one in a billion over the weapon lifetime.

Finally, we have used these approaches to determine the relative likelihood and severity of identified weaknesses of the design in implementing the design principles. These weaknesses vary in likelihood and in safety remaining in the system. In all cases, the environmental likelihoods are very small and additional
safety critical aspects of the system must be compromised to cause the undesired event.

The Impact of High Performance Computing
Recent initiatives to enhance the laboratories’ computing capabilities are revolutionizing our ability to model and simulate weapon performance. The model-based safety assessment process is being integrated into multiple parallel processing, teraflop scale machines and into a greatly enhanced distributed computing system. These computational advancements offer the promise of being able to perform the complex physical response calculations in a fraction of the time; moreover, the parallel and distributed processing capabilities will facilitate performance of many such calculations simultaneously.

With these advancements, we will be able to efficiently search the parameter set for conditions which may compromise assured safety. With the power of the teraflop machine, we will be able to effectively perform high fidelity calculations with higher resolution meshes and more complex physics to investigate carefully any identified potential vulnerabilities.

Finally, we will be able to better characterize the associated uncertainties in our results and perform far more sensitivity calculations to identify critical information requiring further investigation.

Application to Other High Consequence Operations
Our experience in the design and assessment of nuclear weapons offers the promise of improving the safety of other high consequence operations. The principles of design which we have evolved for nuclear weapon may be generalized and particularized to other high consequence systems. The precepts of a safety theme and the associated fundamental principles for assuring safety could be applied to a number of high consequence operations. The concepts of the model-based safety process could be adapted to provide deeper understanding of the performance of these high consequence systems in normal and abnormal environments.

Finally, a probing assessment independent of the designer reporting its insight to executive management has proven to be extremely valuable to the safety of our weapon designs and to the development of Sandia’s safety culture. Similar value may be realized in other high consequence operations.

DISCLAIMER
This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.