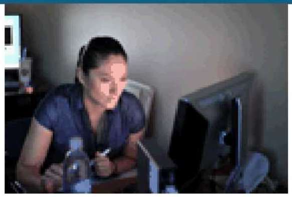
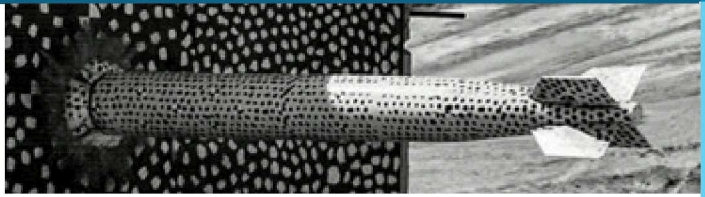
SAND2020-6598C

Using Vital Area Identification Insights in Sabotage Security Effectiveness Evaluation





Alan Evans

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Introduction

- Identifying the combinations of vital equipment at complex nuclear facilities can be very challenging
- Vital Area Identification (VAI) can be used to develop target sets
- Use VAI logic model to identify sabotage themes
- Assess capability of facility security measures to protect against sabotage scenarios for each target set
- Aggregate sabotage protection capabilities for each target set to determine overall facility security effectiveness
- Much more detail presented in paper

Perform VAI to Develop Target Sets

- The VAI method develops a sabotage area tree
  - Cut sets provide lists of the minimum number of areas from which the sabotage top event can be accomplished
  - Single areas and combinations in the list of cut sets are referred to as target sets

- VAI analysis is simplified by mapping the equipment sabotage actions to plant locations
  - Simplifies reduces fault tree complexity and number of cut sets by several orders of magnitude
  - Area mapping obscures the equipment targets within individual areas in target sets
  - Large number of individual sabotage actions can obscure the significance of the individual equipment targets

Identify Sabotage Themes

- Sabotage themes are narrative descriptions of the logic at the top of the sabotage area tree
  - Consist of combination of Initiating Events of Malicious Origin (IEMO) and system disablement actions
  - Generally correspond to those in the fault tree logic employed in Level 1 Probabilistic Safety Analysis
  - Sabotage themes can be determined by reviewing the plant-specific sabotage area tree developed for VAI

- Most target sets will correspond only to one sabotage theme
  - Exceptions to this generalization will likely be target sets consisting of only one area (singles)
  - These singles will generally either be areas where it is infeasible to separate redundant rains of safety equipment, areas containing radioactive material that can be directly dispersed, or areas where a beyond design basis accident or transient can be caused

- Sabotage themes associated with a specific target set can be determined by examining the sabotage actions linked to the areas that compromise the target set in the sabotage area tree model
  - Identified in VAI basic event location table
  - Exceptions to this generalization will likely be target sets consisting of only one area (singles)

Identifying Sabotage Themes Example

- Determine sabotage themes from fault tree – Pressurized Water Reactor Example
  - #1 Initiate small LOCA and disable high pressure safety injection
  - #2 Initiate large LOCA and disable low pressure safety injection
  - #3 Initiate liming transient and disable decay heat removal system
- Examine equipment in target set areas
  - Target set areas with high pressure safety injection system components are theme #1
  - Target seat areas with low pressure safety injection system components are theme #2
- Develop area sabotage actions based upon system requirements
  - Disable both high pressure safety injection pumps

1: GIHM, BRIAN; SNELL, VIC, 2014
2: ADVANCED REACTOR CONCEPTS TECHNICAL REVIEW PANEL, 2012)

Facility Walkdown

- To identify individual equipment targets and to develop detailed scenarios, a walkdown of the target is necessary
  - VAI location focus means not all equipment targets identified in VAI basic event location table
  - Can be performed as part of the security effectiveness evaluation or can be performed separately to develop a reference document of the equipment targets and sabotage scenarios for each target area
- Walkdown should screen specific equipment targets based on their accessibility within the target area and level of resources/skills required to disable them in the context of the DBT considered in security evaluations
- Collection of sabotage equipment targets and sabotage actions on an area-by-area basis can create the assumption that sabotage actions in one are independent of sabotage actions in other areas
  - May have systems that are dependent on a single support system
  - System interactions of this nature should be noted

1: GIHM, BRIAN; SNELL, VIC, 2014

Identify Dominant Sabotage Scenarios

- Sabotage scenarios involving the most vulnerable combinations of equipment targets in the most vulnerable target sets can the be considered in the security effectiveness evaluation
  - Allows analyst to focus on the most significant targets
- The process for focusing on the sabotage scenarios that pose the most significant vulnerability is as follows:
  - Identify target sets in which the areas have the least effective impediments to undetected access
  - Use linkage between target sets and sabotage themes to identify the applicable sabotage theme(s)
  - For each area, walkdown the are to identify the sabotage equipment targets that are most vulnerable based on their accessibility and against the threat in the DBT
  - Repeat the previous step for all other areas in the target set and for all target sets
  - Add the security portion of the scenario

http://www.zionsolutionscompany.com/wp-content/uploads/2014/07/08-Unit-2-Containment-Hatch-Removal-April-20111.jpg

Assess Facility Capabilities

- The output from this proves yields the set of most vulnerable scenarios that can be evaluated by standard security effectiveness evaluation techniques
  - Allows the plant to determine overall plant sabotage vulnerability and identify candidate measures to enhance plant security
- Individual scenario vulnerabilities can be aggregated into a measure of overall security effectiveness
  - Vulnerabilities can be mitigated by security enhancements if security effectiveness is inadequate
- The most vulnerable scenarios can be used for security or emergency response exercises
  - Force-on-Force Exercises
  - Limited Scope Performance Testing
  - Performance Testing
- This approach permits exercise planners to assemble credible scenarios that are desired based on exercise objectives

Conclusion

- Method provides a comprehensive screen of sabotage equipment targets at complex facilities
- Focuses security evaluations on the most vulnerable sabotage scenarios and equipment targets
- Ensures adequate security system effectiveness evaluation