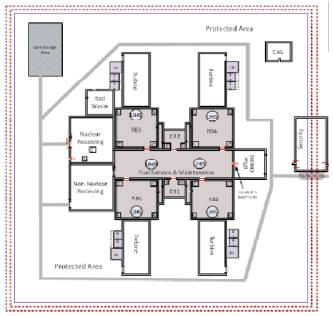
SAND2013-7897C

Exceptional service in the national interest

Sandia National Laboratories



Security Risk Management of Small Modular Reactors

PSA 2013

Ben Cipiti, Greg Wyss, Felicia Duran, Tom Lewis,
Luis Mendoza, Jordan Parks, Dean Dominguez

U.S. DEPARTMENT OF ENERGY | NNSA Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

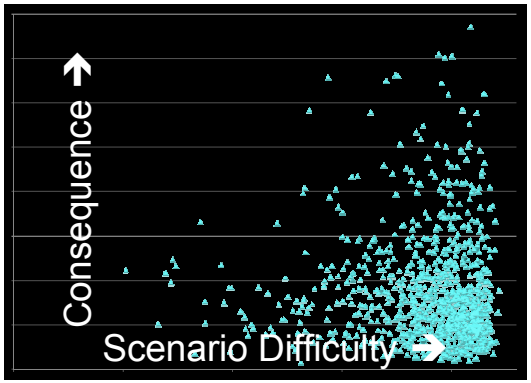
Objective

- The overall goal of this work is to analyze security risks for SMRs and examine new approaches for minimizing protection costs—SMRs in particular face regulatory challenges in applying security to a smaller facility while keeping overall plant costs manageable.
- The RIMES (Risk-Informed Management of Enterprise Security) methodology has been applied to examine a number of sabotage threats for SMRs.
- A STAGE (Scenario Toolkit and Generation Environment) model of a generic SMR design has been developed for response force modeling of adversary attacks.

Assessing Security Risk

- Traditional risk is based on a scenario's likelihood and consequence, but to use this for security, one must either
  - Assess the probability of an attack that has never occurred before (highly uncertain, and can change in an instant), or
  - Limit the adversary (e.g., with a design basis threat) and assess the conditional probability that *this* adversary will succeed if they attempt *this* attack scenario (neglects deterrence of the adversary and makes both risk aggregation and defender cost-benefit analysis difficult)
- The RIMES methodology instead focuses on the *degree of difficulty* for an adversary to successfully accomplish an attack:

Attack scenarios that are both easier and higher consequence are of greater risk. Focus security investments on these "high-risk" scenarios.



Assessing Degree of Difficulty

- For a given scenario, thirteen parameters are assigned a difficulty level (1-5). These levels are not linear.
- Attack Planning and Preparation:
  - Outsider Participation (number of outsiders required)
  - Training & Expertise (skills required, practice)
  - Support Structure (intelligence, network, beliefs)
  - Tools (weapons, explosives, computers, etc.)
  - Insider Participation (number of insiders required)
  - Insider Access (what security access/knowledge is required)
  - Ingenuity (inventiveness of the approach)
- Attack Execution:
  - Situational Understanding (exploiting vulnerabilities of the facility)
  - Stealth & Covertness (requires subterfuge or brute force approach)
  - Outsider Commitment (willingness to get arrested/die for their cause)
  - Insider Commitment (attribution, personal risk)
  - Complexity (number of tasks, timing)
  - Flexibility (is adaptation required)

Attack Preparation Difficulty Matrix

Sandia National Laboratories

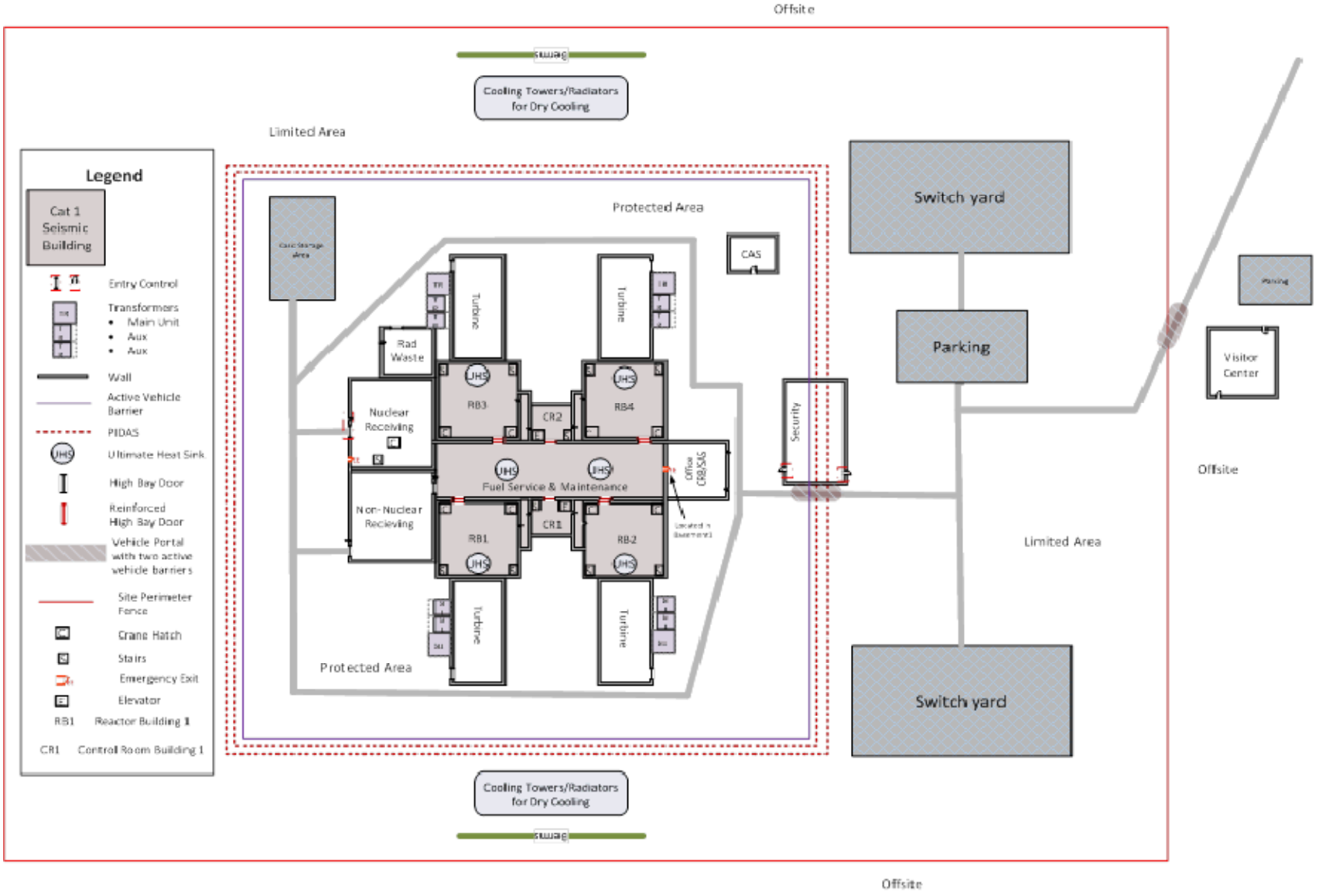
Attack Preparation Dimension	Outsider Partici-pation	Training & Expertise	Support Structure	Tools	Insider Partici-pation	Insider Access	Ingenuity
Level 1	Individual (1)	Self-taught Open source No practice	Minimal, prep. easily concealed	Available on open market	None	None	Straight-forward approach
Level 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

Attack Execution Difficulty Matrix

Sandia National Laboratories

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

Generic iPWR SMR Design



Scenario Development

- Traditionally, target and vital area identification would be informed by a safety PRA (which was not available for this work).
- A preliminary list of common safety and support systems that are typical of any nuclear reactor was compiled.
- We used this list to identify example targets for theft or sabotage scenarios.
  - Fourteen scenarios have been evaluated.
  - Design changes have been examined to determine effect on difficulty level.
- The scenarios were analyzed to determine what would be required to successfully carry out the attack.

Safety and Support Systems

Sandia National Laboratories

- **Ultimate Heat Sink** – More difficult to access for SMRs
- **AC Power** – SMRs may not require AC power after shutdown
- **DC Power** – May be required to open valves for passive cooling in SMRs
- **Isolatable Piping** – Still an issue for SMRs, but no large break LOCAs
- **Control Room & Cable Spreading Room** – No difference
- **Remote Shutdown Panel** – No difference
- **Reactor Protection System (Control Rods)** – No difference
- **HVAC for Control Room** – No difference
- **HVAC for Equipment** – No difference
- **Coolant Injection Pathways** – Small break LOCAs are still possible in SMRs
- **Spent Fuel Pool (Cooling and Integrity)** – Design differences
- **Crane During Refueling Mode** – No difference

Scenarios Examined

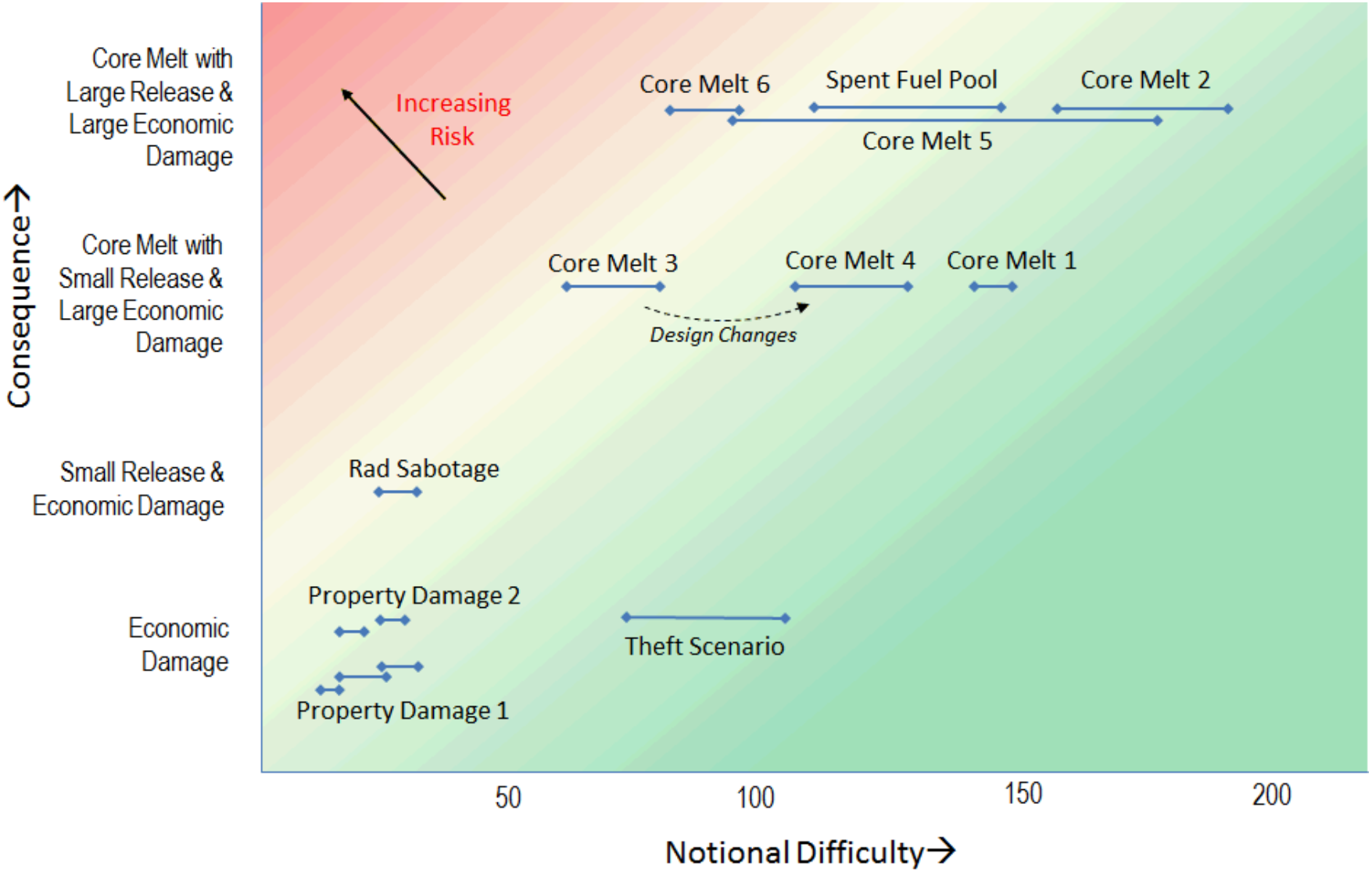
- Scenarios can be grouped by consequence—we felt that it was easier to describe consequence qualitatively:
  - Economic Damage – includes direct property damage possibly with the goal of shutting down operations.
  - Economic Damage & Small Radioactive Release – may include targets to release nuclear material for negative publicity
  - Large Economic Impact with Small/No Release – many core melt scenarios may lead to little release but a big mess on site
  - Large Economic Impact with Large Release – these scenarios create a large release from a core melt or other sabotage event.
- Grouping by consequence helps to focus attention on the lower difficulty scenarios, but recognize that adversaries may choose a different consequence if it is easier to achieve.

Scenario Results

Sandia National Laboratories

Scenario	Outsiders Part	Training	Support	Tools	Insiders Part.	Insider Access	Ingenuity	Situational Understanding	Stealth	Outsider Commitment	Insider Commitment	Complexity	Flexibility	Aggregate Score (Weighted Scores Shown)
Property Damage 1a	1	1	1	1-2	1	1	1	1	1	2	1	1	1	15-17
Property Damage 1b	1	1	1-2	2	1	1	1	1	2	2-3	1	1	1	19-27
Property Damage 1c	2	2	1-2	2	1	1	1	1	2	2-3	1	2	1	25-33
Property Damage 2a	1-2	1	1	2	1	1	1	1	2	1-2	1	1	1	17-21
Property Damage 2b	2	2	1	2	1	1	1	1	2	2-3	1	2	1	25-31
Rad Sabotage	2	1-2	1	2	2	2	1	1	1	2-3	1	2	1	25-33
Theft	3-4	3	3	3	1	1	2	2	1	3-4	1	3	3	73-109
Core Melt 1	1-2	1	1	1	5	3	2	2	3	1-2	4	3	1	146-150
Core Melt 2	1-2	1	1	2	5	3-4	3	2	3	1-2	4	3-4	1	155-195
Core Melt 3	3	3	2-3	3-4	1	1	2	1	1	3	1	3	1	57-81
Core Melt 4	3-4	4	3	3	1	1	3	1	1	4	1	3	2-3	107-131
Core Melt 5	3-4	3-4	3	3	1	1	2-3	1	1	4-5	1	3	2	83-179
Core Melt 6	1	1	1	2	3	3-4	3	1	3	1	4	3	1	81-99
Spent Fuel Pool	3	3	3	3	3	3-4	2-3	1	1	4	4	2	1	117-141

Scenario Results

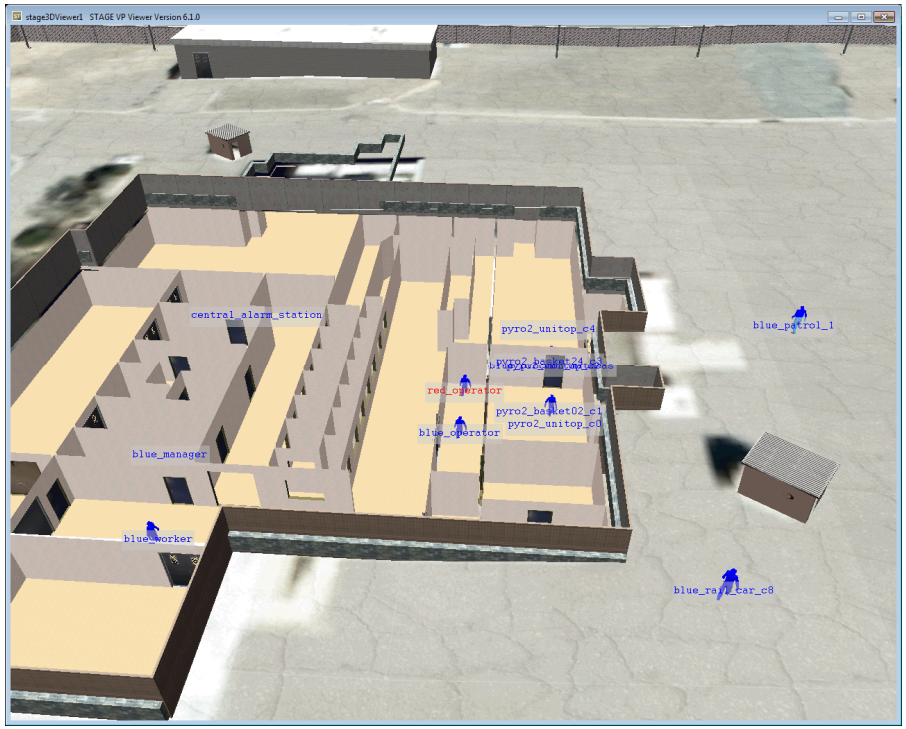


Observations & Insights

- We found the RIMES methodology to have advantages in repeatability, and it allows designers to consider options to manage security risk.
- Scenarios that lead to core melt in general had high difficulty levels, multiple systems needed to be disabled.
- Some economic-damage-only scenarios had fairly low difficulty ratings, but the operator will need to decide if design improvements are warranted.
- The analysis suggests that SMR designs are probably not walk-away safe from large and determined security threats, although more detailed studies are required.

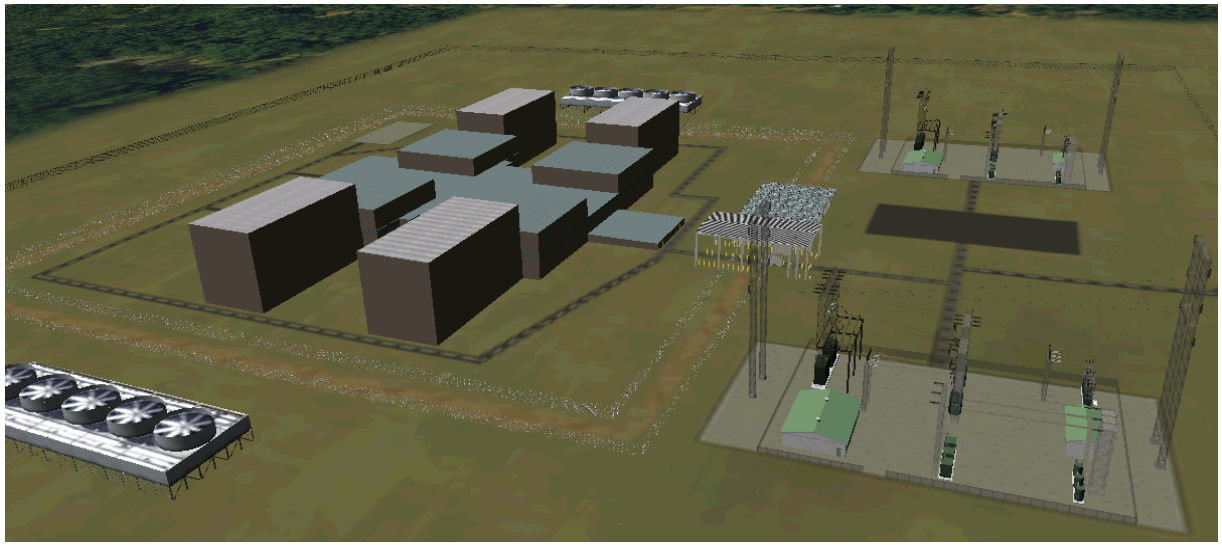
Response Force Modeling

- Presage STAGE (Scenario Toolkit and Generation Environment) software provides a framework to create end-to-end scalable red team/blue team force-on-force combat simulations:
  - Probability-based combat model
  - Event-based entity missions
  - Performance-based databases
  - Logic based behavior
  - Ground navigation
  - Scripting support
  - 2D/3D environment
  - Road Networks
  - Batch Mode



Response Force Modeling

- 2 of the 14 RIMES scenarios have been run to demonstrate the model and provide preliminary results.
- This capability will help to answer questions about response force (and security staffing) needs.
- Future work will evaluate how alternative security features may reduce on-site security staffing needs.



Conclusions/Next Steps

- The RIMES methodology has provided useful insights into current SMR designs, but vendor-specific results will require access to more detailed design information.
- The RIMES scenarios will serve as a baseline to use for future work. Response force modeling can examine different numbers of responders, and alternative security features can be added to determine the potential for reducing security staffing levels.