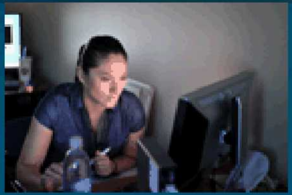
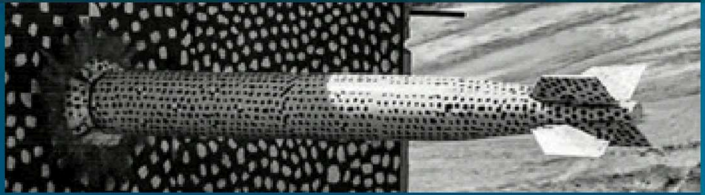
SAND2019-13742C

An Approach to Sabotage Mitigation





Douglas M. Osborn, PhD

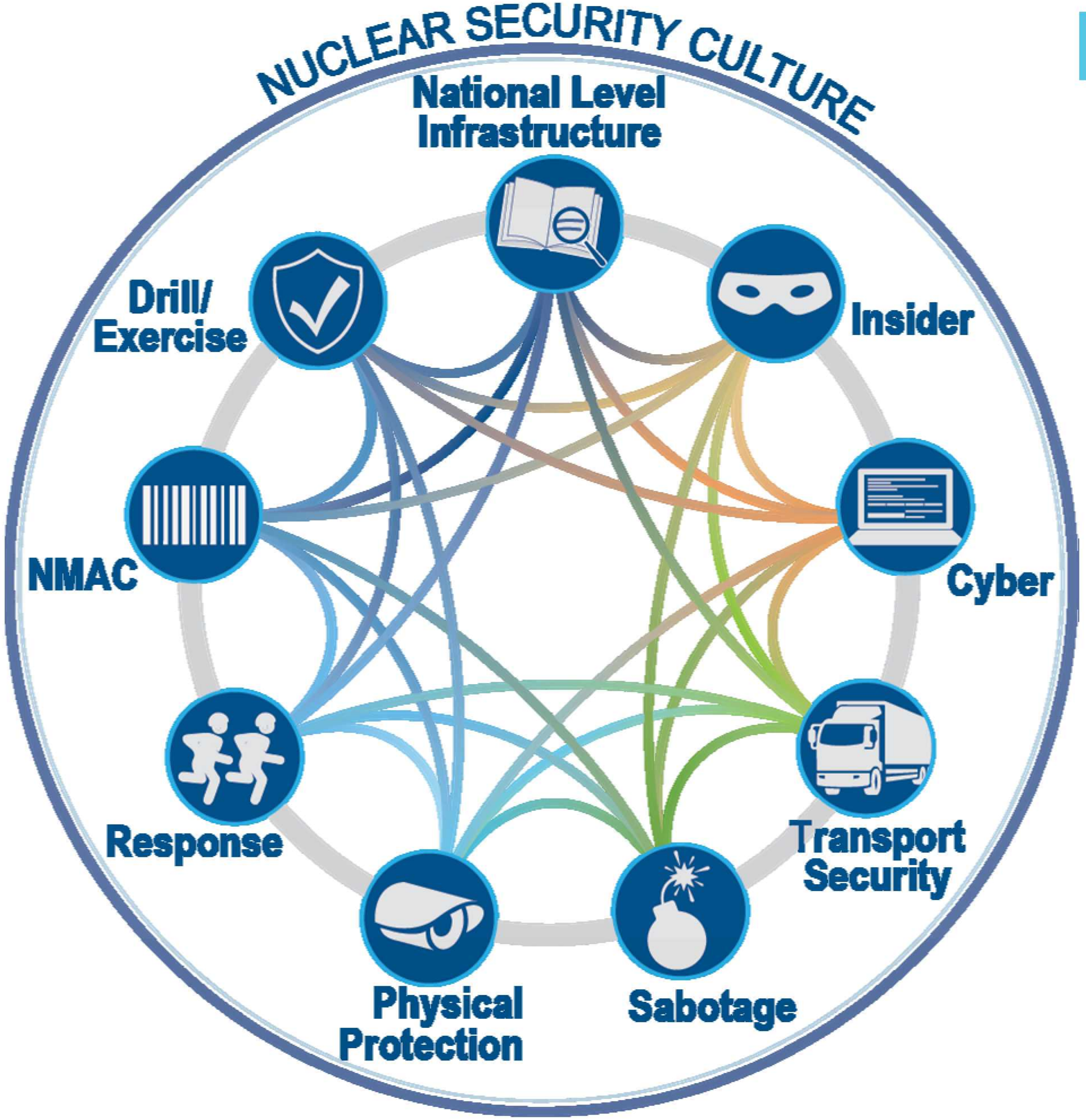
5th Arab Forum on the Prospects of Nuclear Power for Electricity Generation and Seawater Desalination

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.

SAND2019-XXXX

Functional Teams support crosscutting nuclear security approach

Sabotage Mitigation



Physical Protection Regime Objectives

Per Amendment to the Convention on the Physical Protection of Nuclear Material and supported by NSS No. 13

- Protect against unauthorized removal of nuclear material in use, storage, and transport
- Ensure implementation of rapid and comprehensive measures to locate and recover lost or stolen material
- Protect nuclear material and facilities against sabotage
- Mitigate or minimize the radiological consequences of sabotage

Sabotage Targets

- Nuclear or other radioactive materials
- Process or support equipment needed to prevent unacceptable radiological consequences

NSS No. 13 specifies Physical Protection Strategy (PPS) should protect against unacceptable radiological consequences (URC) and high radiological consequences (HRC)

- State is responsible for identifying what constitutes URC and HRC

PPS should protect against any sabotage scenarios that exceed URC thresholds (graded approach)

Types of URC/HRC Thresholds

Possible basis for threshold definition

- Quantitative (safety criteria)
- Qualitative (relative risk)

Release-based or dose-based criteria

- Maximum allowable release or dose
- Usually use existing safety limits
- Requires detailed dispersion modeling

Design limit threshold

- Specifies an unacceptable plant state (e.g., core damage)
- Requires less analytical effort
- Generally more conservative

Two ways Sabotage Can Occur

Direct

- Adversary applies energy directly to the nuclear / radioactive material to cause dispersal
- Adversary gains access to area in which material is located
- Example: Explosive or incendiary device is used to disperse the material (target = material)

Indirect

- Adversary uses energy present in the material or process system to cause dispersal
- Requires initiating a process upset condition and disabling the systems designed to mitigate the upset (target = safety system)
- Example: Disable one or more of the three essential safety functions: reactivity control, cooling, and containment

Vital Areas and Sabotage Prevention

Vital areas contain equipment, systems or devices, or nuclear material that, if sabotaged, could directly or indirectly lead to high radiological consequences

NSS No. 13 – Protect vital areas that contain:

- Inventories of nuclear or radioactive material with potential to exceed HRC if dispersed (direct scenarios)
- A minimum set of equipment needed to prevent indirect sabotage scenarios
- Additional guidance, NSS No. 17 and NSS No. 33T

Safety analyses such as Probabilistic Safety Analysis (PSA) can be used to identify vital areas

Sabotage Mitigation Assessments, Methodologies, & Tools

Methodology

- Design Basis Threat
- Target Set & Vital Area Identification
- Vulnerability Assessment
- Physical Protection Strategy

Tools

- DOE 0470.3c
  INFCIRC/225/R4
- SAPHIRE, EMRALD, VISAC
- FoF, System Response, & Blast Effect Analysis
- URC/HRC & other Impact Analyses

- Variances in nuclear power plant facility types requires a dynamic suite of methods, tools, and subject matter experts

- Advancements in nuclear reactor design require new suite of tools and methods (dynamic PSA & HAZCADS)
  - *IAEA does not have recommendations*

Sabotage Mitigation

Tools/Assessment Methodologies

Methodology	Tools
Design Basis Threat	Sabotage Checklist, & Open Source DBT development
Probabilistic Safety Assessment & Vital Area Identification	SAPHIRE, EMRALD, & VISAC
Force-on-Force, Vulnerability Analysis & Physical Protection Strategy	AVERT, Simajin/Vanguard, Scribe3D, & VISA
Blast Effects to inform Vulnerability Analysis	SHARC & VISAC
System Response to inform Vulnerability Analysis	ORIGEN/SCALE & MELCOR
Unacceptable Radiological Consequences & High Radiological Consequences	MACCS-HYSPLIT, HOTSPOT, RASCAL, & QUIC
GIS & Infrastructure Impact Analysis	FASTMAP

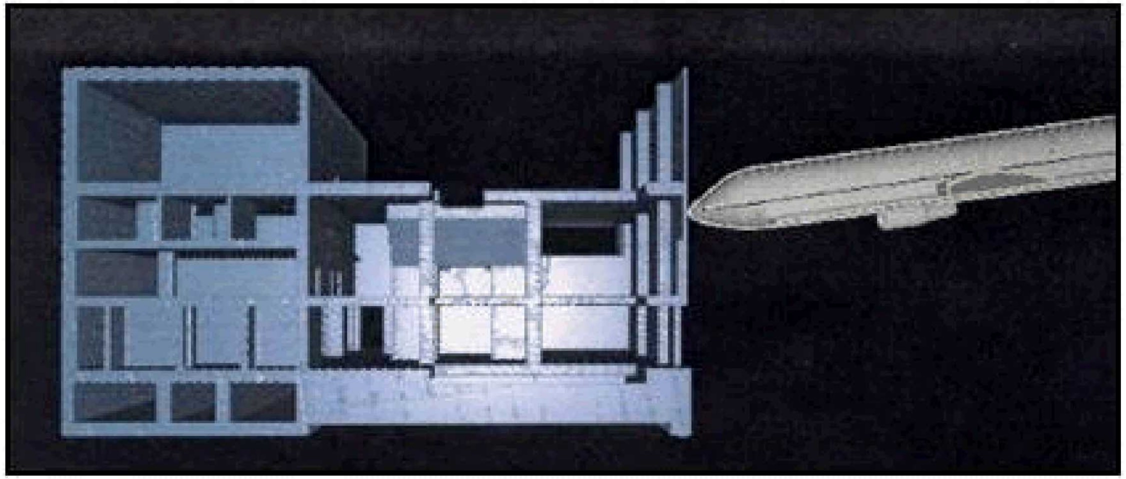
Vital Area Identification and Loss of Large Area Analysis

Probabilistic Safety Assessment (PSA)

- Level 1: Frequency and level of plant damage states such as a loss of coolant accident
- Level 2: Frequency and mode of containment failure and release of radionuclides to the environment
- Level 3: Frequency and extent of environmental impacts such as human health effects

Vital Area Identification (VAI)

- Level 1 PSA applied to VAI models
- Potential for core damage as single cut-sets (single room)
  - Core damage is where VAI stops; asset protection
- Example, main control room
  - Fire
  - Flood



Apply higher order cut-sets from VAI for LOLA

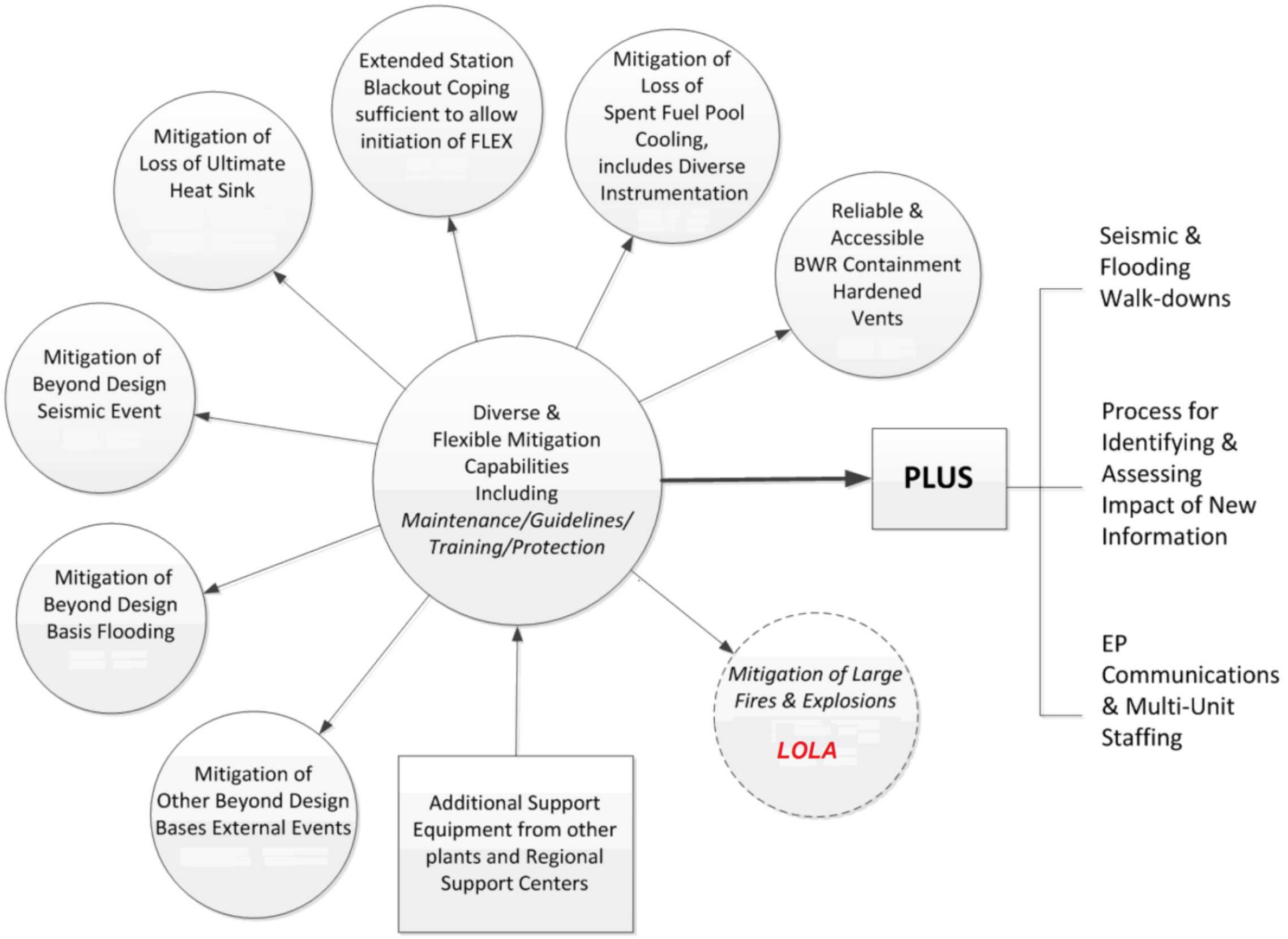
- Spatially informed LOLA – **New Approach**
  - Beyond current regulatory/industry protocols
- Identify rooms and potential scenarios for LOLA
  - New reactor designs can consider passive systems and new safety systems
  - Considerations of true multi-train independence

Loss of Large Area Analysis & FLEX

Incorporation of LOLA mitigation strategies require trade-offs between safety and security
- Certain rooms in the plant required to be locked (security)
- During LOLA, a room must be accessed for mitigative strategy (safety)
  - Should key remain with security or in control room?

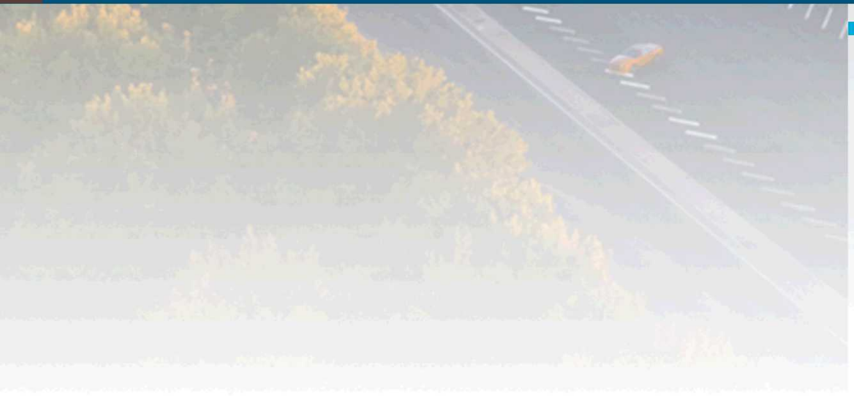
LOLA strategies are responsive and not preventive
- Strategies place plant in safe condition or prevent/minimize public dose
- Not meant to preclude any security event

LOLA strategies transcend security
- Developed from 9/11 terrorist event, but
- Can be used for external events
  - Earthquake
  - Tsunami



Diverse and Flexible Coping Strategies (FLEX) Implementation Guide
NEI 12-06

Questions



Backup slides

What Can We Do With HAZCADS?

Hazard and Consequence Analysis for Digital Systems (HAZCADS) is a systematic framework for addressing hazards initiated by digital I&C systems that can expand to:

- Common-cause failures
- Single point digital threats
- Defense-in-depth
- Dependencies between safety and non-safety systems

The Type 2 and Type 3 System-theoretic Informed Fault Trees (SIFT) cut sets can be treated as goal sets in cyber weakness assessments.

- Cyber weakness assessments provide contextual descriptions for the hazardous control actions.