Proceedings of ICONE14
International Conference on Nuclear Engineering
July 17-20, Miami, Florida, USA

ICONE14-89598

SPATIALLY INFORMED PLANT PRA MODELS FOR SECURITY ASSESSMENT

Timothy A. Wheeler
Sandia National Laboratories
Systems & Structures Department
P.O. Box 5800, Albuquerque, New Mexico 87185-0748

Dr. Willard Thomas
Omicron Safety & Risk Technologies Inc.
2500 Louisiana NE, Suite 410
Albuquerque, New Mexico 87110

Eric Thornsbury
Advisory Committee on Reactor Safeguards – Technical Support Branch
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

ABSTRACT[1]

Traditional risk models can be adapted to evaluate plant response for situations where plant systems and structures are intentionally damaged, such as from sabotage or terrorism. This paper describes a process by which traditional risk models can be spatially informed to analyze the effects of compound and widespread harsh environments through the use of "damage footprints." A "damage footprint" is a spatial map of regions of the plant (zones) where equipment could be physically destroyed or disabled as a direct consequence of an intentional act. The use of "damage footprints" requires that the basic events from the traditional probabilistic risk assessment (PRA) be spatially transformed so that the failure of individual components can be linked to the destruction of or damage to specific spatial zones within the plant.

Given the nature of intentional acts, extensive modifications must be made to the risk models to account for the special nature of the "initiating events" associated with deliberate adversary actions. Intentional acts might produce harsh environments that in turn could subject components and structures to one or more insults, such as structural, fire, flood, and/or vibration and shock damage. Furthermore, the potential for widespread damage from some of these insults requires an approach that addresses the impacts of these potentially severe insults even when they occur in locations distant from the actual physical location of a component or structure modeled in the traditional PRA.

INTRODUCTION

This paper describes a process by which traditional nuclear power plant PRA models can be adapted to model spatial dependencies of systems, structures, and components (SSCs). The purpose of such an analysis is to evaluate the potential impacts of an intentional act of sabotage or terrorism upon a plant's SSCs with regard to the plant's capabilities to achieve a safe shutdown. Intentional acts designed to inflict extensive damage to a facility have the potential to create harsh environmental conditions that uniquely challenge the integrity, availability, and/or operability of SSCs. For example, intentional acts might subject SSCs to blast effects, intense heat from an intentionally set or ensuing fire, subsequent flooding created from broken piping, vibration/shock damage, or other harsh environments depending on the nature of the potential sabotage attack. Furthermore, as opposed to events modeled in many traditional external event PRAs, the potential magnitude of

[1] The views expressed in this paper are solely those of the authors and do not necessarily represent those of either the Advisory Committee on Reactor Safeguards, the United States Nuclear Regulatory Commission (USNRC), Sandia National Laboratories, or Omicron Safety & Risk Technologies.

any particular sabotage-inflicted damage mechanism might extend to numerous rooms and elevations throughout a building and even into adjacent buildings. It also is possible that plant areas might be subjected to multiple damage mechanisms, thus creating a combination of harsh insults that overlap one-another in various combinations.

The problem is further complicated because SSCs might have varying degrees of susceptibility to a given damage mechanism. For example, it might be postulated that all of the SSCs within a given area would be destroyed by structural damage from a certain attack. The function of some of these same SSCs may not be threatened by other damage mechanisms associated with the attack. For example, if a room contains electrical equipment, cabling, and piping, all three of these could be destroyed by sufficient structural damage in the room. But if the same room were subjected to flooding, the flood insult might adversely affect only the electrical components, while not affecting the function of piping and cables.

The objective of traditional plant PRA models is to evaluate plant risk due to random failures, where input data for the systems models are developed from databases of equipment reliability. In the past, spatial information has been applied to these PRA models on a limited basis, usually with regard to internal flooding or internal fires. Where PRA models have been modified to model flooding or fires, these potential insults are analyzed individually, given that randomly-initiated internal flooding or fires are considered independent initiating events. In other words, multiple and concurrent categories of insults are not addressed. Furthermore, some types of system-level components in traditional PRA models are often ignored or treated superficially. For example, piping and cables are often treated superficially because the probability of their failure in conjunction with other plant failures is so small that it can be safely neglected in the analysis. However, these types of components are critical to system operation, and thus must be accounted for in security assessments because security-related events are, by their nature, location-based events.

In the process described in this paper, the resulting damage that would be incurred by a plant from a hypothetical attack scenario is mapped onto plant layout drawings. The resulting map is described as a damage footprint. The damage footprint is used to identify the types and locations of damage insults that could render SSCs inoperable based on their spatial dependencies. In effect, a damage footprint represents a special category of a “common cause initiating event.” As will be described, significant modifications must be made to traditional risk models to incorporate damage footprints.

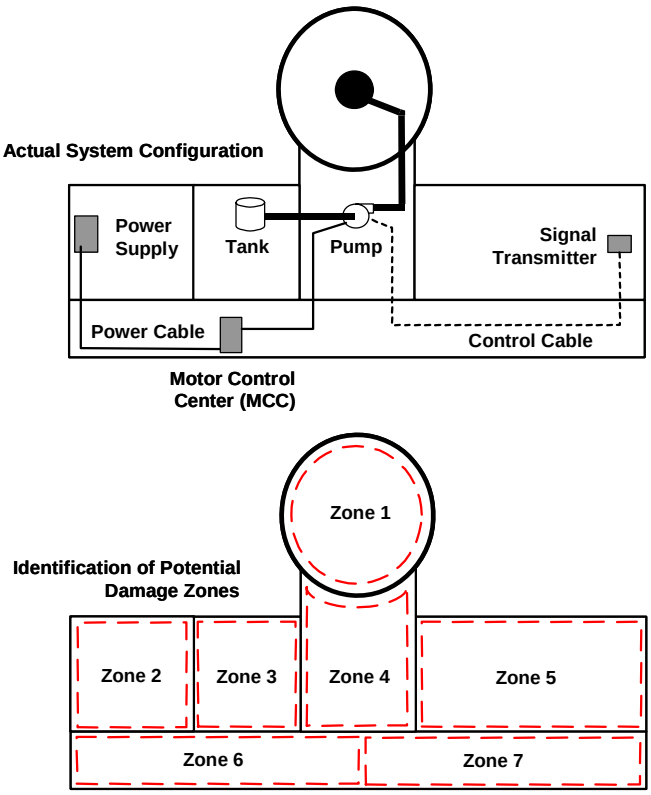
This paper is organized as follows. First, the concept of a damage footprint is illustrated through use of a graphical example where a pumping system is exposed to a hypothetical damage footprint. Next, a modeling approach for integrating damage footprints into traditional plant PRA models is presented. Additional issues associated with this modeling approach are subsequently discussed, followed by overall conclusions.

CONCEPT OF A DAMAGE FOOTPRINT

As previously noted, a damage footprint is a spatial mapping of the types of harsh environments to which various areas (zones) within plant buildings are subjected as a consequence of an intentional act. Regions where various harsh environments overlap within the same zone(s) represent potential sources of multiple failure mechanisms for those SSCs dependent on such zones. The concept of a damage footprint and its application to evaluating the potential for system failure is described in more detail below.

Consider a simple coolant injection system involving a pump that takes suction from a tank and discharges to the reactor vessel. The physical layout of this system is illustrated in the upper half of Figure 1. Here, the pump and tank are located in a common building, but in rooms that are separated by a robust wall. Successful operation of this injection system not only relies on the physical integrity of this water-filled piping system, but the electrical support systems and a control system as well. In this example, the pump receives motive power from a power supply located in a remote room of the building, which passes electrical current through cabling that

FIGURE 1. EXAMPLE TRANSFORMATION OF PLANT CONFIGURATION TO DAMGAGE ZONES



is routed through a motor control center (MCC) in an adjacent room. For the pump to start and for operators to control its speed, it must receive a low voltage control signal from a sensor that monitors reactor conditions (e.g., reactor water level). In this example, the signal transmitter and control cables are also distributed among several rooms of the building.

In the lower portion of Figure 1, the building floor plan is redefined into a set of areas, or zones. Each zone represents a region of space within which the physical response of the building to an intentional act is assumed to be uniform. That is, all equipment within a particular zone would be subjected to a similar level of damage from each type of harsh environment generated by the intentional act (e.g., fire, shock, and flood). Since buildings at nuclear power plants are often highly compartmentalized structures, it is reasonable to define the zones based on the architectural design of the floor plan – defining each room, hallway, or stairwell as its own zone. However, for very large areas such as turbine halls or even containment structures, such large areas can be subdivided into smaller zones. In this example, the containment building (Zone 1) is treated as a single zone, and the adjacent building containing the example injection system is represented by six zones.

For a hypothetical act of sabotage, the extent of damage caused by each harsh environment associated with that act must be mapped onto the plant zones. This mapping of damage for each harsh environment onto the plant zones creates a damage footprint for each environment. A composite damage footprint is created by superimposing the damage footprints for each of the harsh environments onto each other. Illustrations of damage footprints are shown in Figure 2. These footprints correspond to the layout of the example plant configuration previously displayed in Figure 1.

The failure criteria for this example consider three distinct damage mechanisms: (1) structural damage to a zone and its contents, (2) shock to equipment located in a given zone (i.e., excessive lateral acceleration), and (3) fire damage within a given zone. For each harsh environment, a definition of failure criteria for the SSCs must be defined. If conditions within a zone exceed the failure criteria for a particular environment, then all SSCs located in that zone that are susceptible to damage from that environment are considered to be destroyed.[2] In the case of structural damage, all equipment in the zone would be disabled. However, equipment susceptible to damage by fire, shock, or flood can vary depending on the specific type of equipment in the zone.

The structural damage footprint (top portion of Figure 2) indicates that Zone 5 has been subjected to structural insult,

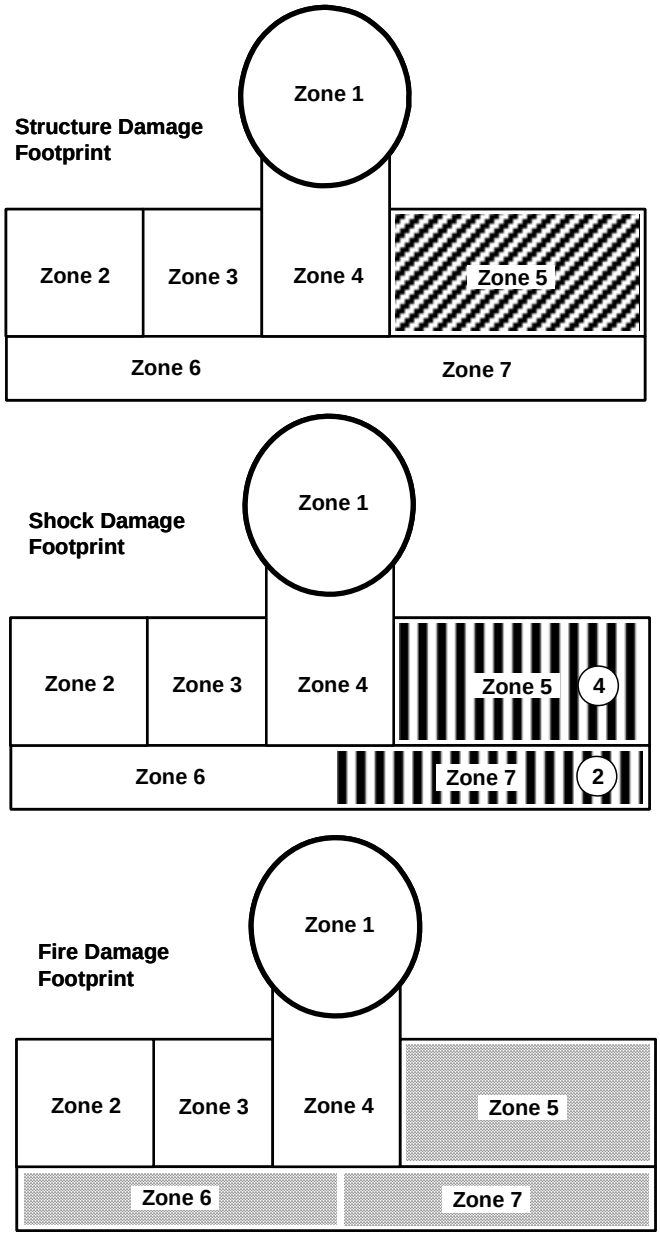


FIGURE 2. EXAMPLE DAMAGE FOOTPRINTS FOR THREE DAMAGE MECHANISMS

and all equipment within Zone 5 has been structurally damaged. However, structural damage is limited to this one zone. A shock insult, which is illustrated in the middle picture of Figure 2, subjects Zones 5 and 7 to some level of excessive lateral acceleration.

In this example, equipment in Zone 5 experiences accelerations of a "Level-4" magnitude (in addition to the structural insult), whereas equipment in Zone 7 experiences accelerations of a "Level-2" magnitude. Finally, an example fire damage footprint is shown in the bottom picture. Here, a fire has occurred in Zones, 5, 6, and 7.

The composite damage footprint for this example situation results in the following component failures:

[2] In this example, the failure criteria are applied in a binary pass/fail manner. That is, a probabilistic treatment of failure is not explicitly considered. However, in principle, information regarding the level of confidence associated with zone failure analysis could be included to refine the analysis using a probabilistic approach.

- Loss of the injection pump actuation signal transmitter (Zone 5) by structural damage.
- Loss of pump control cables (Zone 7) by fire (here the level of shock damage is presumed to be insufficient to destroy cabling),
- Loss of motive power to the pump as a result of fire damage to the MCC and power cables (Zone 6).

Although the pump, piping, and water supply tank all survive in this example, the injection system is nonetheless disabled due to the above electric power and/or control failures.

METHODOLOGY

The methodology described here is based on use of PRA models that use "large" fault trees to model systems (as opposed to some PRA models that employ "small" fault tree models combined with "large" event trees). This methodology also presumes that the PRA modeling software has the capability to transform fault tree basic events into physical locations. The software used in the work that forms the basis of this paper was the "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE)" code, developed at Idaho National Laboratory (1) for the USNRC. At a high level, the methodology for integrating damage footprints into PRA models involves several major steps as outlined in Figure 3.

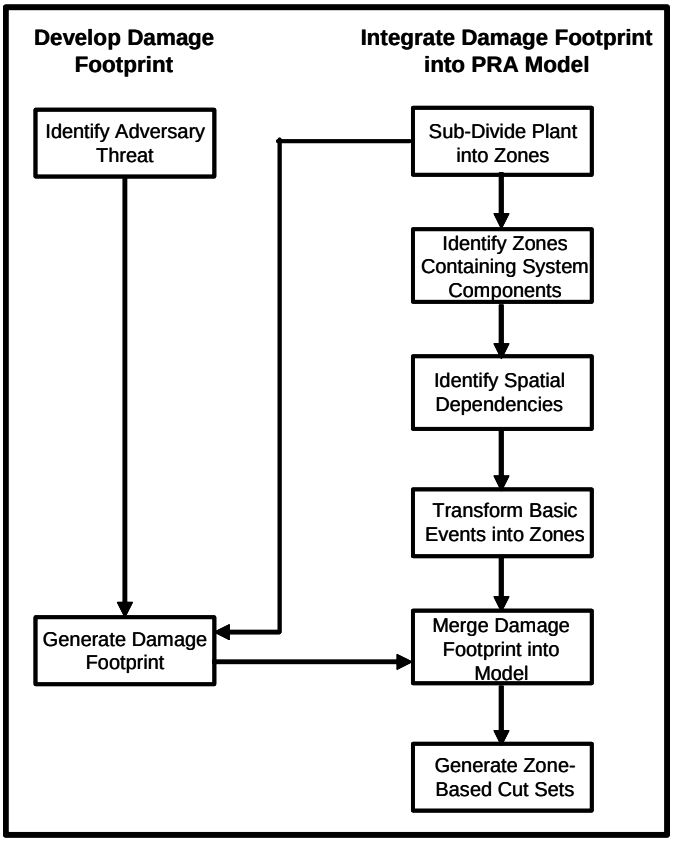


FIGURE 3. OVERVIEW OF ANALYSIS METHOD

Plant information from various diagrams, documents, and walk downs is assembled to identify the physical plant locations for components, including any pipes and cabling that are important to each SSC explicitly modeled in the PRA.

Sub-Divide Plant Into Zones

First, all elevations of the buildings that house SSCs associated with the emergency core cooling systems must be sub-divided into zones. A typical nuclear power plant analysis might include the reactor containment, reactor building, auxiliary building, turbine hall, control building, diesel generator building, pump houses, and/or water intake channels. The process of identifying the zones upon which each PRA basic event depends is very tedious and labor-intensive. The plant's fire fighting plans provide a good basis for a zoning scheme. Such plans at nuclear power plants often are based very closely along the actual architectural floor layouts (i.e., each fire fighting zone often is an actual room, hallway, stairwell, or other structure). The zones could also be given the same names as defined in the licensee's fire fighting plans. This can prove advantageous when communicating results among plant and utility personnel.

Identify Zones Containing System Components

Next, each SSC that is explicitly modeled as a basic event in the PRA must be linked to the zone in which it physically resides. This type of information is typically available through the use of equipment layout drawings or even some Piping and Instrumentation Diagrams (P&IDs). For certain components, licensee databases or plant systems engineers may need to be consulted.

Identify Spatial Dependencies

As stated earlier, harsh environments in zones distant from the component could render a component functionally inoperable. Three key spatial dependencies must be incorporated into the PRA for SSCs explicitly modeled as a basic event:

A. The locations of all system piping that is essential for a component to successfully perform its function,
B. The locations of all power cabling essential for successful operation of the component, and
C. The locations of all command and control cabling essential for successful operation of the component.

Piping and Mechanical Drawings are extremely useful for identifying the physical plant locations for system piping, but plant walk downs and consultations with plant systems engineers are extremely valuable as well. A similar process is used to identify the physical plant locations for any cables (both power and control) that are important to the component.

Transform Basic Events Into Spatially Informed Basic Events

All zone locations that are relevant to each PRA basic event are cataloged and subsequently incorporated into the fault tree models by transforming the fault tree basic events that represent random failures into basic events that represent physical damage from harsh environments in specific physical locations. The resultant basic events represent a spatially

informed model of the Emergency Core Cooling System (ECCS) and other systems modeled in the PRA.

Generate Spatially Informed Cut Sets

In the final steps, the damage footprints developed in a separate but complementary part of the analysis are merged into the PRA model to represent either failure or success for each spatially informed basic event. System fault trees are then solved to generate system-level cut sets that are expressed in terms of physical damage to specific plant locations.

The transformation of basic events into plant locations is illustrated in Figure 4. Here, the PRA event being transformed represents failure of the pump system previously shown in Figure 1. The original PRA event representing pump failure (shown on the upper left of Figure 4) is transformed into an "OR" logic gate. The "OR" gate means that the pump will fail if any one or more of its inputs occur. The transformation in Figure 4 is based on the susceptibility of individual components in the pump system as summarized in Table 1. In this hypothetical example, the potential shock levels range from 1 through 4, with 4 being the most severe. The signal transmitter has a shock damage threshold that corresponds to shock level 3, such that this transmitter will fail at either shock level 3 or 4. The MCC has a shock damage threshold that corresponds to shock level 4. It is assumed that the other components would be unaffected by potential shock insults.

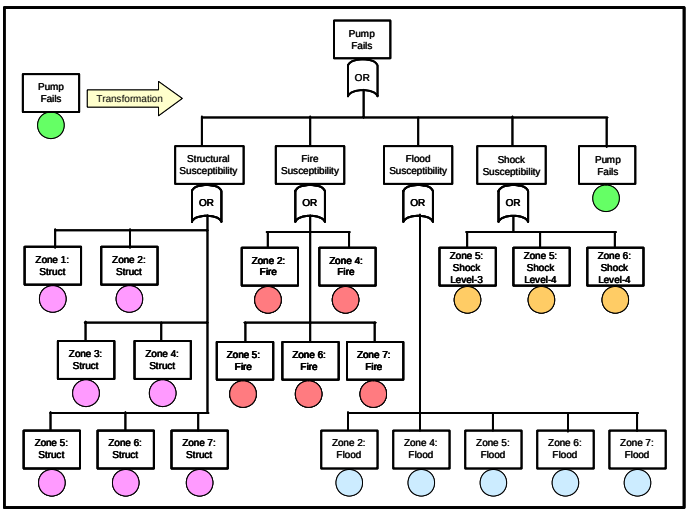


FIGURE 4. TRANSFORMATION OF BASIC EVENTS INTO LOCATIONS

The resultant fault tree model (Figure 4) is solved for the composite damage footprint associated with any hypothetical attack. Initially, all the events are set to a logic value of "FALSE" in the SAPHIRE code.[3] Then, the value for each individual spatially informed basic event is changed based on the locations of the various harsh environments as represented

[3] The use of the logical "FALSE" versus the quantitative 0.0 yields a tremendous computational advantage in SAPHIRE. Partially solved sub-branches with FALSE values in intermediate cut sets are eliminated from further solution, greatly reducing run times.

TABLE 1. SUSCEPTIBILITY OF EXAMPLE PUMP SYSTEM TO POSTULATIED DAMAGE MECHANISMS

Zone	Component	Damage Mechanism Susceptibility			
		Structural	*Fire*	*Flood*	*Shock*
1	Discharge piping	X			
2	Power supply, power cable	X	X	X	
3	Tank	X			
4	Pump	X	X	X	
5	Signal transmitter, control cable	X	X	X	X (level 3 or 4)
6	MCC, power cable	X	X	X	X (level 4)
7	Control cable	X	X	X	

in the damage footprint. Events representing zones subjected to a harsh environment are subsequently reset to a probability of 1.0; otherwise they remain "FALSE." The resultant model is then solved, with the solution expressed in terms of cut sets composed of the spatially informed basic events rather than specific system components. Figure 5 shows the events that would contribute to cut sets once the example damage footprint is applied.

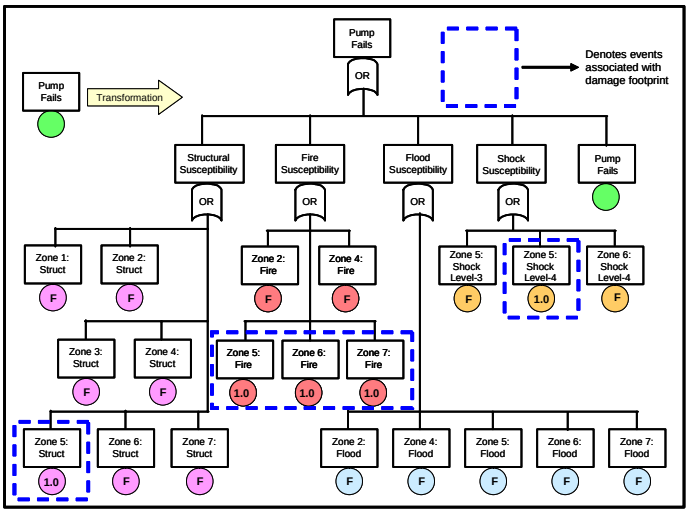


FIGURE 5. BASIC EVENTS WITH DAMAGE FOOTPRINTS APPLIED

The location transformation step described above is a critical step in the analysis, given that a component would lose its ability to operate if a suitable insult occurs in a physical location that contains a power supply, cable, or pipe section upon which that component is dependent. Again, a component can be rendered inoperable by an insult in a location distant from the physical location of the component because of damage to an important supporting component. The process shown in Figure 4 explicitly captures the susceptibility of a component to insults in distant locations.

Event Tree Solution

Once the system fault trees have been solved for spatially informed cut sets, one can determine whether or not the

hypothetical sabotage attack would result in core damage by solving the PRA event trees. However, unlike a traditional random failure analysis, the intent of this analysis is to determine if adequate equipment would survive to ensure the capability to achieve a safe shutdown configuration. Thus, the spatially informed system cut sets generated in the solution of the system fault trees represent a deterministic model of success or failure for each system. In other words, if any system fault tree solution results in so much as a single spatially informed cut set, then the system would be rendered inoperable from the impacts associated with the hypothetical attack. Multiple spatially informed cut sets would imply that the attack would create numerous combinations of harsh environments in various locations that would result in system failure.

Each system modeled in the PRA fault trees will either fail or succeed based on this deterministic assessment. Hence, the question to be answered for each hypothetical attack scenario is – does the resultant combination of system failures result in a core damage outcome or not? This question can be answered in a straight forward manner by selecting the appropriate event tree and tracing by hand the sequence of system failures and successes through the tree.[4]

Human Reliability and Recovery Events

For PRA basic events that rely on human operator actions, the same principles regarding failure or success apply as for SSCs. A PRA recovery event may fail either due to the destruction of the components necessary to take the action or a harsh environment which would prevent the operator from completing the action. An important consideration when assessing harsh environments for operators is to include both the actual location of the human action and the access route to those locations. For human actions which are still possible, the human reliability analysis may need to be revisited to account for the harsh environment's effects on the performance shaping factors included in the original PRA.

Furthermore, it should be noted that the result of a core damage outcome does not imply that the plant is inherently incapable of successfully surviving the hypothesized sabotage attack. It does imply that the plant, as modeled by the PRA, could be susceptible to such an attack in the absence of special measures taken by the licensee to further study and prepare to respond to, prevent, or mitigate the impacts of such an attack.

ADDITIONAL MODELING ISSUES

Limitations on Equipment Location Data

While a PRA contains numerous basic events, and thus models a large number of components, there is an enormous amount of critical equipment, such as cables and pipes, typically not included in the PRA. Therefore, the completeness of the spatial transformation of a PRA basic event depends upon the extent to which locations of cabling and piping can be determined. Identifying spatial information can be especially difficult for cables, as it is not unusual for licensees to have limited records regarding exact cable routing. This lack of spatial information regarding cable routing and piping can be treated with either a best-estimate or conservative approach. A best-estimate approach would gather as much information as possible, and then make logical estimates of locations for missing equipment. A conservative approach would presume that any PRA basic event for which complete information is not available fails as a result of the hypothetical attack. In many cases, a system can consist of such a large number of supporting components spread over many areas that the two options may produce similar results.

Timing of Component Failures

The timing of failures can also be an important modeling issue, depending on the types of insults and the types of functions. For example, structural damage could be expected to occur at a precise moment in time, resulting in the immediate destruction of all components located within the structural damage footprint. A fire, on the other hand, may take some time to spread through multiple areas. In this circumstance the type of function that a component performs is important. If a component such as a pump must continue to operate for a long period of time, then whether or not it ceases to function at time zero or some time later on may be irrelevant.[5] But a component such as an actuation circuit, which merely sends a start signal, may be credited as surviving a fire if the fire does not reach the component before it performs its function.

Instrumentation and Control Failure Modes

Instrumentation and control systems may require additional consideration. Depending on their design, such systems may or may not perform their intended functions when subjected to a particular insult. Extra effort may be necessary to identify the behavior of instrumentation and control systems as influenced by the postulated harsh environments.

Harsh Environment Phenomenology

Even if the threat capabilities of an adversary are well defined, there may be deterministic or stochastic uncertainties regarding the extent of damage that the adversary could cause within plant areas, thereby leading to uncertainties in the damage footprint. Because the method presented here applies failure criteria in a binary pass/fail manner, sensitivity analyses might be useful to address damage footprint

[4] The selection of the appropriate event tree is based upon the nature of the hypothetical attack. If a LOCA is created directly as a result of the attack, then a LOCA tree is appropriate. Otherwise it is reasonable to assume that any sabotage attack would be characterized as a transient initiator.

[5] However, the timing for failure of core cooling systems would be critical input to any source term calculations. In such cases the fire analysis associated with the threat assessment would be the basis for determining the time-to-failure for electrically dependent equipment.

uncertainties. More specifically, multiple sets of damage footprints could be generated for a given hypothetical attack to capture uncertainties regarding the extent of damage caused by the attack. In this way a spectrum of potential damage footprints could be assessed, resulting in a range of potential plant responses and outcomes to a hypothetical attack scenario.

CONCLUSIONS

In conclusion, this paper presents a straightforward approach to spatially inform a PRA for the purpose of analyzing the effects of security-related events at nuclear power plants. The spatially informed PRA is then combined with a "damage footprint" to first evaluate the functionality of each safety system. Then the ability of the overall plant to ensure a safe shutdown capability is evaluated.

The information collection process required to support this approach can be labor intensive and incomplete. However, modern software programs that facilitate the transformation of PRA random failure basic events into spatially informed basic events are a valuable tool that allows one to analyze the complex events that might occur from an intentional act of sabotage or terrorism, and to assess their impact upon plant safety.

REFERENCES

1) Theodore Wood, "Testing, Verifying, and Validating SAPHIRE Versions 6.0 and 7.0," NUREG/CR-6688, October 2000. Idaho National Laboratory, Idaho Falls, Idaho.