# Assessing Security Effectiveness

WINS
Security of Small Modular Reactors Workshop
November 21, 2019

Michael Sleigh, PE
Fellow Engineer
Asset Protection and Development
Westinghouse Electric Company LLC

Westinghouse

# Legal

This document may contain technical data subject to the export control laws of the United States. In the event that this document does contain such information, the Recipient's acceptance of this document constitutes agreement that this information in document form (or any other medium), including any attachments and exhibits hereto, shall not be exported, released or disclosed to foreign persons whether in the United States or abroad by recipient except in compliance with all U.S. export control regulations. Recipient shall include this notice with any reproduced or excerpted portion of this document or any document derived from, based on, incorporating, using or relying on the information contained in this document.

Westinghouse

# Agenda Topics

- Westinghouse SMR Overview
- Westinghouse Security Team
- Key Messages and Case Studies
  - Designers
  - Licensing
  - Security
    - Target Sets
    - Margin
- Questions

Westinghouse

# Westinghouse SMR Overview

- The Westinghouse SMR is a >225 MWe integral pressurized water reactor. It utilizes passive safety systems and proven components to achieve the highest level of safety and reduced the number of components required.
- The Westinghouse LFR is a 400-500 MWe Gen IV Lead Fast Reactor.
- Westinghouse is collaborating on other SMR designs as a design partner.

Westinghouse

# Westinghouse SMR Overview

- Westinghouse is also currently developing the eVinci™ micro reactor. The small size of the generator allows for easier transportation and rapid, on-site installation in contrast to large, centralized stations. The reactor core is designed to run for more than 10 years, eliminating the need for frequent refueling.
  - Fully factory built, fueled and assembled
  - Combined heat and power – 0.2 to 15 MWe
  - Target less than 30 days onsite installation
  - High reliability and minimal moving parts
  - Green field decommissioning and remediation

# Asset Protection & Development

- Westinghouse's Nuclear Security Team is called Asset Protection & Development located at Westinghouse's Cranberry Township, PA HQ.
- Group Overview
  - Industry/Site Experience:
    - Security Management and Training
    - Development of Target Sets and Protective Strategies
    - Security System Installation and Support
    - Overall Plant Operations
  - Engineering Design Expertise In:
    - Physical and Cyber Security (all aspects)
    - Aircraft Impact/Loss of Large Area
    - Physical Security Systems (interface with Cyber Security Systems)
      - Electrical Engineering
      - Mechanical Engineering
      - Civil Engineering
      - Computer Engineering
      - Professional Engineers Certified and Accredited
      - Security SME

Westinghouse

# Asset Protection & Development

- While we are engineers by trade, with significant plant operating experience, we also have full security resumes including training and/or certifications in/with:
  - Risk Assessment
  - Firearms (Assault Rifles, Handguns, Sniper/Precision)
  - Explosives (Handling, Breaching, Grenades, IED/VBIED, Blasts Effects, etc.)
  - Less-Lethal (Stun, Smoke, Gas, etc.)
  - Mechanical/Ballistic Breaching
  - Tactics (both standard military and unconventional)
  - Defeating Security Systems
  - Emergency Tactical Medicine

Westinghouse

# Asset Protection & Development








Westinghouse

# Key Messages

- Designers
  - Involve Security SMEs early and often

# Case Study: “Intrusion-proof Doors”

- Corridor and security area inside the power block set up by an engineer not familiar with security requirements
- Turnstiles were included as it was believed they were needed to for access control
- An equipment bypass door was installed further down the corridor
- When pointed out that this door circumvented the security measures in place in the corridor. The reply was “we did think about that, and we specified an intrusion-proof door for that location”……

**Intrusion-proof Doors … Aren’t**

Westinghouse

# Key Messages

- Designers
  - Involve Security SMEs early and often
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption

Westinghouse

# Case Study: “We Won’t Even Need a Fence”

- The design is so safe we will not even need security, will not have a protected area and won’t even need a fence
- Typically SMRs or Micro-Reactors jump to the conclusion that because they are smaller and safer the rules created for large light water reactors don’t apply
- While there are certainly rule items that are challenging and may need changing or updating – change in regulation should not be the first consideration
- Look at where you can meet the rule but in a different way than an existing plant

**Shift your paradigm**

Westinghouse

# Key Messages

- Designers
  - Involve Security SMEs early and often
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption
- Security
  - Stay engaged

Westinghouse

# Case Study: “It Would be Difficult”

- Proposed design change to add new operator work stations outside of the main power block
- Workstations would be able to monitor important safety functions and have some limited control of some systems, (but not required safety systems)
- Review of the Target Set Analysis showed that there was a potential interconnection with target set equipment
- When asked if it would be impossible to manipulate the target set equipment from the new work station, the response was “well, it would be very difficult to do”…..

**Difficult ≠ Impossible**

# Key Messages

- Designers
  - Involve Security SMEs early and often
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption
- Security
  - Stay engaged
  - Look holistically

Westinghouse

# Think Operationally

- Plant must still operate
- People have to get in an out, deliveries must be made.
- Safety of personnel
- Safety of visitors
- Correctly size the Physical Protection System and Security Force in order to meet regulations and to control costs

# Case Study: "Screen Doors on a Submarine"

- Life safety engineer convinced the design review committee that an additional fire exit (door) was needed from a battery room in the power block
- Additional exit was through a power block exterior wall and completely circumvented the security strategy
- No security reviews were done before this was approved, and this was caught during a drawing review for another part of the project
- After a close review of the rules, worked with the engineer to redesign a secondary exit from the room that was not a security concern

**Look for alternatives that meet the rule**

Westinghouse

# Key Messages

- Designers
  - Involve Security SMEs early and often
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption
- Security
  - Stay engaged
  - Look holistically
  - Get engineering support

Westinghouse

# Target Sets

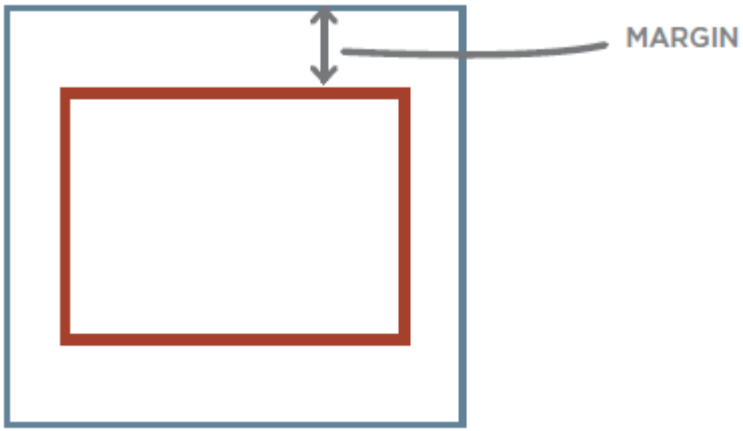
- That minimum set of equipment or actions that must be protected to prevent an undesirable outcome
  - Generally, for an operating nuclear site, that means preventing a core damage event
- May have other names, such as Safety Case Studies or Fault Scenarios
- It is the heart of what is being protected
  - Incomplete or incorrect target sets may drive the physical protection system to protect the wrong things and drives any assessments or effectiveness reviews to inaccurate conclusions

Westinghouse

# Target Sets

- Historically, these target sets have been developed by site individuals with significant operating experience in different disciplines (Operations, Maintenance, Engineering, Security, etc.) using an Expert Panel type approach
- This type of approach relies heavily on having the right people with the right experience as well as the plant itself having operating and maintenance history
- Support systems are often overlooked in this type of approach

# Margin




**Target sets created without detailed, repeatable, analysis has uncertainty which drives need for larger margins**

Westinghouse

# Fault Tree Target Set Analysis (FTTSA) Method

- The FTTSA Method utilizes the existing Probabilistic Risk (or Safety) Assessment (PRA/PSA) logic model to aid in the development of target sets
- The PRA/PSA logic model is a very accurate and robust representation of plant systems and their inter-dependability
- Thousands of hours are spent creating, documenting, verifying, and maintaining a PRA/PSA during its lifecycle

Westinghouse

# Fault Tree Target Set Analysis (FTTSA) Method

- Using this logic model, the target sets consider ALL support systems and sequences included in the model
- FTTSA utilizes the logic diagram of the PRA/PSA (Fault Trees) to identify equipment and actions which can lead to core damage
- The FTTSA Method is a repeatable, defendable, and auditable process that PROVES the Target Set Accuracy and Completeness

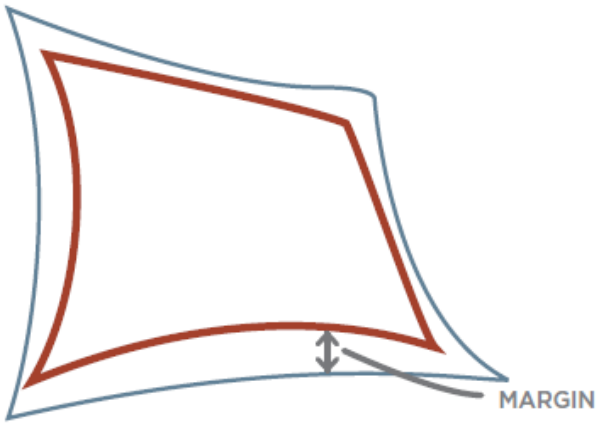
Westinghouse

# Fault Tree Target Set Analysis (FTTSA) Method

- The FTTSA normalizes all PRA/PSA probability, to remove reliability and then applies a location based methodology which considers flood propagation, cable routing and equipment locations
- Security SMEs create and use screening criteria based on tactics and adversary ability to determine Target Sets
- These Target Sets are presented to plant operators and system engineers for final validation

Westinghouse

# Margin




**Detailed, engineering driven Target Sets can reduce the uncertainty and allow for narrower margins**

Westinghouse

# Key Messages

- Designers
  - Involve Security SMEs early
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption
- Security
  - Stay engaged
  - Look holistically
  - Get engineering support
  - Have patience

Westinghouse

# Case Study: “We need a lift in Guard Tower”

- Turbine building design had defensive fighting positions for armed responders, turbine elevator stopped one floor below the level of these positions. Phone call from the architect designing the turbine building went something like this:

Architect: We need to add elevators to reach all the way to the defensive fighting position

Me: No we don’t, they can walk up a flight of stairs, that is not uncommon for a guard tower

Architect: What if they physically can’t climb the stairs?

Me: (spends next 15 minutes explaining the fitness requirements for an armed responder)

Westinghouse

**Not everyone understands the concept**

# Key Messages

- Designers
  - Involve Security SMEs early
- Licensing
  - Shift your paradigm to thinking about how you meet a rule vice why we need to get a rule change or an exemption
- Security
  - Stay engaged
  - Look holistically
  - Get engineering support
  - Have patience

**Don’t work in a silo**

Westinghouse

# Contact Information

Mike Sleigh
Fellow Engineer
+1-412-940-8463
sleighm@westinghouse.com

Steve Reed
Engineering Manager
+1 (412) 374-4562
reedsj@westinghouse.com

Westinghouse

# Questions

Mike Sleigh
Fellow Engineer
+1-412-940-8463
sleighm@westinghouse.com

Steve Reed
Engineering Manager
+1 (412) 374-4562
reedsj@westinghouse.com

Westinghouse