ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis
Columbia, SC, September 22-26, 2013, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2013)

SAND2013-3966C

SECURITY RISK MANAGEMENT OF SMALL MODULAR REACTORS

Benjamin B. Cipiti, Gregory D. Wyss, Felicia A. Durán, and Tom G. Lewis
Sandia National Laboratories*
P.O. Box 5800 MS 0747, Albuquerque, NM 87185-0747
bbcipit@sandia.gov

ABSTRACT (Abstract Head)

Traditional physical security analysis of nuclear facilities utilizes probabilistic risk assessment to inform a vulnerability assessment. However, determining a range of possible security threats to a nuclear facility using probability of attack is extremely difficult to model. Recent work at Sandia National Laboratories (SNL) characterizes a facility's security risk for a scenario in terms of level of difficulty an adversary would encounter in order to be reasonably sure of success (the Risk Informed Management of Enterprise Security (RIMES) methodology). Scenarios with lower levels of difficulty can then be addressed through design changes or improvements to the physical protection system. This work evaluates the level of difficulty of a number of attack scenarios for Small Modular Reactors (SMRs), and provides insight to help designers optimize the protection of their facilities. The methodology and general insights are described here.

Key Words: Security, SMR, RIMES, Risk Assessment

1 INTRODUCTION

Nuclear facilities face increasing economic challenges in meeting safety, security, and safeguards regulations. Small Modular Reactors (SMRs) in particular need to optimize these costs in order to produce power economically. The goal of this work was to apply the Risk Informed Management of Enterprise Security (RIMES) methodology as an additional security tool for optimizing design changes during security risk assessment.

The RIMES methodology focuses on the level of difficulty of a particular attack scenario as opposed to trying to model the probability that the attack scenario will occur. Then scenarios can be compared based on their consequence and difficulty level. The shift to attack difficulty allows designers to manage risk more effectively by targeting security investments where they are needed most.

The methodology was applied to a generic integral pressurize water reactor (iPWR) SMR design that was developed in parallel with this work. This generic design pulled from many of the common features of iPWRs as available in the open literature in order to provide a basis for security, safety, and safeguards analyses. The goal of the analysis is to develop insights into managing security risks that would be applicable to all SMR designs as opposed to focusing on one specific design.

* Sandia National Laboratories is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

2 BACKGROUND

SMRs face licensing issues with the Nuclear Regulatory Commission (NRC) since past regulations were written for large LWRs—some of the regulations do not fit as well with smaller reactor designs. These issues were first outlined in an American Nuclear Society Special Committee on Small and Medium Sized Reactor Generic Licensing Issues [1]. NRC has been working with the SMR vendors and the Nuclear Energy Institute to address these issues. The concerns related to physical security are focused on staffing requirements and overall costs. If physical security design and staffing requirements are the same as large LWRs, the costs would be proportionally much larger for SMRs that produce less electricity. Also, smaller source terms and use of new technology may provide opportunities for limiting security staffing. New analyses are required to determine if these costs can be minimized while still achieving adequate physical protection.

2.1 RIMES Methodology

Traditional security risk assessment considers three components: threat, vulnerability, and consequence. For high consequence facilities, attacks are so rare that estimating the probability of attack is extremely difficult. As a result, analysts neglect the probability of attack and assess a conditional risk given that the attack would occur. However, the use of conditional risks limits the effectiveness of doing cost-benefit analyses.

The RIMES methodology instead considers the degree of difficulty for an adversary to successfully accomplish a specific attack scenario [2]. The triplet for security risk then becomes $<s_i, d_i, c_i>$ where d_i is the degree of difficulty for an adversary to successfully accomplish attack scenario s_i at a specific target in order to cause consequence c_i. The RIMES methodology then plots the consequence as a function of difficulty for a large cross-section of attacks of interest. The security analyst would be most concerned with scenarios with both a higher consequence and lower difficulty. Security upgrades may then be considered that will either reduce the consequence or make the attack more difficult.

Although the work described here is focused on an individual facility type, RIMES is also meant to be applied across an entire enterprise to determine if there are other easier targets. For example, in the nuclear fuel cycle, theft of material after mining might be easier than theft of material from a reactor. This type of analysis across the entire enterprise helps to keep security costs reasonable for individual facilities.

The RIMES methodology examines 7 parameters during attack planning and preparation and 6 parameters during attack execution, for a total of 13 parameters. Each dimension is given a difficulty level from 1-5. Table I describes the general characteristics of each level. These levels are not linear, and generally thought to vary by powers of 3. For example, a level 3 is felt to be three times more difficult than a level 2. This powers of 3 scaling is also used in aggregating the scores.

The 13 parameters are described to a limited degree in Tables II and III, although the level guidelines have been developed with more detail than shown here. These parameters are felt to adequately model a broad range of types of attacks.

Table I. RIMES difficulty levels

Level 1	Level 2	Level 3	Level 4	Level 5
Easy to get/do	Moderately easy to get/do	Difficult	Very difficult	Extremely difficult to get/do
Capability available by legal means	Requires capability similar to criminal activity	Requires capability similar to organized criminal activity	Requires sophisticated capability similar to large corporation	Requires state-supported capability
Requires no special skills	Requires low-level skills (~days of training)	Requires moderate-level skills (~months of training)	Requires high-level skills (~many months of training)	Requires highly specialized skills (~multiple years of training)
Achievable in very short time (~days)	May require ~weeks to achieve	May require ~months to achieve	May require ~many months to achieve	May require very long time to achieve (~multiple years)
Easily accessible by general public	Accessible to public with moderate-level knowledge	Accessible to specialized groups		Accessible only by elites.
Essentially no early warning signatures - little risk to adversary of disruption	Some early warning signatures – some risk of disruption			Very large early warning signatures – great risk of disruption
Rudimentary				Very sophisticated

Note that for each attack scenario, each of the 13 parameters may be assigned a different difficulty level. For example, a stealthy scenario that requires insiders will likely have higher difficulty ratings for the Insider Participation, Insider Access, Stealth & Covertness, and Insider Commitment parameters while possible having low difficulty levels for other areas. A brute force outsider attack will likely have higher difficulty ratings for Outsider Participation, Training, Tools, and Outsider Commitment with lower difficulty ratings for other areas.

The powers of 3 scoring system helps to account for the various levels of difficulty. For example, a scenario with difficulty ratings of all 1's except for a simgle difficulty rating of 5 would still lead to a high overall difficulty. It should be noted that aggregating a scenario down into one final score is not as useful for risk management as looking at the entire table of difficulty ratings. The aggregate score may show problem scenarios that should be addressed, but these aggregate numbers should be taken lightly.

Table II. Attack preparation difficulty matrix

Attack Preparation Dimension	Outsider Partici-pation	Training & Expertise	Support Structure	Tools	Insider Partici-pation	Insider Access	Ingenuity
Level 1	Individual (1)	Self-taught Open source No practice	Minimal, prep. easily concealed	Available on open market	None	None	Straight-forward approach
Level 2	Small Team (2-5)	Professional training in one area	Small, ~10 support personnel,	Legally available but controlled	Potentially 1 (unwitting)	Limited, low-level security access	Rare but known approach
Level 3	Large Team (6-12)	Professional Training in critical tasks	Training facilities, skilled intelligence	Typical of insurgency, terrorist enterprises	1 Insider	Access to moderately protected areas	Logical but no instance of historical use
Level 4	Few Large Teams (12-36)	Professional training in all areas, practice on mock-ups	Professional sub-state intelligence network	Typical of small military units, state of the art	Multiple Independent	Restricted areas, compromise of multiple controls	Very imaginative, not likely to be anticipated
Level 5	Many Large Teams (40+)	Professional training in all areas, cross-training, well-rehearsed	Massive, state-supported, extensive intelligence network	Typical of special ops, heavy military, special purpose	Multiple Coordinated	Highly restricted areas, compromise multiple rig-orous cont.	Unique, total surprise, completely befuddle defenses

Table III. Attack execution difficulty matrix

Attack Execution Dimension	Situational Under-standing	Stealth/ Covertness	Outsider Commitment	Insider Commitment	Complexity	Flexibility
Level 1	Minimal, predictable vulnerabilities	None or minimal	Minimal risk	None	Single attack with simple mode	Single course of action
Level 2	Vulnerabilities require skillful observation	Some subterfuge required	Risk of attribution, little risk of casualties	Minimal personal risk, unintentional	Single avenue of attack with a complex task	Single course with minimal adaptation
Level 3	Vulnerabilities unpredictable and infrequent	Requires undetection over moderate time	Direct attribution likely, fatalities possible	Modest personal risk, attribution possible	Several coordinated attacks, some complex	Some adaption required
Level 4	Vulnerabilities unpredictable and infrequent with small signatures	Requires undetection over significant time	Fatalities likely, direct attribution	Significant personal risk, attribution probable	Multiple complex attacks that require coordination	Adaptation like required
Level 5	Extraordinary, vulnerabilities are fleeting and few	Multiple undetected operations over extended time	Selfless team sacrifice, attribution of supporters almost certain	Extreme personal risk, attribution certain,	Multiple, complex tasks that require precise timing	Significant tactical adjustment required

2.2 SMR iPWR Generic Design

Although a wide variety of SMR designs exist today, the more near-term designs are similar to current large LWRs. The integral PWR SMR designs include the steam generator within the reactor pressure vessel. In addition to smaller core sizes, these designs include fewer penetrations into the reactor vessel, more reliance on passive safety, and reduced need for operator action following accidents. These reactors are designed with the latest ideas in reactor safety.

The NuScale, Babcock & Wilcox mPower, and Westinghouse SMR designs are the farthest along of the iPWR SMRs, and also have the most information available. However, in order to provide results for this work that would be applicable to all, a parallel effort at Sandia developed a generic SMR design strictly for these types of security, safety, and safeguards analyses. This design pulled from open literature from the vendors and other open reactor designs. The full generic design, including all references used, is described in [2].

Figure 1 shows the overall plant layout for the generic design. This design assumes a 300 MWe reactor with up to four units per site. One control room is designed to control two reactors, and all four reactors share a common fuel service and maintenance building. The physical protection system is a fairly standard design with critical assets insider a Perimeter Intrusion Detection and Assessment System (PIDAS), while the entire site is contained within a Limited Area.

The nuclear island is arranged to control and minimize access of personnel/equipment entering safety-related structures. Access to the nuclear island is restricted by security measures throughout the complex. Safety-related equipment and nuclear material is placed below grade. Outside of the nuclear island, several other non-safety structures exist.

The reactor building is a seismic category 1 reinforced concrete structure. The building is 7 stories, with 5 below grade which house most critical components. Below grade, the building is divided into two sections with redundant systems in order to prevent/slow the progression of antagonistic conditions. The two above grade floors house non safety grade diesel generators, diesel tanks, HVAC equipment, and an ultimate heat sink (UHS) tank.

Reference 2 also describes the reactor building layout in detail and physical protection elements in place. Again, the purpose of the generic design is simply to provide a starting point on which to base the security analyses.

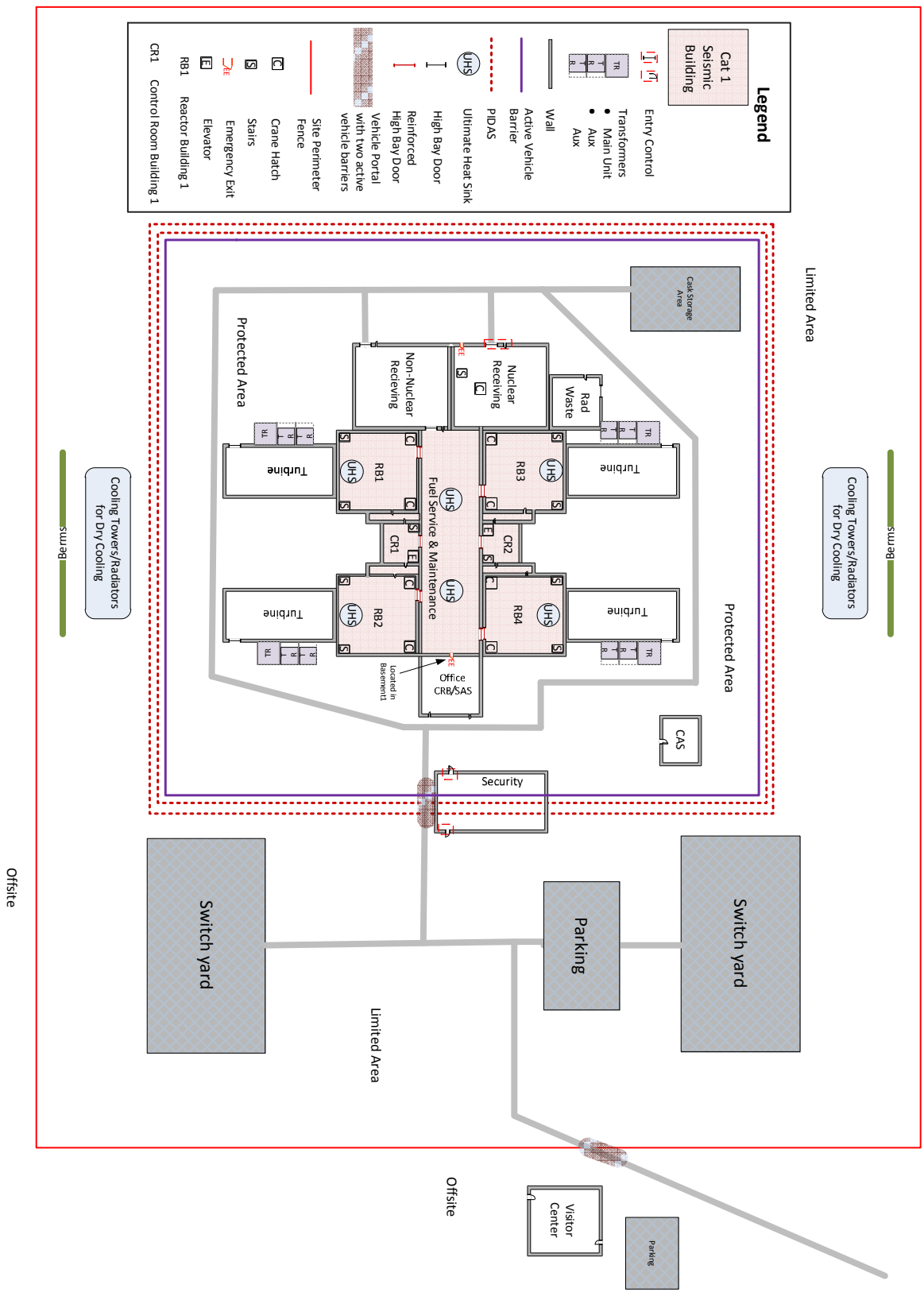

Figure 1. Generic SMR design site layout

3 RIMES ANALYSIS

The focus of RIMES is security risk management as opposed to security risk assessment. RIMES is not used instead of, but rather in conjunction with convention physical protection vulnerability assessment methods. Scenario discovery will likely use other methods, but RIMES allows designers to focus on a subset of scenarios of concern. Traditionally, a path analysis, scenario analysis, and neutralization analysis would be done first. Target and vital area identification are informed with a safety PRA. Since that information was not available, a list of target areas and critical systems was first developed in order to determine targets for attack scenarios.

This analysis looked at both theft and sabotage scenarios. The consequences of these scenarios were ranked qualitatively into four groups: economic damage only, economic damage with small release, large economic damage with core melt, and large economic damage with large release. For the core melt scenarios, the analysis examined the general safety systems that are expected in SMR designs to determine what combination of systems would need to be disabled in order to cause fuel damage and possibly release.

Expert elicitation was used for the RIMES analysis. Roughly 6 technical staff members at Sandia were involved in the discussions with backgrounds that included security risk, reactor safety, reactor design, and response forces. The difficulty matrices helped to keep the results consistent, although there were occasional minor disagreements about difficulty levels,. Any such disagreements were only 1 difficult level off, and usually made only a minor impact on the overall scoring.

A total of 15 scenarios have been examined, though additional scenarios are currently being considered. These include 5 economic damage only scenarios, 1 economic damage with small release scenario, 1 theft scenario, 7 core melt scenarios with varying consequence, and 1 spent fuel sabotage scenario. Some of these scenarios considered design perturbations to examine how design changes can affect difficulty levels.

Notional results are shown in Table IV to demonstrate how results may look. The aggregate score uses the powers of 3 scaling, so a level 1=1, level 2=3, level 3=9, level 4=27, and level 5=81. The levels in the table use this scoring and add up the total to determine the aggregate. Ranges propagate into a range for the aggregate score. When multiple scenarios are examined, the results are plotted like shown in Figure 2.

Scenarios with lower consequence typically have lower difficult ratings. Some of the economic sabotage scenarios would simply shut a plant down for a time and are not a safety concern. The plant operator will need to determine if these risks are acceptable, or if minor modifications should be considered to provide additional protection. Scenarios of concern are those with higher consequence and lower difficulty. As shown in Figure 2, if one core melt scenario is found to be easier than others, design changes can be considered to make that scenario more difficult.

Table IV. Notional RIMES scoring

Scenario (Difficulty Levels Shown)	Outsiders Part	Training	Support	Tools	Insiders Part.	Insider Access	Ingenuity	Situational Understanding	Stealth	Outsider Commitment	Insider Commitment	Complexity	Flexibility	Aggregate Score
Scenario 1	2	1	1	3	1	1	1	1	2	3	1	1	1	33
Scenario 2	3	2	1	2	3	3	1	1	3	2-3	3	1	1	59-65
Scenario 3	3	1-2	1	3	1	1	1	1	1	3-4	1	3	1	45-65

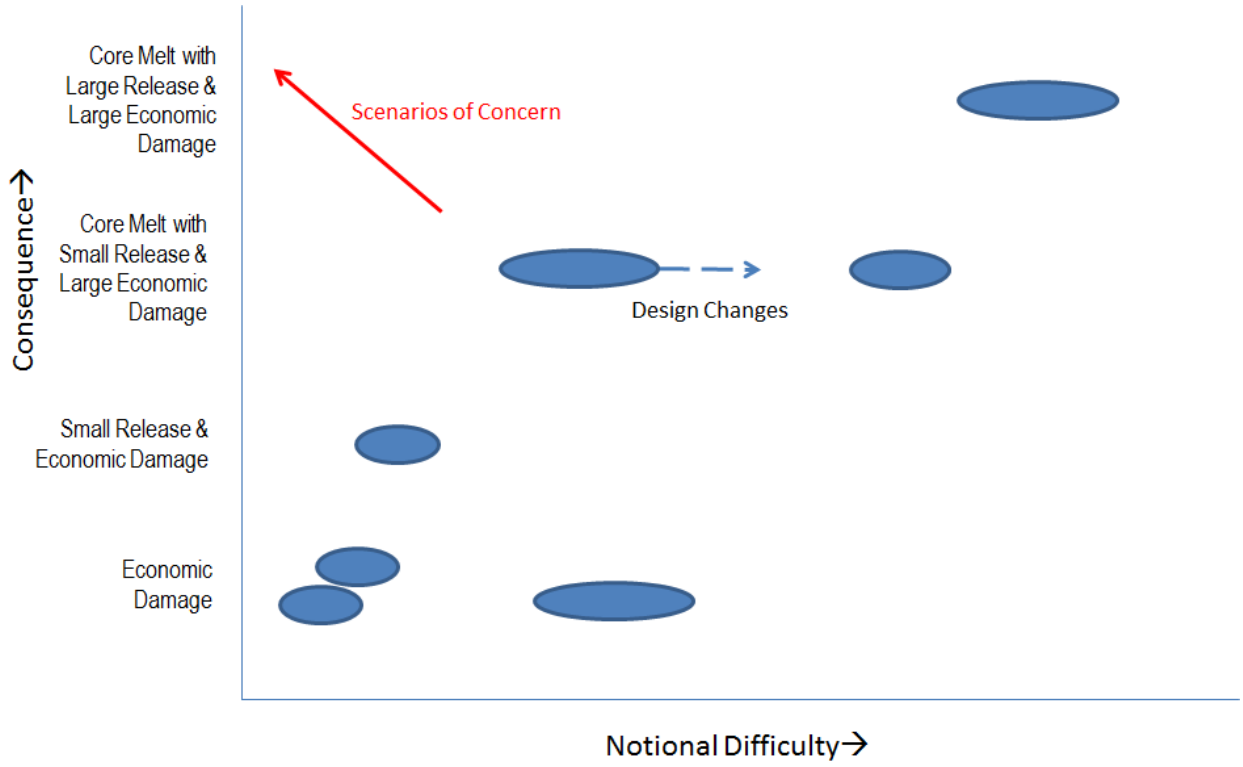

Figure 2. Notional plot of consequence vs. difficulty

4 PRELIMINARY INSIGHTS

The generic SMR design included many of the common safety components and critical systems that the iPWR designs currently contain. Scenarios that led to core melt were in general found to have fairly high difficulty levels, with multiple parameters in the 3-4 range and the occasional level 5. Multiple systems needed to be disabled in order to achieve core melt, and the existing protection system is fairly robust to these types of attacks. One core melt scenario that relied on outsider attack with a more moderate difficulty rating (lower than others) was found to be easily addressed with a rather simple design change that would be an inexpensive modification.

Some economic damage only scenarios had low difficulty ratings, but these scenarios were not a safety concern at all. In these cases, the plant operator would need to make a decision whether to make design changes to make the sabotage more difficult. Modifications were examined that appreciably increased the attack difficulty with a rather simple changes.

More specific results will require analysis on actual designs. In many cases the analyses done in this work might change considerably depending on the final design. Security staffing is a large concern right now with the SMR vendors since they would like to minimize staffing to reduce costs. This work is also evaluating response force needs as part of the analysis. Although more detailed studies are required, the scenarios examined for this work suggest that SMR designs will not be walk-away safe from security threats, and that core damage is always possible if an outsider group gains access to a facility.

5 CONCLUSIONS

The RIMES methodology has been found to provide a new approach to security risk management for nuclear fuel cycle facilities. RIMES helps the designer to optimize security investments by focusing on scenarios with higher consequence and lower difficulty. The methodology was found to provide repeatable results due to the use of the difficulty matrices, but the difficulty levels for the 13 parameters are the most important outcome of this work. Aggregation to develop scores for each scenario can be useful, but should not be used as the sole reporting method for the results of this work.

As applied to iPWR SMR designs, the RIMES methodology was used to develop preliminary insights into these reactor designs. In general, the designs are very robust to core melt sabotage scenarios, but initial designs are always likely to include some vulnerabilities. This analysis found that rather simple structural design changes are able to address the scenarios that had slightly lower difficulty ratings than others of similar consequence.

6 ACKNOWLEDGMENTS

This work was funded through the Nuclear Energy Enabling Technologies and Material Protection Accounting and Control Technologies programs in the Department of Energy Office of Nuclear Energy. The authors would like to acknowledge parallel work through the Small Modular Reactor program that was used to help build the generic SMR design. The authors would also like to acknowledge Timothy Wheeler and Greg Baum at Sandia National Laboratories for their expertise during the RIMES ranking process.

7 REFERENCES

1. "Interim Report of the American Nuclear Society President's Special Committee on Small and Medium Sized Reactor (SMR) Generic Licensing Issues," American Nuclear Society (July 2012).
2. T.G. Lewis, B.B. Cipiti, S.E. Jordan, and G.A. Baum, "Generic Small Modular Reactor Plant Design," SAND2012-10406, Sandia National Laboratories, Albuquerque, NM (December 2012).