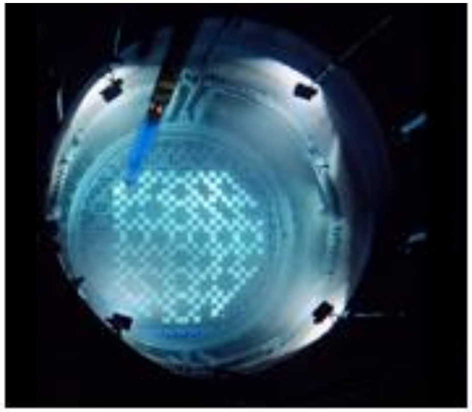
TRAINING FOR NUCLEAR FACILITY SABOTAGE ANALYSIS

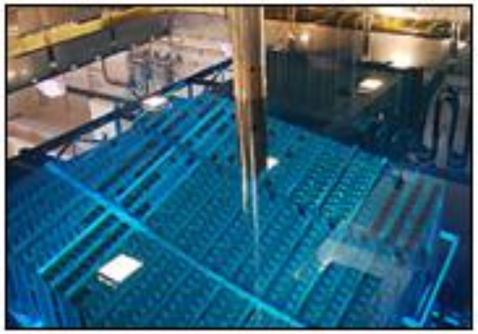
International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

Nov. 11-Nov.18, 2017

R. E. Hale Oak Ridge National Lab (ORNL)
J. W. Hockert (XE Corporation)
N. M. Winowich Sandia National Lab (SNL)
R. J. Belles ORNL
P. W. Gibbs ORNL
C. F. Weber ORNL
C. D. Sulfredge ORNL

Nuclear Facilities are sabotage risks



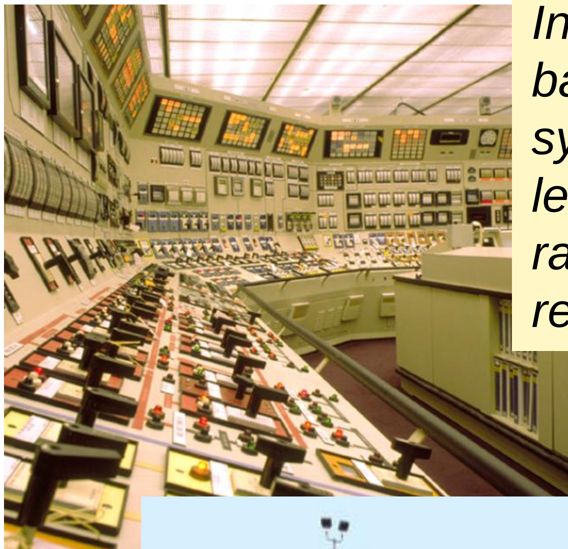



Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances".

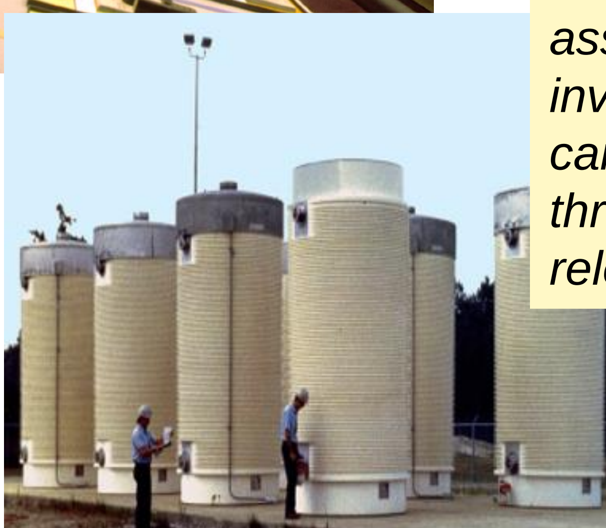
–INFCIRC 225, Rev 5 (NSS-13)

How do we protect different systems and inventories from sabotage threats?

Vital Areas (VA) are established to include potential direct release, and indirect release



Indirect sabotage based upon system failures leading to radiological release



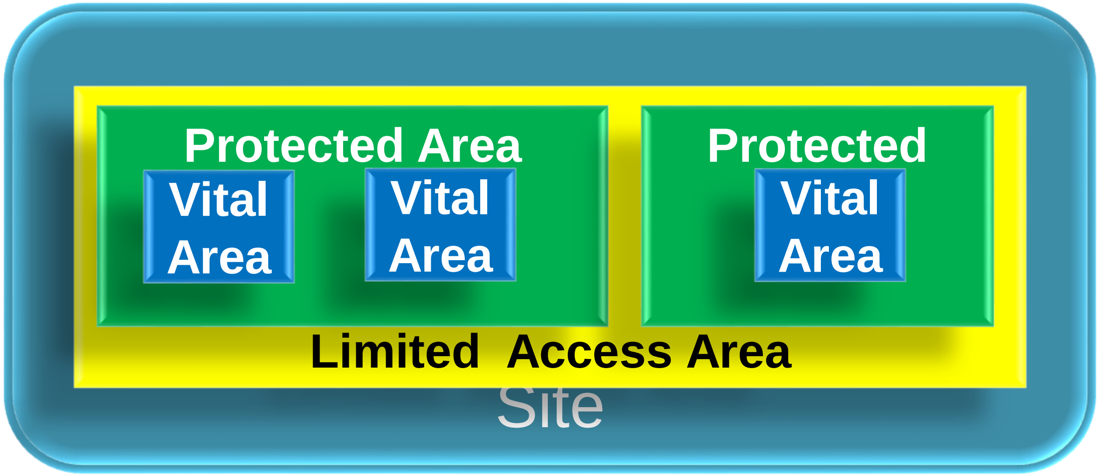
Direct sabotage associated with inventories that can be directly threatened for release.

"Nuclear material in an amount which if dispersed could lead to high radiological consequences and a minimum set of equipment, systems or devices needed to prevent high radiological consequences, should be located within one or more *vital areas*, located inside a *protected area*."

(NSS-13, Section 5.21)

How do we define Vital Areas?

Vital areas are defined as areas with nuclear material inventories or that contain components critical to protect nuclear material



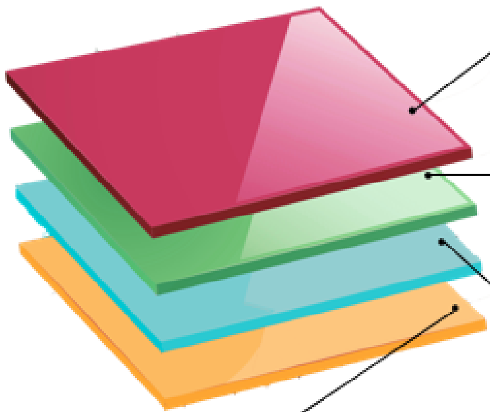
How do we determine vital areas in a nuclear power plant?

Limited Access Area: Designated area containing a *nuclear facility* and *nuclear material* to which access is limited and controlled for physical protection purposes.

Protected Area: Area inside a *limited access area* containing Category I or II *nuclear material* and/or *sabotage* targets surrounded by a *physical barrier* with additional *physical protection measures*.

Vital Area: Area inside a *protected area* containing equipment, systems or devices, or *nuclear material*, the *sabotage* of which could directly or indirectly lead to high radiological consequences.

IAEA Nuclear Security Series (NSS) documents provide guidance



Fundamentals – NSS-20
Objectives & Essentials of a State's Nuclear Security Regime

Recommendations – NSS-13
(application of Fundamentals)
Recommendations on the Physical Protection Of Nuclear Material & Nuclear Facilities

Implementing Guides –
(application of Recommendations)
NSS-7 *Nuclear Security Culture*
NSS-8 *Preventive and Protective Measures against Insider Threats*

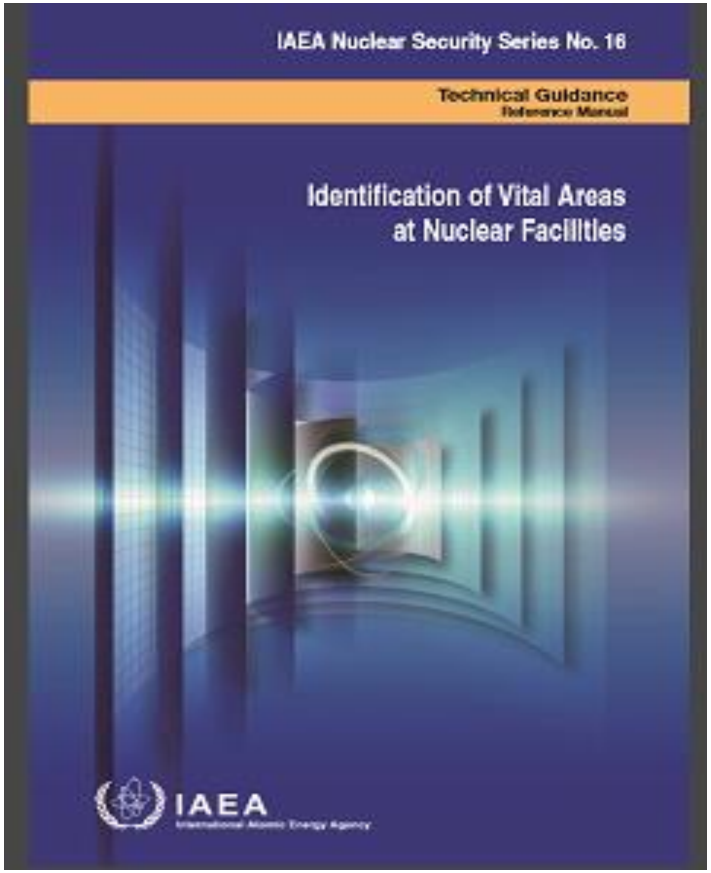
Technical Guidance –
NSS-16 *Identification of Vital Areas at Nuclear Facilities*
NSS-17 *Computer Security at Nuclear Facilities*

Tiered guidance steps through consideration of nuclear security threats

Not necessarily written with different facility focus groups in mind

Can we look at a single area for training purposes?

NSS-16 outlines guidance to ensure minimum set of Vital Area Equipment



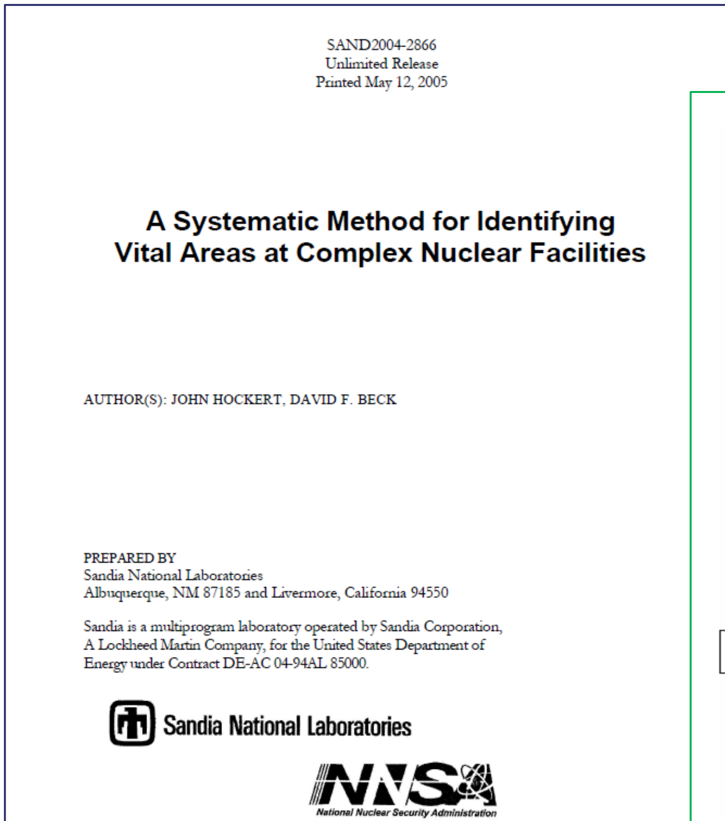
Vital Area Equipment is described by standard NSS-16

The objective of this standard is to provide a structured approach to identifying the areas that contain equipment, systems, and components to be protected against nuclear sabotage.

NSS-16 provides detailed guidance with regard to the identification of vital areas, that is, the areas to be protected in high consequence facilities.

How was this guidance developed?

Methodology based on original work by Sandia National Laboratories



SAND2004-2866
Unlimited Release
Printed May 12, 2005

A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities

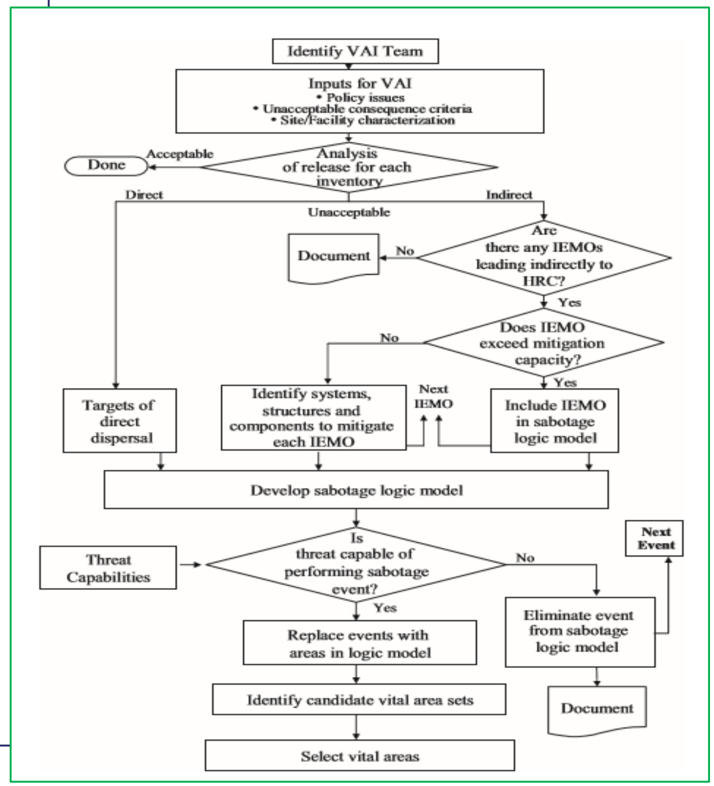
AUTHOR(S): JOHN HOCKERT, DAVID F. BECK

PREPARED BY
Sandia National Laboratories
Albuquerque, NM 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, A Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC 04-94AL 85000.

Sandia National Laboratories

NNSA
National Nuclear Security Administration

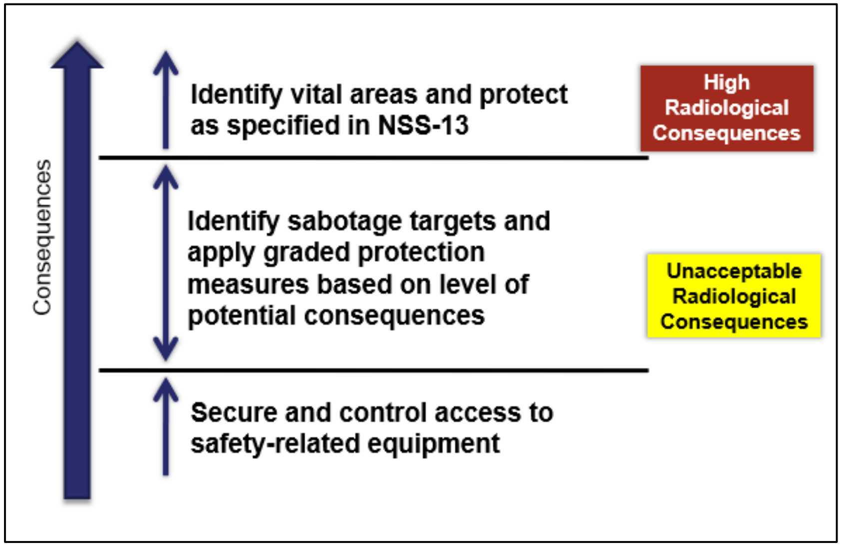


Method first outlined in workshop that was observed by IAEA staff experts and the methodology and training approach was deemed worthy of further development into NSS-16

Methodology developed in 2005 and implemented in 2012 through NSS-16

Methodology allows graded approach to safety based upon level of consequence

- ***The State sets consequence levels* for:**
  - Unacceptable Radiological Consequences (URC)
  - High Radiological Consequences (HRC)
- Competent authority specifies required protections for facilities that range from URC to HRC
- Damage to NPP core is by definition HRC



Level of consequences = level of protection

How are HRC levels established and calculated?

HRC Simplification for Nuclear Power Reactors

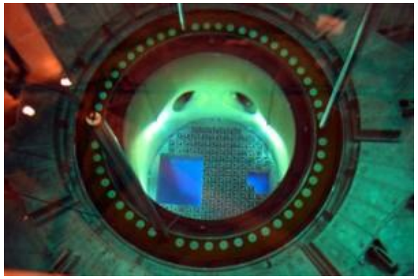
Largest NPP Radioactive Inventories

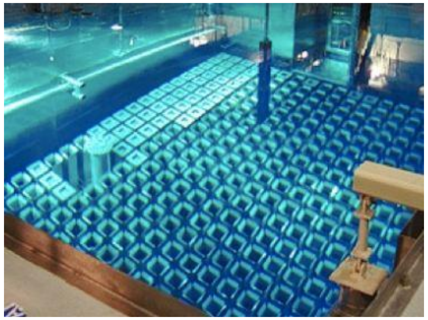
Reactor Core

- High Radiological Consequences per NSS 13 (5.20)

Compare remaining inventories with HRC / URC Threshold

- Spent Fuel Pool / Storage
- Radioactive Waste
  - Gaseous Waste Tanks
  - Solid Waste
  - Liquid Waste



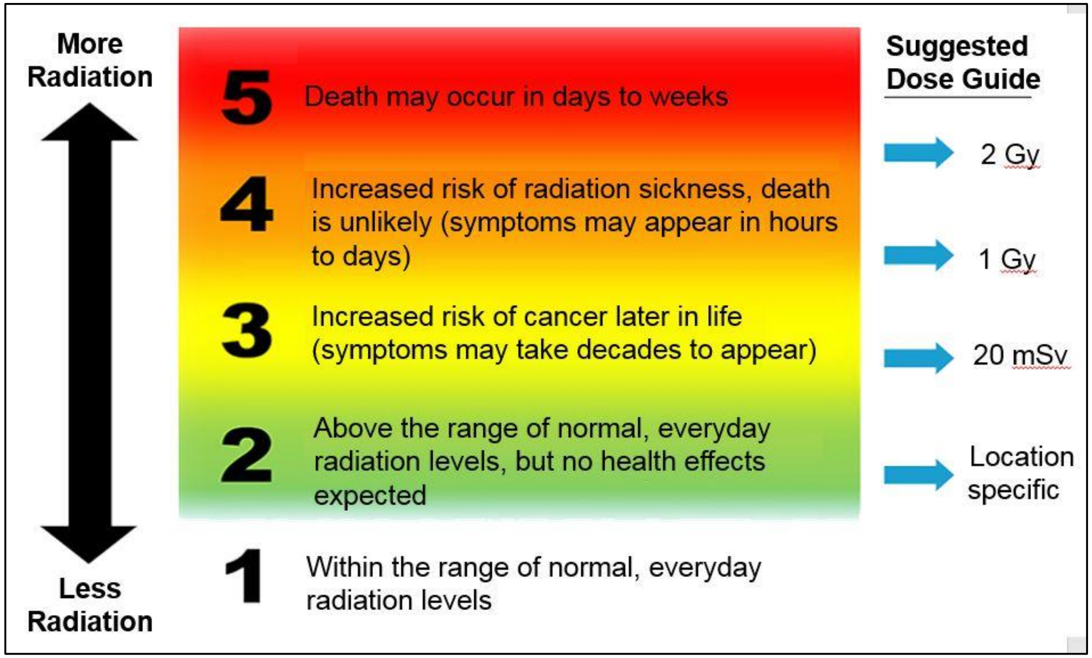


How are URC levels established and calculated?

URC is Based on Radiation Dose

Consider these key questions about URCs:

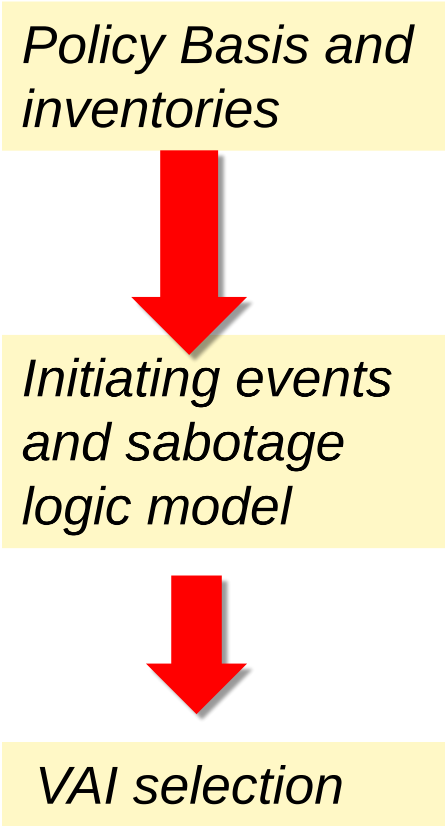
1. What dose level results in unacceptable health consequences?
2. How and where is the dose calculated? The site boundary? Time of exposure?
3. How is "loss of use" considered? (for example, evacuation of an area for a period of time)



The amount of radiation that the body absorbs (a radiation dose) determines health consequences. Measurable units include: gray (Gy), Sievert (Sv), rad., or rem. This module uses Sv.*

Once HRC/URC limits established what process do you follow?

Process includes 10 steps in three phases



How best to train multi-disciplinary groups on this methodology?

Phase I: Policy Basis and Inventories

I. Address policy considerations—The regulatory body must make key policy decisions (such as URC criteria) that form the basis for VAI.

II. Evaluate site and facility characteristics—Determine the inventories of nuclear and radioactive material and the facility and site characteristics needed to determine whether sabotage could lead to URC.

III. Perform conservative analysis—Determine whether the complete release of any inventory could exceed the URC criteria. Include direct dispersal of any such inventory as an event in the sabotage logic model and continue with the process described below.

Policy Basis and inventories Established to lay guidelines for sabotage logic model

Policy considerations are managers, and inventories are ops/facility safety

Phase II: Develop Sabotage Logic Model

IV. Identify initiating events of malicious origin (IEMO) -Identify any initiating events (IE) [6] that can, alone or in combination with other malicious acts, lead indirectly to URC and identify the systems required to mitigate those IEs.

V. Develop sabotage logic model—Construct a sabotage logic model that identifies the combinations of events that would lead to URC.

VI. Assess threat capabilities—Eliminate from the sabotage logic model any events that the assumed threat does not have the capability to perform.

VII. Identify areas corresponding to sabotage logic model events—Identify the locations (areas) in which direct dispersal, IEMOs, and the other events in the sabotage logic model can be accomplished. Replace the events in the sabotage logic model with their corresponding areas.

Sabotage logic models created from event trees and modified into sabotage fault trees with locations as terminal points

Sabotage logic model development is safety analysis

Phase III: Solve Sabotage Logic Model and identify Vital Areas

VIII. Identify candidate VA sets—Solve the sabotage area logic model to identify the combinations of locations that must be protected to ensure that URC cannot occur.

IX. Select a VA set—Select the VA set that will be protected to prevent sabotage leading to URC.

Complement of sabotage model solved for prevention sets with optimized selection of VA's determined based upon cost and other factors

Final selection of VAs includes managers, ops, facility safety and protection force

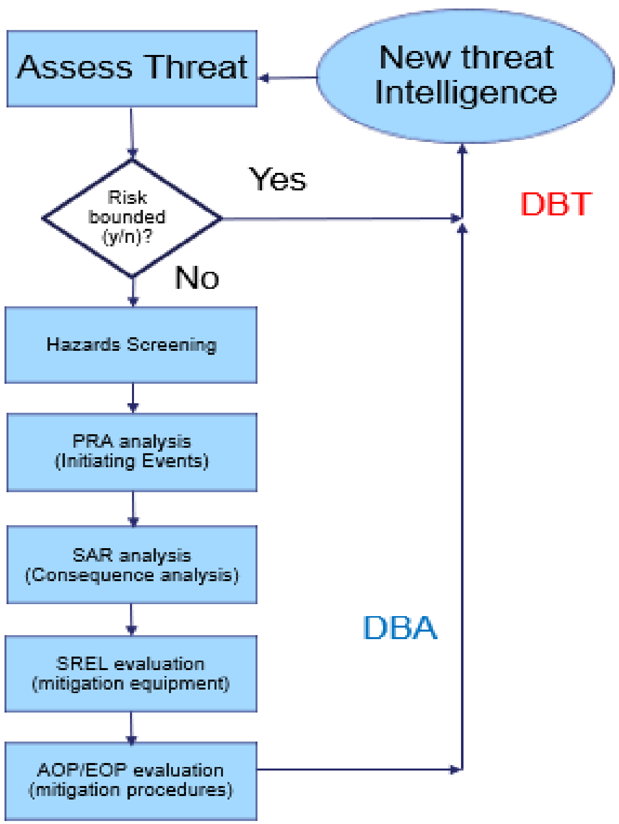
Training must focus on risk, and reflect the needs/responsibilities of managers, protective force, operations, and safety analysts

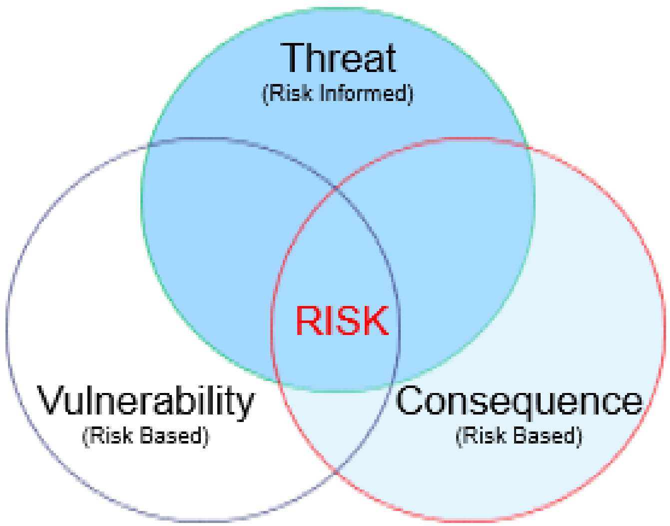
- **Managers/Regulators** → **Compliance against requirements**
- **Protective Force** → **Physical protection and response to sabotage**
- **Operations** → **Operational response to sabotage events**
- **Safety Analysis** → **Facility analysis of automatic plant response**

Each group has different responsibilities and areas of expertise

What documentation can be leveraged for this training?

Safety analysis documents indirectly reference potential sabotage risks





Content material needs to be "layered" and "branched" to allow rapid tailoring to meet audience needs

Safety analysis documents help to define risk be must usually be refocused to sabotage threats

How do we leverage this existing documentation?

Start with familiarizing target audiences with applicable documentation and sabotage considerations

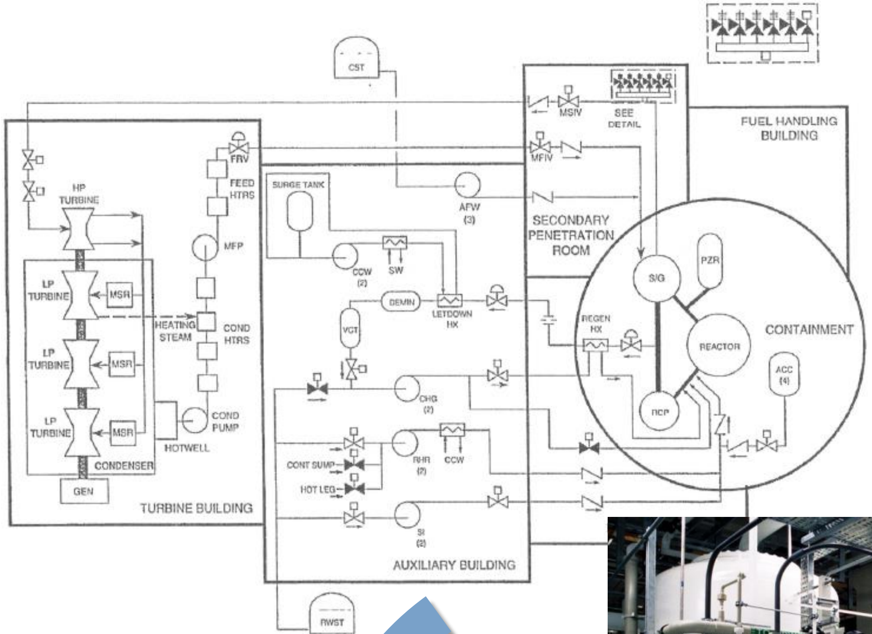
Reference	Security Force	Oversight/ Facility Managers	Operations/ Engineering
Hazards Assessment (HA)		✓	✓
Design Description (DD)	✓	✓	✓
Safety Analysis Report (SAR)			✓
Probabilistic Risk Assessment (PRA)			✓
Safety Related Equipment List (SREL)			✓
Abnormal/ Emergency Operating Procedures (AOP/EOPs)	✓	✓	✓
Technical Safety Requirements (TSRs)		✓	✓
Vital Area Identification/ Sabotage Report (VAI/SR)	✓	✓	✓
Facility Walkdown (FW)	✓	✓	✓

Different documents are designed for different audiences

All references reviewed for potential sabotage related information and categorized for audiences

Is there information that can be used as a training example?

Utilize Lone Pine Nuclear Power Plant (LPNPP) as example

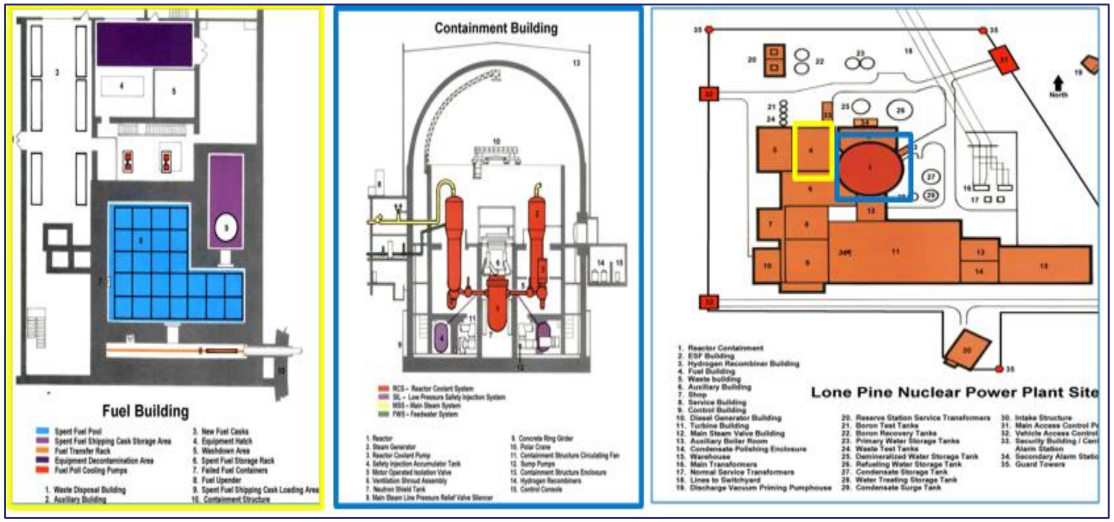


Lone Pine is a surrogate facility based upon a 4-loop Westinghouse PWR

LPNPP reference documents used at ITC-26

Why use LPNPP for training example?

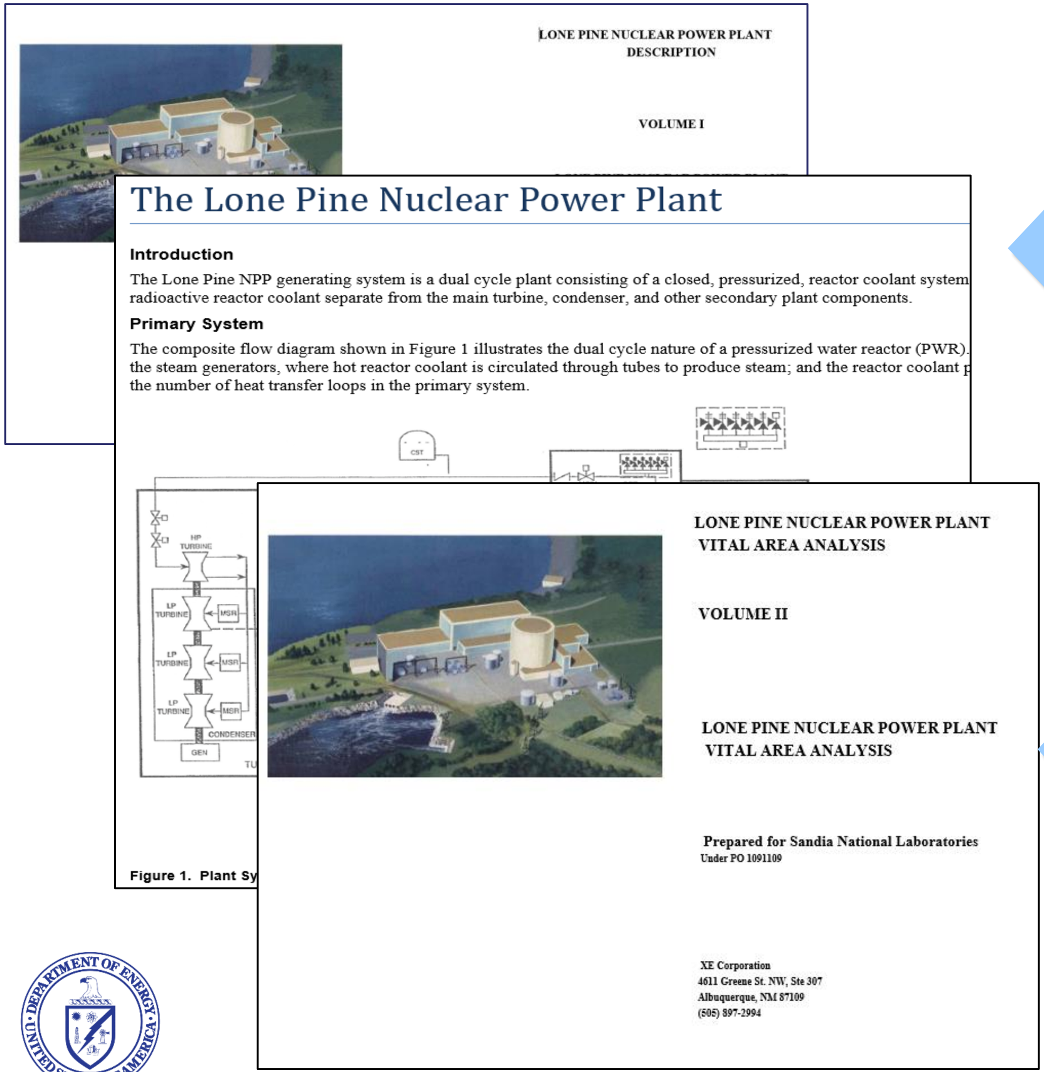
LPNPP fictional facility ensures no publishing of actual plant data



Lone Pine Nuclear Power Plant was developed to be a surrogate facility that allows training on a conceptual nuclear power plant that has all the features of an actual plant

The LPNPP system diagrams and descriptions are drawn directly from the NRC course material for the 104P, 304P, and 504 courses that are in the nuclear library

LPNPP Sources of Site and Facility Information



Documentation includes facility descriptions, including summary of deterministic safety analysis description of plant response to design basis accident and transients. (Volume 1)

VAI analysis documented in Volume 2.

What is considered in LPNPP VAI?

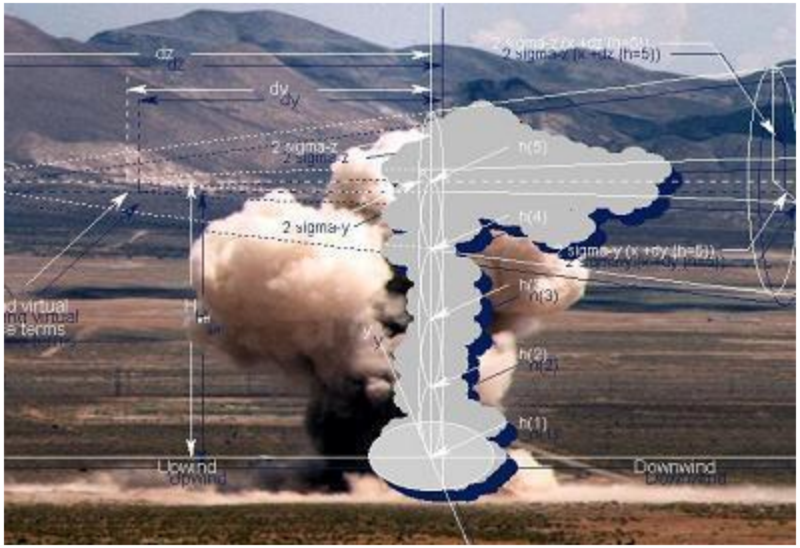
Direct sabotage sequences not analyzed in LPNPP VAI analysis

Useful primarily for modeling consequences of direct attack

Direct sequences straightforward with inventories

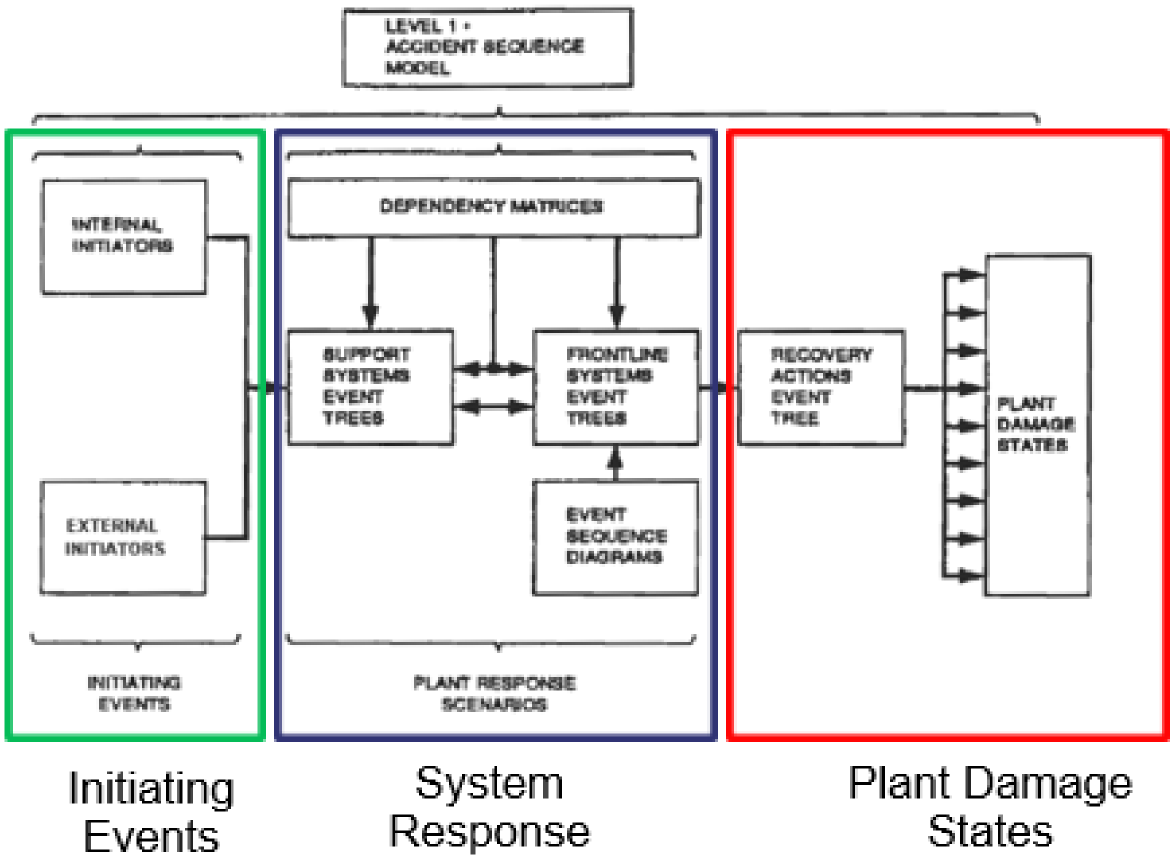
Model plume coverage after a fire / explosion dispersal event

Dependent upon atmospheric and geographic conditions



How are indirect sabotage sequences identified?

Indirect sabotage analyzed based upon initiating events of malicious origin (IEMO)



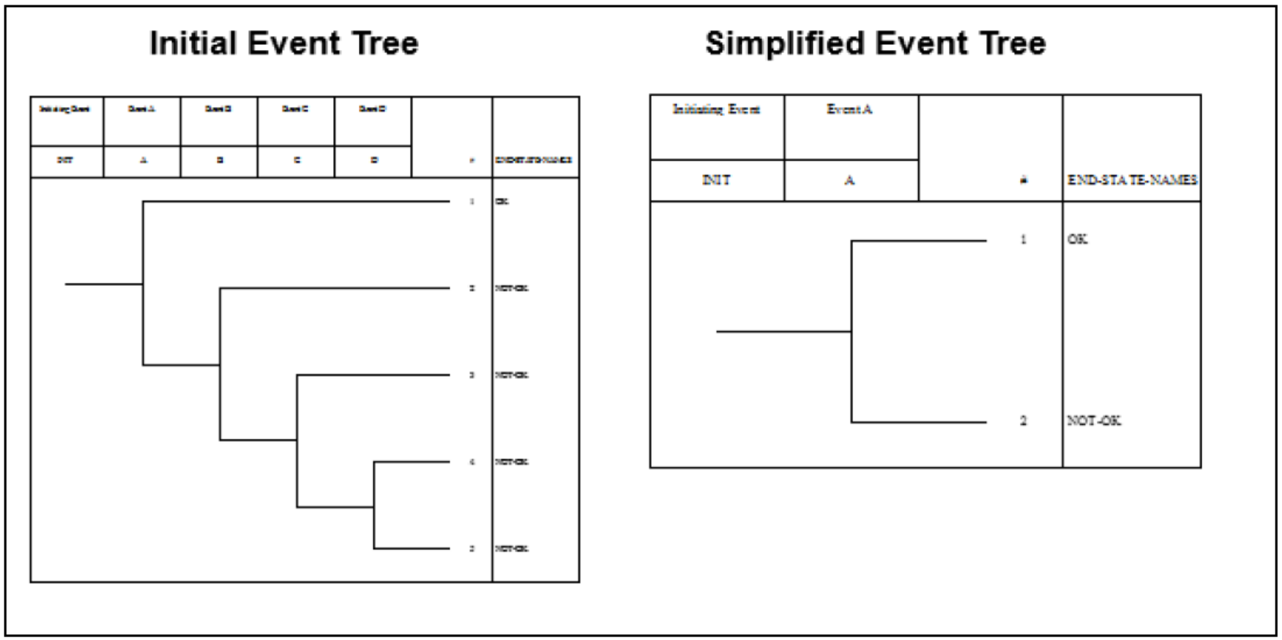
Anything that can happen by accident can be made to happen.

Initiating events converted to fault trees

Sabotage fault trees generated from modified event trees

How do we narrow down sequences for consideration?

Event trees are aggregated and modified for sabotage and converted to fault trees



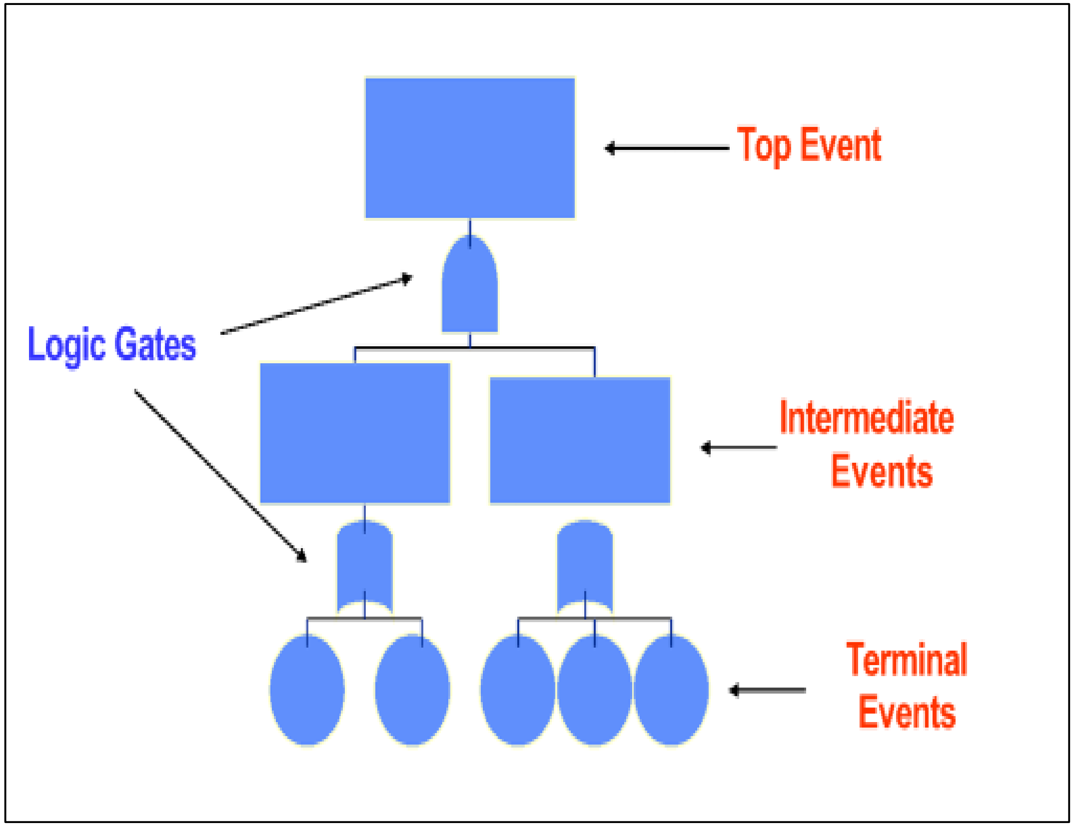
How are the fault trees constructed?

Anything that can happen by accident can be made to happen.

Initiating events converted to fault trees

Sabotage fault trees generated from modified event trees

Fault trees start with HRC top event and Terminal basic events attached to locations



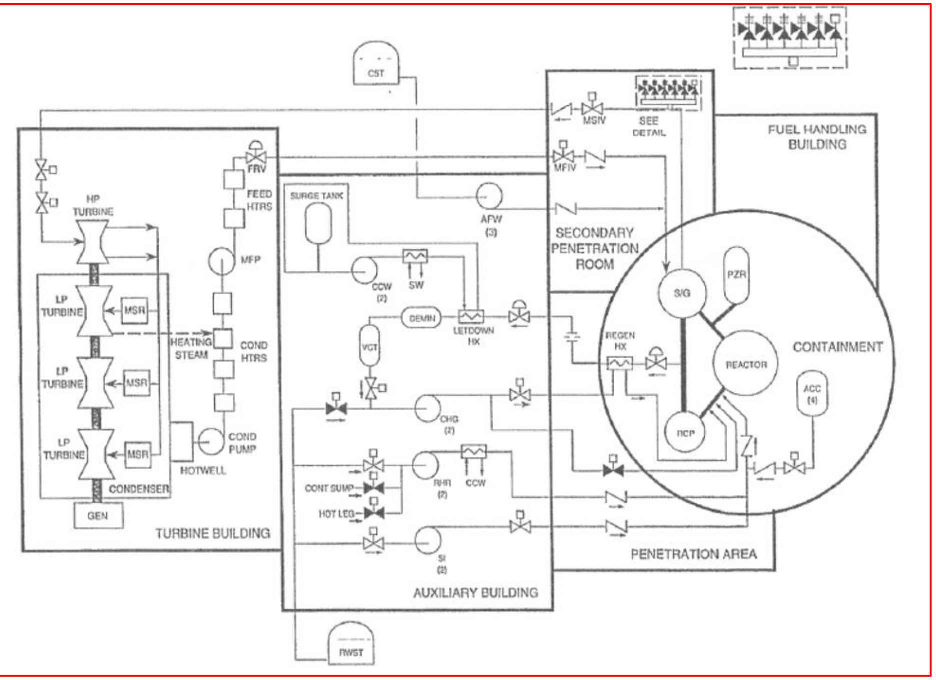
Links combinations of malicious acts that can lead to HRC

- Top Event –HRC
- Intermediate events – AND / OR combinations of events leading to Top Event
- Terminal Events – Destruction or disablement of components or structures

Structure is identical to fault trees used in Probabilistic Safety Analysis

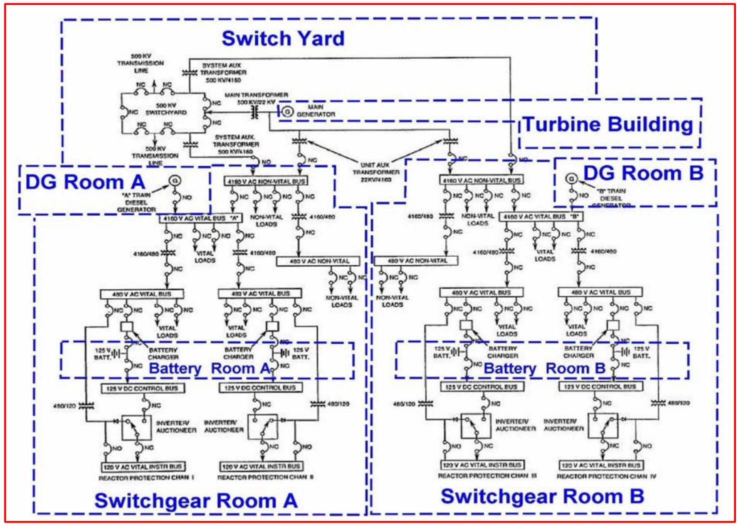
How do we determine the terminal event locations?

Facility Layout used to establish potential sabotage threat locations



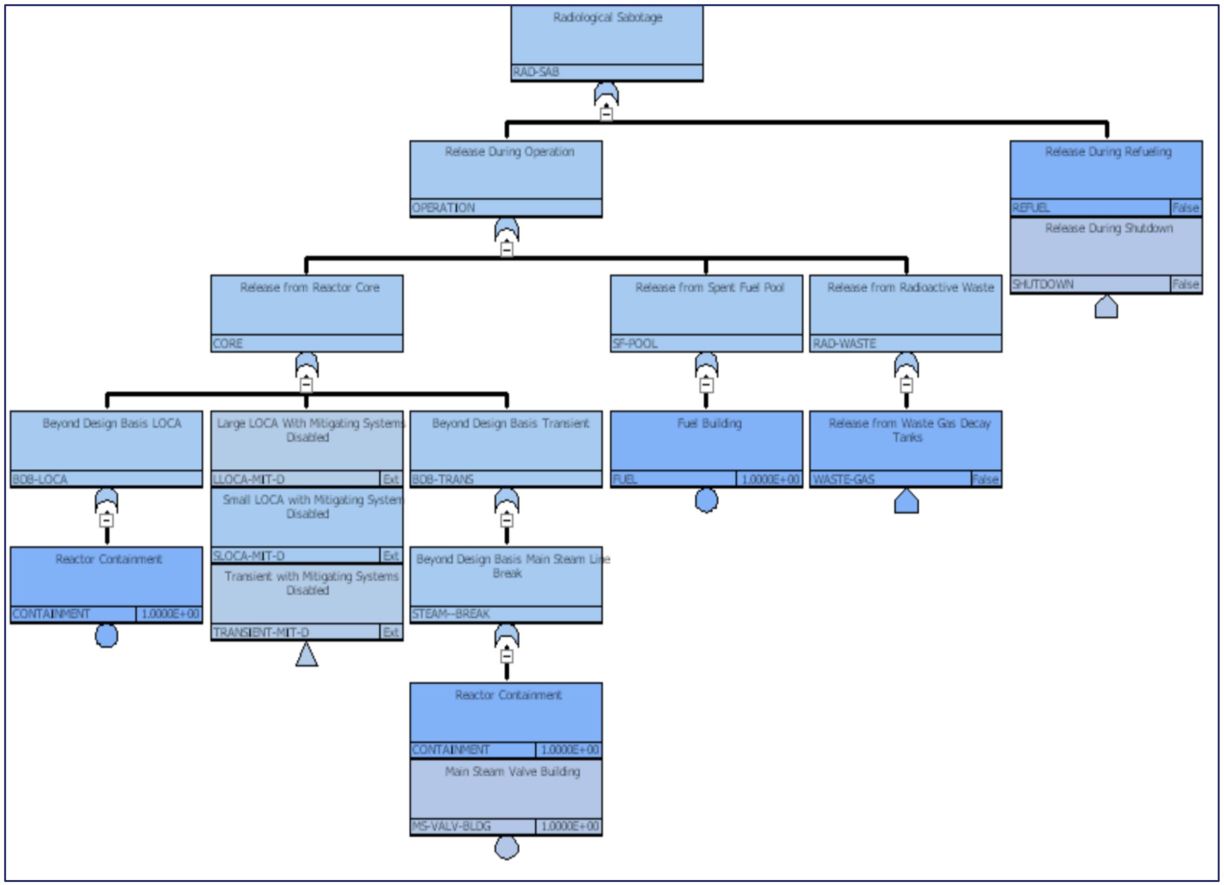
Facility layouts used to identify major equipment in buildings

PIDs over-laid with building/area locations.



What does the LPNPP sabotage model look like?

LPNPP full sabotage logic model developed for multiple events



Full model includes plant operations and placeholders (house events) for other modes of operation including refuelling/defueling and waste operations

How are the final sequences reduced?

LPNPP sabotage logic model includes sabotage actions tied to locations

Basic Event	Location	Rationale
AFW-DISCHARGE-A (Disable Discharge from AFW Pump A)	AFW-PUMP-RM-A (AFW Pump Room A)	Location of pump discharge line.
	CONTAINMENT (Reactor Containment)	Location of pump discharge line.
	CONTROL-RM (Control Room)	Control of motor operated valves in discharge line.
	SWG-RM-A (Switchgear Room A)	Motor control centers for discharge line motor operated valves.
AFW-PUMPA-CONTROL (Disable Control to AFW Train A Pump)	BATT-RM-A (Battery Room A)	Control power for pump.
	CABLE-SPREAD (Cable Spreading Room)	Control cables for pump
	CONTROL-RM (Control Room)	Control of pump
AFW-PUMPA-DIS (Disable AFW Train A Pump)	AFW-PUMP-RM-A (AFW Pump Room A)	Location of pump
AFW-SUCTION-A (Disable Suction to AFW Train A Pump)	CONTROL-RM (Control Room)	Control of motor operated valves in suction line.
	CST (Condensate Storage Tank)	Water source.
	CST-PIPING (Piping from Condensate Storage Tank)	Piping from water source accessible only through 2 man ways in the Protected Area.
	SWG-RM-A (Switchgear Room A)	Motor control centers for suction line motor operated valves
AFW-DISCHARGE-B (Disable Discharge from AFW Pump B)	AFW-PUMP-RM-B (Auxiliary Feedwater Pump Room B)	Location of pump discharge line.
	CONTAINMENT (Reactor Containment)	Location of pump discharge line.
	CONTROL-RM (Control Room)	Control of motor operated valves in discharge line.
	SWG-RM-B (Switchgear Room B)	Motor control centers for discharge line motor operated valves

Basic event location table and sabotage action table used to ensure IEMO threats are credible

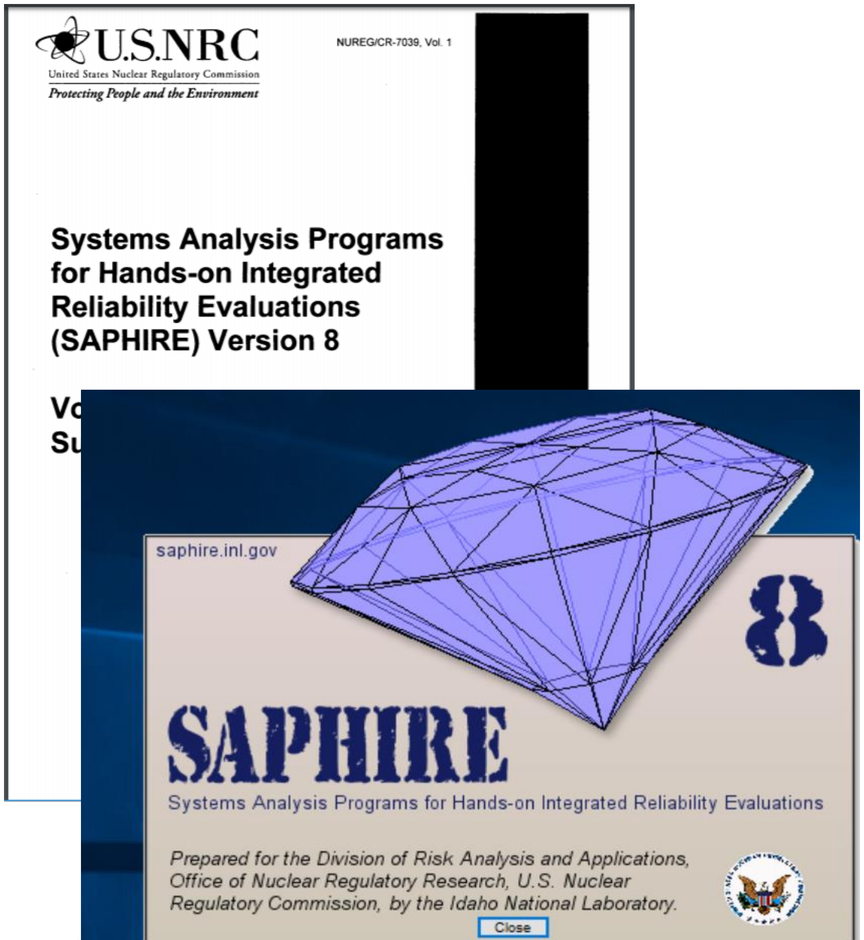
The radiological sabotage actions in the single areas area as follow:

Area	Radiological Sabotage Actions
Control Room	• Initiate LOCA and disable mitigating systems. • Initiate loss of offsite power transient and disable mitigating systems (auxiliary feedwater)
Cable Spreading Room	• Initiate loss of offsite power transient and disable mitigating systems (auxiliary feedwater) by interrupting control signals
Reactor Containment	• Create beyond design basis LOCA • Initiate large or small LOCA and disable mitigating systems • Initiate loss of offsite power transient and disable mitigating systems
Scram Relay Room	• Initiate loss of offsite power transient and disable mitigating systems (reactor protection system)
Main Steam Valve Building	• Create beyond design basis main steam line break transient.
Fuel Building	• Explosive dispersal of spent fuel in spent fuel pool within 60 days of refueling.

Non-credible sabotage actions in areas are used to eliminate sequences from sabotage logic model

What software is used to solve the fault trees?

VAIs determined from solutions to reduced sabotage area logic model



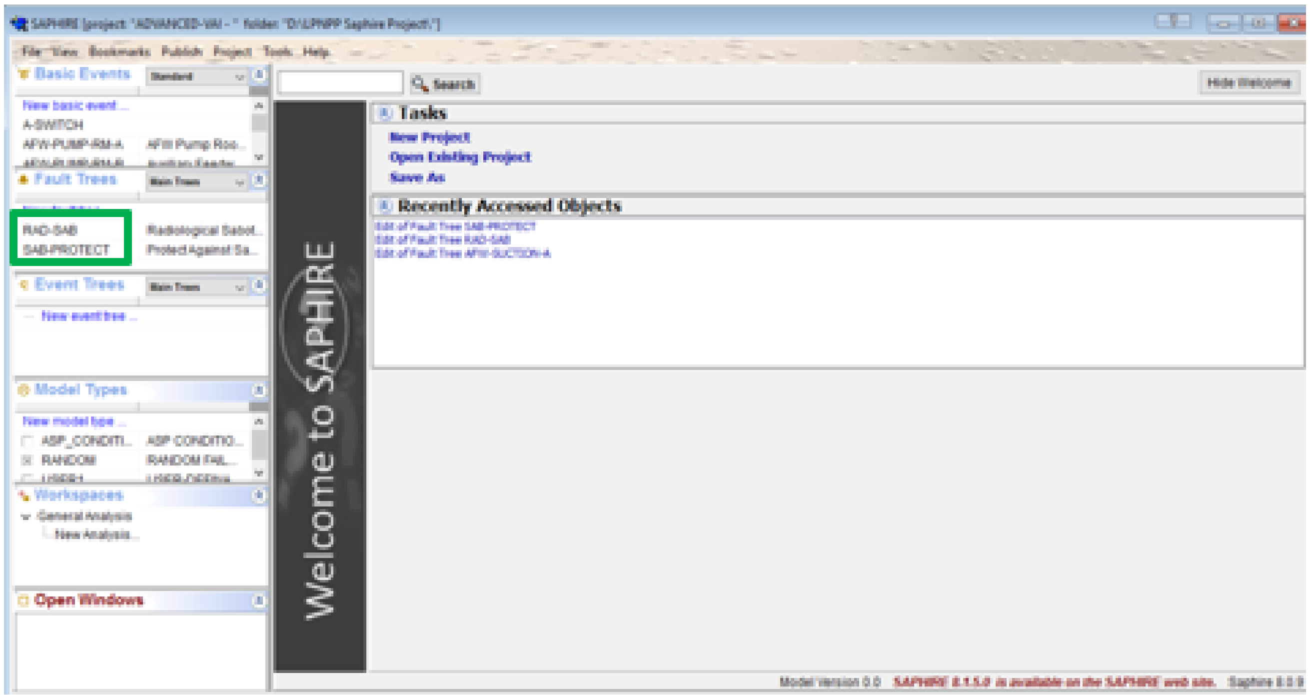
Any PRA software can solve fault tree models

Should use same software developed for PRA

Comparison of different models is based upon implementation of sabotage rules, not Boolean solvers.

What does the output look like?

SAPHIRE LPNPP Models were developed

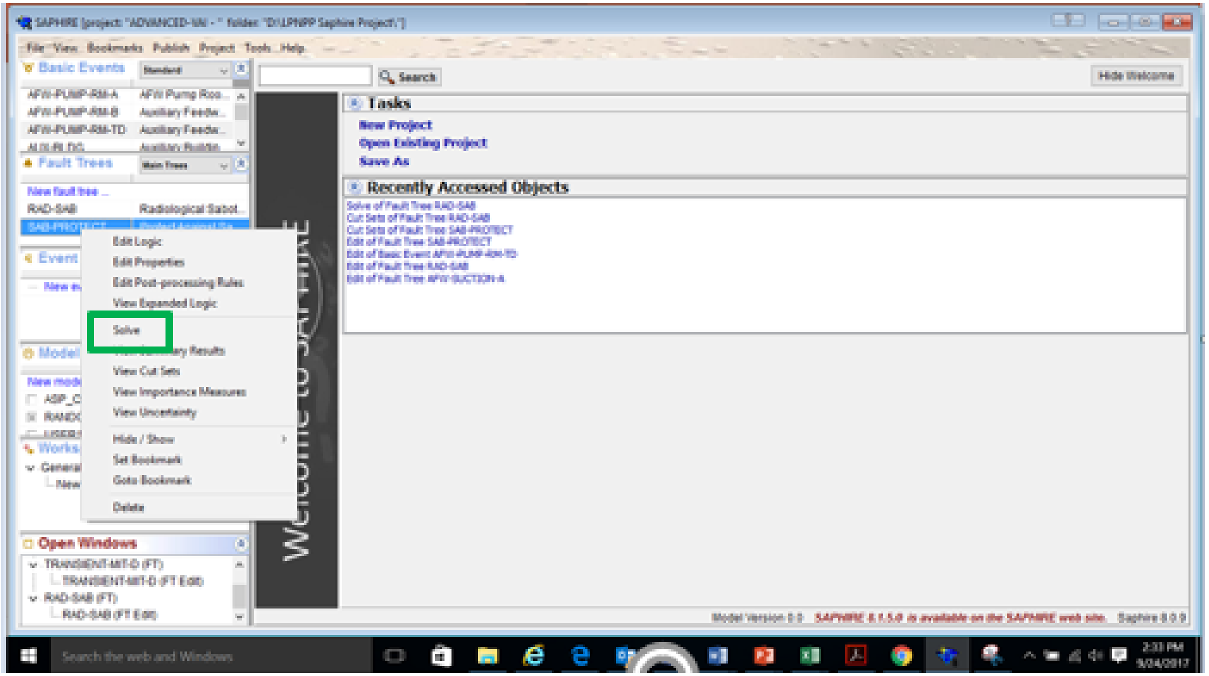


SAPHIRE model includes both sabotage target sets (RAD-SAB) and protection sets (SAB-PROTECT) .

Two models developed including radiological sabotage model and sabotage protection model.

How do we solve the sabotage models in SAPHIRE?

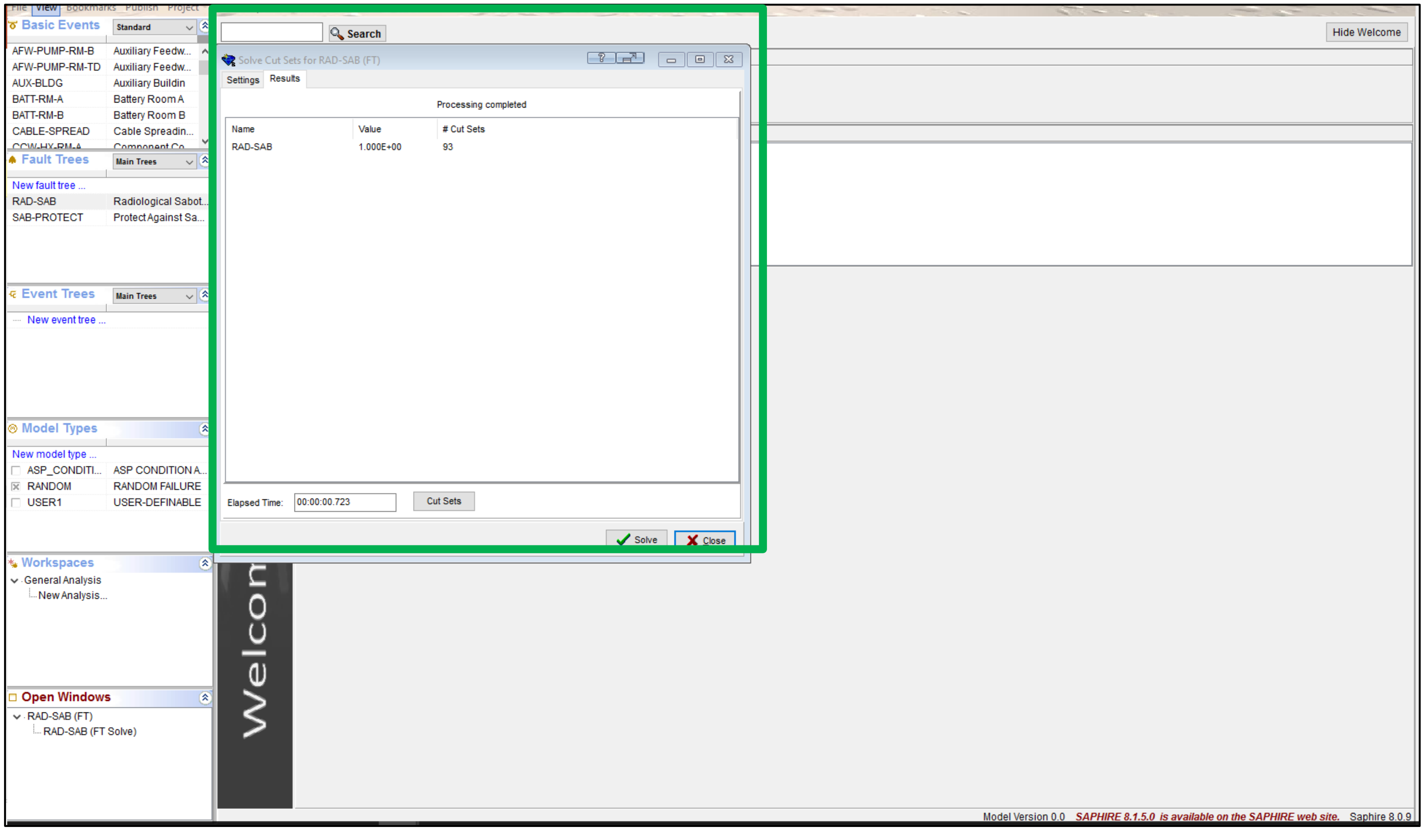
Finding the Cut Sets –Solutions to the Sabotage logic model



Solution of fault tree is automatic in SAPHIRE upon hitting “Solve” .

What are the “cut sets” and what do they mean?

Cut Sets Are the Minimum Complement of Equipment/Locations

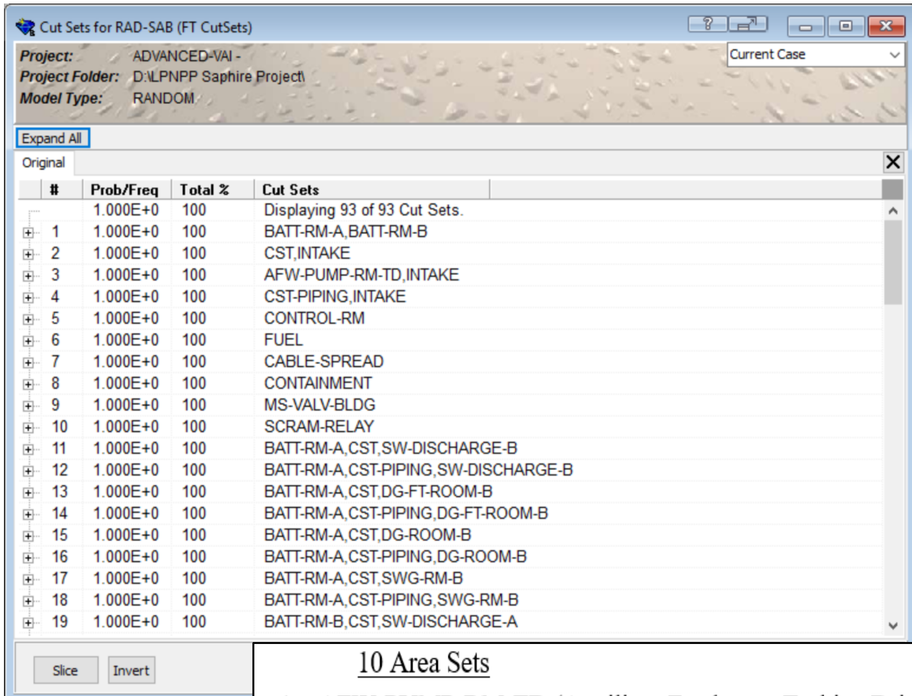


Cut sets include "singles", "doubles" and "triples" for number of areas needed.

Rad-Sab model solution includes 93 cut sets as identified in LPNPP Vol. 2 (VAI) and seen here.

How are the final Vital Areas chosen from the cut sets?

Vital Area Sets Come from "Solving" the Fault Tree and optimizing



Considerations for Selection of Vital Areas

- Ease, effectiveness, and cost of protecting the vital areas
- Impacts on safety and emergency response
- Impacts on operation/maintenance
- Availability of protected components, equipment, and devices (Temp VAs)
- Other factors established by facility or competent authority

10 Area Sets

1. AFW-PUMP-RM-TD (Auxiliary Feedwater Turbine Driven Pump Room), BATT-RM-A (Battery Room A), CABLE-SPREAD (Cable Spreading Room), CONTAINMENT (Reactor Containment), CONTROL-RM (Control Room), CST (Condensate Storage Tank), CST-PIPING (Piping from Condensate Storage Tank), FUEL (Fuel Building), MS-VALV-BLDG (Main Steam Valve Building), SCRAM-RELAY (Scram Relay Room)
2. AFW-PUMP-RM-TD (Auxiliary Feedwater Turbine Driven Pump Room), BATT-RM-B (Battery Room B), CABLE-SPREAD (Cable Spreading Room), CONTAINMENT (Reactor Containment), CONTROL-RM (Control Room), CST (Condensate Storage Tank), CST-PIPING (Piping from Condensate Storage Tank), FUEL (Fuel Building), MS-VALV-BLDG (Main Steam Valve Building), SCRAM-RELAY (Scram Relay Room)

How is this information used?

Protect Vital Areas and develop sabotage checklists for different VA's and groups

FACILITY INFRASTRUCTURE (cont.)	n/a	1 Prepared	2	3 Not prepared	Facility Protective Force	Facility Oversight / Regulation	Engineering/ Operations	Applicable Documentation	Lone Pine Score/NOTES
Storage Tanks / Vessels / Pits									
15. Appropriate secondary containment for storage tanks/vessels and pits is provided							X	DD/FW	
16. There are overfill protection / notification procedures							X	AOP/EOP	
Process Control Systems									
17. There is backup power to process control systems						X	X	PRA/SAR	
18. Access to process controls is limited					X	X	X	VAI/SR	
Telephone and Data Lines									
19. There are backup communications for reaching emergency response personnel					X	X	X	DD/AOP/EOP	
20. Backup systems include wireless communication as well as land line communication					X	X	X	DD/AOP/EOP	
21. There is a clear emergency protocol for whom to notify					X	X	X	DD/AOP/EOP	
22. All telephones are properly labeled with appropriate emergency notification procedures					X	X	X	DD/AOP/EOP	
Water Supply									
23. There is a system in place to verify water quality							X	DD	
24. All access points to water supply are secured					X			FW	
Backup Power Systems									
25. Multiple types of backup power are available						X	X	DD/SAR/TSR	
26. Backup power systems can be easily implemented (How)							X	DD/SAR/TSR	
27. There is an automatic transfer if needed						X	X	DD/SAR/TSR	
28. If a backup generator is used it is easily started, adequate fuel is available, and it will run sufficiently long based on required operations						X	X	DD/SAR/TSR	
29. Critical systems are covered by backup power						X	X	DD/SAR/TSR	
30. Backup emergency systems includes lighting, sprinklers, ventilation, communication and alarms						X	X	DD/SAR/TSR	

HA-Hazards Assessment; **DD**-Design Description, **SAR**-Safety Analysis Report, **PRA**- Probabilistic Risk Assessment, **SREL**-Safety Related Equipment List, **TSR**-Technical Safety Requirements, **AOP/EOP**-Abnormal and Emergency Operations Procedures, **VAI/SR**-Vital Area Assessment/Sabotage Report, **FW**-Facility Walkdown

Checklist developed from American Chemical Society sabotage checklist and modified to include potential documentation sources and audiences for information

Checklists used to ensure sabotage considerations remain a part of plant design modifications and operations

SUMMARY

Sabotage training is a multi-disciplinary effort that involves engaging several different audiences

The fictitious Lone Pine Nuclear Power Plant was used in conjunction with methodology in NSS-16 to develop a training example for Vital Area Identification (VAI).

Sabotage logic models were built from fault trees using SAPHIRE and protection sets identified by solving the model.

Checklists were developed to extend results towards monitoring facility readiness against sabotage

For hardware components, method is straightforward, but questions remain....what about Cyber?