SAND2020-9431PE

United States

Nuclear Regulatory Commission

Department of Energy National Nuclear Security Administration

National Approach to VAI and Target Set Identification

DOE-NNSA

Douglas M. Osborn, PhD

Joseph Sandoval

USNRC

Stacy Prasad

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.

Vital Area Identification

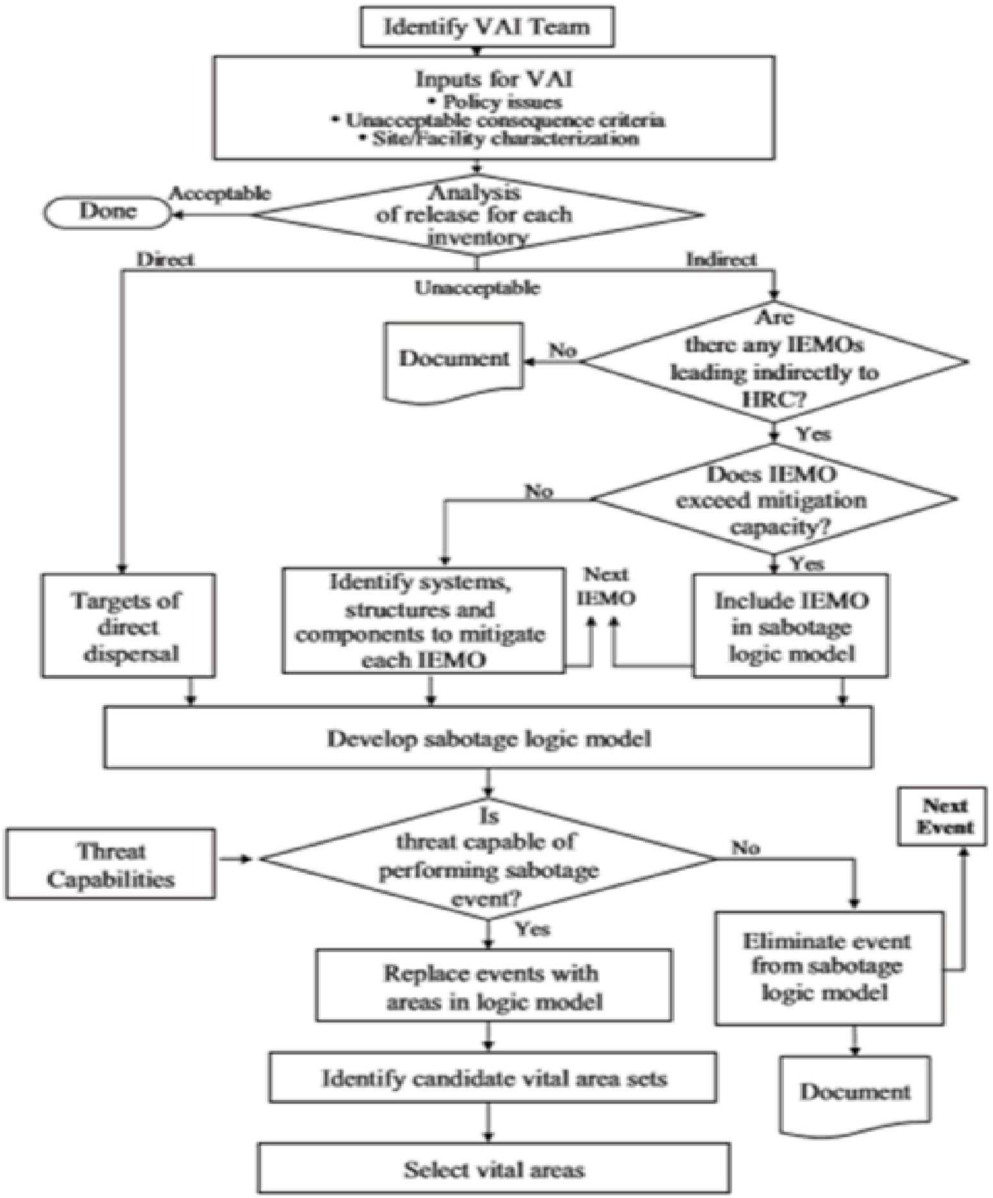
- The Probabilistic Safety Analysis (PSA) is a tool that can assist in determining what structures, systems, and components are important to protection from a security perspective
  - Event Tree/Fault Tree Analysis
  - Level 1 PSA = Initiating Event to Core Damage
  - Level 1 PSA Cut-sets to Protection Set
- Comprehensive, structured analysis is used to identify accident scenarios and derive numerical risk estimates
  - Overall risk from operating the facility
  - Accidents with highest contribution to risk
  - Design enhancements that reduce risk
  - Radiological consequence estimates
  - *Does not consider the dynamic nature of people nor reactor phenomena*

Steps of VAI Methodology

Steps in the systematic and structured VAI process, and are as follows:

1. Identify the inventories of radioactive material for which radiological sabotage is a concern. Include sabotage of these inventories as events in the sabotage logic model
2. Determine whether direct dispersal of each inventory of concern is possible; if so, include direct dispersal of each such inventory as an event in the sabotage logic model.
3. Identify any initiating events that can, alone or in combination with other malicious acts, lead indirectly to radiological sabotage of each inventory of concern. An initiating event that is deliberately caused by an adversary to cause a radioactive release from a facility is called an initiating event of malicious origin (IEMO). Identify the systems required to mitigate those IEMOs (if mitigation is possible) and the success criteria for those mitigating systems.
4. Using the information obtained in Step 3, develop the portions of the sabotage logic model that represent the combinations of events that could lead indirectly to radiological sabotage.
5. Eliminate from the sabotage logic model any events that the design basis threat (DBT) does not have the capability to perform.
6. Identify the areas corresponding to sabotage logic model events; that is, areas in which direct dispersal, initiating events, and the mitigating system disablement events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.
7. Solve the sabotage area logic model to identify the target sets; the combinations of areas to which the adversary must gain access in order to cause radiological sabotage.
8. Find the prevention sets of the sabotage area logic model (or find the Boolean complement of the result of Step 7) to identify the candidate vital area sets; the combinations of areas that must be protected to prevent radiological sabotage.
9. Select one or more prevention vital area set that will be protected to prevent radiological sabotage.

Flow Chart of VAI Methodology



Vital Area Policy Decisions

10 CFR 73.55 – Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage

Insider Mitigation Program: Must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage.

Vital areas

I. Vital equipment must be located only within vital areas, which must be located within a protected area so that access to vital equipment requires passage through at least two physical barriers, except as otherwise approved by the Commission and identified in the security plans.
II. The licensee shall protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency and satisfy the vital area entry control requirements of this section.
III. Unoccupied vital areas must be locked and alarmed.
IV. More than one vital area may be located within a single protected area.
V. At a minimum, the following shall be considered vital areas:
   a) The reactor control room;
   b) The spent fuel pool;
   c) The central alarm station; and
   d) The secondary alarm station in accordance with § 73.55(i)(4)(iii).
VI. At a minimum, the following shall be located within a vital area:
   a) The secondary power supply systems for alarm annunciation equipment; and
   b) The secondary power supply systems for non-portable communications equipment.

Vital Area Access

I. Licensees shall control access into vital areas consistent with access authorization lists.
II. In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area.

Target Set Identification

- Informed by VAI results
- Site-specific analyses and methodologies are used to determine and group the target set equipment or elements under all modes of nuclear power plant operation
- **NRC Regulatory Guide 5.81** – Target Set Identification and Development for Nuclear Power Reactors (*OUO*)
  - Regulatory Guide 5.81 provides licensees with guidance on meeting the requirements described in section 73.55(f) of title 10 of the *Code of Federal Regulations* (10 CFR), "Target Sets." Specifically, it sets forth approaches that the NRC considers acceptable for use by applicants or licensees in analyzing, developing, documenting, and evaluating target set elements and target sets, including operator actions that may be credited to prevent core damage (*e.g.,* non-localized fuel melting, and/or core destruction) or loss of spent fuel coolant and exposure of spent fuel.
  - The 2019 revision of RG 5.81 (Revision 1) incorporates lessons learned from operating experience. Specifically, this revision clarifies issues that have been identified through interactions with stakeholders and inspection activities since the original publication of the 2010 guide.
- EPRI 1007975 - Probabilistic Consequence Analysis of Security Threats–A Prototype Vulnerability Assessment Process for Nuclear Power Plants
  - Provides an approach to estimate the frequency of threat occurrence using past security event data, probability of threat success considering the probability of neutralizing the threat, and consequence estimation are provided considering existing NPP consequence tools such as plant PRA (PSA) models
  - This approach considers threat scenarios from threat characterization through plant damage consequences (core damage and radionuclide release) and public health consequences (off-site fatalities)

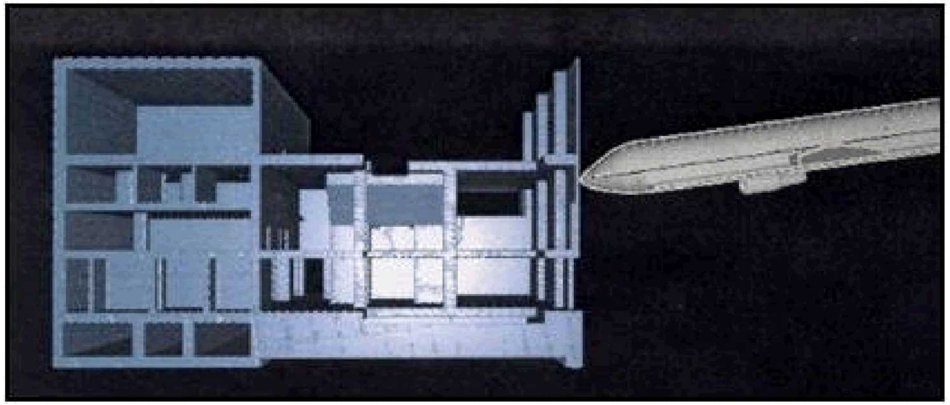
New Reactors and Large Area Analysis (LOLA) – NUREG-0800

- USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Editions, NUREG-0800
  - Section 19.4, Part II acceptance criteria for LOLA

1. Staging of fire brigade equipment,
2. Dispersal of personnel,
3. Airlifted resources,
4. Command and control,
5. Evaluating capabilities of offsite resources,
6. Evaluation of memorandums of understanding (MOUs) for offsite resources
7. Coordination with regional resources,
8. Controlling emergency response vehicles and dosimetry for responders,
9. Communication equipment,
10. Mass causalities
11. Triage areas,
12. Firefighting training and exercises,
13. Means for feeding the fire protection ring header,
14. Boiling water reactor: Containment venting and vessel flooding,
15. Use of plant equipment during loss of power situations,
16. Compartmentalization,
17. SFP mitigative measures,
18. Training,
19. Water spray scrubbing and runoff, and
20. Staging of equipment for water spray scrubbing.

VAI & Loss of Large Area Analysis (LOLA)

- Level 1 PSA
- Vital Area Identification (VAI)
  - Level 1 PSA applied to VAI models
  - Potential for core damage as single cut-sets (single room)
  - Example for main control room
    - Fire
    - Flood
- Apply higher order target-sets from VAI for LOLA
  - Spatially informed LOLA
    - Beyond current NRC protocols
  - Identify rooms and potential scenarios for LOLA
    - New reactor designs can consider passive systems and new safety systems
    - Considerations of true multi-train independence



Future Reactor Builds & VAI / Target Set Identification

- Static Level 1 PSA does not do sufficient job capturing *passive safety* equipment
  - Passive safety ≠ Passive Security
  - Integrated Cyber-Physical Assessments

- From 10CFR73.55: The physical protection program must be designed to *prevent significant core damage* and spent fuel sabotage
  - Requires Level 2 PSA
  - Application of "Diverse and Flexible Coping Strategies (FLEX)" – Reference: NEI12-06

- Conflict of Vital Area policy decisions (10CFR73.55), Emergency Plans (10CFR50.47) & URC/HRC limits (10CFR100) for decommissioning activities
  - No emergency planning zone but security is not commensurate to potential consequences

- Investigation into new methods:
  - Dynamic PSA
  - System Theoretic Process Analysis (STPA)

Other Nuclear Facilities

- Besides nuclear power plants, no other DOE- or NRC-regulated nuclear facilities use VAI
- Other nuclear facilities consider target sets along NRC or DOE guidance for facility type
  - Informed through various hazard assessments and policy guidance
  - Graded approach is based on maternal at risk

VAI and Target Set References

1. Varnado, G.B., and N.R. Ortiz, “Fault Tree Analysis for Vital Area Identification,” NUREG/CR-0809, SAND79-0946, Albuquerque NM, U. S. Nuclear Regulatory Commission, Washington DC (1979).
2. Varnado, G.B., and R.A. Haarman, “Vital Area Analysis for Nuclear Power Plants,” SAND80-0553C, Sandia National Laboratories, Albuquerque NM (1980).
3. Varnado, G.B., and D.W. Whitehead, “Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants,” SAND2008-5644, Sandia National Laboratories, Albuquerque NM (2008).
4. Zamanli, J., and Chwasz, C., “Nuclear Power Plant Security Assessment Guide,” NUREG/CR-7145, Nuclear Systems Analysis Operations Center Information System Laboratories, Inc., U.S Nuclear Regulatory Commission, Washington DC (2013).
5. IAEA, “Identification of Vital Areas at Nuclear Facilities,” IAEA Nuclear Security Series No. 16, International Atomic Energy Agency, Vienna, Austria (2012).
6. Wood, S.T., et al., “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 1 Summary Manual,” NUREG/CR-6952, Vol. 1, Idaho National Laboratory, Idaho Falls ID (2008).
7. Smith, C.L., and S.T. Wood, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8, Vol. 1 Overview and Summary,” NUREG/CR-7039, Vol. 1, Idaho National Laboratory, Idaho Fall, ID (2011).
8. IAEA, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13,” International Atomic Energy Agency, Vienna, Austria (2011).
9. NRC, “Standard Review Plan, Chapter 13.6.2 Physical Security – Design Certification,” NUREG-0800, Chapter 13.6.2, U.S. Nuclear Regulatory Commission, Washington DC (2010).
10. M.L Garcia, “Vulnerability Assessment of Physical Protection Systems,” Elsevier, Burlington, MA (2006).
11. F.A. Duran, D. Dominguez, M.J. Parks, and R.M. Ward, “Modeling and Simulation of Insider Adversary Scenarios,” *Proceedings of the 53rd Annual Meeting of the INMM,* Institute of Nuclear Materials Management, Orlando FL (2012).
12. M. P. White, et al., “Effects of Impact and Explosion,” Summary Technical Report of Division 2, National Defense Research Committee, Washington, DC (1946).
13. L. A. Young, B. K. Streit, K. J. Peterson, D. L. Read, F. A. Maestas, “Effectiveness/Vulnerability Assessments in Three Dimensions (EVA-3D) Versions 4.1F and 4.1C User’s Manual – Revision A,” WL-TR-96-7000, Applied Research Associates, Inc., Albuquerque, NM (1995).
14. P. E. Dunn, J. E. Madrigal, D. A. Parsons, J. C. Partch, D. A. Verner, and L. A. Young, “Modular Effectiveness/ Vulnerability Assessment (MEVA) Software User’s Manual,” Applied Research Associates, Inc., Albuquerque, NM (1999).