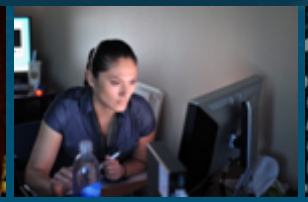
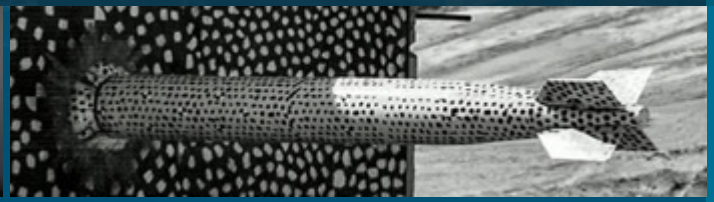
SAND2021-14275C

Sandia National Laboratories

Integrated Safety-Security Analysis Using Dynamic Event Trees





PRESENTED BY

Brian Cohn

U.S. DEPARTMENT OF ENERGY | NNSA

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.

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

Nuclear security analysis is based on vital area identification (VAI)

- Uses static fault tree/event tree (FT/ET) analysis to determine vital equipment to protect
- Vital areas are based on preventing core damage from sabotage

Challenges with VAI structure

- FTs are sourced from safety analysis with only safety assumptions
- Physical protection system is assumed to instantly fail if any vital area is sabotaged
- Little communication between safety and security risks

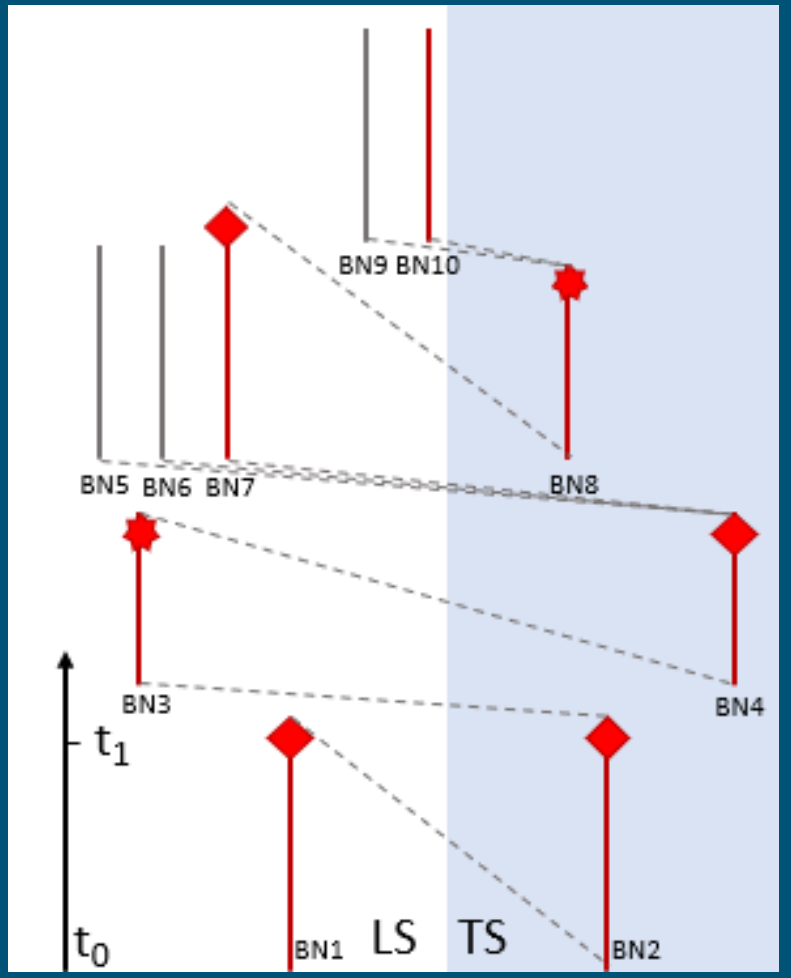
Background

Past research introduced Leading Simulator/Trailing Simulator (LS/TS) method

- Based on Dynamic Event Trees
- Combines safety and security analysis (2S)
- Models timing effects of sabotage

Security-security analysis performed previously

- Models effectiveness of LS/TS
- Compared to analysis with one model



Integrated Safety-Security Case Study Overview

Developed to model 2S interactions

- Scribe3D models security behavior
- MELCOR models reactor response

Lone Pine Nuclear Power Plant

- 1150 MW PWR

2S Scenario

- Adversary sabotages auxiliary feedwater (AFW) system

Code Description

MELCOR

- Nuclear reactor system code
- Used by the NRC to evaluate reactor accident evolution
- Models all aspects of a nuclear accident
  - Initiating event
  - Safety systems
  - Fuel damage and relocation
  - Radionuclide release

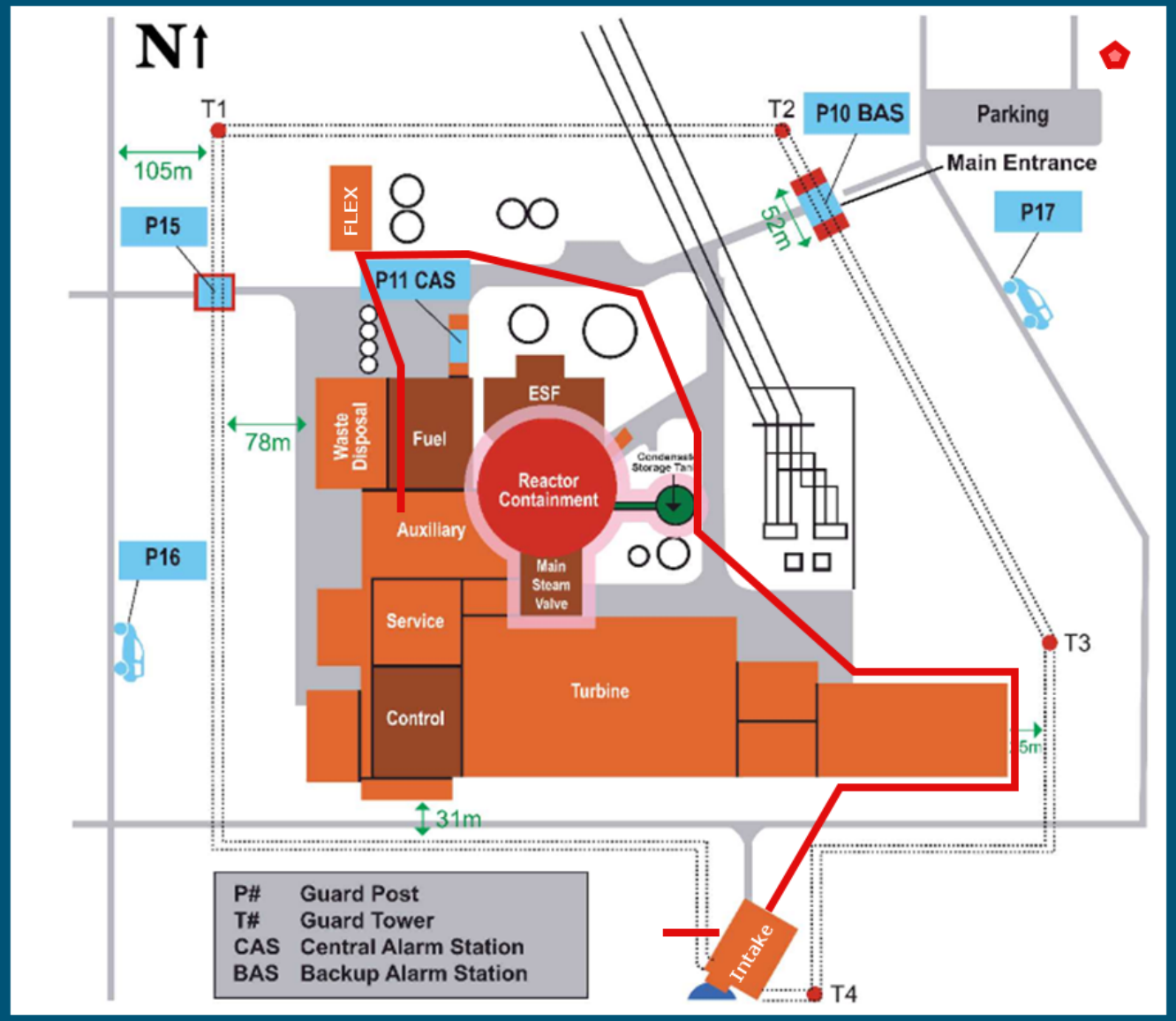
Scribe3D

- Nuclear FoF code
- Analyst-created 2D and 3D maps
- Allows for timeline generation and simulation of security scenarios

Lone Pine Hypothetical Vital Areas

Vital Area	Area Location
Auxiliary Feedwater Turbine Driven Pump Room	Engineered Safety Building
Battery Room A	Control Building
Cable Spreading Room	Control Building
Reactor Containment	Containment Building
Main Control Room	Control Building
Condensate Storage Tank	Site Protected Area
Condensate Storage Tank Piping	Site Protected Area
Spent Fuel Pool	Fuel Building
Main Steam Valve Building	Site Protected Area
Scram Relay Room	Control Building

Scenario Description



Adversary Targets

- Intake Structure
- Condensate Storage Tank (CST)
- FLEX Building

Responder Actions

- Scram Reactor
- Interrupt Adversaries
- Realign new water source to AFW
- Use FLEX to restore AFW

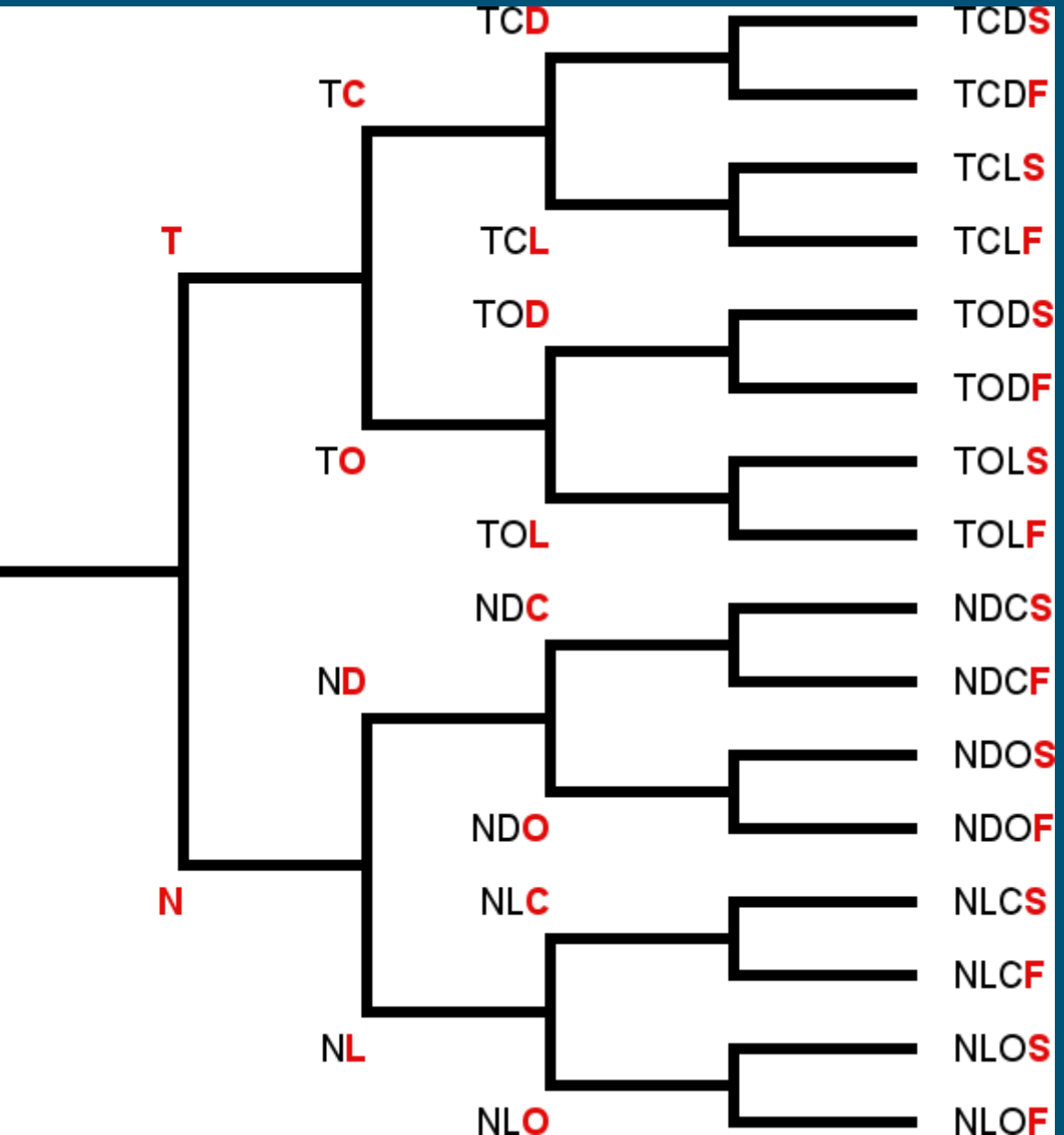
Scenario Description (cont)

Branching Condition	Child Branch	Short Name	MELCOR Effects	Scribe3D Effects
Time of adversary detection	Timely detection	T	Immediate rector scram	Mustering of responders begins immediately
	Non-timely detection	N	Reactor scram on CST sabotage	Mustering of responders begins on CST sabotage
Adversary engagement	Close adversary victory	C	FLEX available at 8 hours into the scenario	All responders killed, many adversaries killed, adversaries skip FLEX sabotage
	Overwhelming adversary victory	O	FLEX sabotaged by adversaries	All responders killed, few adversaries killed, adversaries sabotage FLEX building
Damage to CST	CST degraded	D	1m^2 hole in CST	N/A
	CST lost	L	CST unavailable	N/A
Operator Realignment	Realignment successful	S	AFW restored at time realignment completes	RED 2 killed, operator performs realignment action
	Realignment failed	F	AFW not restored during scenario	Operator and BLUE 1 killed

DET Branching

- 4 branches
- Binary branching options
- Intended for demonstration

General Results



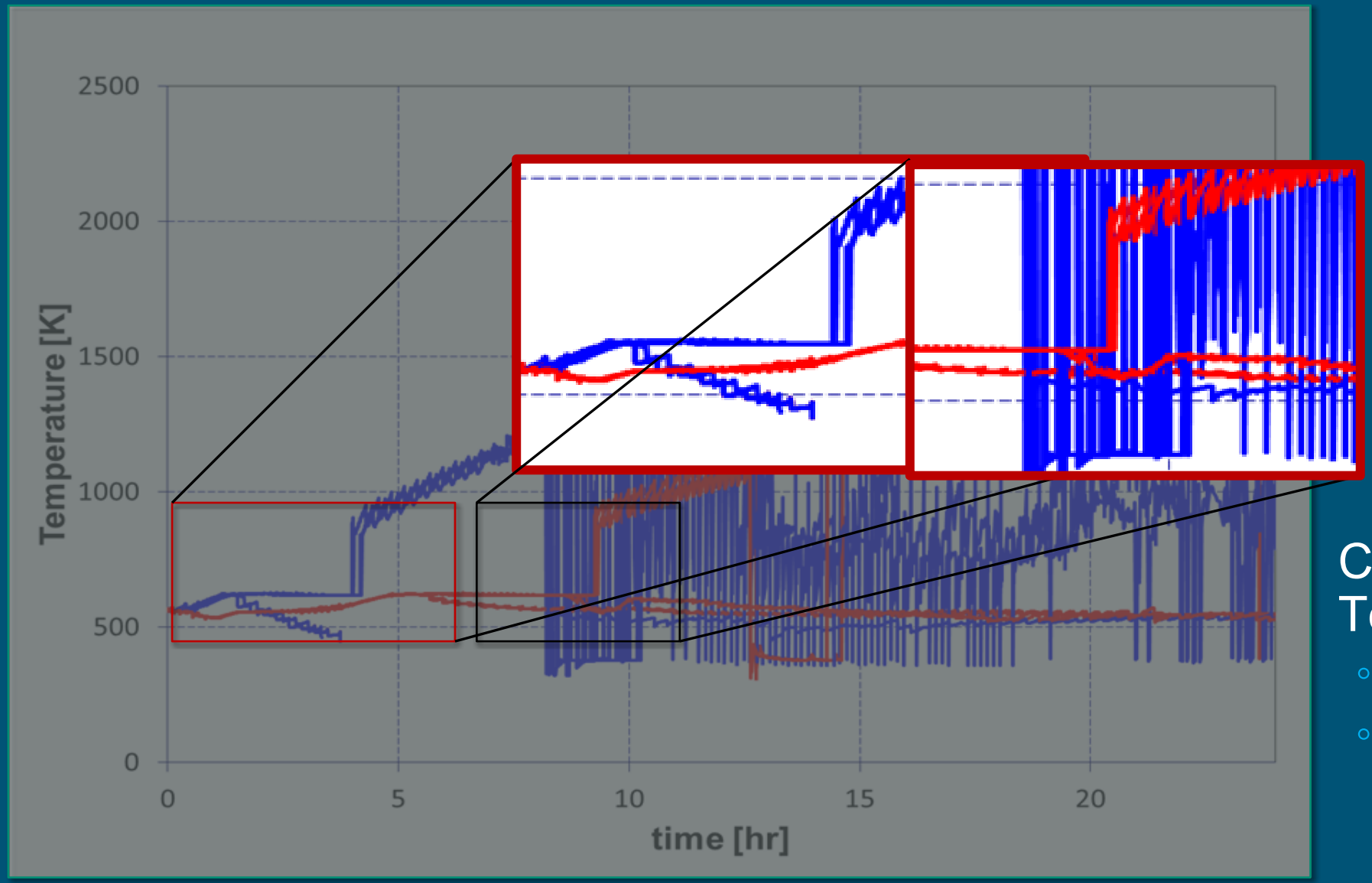
Generated DET

- Security and safety branches
- Order of events can vary depending on timing

Branch IDs

- T: Timely Detection
- N: Non-timely Detection
- C: Close adversary win
- O: Overwhelming adversary win
- L: Loss of CST
- D: Degradation of CST
- S: Realignment Success
- F: Realignment Failure

General Results (cont)



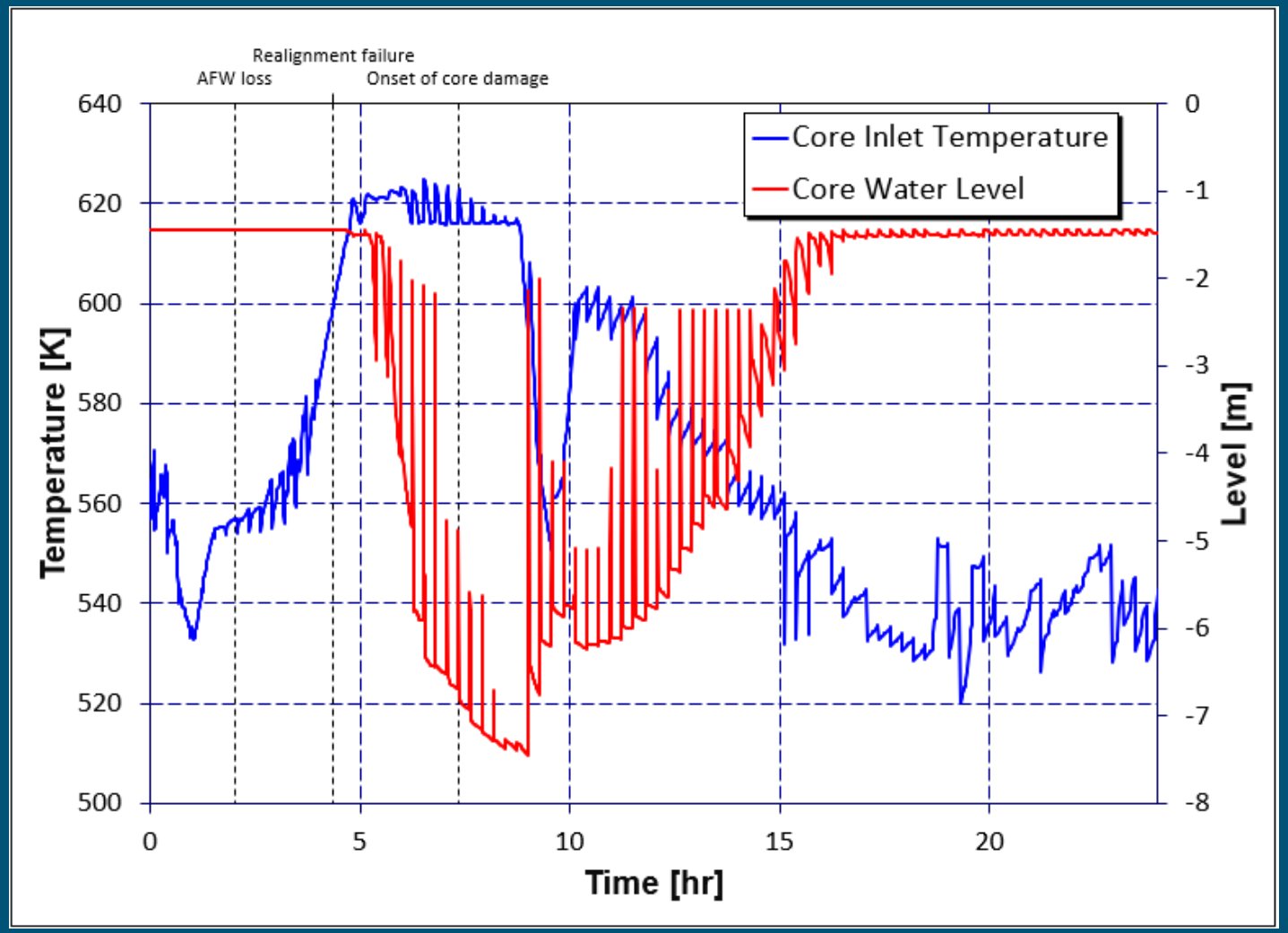
Core Inlet Temperatures

- Blue: CST Lost
- Red: CST Degraded

General Results (cont)

Sequence TCDF

- Regular spikes are nonphysical
- Core inlet temperature remains constant while coolant boils off
- FLEX restores AFW at 8 hours



2S Results

2S Results

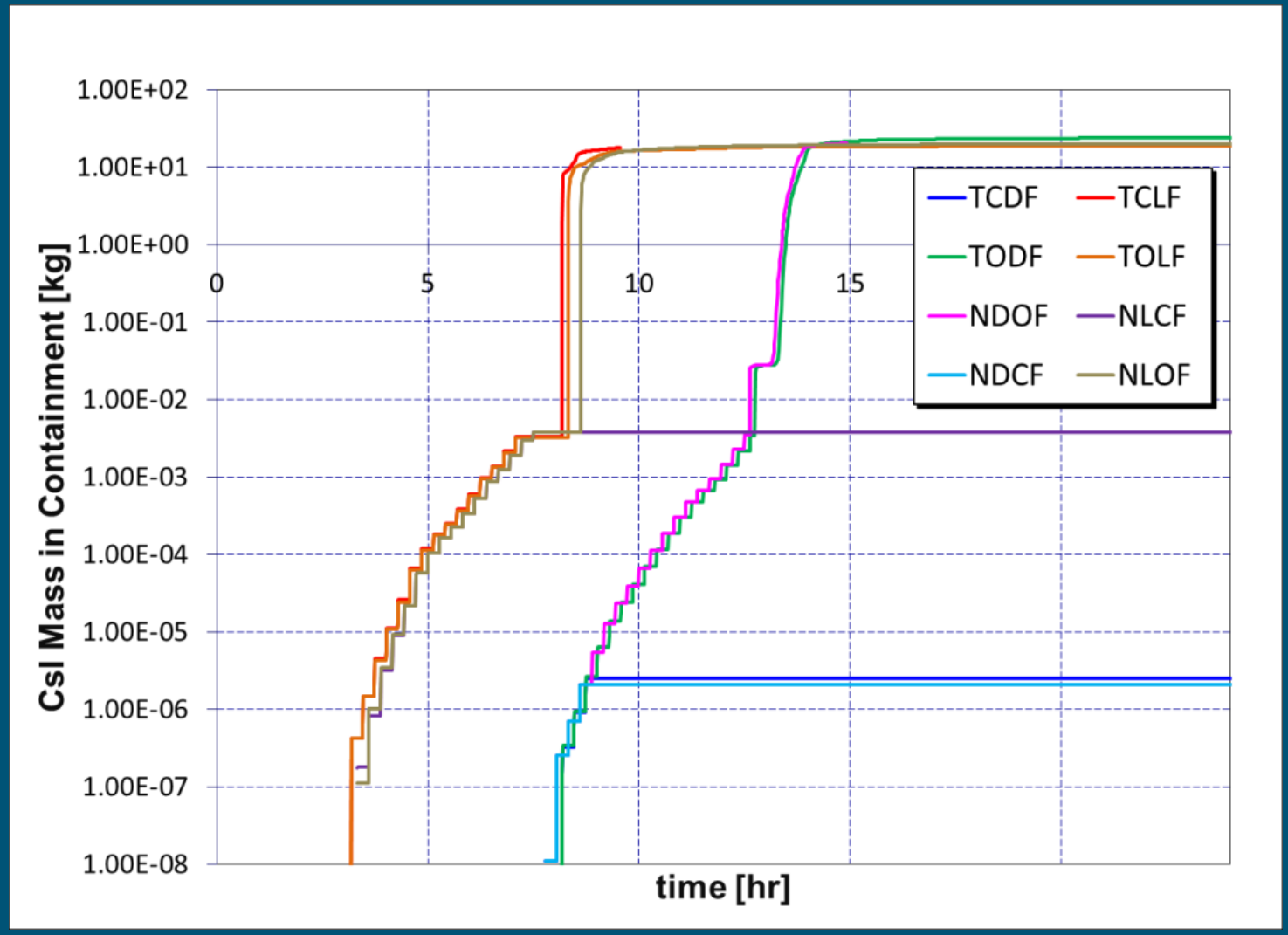
- Depend on timing and extent of sabotage to systems

Effects extend beyond onset of core damage

- Radionuclide releases drive public health consequences of sabotage

Mitigation systems that reduce radionuclide release may be worthwhile without preventing a release

2S Results (cont)



Conclusions

Case study performs integrated 2S analysis

- Under VAI, the case study scenario is considered unacceptable
- Core damage can be mitigated by realignment action

LS/TS method combines security and safety models

- Information passes between models when necessary

Integrated 2S analysis introduces new insights

- Timing effects of security scenarios on NPP state
- Consequences of system sabotage
- Effects of mitigation actions and systems