Focus areas for a Level 2 PSA that supports a site NPP risk analysis

D.M. Helton
United States Nuclear Regulatory Commission, Rockville, Maryland, USA

M. Zavisca & M. Khatib-Rahbar
Energy Research Incorporated, Rockville, Maryland, USA

ABSTRACT: The US Nuclear Regulatory Commission is developing a site Level 3 probabilistic safety analysis (PSA) for the two operating nuclear power plants, and associated spent nuclear fuel storage facilities at the Vogtle site. The development of this integrated PSA, along with its intended end-uses, shifts the focus in the Level 2 (accident progression and radiological source term) portion of the analysis toward greater realism. This paper describes ways in which this focus affects the analytical approach. Presently in the US, Level 2 PSAs for operating reactors are most frequently performed in either a simplified manner (to support environmental impact studies), or for comparison with a (safety case-related) figure-of-merit. These applications often rely on simplifying assumptions. The present Vogtle analysis is novel in its scope, encompassing all major radiological sources on the site in concert, while assessing a range of hazards and plant operating configurations. As risk assessment technology advances, as computational capabilities increase, and in light of the multi-unit event at Fukushima Daiichi, this type of PSA activity is expected to proliferate. Interactions between the nuclear safety and risk communities at this stage will facilitate the development of more efficient methods. This paper will describe the approach being taken in several areas of the reactor and the spent fuel pool Level 2 PSA to promote realism in the treatment of the overall site risk. These areas include structural failure characterization, modeling of severe accident phenomena, survivability of equipment and instrumentation, and modeling of accident management actions. Whereas a systems-level view of the subject site design and operation would suggest very little dependency between the two reactors and the SFPs, this paper will make the case that after one or more radiological sources have proceeded to a severe accident (i.e., fuel melting) the detailed overall site accident progression becomes very inter-dependent.

1 INRODUCTION

The United States Nuclear Regulatory Commission (US NRC) is developing a site Level 3 probabilistic safety analysis (PSA) for the two operating nuclear power plants, and associated spent nuclear fuel storage facilities at the Vogtle site in Georgia, USA. In nuclear power plant risk assessment terminology, Level 3 refers to the modeling of accidents from their initiation to the offsite consequences caused by the accidents (public health effects and property damage). The scope of the Vogtle Level 3 PSA is events caused by both internal and external hazards, excluding acts of sabotage. The development of this integrated (a.k.a., extended) PSA, along with its intended end-uses, shifts the focus in the Level 2 (accident progression and radiological source term) portion of the analysis toward greater realism.

This paper describes ways in which this focus affects the analytical approach. Presently in the US, Level 2 PSAs for operating reactors are most frequently performed in either a simplified manner (to support environmental impact studies), or for comparison with a safety case-related figure-of-merit such as large early release frequency. These applications often rely on simplifying assumptions. The present Vogtle analysis is novel in its scope, encompassing all major radiological sources on the site in concert, while assessing a range of hazards and plant operating configurations.

This paper will describe the approach being taken in several areas of the reactor and the spent fuel pool Level 2 PSA to promote realism in the treatment of the overall site risk. Specifically, the following sections describe the modeling approach in the areas of structural failure characterization, severe accident phenomena, survivability of equipment and instrumentation, and severe accident management. In each section, examples are given where realistic treatment

leads to better estimation of site-wide accident interactions. In addition to the interplays between radiological sources within a given modeling area, the paper will also point out the way in which these different modeling results inherently affect the other modeling areas. Whereas a systems-level view of the subject site design and operation would suggest very little dependency between the two reactors and the SFPs, this paper will make the case that after one or more radiological sources have proceeded to a severe accident (i.e., fuel melting) the detailed overall site accident progression becomes very interdependent.

2 STRUCTURAL FAILURE CHARACTERIZATION

In the structural failure characterizations for the reactor and spent fuel pool Level 2 PSA modeling, NRC is relying on a combination of (i) past assessments, (ii) new calculations using three-dimensional finite element analysis in conjunction with statistical data for the failure strain of the liner materials, as well as models for tearing of the liner, and (iii) assessments using engineering criteria. Of particular interest here are the characterizations of containment severe-accident-induced failure and spent fuel pool seismic failure.

Vogtle's physical layout is typical of dual-unit US pressurized water reactors. The two containments are each surrounded by other structures for large portions of the azimuth (the extent varies by elevation), namely the equipment building and the main steam valve rooms. The spent fuel pools are located in-line, between the two reactor containments, with a distinct pool for each reactor. The two pools are normally hydraulically connected to one another through a common cask loading pool, via fuel transfer gates that extend to an elevation just above the spent fuel storage racks. The containment design is typical of pre-stressed concrete containments, having a tendon gallery (square cross-section tunnel) that extends the full 360-degrees of the azimuth, oriented just below the containment's external wall. The tendon gallery is accessed through three vertical shafts: one accessed in the yard (i.e., open to the environment), one accessed through the control building roof, and the other accessed through the equipment building. Numerous electrical and piping containment penetrations exist in both the portions of the containment surrounded by other structures and those leading to the yard. The containment has three access points: the main equipment hatch opens to the yard, the personnel airlock leads to the equipment building, and the emergency airlock leads to one of the tendon gallery access shafts.

The results of the new containment calculations have been compared back to the structural assessments performed by the licensee during the Individual Plant Examination study (1990s), and are also leveraging the failure characterization work stemming from extensive experimental and analytical investigation performed at Sandia National Laboratories (e.g., Petti et al., 2013).

The updated containment analyses estimate that the internal static pressure at which enhanced leakage initiation would occur is roughly the same as estimated in the IPE study (e.g., 7% variation relative to the failure pressure) for the wall-basemat junction, the equipment hatch, the emergency airlock, and the personnel airlock. For the wall-basemat junction failure, the assessments indicate that cracks would develop at the base of the wall and basemat slab and that the likely leakage path would be through cracks in the concrete extending to the tendon gallery under the containment wall (this was not addressed by the IPE analysis). This in turn would pressurize the tendon gallery, potentially failing the doors connecting to the access shaft. The resulting failure area for all of the aforementioned failure locations is expected to be only large enough to prevent further pressure escalation. Based on site-specific MELCOR analyses focusing on long-term molten core concrete interaction, and separately on the results of the structural analysis, this leakage area could range from $2 \cdot 10^{-3}$ m^2 to 0.1 m^2.

From a site Level 3 PSA perspective, the range of potential static over-pressure failures presents an interesting spectrum of possibiilities between environmental radiological releases and habitability / survivability concerns. First, wall-basemat junction failure in to the tendon gallery may cause habitability concerns (temperature, combustible gas, and radiological) in areas near the equipment building tendon gallery access shaft. This in turn has implications for both instrument and equipment survivability and local operator accident management actions, some aspects of which are discussed later. The surrounding structures are relatively compartmentalized, but clearly not designed to accommodate combustion events. Thus, the zone of influence of these habitability and survivability concerns becomes greater if a combustion occurs.

Similarly, other potential failure locations include a mix of release pathways, ranging from those that are preferentially directly to the environment (the equipment hatch), those that are preferentially in to surrounding structures (the personnel airlock), and those that have components of both (the emergency

airlock). It's also important to note that the non-catastrophic nature of the rupture will limit the rate of change of containment and ex-containment conditions following failure, which may affect the likelihood of combustion and its effects. While a particular failure location must be assumed for deterministic reactor analysis, the range of failure locations may be an important modeling uncertainty for the integrated risk analysis.

The spent fuel pool assessments are ongoing as of this writing, but preliminarily indicate that spent fuel pool failure caused by very large seismic accelerations (e.g., accelerations that are an order of magnitude higher than the plant's design basis), were it to occur, would preferentially occur at the bottom of the pool wall. The failure would be oriented such that the associated tear in the spent fuel pool liner would potentially occur at an elevation above the rack baseplate. In terms of propagating effects, the immediate implication is the flooding of areas that surround the backside of the pool wall. Much of this flooded area does not contain instrumentation or other equipment, and does have floor drains. If the drains are not able to keep up with the water flow, the potential exists for the failure of doors leading to internal flooding in areas that contain instrumentation and accident mitigation equipment. This also has the potential to affect both reactor and spent fuel pool accident management actions. In this case, a simplified SFP MELCOR model has been developed to aid in the tracking of conditions within and around the SFP, prior to significant fuel uncovery (at which point a more detailed MELCOR model is employed). These inter-dependencies from a structural failure and physical layout perspective represent important considerations for the integrated site risk analysis.

3 SEVERE ACCIDENT PHENOMENA

MELCOR 2.1 is being used to support the deterministic accident progression modeling in the Vogtle project. MELCOR is a fully integrated, system-level computer code that models the progression of severe accidents in light-water reactor nuclear power plants. MELCOR development is led by Sandia National Laboratories under NRC sponsorship, and is the successor to the Source Term Code package. A broad spectrum of severe accident phenomena in both boiling and pressurized water reactors is treated in MELCOR in a unified framework. These include thermal-hydraulic response in the reactor coolant system, reactor cavity, containment, and confinement buildings; core heatup, degradation, and relocation; core-concrete attack; hydrogen and other combustible gas production, transport, and combustion; and fission product release and transport behavior. In some cases, MELCOR results are used as boundary conditions to stand-alone tools to investigate specific phenomena (e.g., detonation).

In the Vogtle project, MELCOR is being used for confirmatory reactor Level 1 success criteria and accident sequence development activities (leveraging the licensee's existing Level 1 PSA), reactor severe accident progression (Level 2 PSA) activities, and all aspects of the spent fuel pool deterministic accident progression modeling. When convolving the physical characteristics of the Vogtle plant with the strengths and limitations of MELCOR, it was decided to construct and exercise three MELCOR models. The first represents one unit's reactor and containment in detail, along with a simplified treatment of the surrounding structures. The second represents both spent fuel pools and the fuel handling building, in a detailed fashion. The third model represents one containment, both spent fuel pools, and the fuel handling building in a simplified manner that is conducive to fast-running sequence timing calculations prior to fuel melting. As of this writing, the first and third models have been developed and extensively tested. The second model is currently under development.

Beyond the general need for more models and additional modeling flexibilities, the site risk characterization being developed leads to specific situations where the project scope influences accident modeling decisions. The first example is one that was highlighted by both the Fukushima Daiichi accident, as well as the concurrent NRC State-of-the-Art Reactor Consequence Analysis project (Chang et al., 2012), and involves the modeling of hydrogen (and other combustible gas) generation and transport. Customarily, combustible gasses are tracked within the containment as a potential cause of containment failure. However, when they leak out of containment, they pose a challenge to reactor accident management, site accident management, and as a potential means of instigating or exacerbating an accident at another onsite radiological source (e.g., the spent fuel pool). Given the proximity and inter-connectedness of the auxiliary building, fuel handling building, equipment building, and control building, a combustion event in one of these structures has the potential to cause problems in any of the other. That said, these buildings at Vogtle are generally very compartmentalized, which may limit the zone of influence of a combustion event. However, this compartmentalization makes realistic modeling of such events difficult with the current state-of-practice. Here the project is taking a bal-

anced approach. Pathways between the containment and these structures are modeled and the various elevations of the structures are modeled. However, details about compartmentalization within an elevation (e.g., the breakdown in air space volumes, the failure characteristics of intervening doors, etc.) are not modeled. This allows for statements about the potential for spatial interactions, without investing the significant resources needed to model the issue in a more sophisticated fashion (which might belie the uncertainties in leakage pathways and combustible gas transport modeling).

As another example of where the project is striving for greater realism, MELCOR results are being used directly in the assessment of accident management actions. This will be discussed in more detail later in the paper; here the focus is on the MELCOR modeling. Since the occurrence of a significant event onsite could impact the effectiveness of diagnosis or implementation activities associated with accident management, it is important to account for such events in the context of the human reliability modeling. Specifically, the onset of core damage, the rupture of the vessel, a combustion event, and the failure of containment are each being tracked closely from both the traditional accident release perspective and as a discrete event that could affect the reliability of the ongoing diagnosis and implementation activities. This situation was seen most clearly in the Fukushima accident, in which combustion events interrupted efforts to restore power, damaged hardware (e.g., a vent valve, fire hoses), injured personnel, scattered radiological material which in turn affected access, and caused evacuation of non-essential personnel (INPO, 2011), (Government of Japan, 2011), and (The National Diet of Japan, 2012).

4 SURVIVABILITY OF EQUIPMENT AND INSTRUMENTATION

The purpose of equipment and instrumentation survivability assessment is to ensure that hardware is not being credited when it would in fact be expected to fail due to the environmental conditions to which it is exposed. Instrumentation survivability is critical to the navigation through severe accident management guidelines because plant conditions (as measured through instrumentation) is the means of establishing accident management priorities and weighing the pros and cons of taking a specific action.

The two main tools for establishing the loads on instrumentation and equipment are the scenario characterization (e.g., stuck-open relief valves, interfacing system pipe ruptures) and the deterministic analyses (in this case the aforementioned three-dimensional finite element analysis and MELCOR analysis). The conditions of interest are humidity, static and dynamic pressure, temperature, and radiation. All of these except radiation are readily calculated by MELCOR, though dynamic temperature and pressure estimation requires additional investigation using separate tools for specific phenomena (e.g., detonation). Near-field radiation can also be estimated based on MELCOR outputs (e.g., see Section 4.3.5 of LaChance et al., 2012), however the Vogtle project handles this more qualitatively. Tentatively, ex-containment equipment not exposed to high radiation fields during design-basis accidents (and thus not subjected to high radiation fields during environmental qualification) is assumed to fail if exposed to such conditions during a given scenario (e.g., equipment near an interfacing system pipe rupture unsubmerged break following core damage). The same general treatment is given for humidity.

Temperature and pressure loads are extracted for various plant locations using the MELCOR results of representative scenarios, in order to develop trends. These loads are compared for various phases of the accident (post core-damage) against the environmental qualifications of the plant equipment and instrumentation within the same location, to estimate whether the equipment / instrument's survival is: (i) likely; (ii) not likely; or (iii) indeterminate. In some cases significant interpretation is required (e.g., the environmental qualifications do not explicitly account for dynamic loads caused by combustion events), which increases the likelihood of reaching an indeterminate finding in those circumstances. A list is made of those that are indeterminate for future investigation, depending on their overall contribution to the release category results. As discussed in the previous section, the MELCOR model is capable of calculating environmental conditions in the containment with high resolution (relative to the spatial resolution of equipment qualification information), and low resolution in the surrounding structures.

As an example of where site integration presents new challenges, consider the case of a hydrogen deflagration in the equipment building (the portion of the auxiliary and fuel handling buildings directly adjoining containment), caused by containment penetration leakage. Such an event has the potential to cause high pressures (and temperatures) in this area of the plant. As is typical of PWR designs, the cabling for ac power and dc control for the spent fuel pool cooling pumps is also located in this general area. Thus, hydrogen (or carbon monoxide) emanating from a reactor accident, migrating in to the equipment building from a containment penetration

leak, has the potential to damage equipment and instrumentation used for normal, abnormal, and accident SFP cooling. This type of interaction can only be assessed by investigating the containment leakage paths and environmental loads caused by the reactor accidents, and comparing them on a spatial basis, to the equipment and instrument environmental capacities of potentially-affected equipment.

A second example posits a similar situation, but in reverse. In the unlikely event that an SFP drainage accident goes unterminated (e.g., due to a large seismic event tearing the SFP liner), the resulting oxidation of SFP fuel in a steam environment can produce hydrogen (the same as a reactor accident), resulting in a hydrogen combustion event. Due to the proximity of the SFP to the auxiliary and control buildings, that has the potential to damage instrumentation used in reactor accident management (e.g., containment purge instrumentation used in controlled venting, hydrogen sampling equipment used in assessing the likelihood of in-containment hydrogen combustion events). This has the potential to adversely affect concurrent accident management activities associated with preventing core damage or mitigating fission product release from the reactor.

5 ACCIDENT MANAGEMENT

The final area of focus in this paper is accident management, which is affected by each of the previous areas. Here, the central focus is the plant's Severe Accident Management Guidelines (SAMGs), with other procedures and guidance (e.g., the Extensive Damage Mitigation Guidelines (EDMGs)) playing a supporting role. Again, the MELCOR results are used to characterize the accident. Specifically, output streams have been built in to the MELCOR model to provide all parameters used by the SAMG diagnostic flow chart and severe challenge status tree, as well as the computational aids that accompany the 12 specific guidelines documents. The exceptions are two guideline entry conditions that are based on projected or measured site doses, which for this project are assessed using trial runs of the US NRC's incident response computer code RASCAL (Radiological Assessment System for Consequence AnaLysis). The plant is being studied as it existed in 2012, so the changes presently being made to the US SAMGs (e.g., see LaBarge et al., 2013) do not apply. Similarly, the changes that will be made in response to ongoing NRC rulemaking related to SAMGs (e.g., US NRC, 2013) also do not apply.

The three basic steps of the human reliability analysis being performed to characterize accident management are identification of those actions to be modeled deterministically (based on a finite number of accident progression analyses), the assignment of screening (or simplified) probabilities that the action is not performed, and the development of more detailed probability bases for a subset of these actions. Identification is based on three aspects of the potential action: priority (relying on the hierarchical nature of the Vogtle SAMGs); duration of time that the entrance criteria for that action are met; and habitability. The screening probabilities are based on a combination of considerations related to: (i) instrumentation availability, (ii) priority, (iii) dependency, (iv) duration of entrance conditions being met, (v) the occurrence of significant accident progression events (vessel failure, containment failure, and combustion events), (vi) familiarity relative to emergency operating procedure and EDMG training, and (vii) survivability considerations. The goal is to then extract the trends and insights from these detailed analyses to inform an otherwise experience-based probabilistic modeling of accident management. The approach for the more detailed probability bases for a subset of the actions is under development.

Again, two examples are given where site integration adds complexity to the assessment of this focus area. The first example simply deals with the fact that the current (circa 2012) site accident management infrastructure is predominantly focused on dealing with a single-unit accident. Most notably, there is a single technical support center, a single operations support center, and (in some instances) a single set of supporting accident management equipment. Having multiple TSCs or OSCs is not inherently necessary, and limitations on staffing and equipment are being addressed through ongoing NRC activities. Nevertheless, it is the case that the accident management response involving more than one radiological source on-site will be coupled. To the extent that there may not be sufficient capacity to deal with multiple events completely in parallel, actions for a given source (be it diagnosis or implementation-oriented) will have to be prioritized within the overall site response. In cases where insufficient equipment exists, a decision will be needed to prioritize the deployment of that equipment (e.g., an ac-independent pump) to one radiological source over another. At best, the timing of the accident is such that it can be used in a serial fashion to try and mitigate the concurrent accidents. Given the potential number of instances where competing demands may exist in the site PSA, it may be necessary to take a retrospective approach (i.e., identify important instances of conflicts once results have been obtained without consideration of conflicts).

The second example is one where an accident at one radiological source creates a habitability challenge in an area needed to take a local action to mitigate an accident at another radiological source. For instance, if all cooling is lost to the SFP and the decay heat in the SFP is high, it will eventually begin to boil. This creates a high-humidity, high-temperature condition within the fuel handling building. Portions of the fuel handling building are connected to the auxiliary and equipment buildings through normal doors. This potentially inhibits access to these areas, and poses operational challenges for preparing individuals to go in to these areas (fire-fighting turnout gear is typically designed for dry, rather than wet, heat). As such, an action that relies on connecting temporary hoses to a fire-header standpipe in order to refill a tank that will be used as part of a reactor mitigation strategy, could be greatly complicated if that stand-pipe is in the affected area of the auxiliary building. In related existing human reliability analysis guidance (Cooper, 2012) this plays in to the assessment of both feasibility and reliability.

6 CONCLUSION

This paper has described the approach being taken in several areas of the reactor and the spent fuel Level 2 PSA portions of the US NRC's Vogtle site PSA project to promote realism in the treatment of the overall site risk. While there are a number of complex challenges associated with analyzing and preparing for multi-unit nuclear power plant accidents, this paper shows the values of applying the existing tool set, in order to anticipate challenges that may arise, so that they can be contemplated and addressed prior to an accident occurring. As risk assessment technology advances, as computational capabilities increase, and in light of the multi-unit event at Fukushima Daiichi, this type of PSA activity is expected to proliferate within the US and elsewhere. Interactions between technical disciplines within the nuclear safety and risk communities at this stage will facilitate the development of more efficient methods. Interactions will also aid in identifying the potential site complexities that are more likely to manifest themselves for given design types, versus those that are simply theoretical.

REFERENCES

Chang et al., "State-of-the-Art Reactor Consequence Analyses (SOARCA) Report," NUREG-1935, US Nuclear Regulatory Commission, 2012.

Cooper et al., "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines," NUREG-1921 and EPRI TR-1023001, 2012.

Institute of Nuclear Power Operations (INPO), "Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station," INPO 11-005, November 2011.

Government of Japan, "Investigation Committee on the Accident at the Fukushima Nuclear Power Stations of Tokyo Electric Power Company, Interim Report," December 26, 2011.

LaBarge et al., "Insights from Development of the Combined PWR SAMG," *ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Columbia*, SC, September 22-26, 2013.

LaChance et al., "Discrete Dynamic Probabilistic Risk Assessment Model Development and Application," SAND2012-9346, Sandia National Laboratories, 2012.

The National Diet of Japan, "The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission," July 2012.

Petti et al., "Effects of Degradation on the Severe Accident Consequences for a PWR Plant with a Reinforced Concrete Containment Vessel," NUREG/CR-7149, US Nuclear Regulatory Commisison, 2013.

US NRC, "Onsite Emergency Response Capabilities," Proposed Rule, in *Federal Register* Vol. 78, No. 221, 68774-68775, November 15, 2013.