INL/MIS-21-62184-Revision-0

Dynamic Assessment in Security Strategy

April 2021

Changing the World's Energy Future

Robby Christian

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-21-62184-Revision-0

Dynamic Assessment in Security Strategy

Robby Christian

April 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Dynamic Assessment in Security Strategy

Probabilistic Methods & Tools
Idaho National Laboratory

www.inl.gov

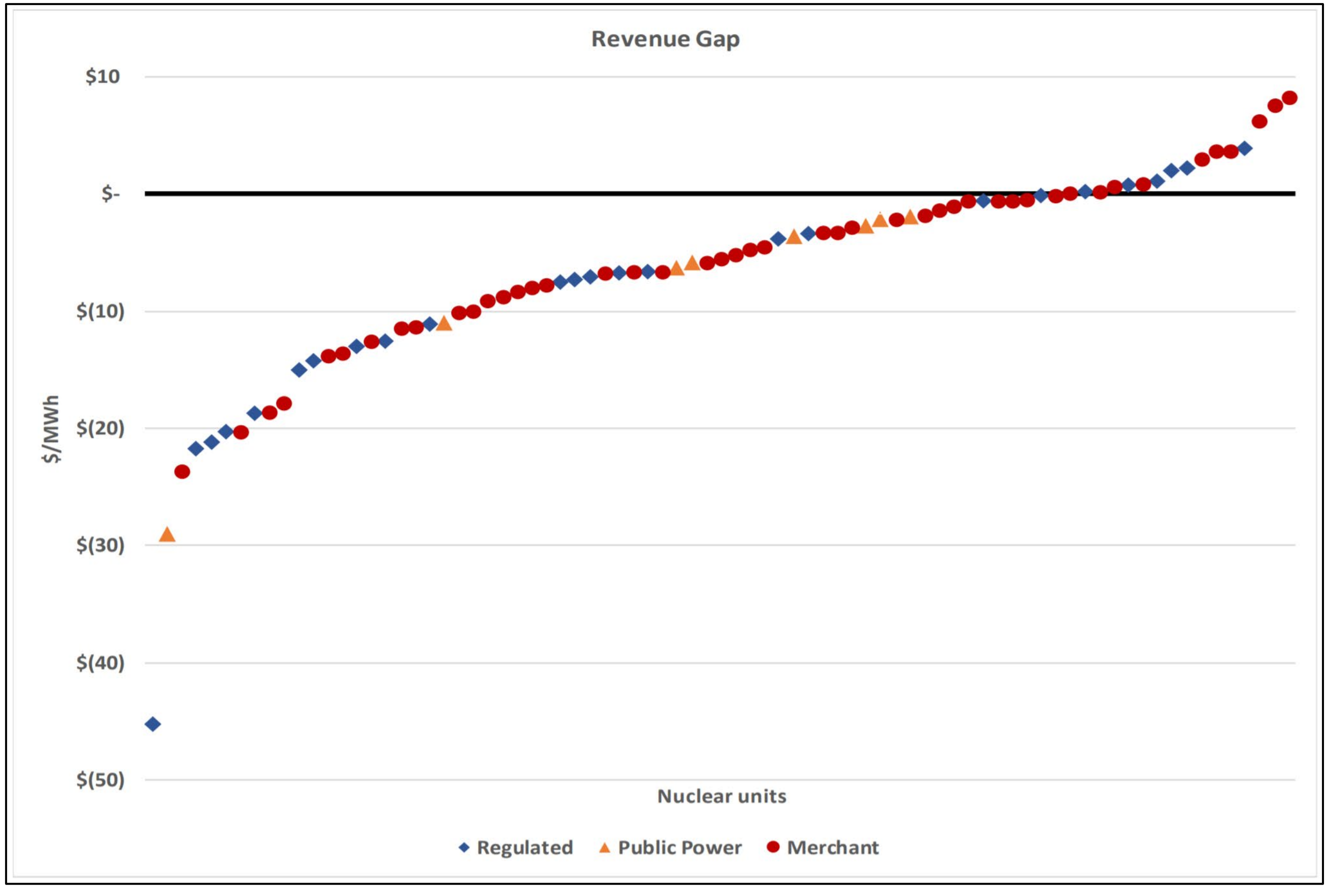
Idaho National Laboratory

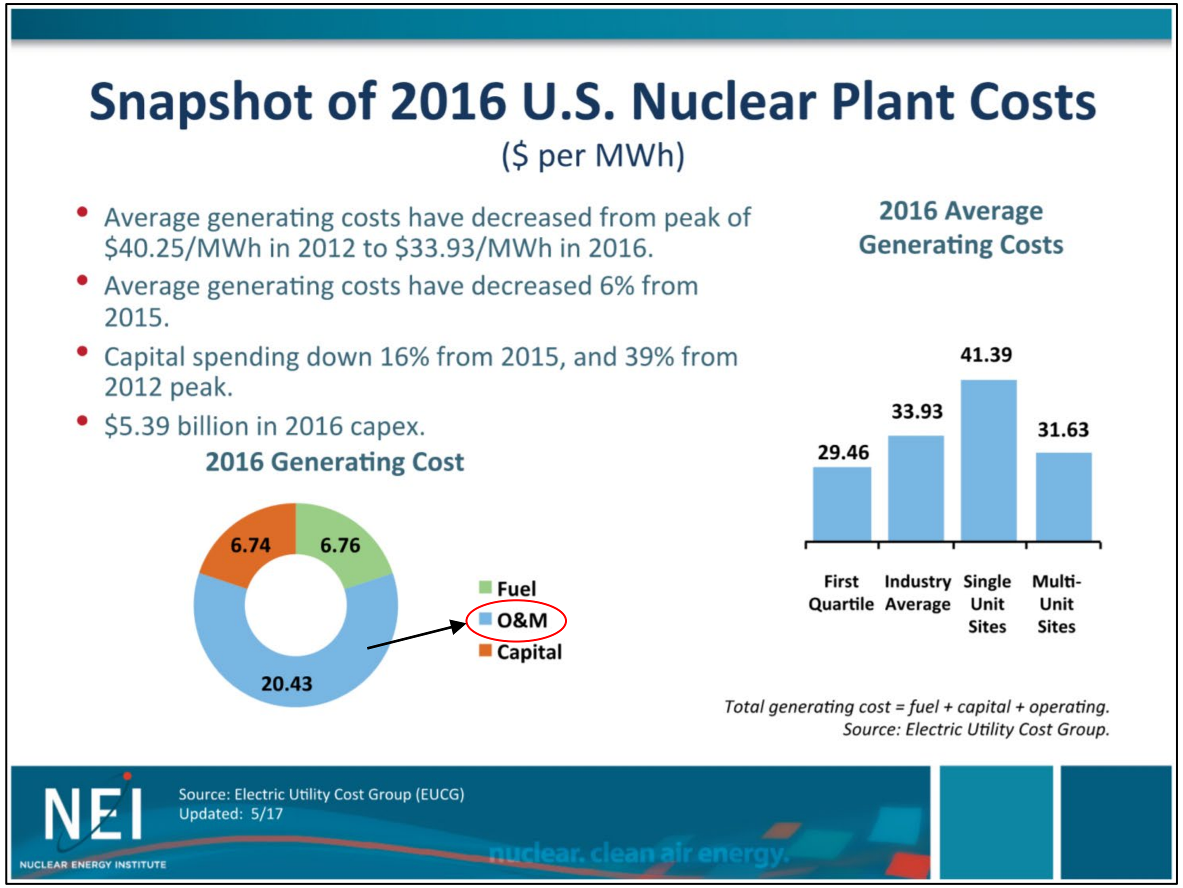
Organization

- Background
- Objective
- Methodologies
- Selected case studies
- Summary

Background: Financial

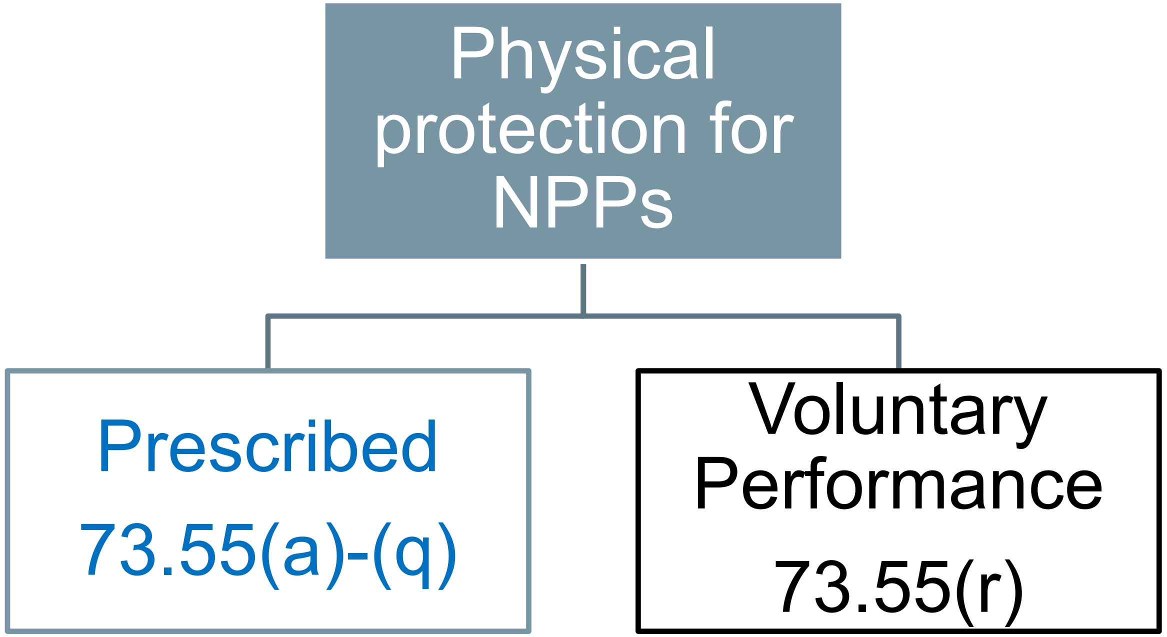
- LWRS pathway





* Idaho National Laboratory (2017). Economic and Market Challenges Facing the U.S. Nuclear Commercial Fleet – Cost and Revenue Study (INL/EXT-17-42944)

Background: Regulations



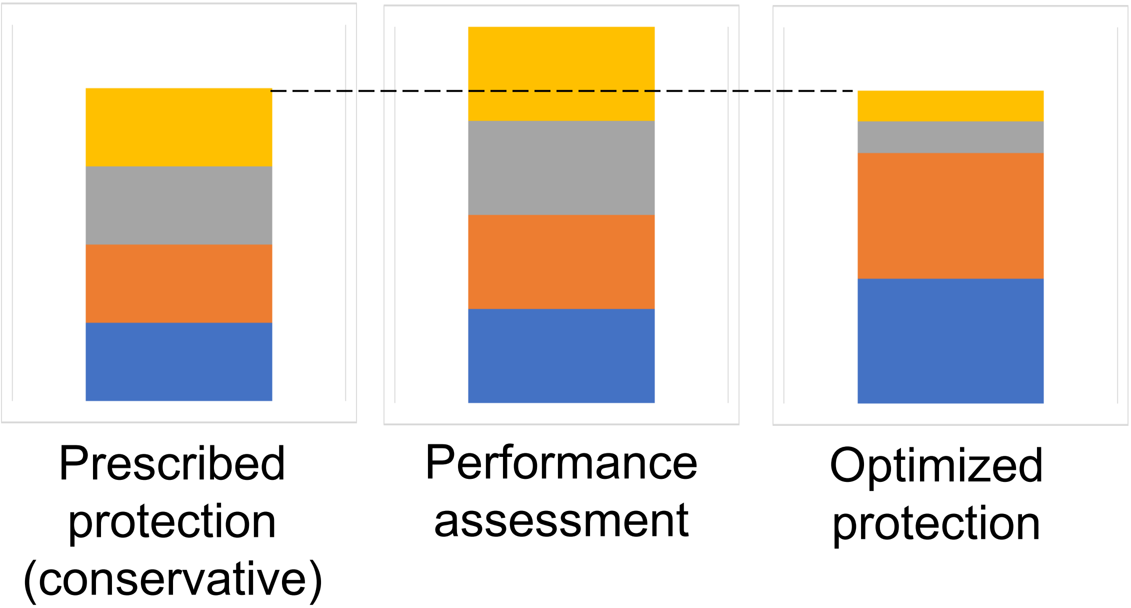
- Examples of prescriptive requirements:
  - Clause (k)(5)(ii): A minimum of 10 armed responders
  - Clause (n)(2): Testing of the intrusion alarm system at least every 7 days
  - Clause (i)(6)(ii): A minimum illumination level of 0.2 foot-candles

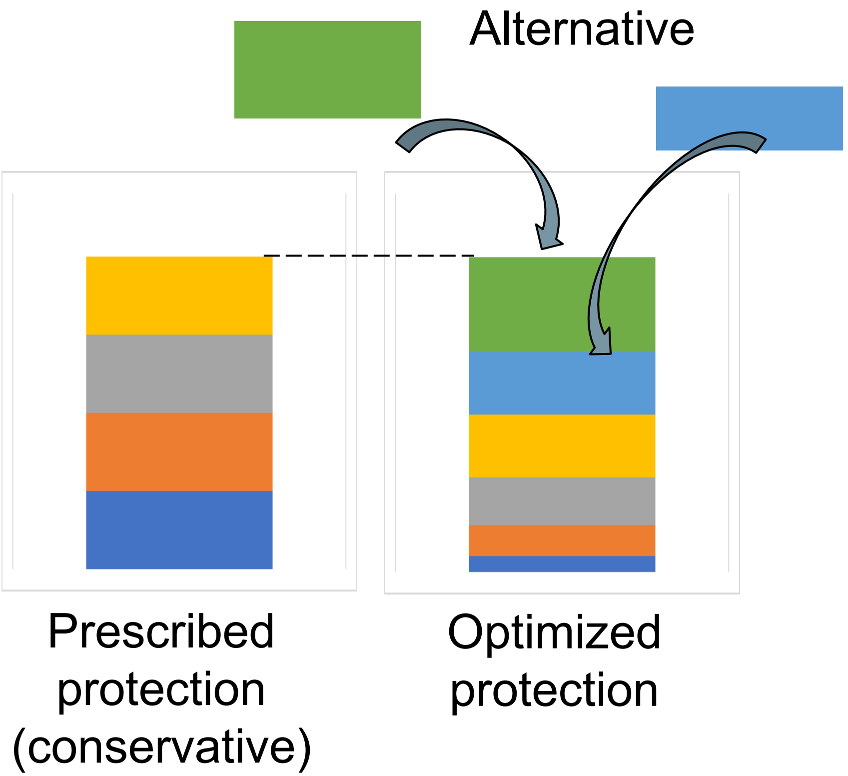
- Questions:
  - Provide alternatives to prescriptive requirements while maintaining security performance?
  - Optimize security posture by employing alternative technologies and methods
    - Advanced weapon systems?
    - Non-lethal neutralization options?
    - New sensor technologies?

* US NRC, 10 CFR 73.55: Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage

Objective

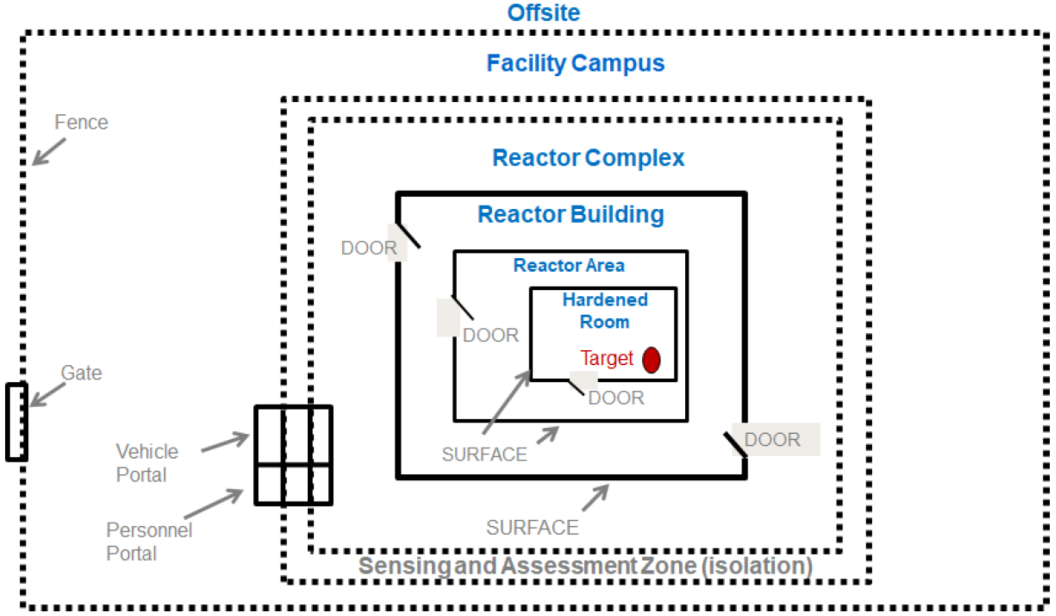
- Goal: A framework to optimize physical protection design and costs through performance-based analyses
- Approach: Leverage INL's dynamic risk modeling tool EMRALD



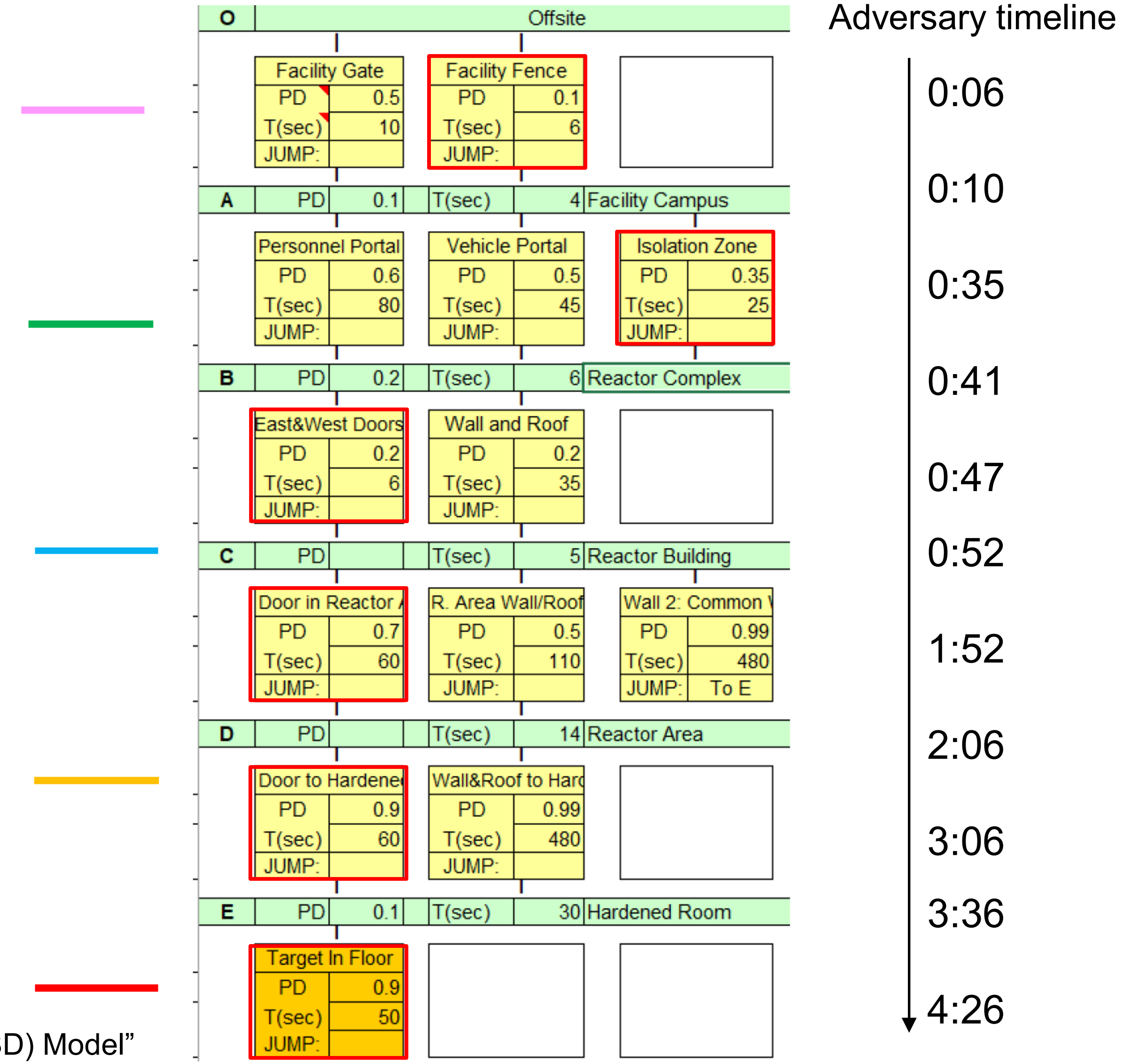


Conservatisms in Current Design Methodology

Hypothetical facility & Adversary Sequence Diagram (ASD):

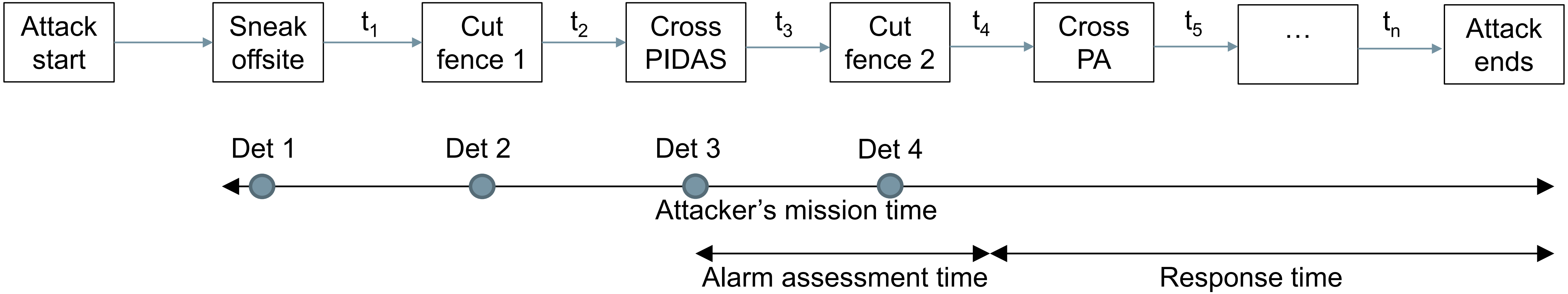


- Adversary traversal time (T) and Probability of Detection (PD) for each area/barrier are assessed independently of other areas/barriers
- Conservative values for T and PD



* Sandia National Laboratories, "ITC-28: Adversary Sequence Diagram (ASD) Model"

Conservative Approach



$$P_E = P_I \times P_N$$

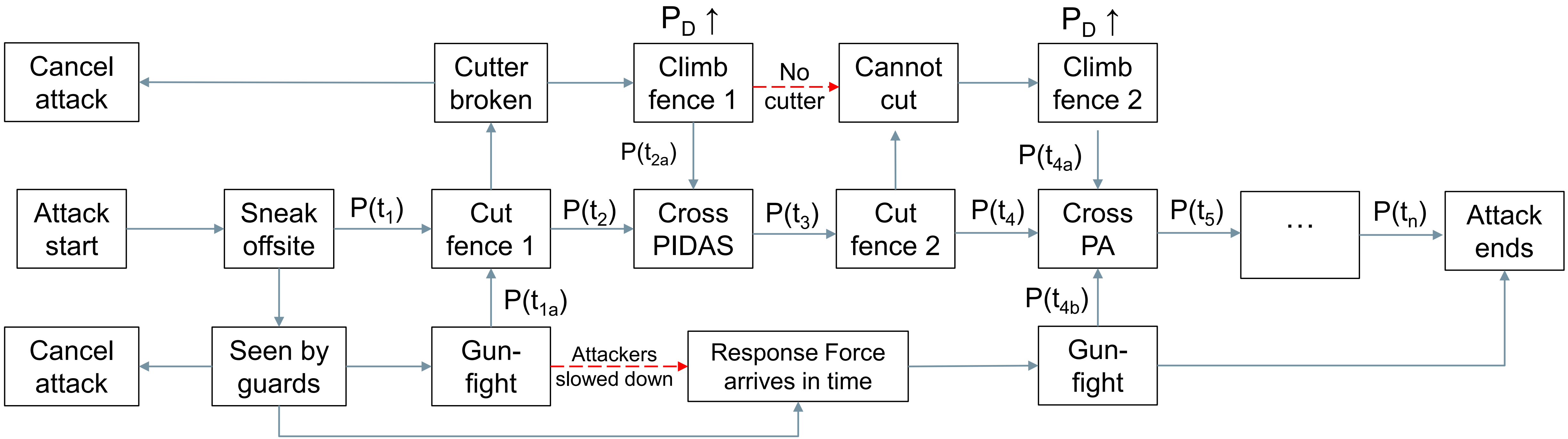
$$P_I = 1 - \prod_{1}^{3} (1 - P_D)_i$$

P_E: Probability of PPS effectiveness
P_I : Probability of timely interception
P_D: Probability of detecting intruders
P_N: Probability of neutralizing attackers

A More Realistic Approach

- Despite the conservative assumptions regarding the attackers' capabilities, there are various ways an attack plan can go wrong
- The different ways in which things go wrong may affect the next steps of attack/intervention → **(1) Dynamic dependencies, (2) Mission time may not be constant**

$$P_E = P_D \times P_t|D \times P_N|t$$



Current vs. Proposed Approach

- Summary of the current approach:
  - Simple and intuitive spreadsheet tool
  - Static and conservative analysis → costly and time-intensive design, analysis, and updates
  - Modeling of physical protection elements only
- Proposed approach:
  - Leverages advanced simulation tools
  - Enables dynamic and realistic analysis
  - Incorporates safety-related systems and actions to mitigate the adverse effects of sabotage attacks

EMRALD

(Event Model Risk Assessment using Linked Diagrams)

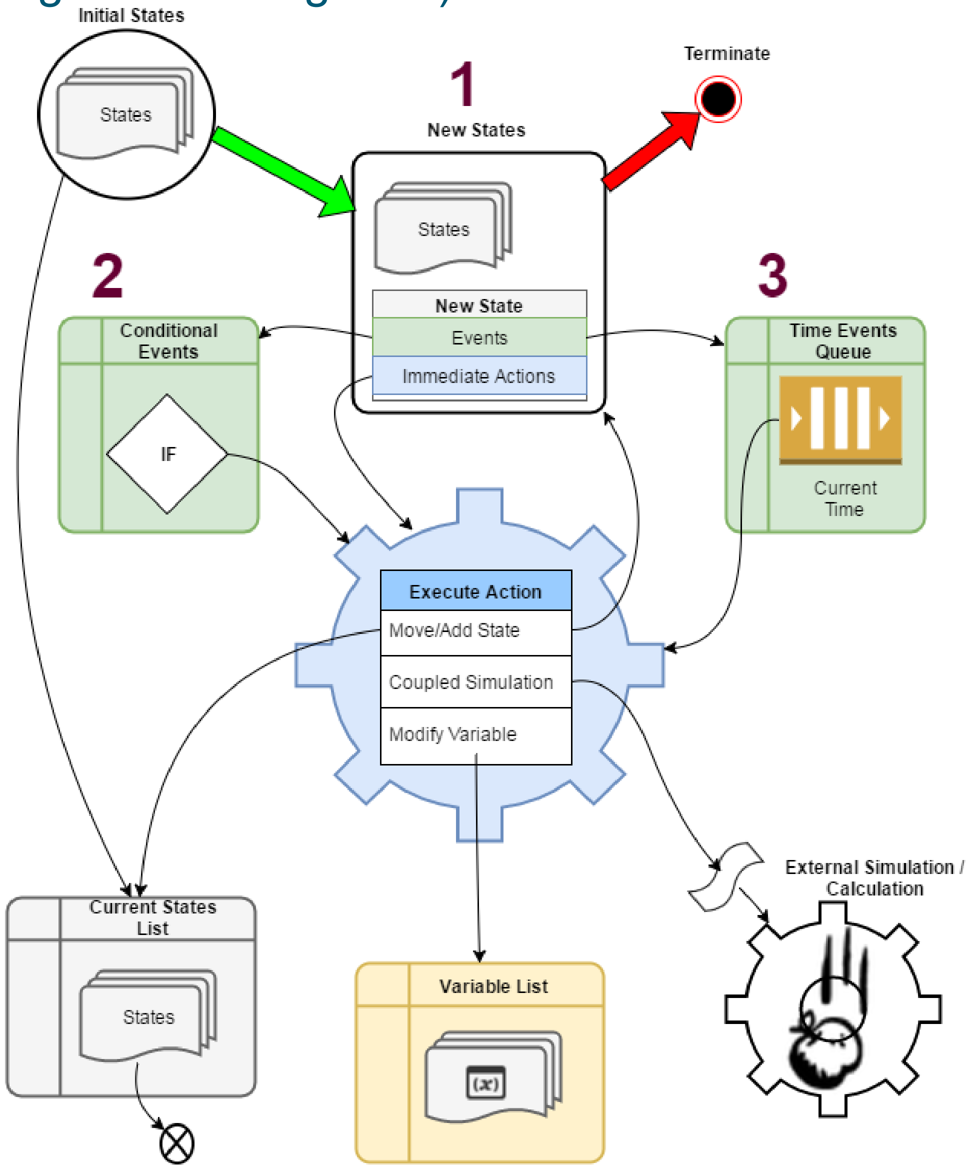
- Dynamic probabilistic risk assessment (PRA) model based on a three-phased discrete event simulation

  To begin, add initial start states to the Current and New States Lists.

  1. When there are States in the New States List, for each State:
     - Add the Events to the Time Queue or Conditional List
     - Execute any Immediate Actions.

  2. If any Conditional Events criterion is met:
     - Execute that event's action/s
     - (Go to Step 1.)

  3. Jump to the next chronological event
     - Execute that event's action
     - (Go to Step 1.)



EMRALD Modeling

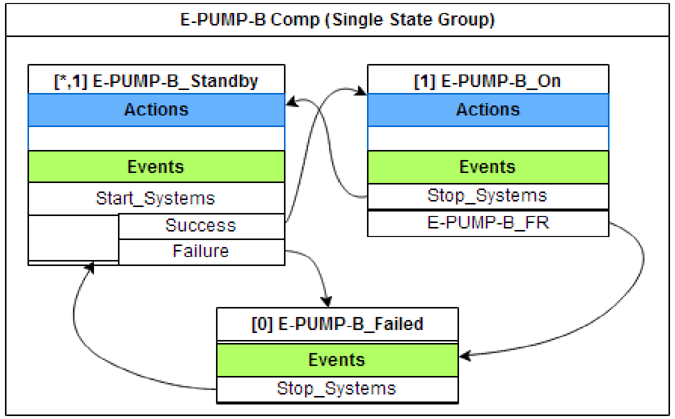
States

- Actions (transition, change variables, run script)
- Events → Action (sampling, conditions, time, etc.)

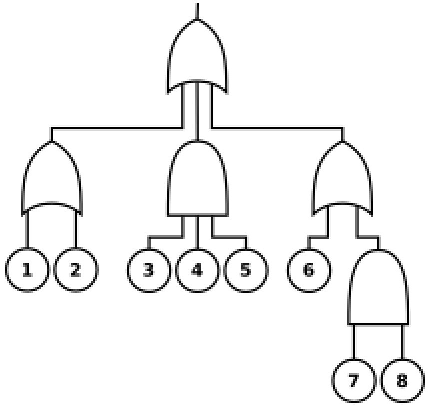
State
Actions
Transition
Change Variable
Run Script
Events
Failure Rate Sampling
Timer
State Change
Logic Tree
Evaluate Variable
External Event

Diagrams

- Components
- Systems
- Plant response



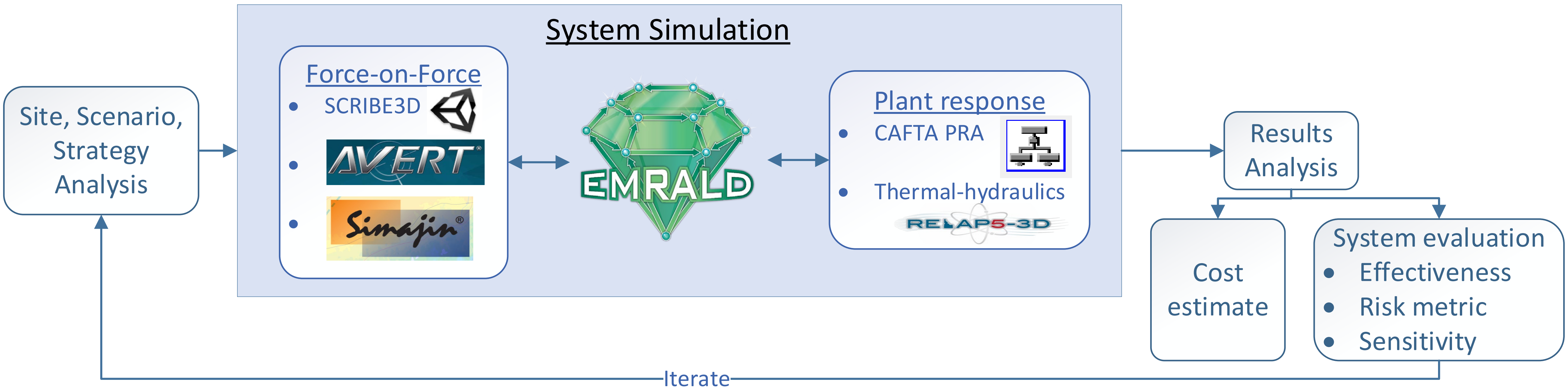
Logic Trees



Variables

External Links

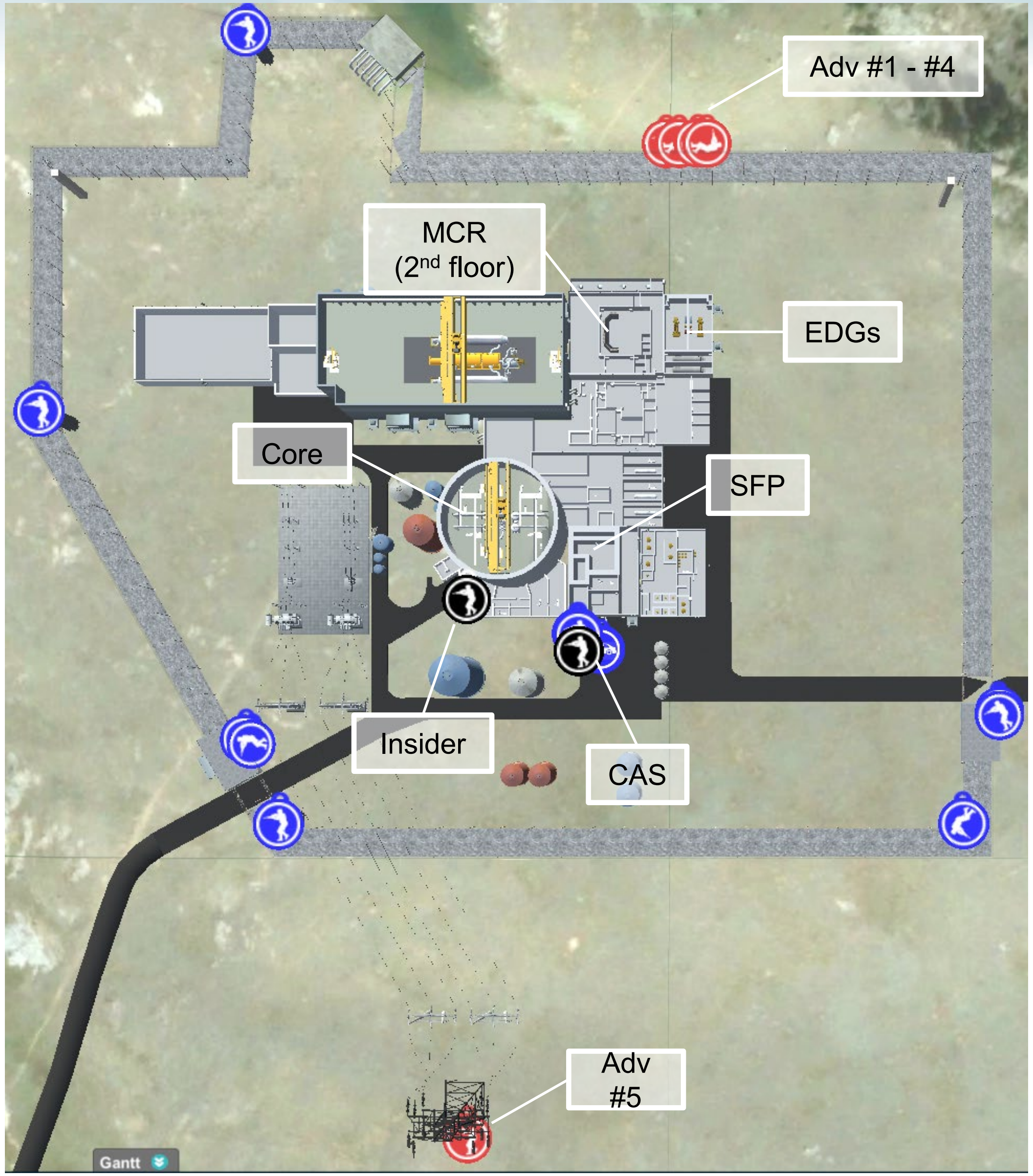
Proposed Framework



Case Study 1: Static vs Dynamic FoF

Attack scenario:
- Insider (technician) does maintenance on TDPs
- Adv #5 attacks transmission tower
- Adv #1–4 attack 2/2 EDGs

Step	Action	Purpose	Action time (seconds)
1	Adv-5 places explosive charges on the legs to the main power line towers and waits for the detonation cue.	Isolate LPNPP from offsite power	200
2	Adv-1, 2, 3, & 4 sneak on foot to the north side of the facility.	Evade detection by tower guards	300
3	Adv-3 cuts a hole in the outer fence.	Infiltrate the protected area	20
4	Adv-3 enters PIDAS and heads to the inner fence, followed by Adv-1, 2, & 4.		5
5	Adv-3 cuts a hole in the inner fence.		20
6	Adv-1, 2 , 3, & 4 enter the protected area and go towards the generator room.		10
7	Adv-3 unlocks the door to the generator room.	Infiltrate the generator room	20
8	Team-1 (i.e., Adv-1 and 2) goes to Emergency Diesel Generator (EDG) A, and Team-2 (i.e., Adv-3 and 4) goes to EDG B.	Destroy EDGs	20
9	Team-1 sets up explosives at EDG A while Team-2 sets them up at EDG B.		40
10	Team-1 detonates EDG A, and Team-2 detonates EDG B.		0
11	Adv-5 detonates the main power line upon hearing explosions or gunshots inside LPNPP.	Create an SBO event	0



Static Analysis with DEPO

Step	Action	Purpose	Action time (seconds)
1	Adv-5 places explosive charges on the legs to the main power line towers and waits for the detonation cue.	Isolate LPNPP from offsite power	200
2	Adv-1, 2, 3, & 4 sneak on foot to the north side of the facility.	Evade detection by tower guards	300
3	Adv-3 cuts a hole in the outer fence.	Infiltrate the protected area	20
4	Adv-3 enters PIDAS and heads to the inner fence, followed by Adv-1, 2, & 4.		5
5	Adv-3 cuts a hole in the inner fence.		20
6	Adv-1, 2, 3, & 4 enter the protected area and go towards the generator room.		10
7	Adv-3 unlocks the door to the generator room.	Infiltrate the generator room	20
8	Team-1 (i.e., Adv-1 and 2) goes to Emergency Diesel Generator (EDG) A, and Team-2 (i.e., Adv-3 and 4) goes to EDG B.	Destroy EDGs	20
9	Team-1 sets up explosives at EDG A while Team-2 sets them up at EDG B.		40
10	Team-1 detonates EDG A, and Team-2 detonates EDG B.		0
11	Adv-5 detonates the main power line upon hearing explosions or gunfights inside LPNPP.	Create an SBO event	0

CDP

Assessment & comm time

Response Force prep. time

- P_I = Prob. detection up to CDP = 0.05
- $P_N = \cup_{i=1}^{4} P_{i-th\ Adv\ neutralized}$
  - P_N for 1 Adv = 1-(1-P_{SPO})*(1-P_{RF}) = 0.5707
  - P_N all Advs = $(0.5707)^4$ = 0.1061
- **$P_E = P_I * P_N$ = 5.3E-3**
- Sabotage outcome:
  - P(LOOP, 2 EDGs, no TDPs) = P_E = 5.3E-3
  - P(SBO, no TDPs) = 1-P_E = 0.9947

Dynamic Analysis with EMRALD

Step	Action	Purpose	Action time (seconds)
1	Adv-5 places explosive charges on the legs to the main power line towers and waits for the detonation cue.	Isolate LPNPP from offsite power	200
2	Adv-1, 2, 3, & 4 sneak on foot to the north side of the facility.	Evade detection by tower guards	N(300,30)
3	Adv-3 cuts a hole in the outer fence.	Infiltrate the protected area	N(20,2)
4	Adv-3 enters PIDAS and heads to the inner fence, followed by Adv-1, 2, & 4.		N(5,0.5)
5	Adv-3 cuts a hole in the inner fence.		N(20,2)
6	Adv-1, 2, 3, & 4 enter the protected area and go towards the generator room.		N(10,1)
7	Adv-3 unlocks the door to the generator room.	Infiltrate the generator room	N(20,2)
8	Team-1 (i.e., Adv-1 and 2) go to Emergency Diesel Generator (EDG) A, and Team-2 (i.e., Adv-3 and 4) go to EDG B.	Destroy EDGs	N(20,2)
9	Team-1 sets up explosives at EDG A while Team-2 sets them up at EDG B.		N(40,4)
10	Team-1 detonates EDG A, and Team-2 detonates EDG B.		0
11	Adv-5 detonates the main power line upon hearing explosions or gunfights inside LPNPP.	Create an SBO event	0

Dynamic scenario assumptions:

- If SPO engages Adv while still in range, Adv is delayed.
- If an Adv team member is shot, his teammate is delayed.
- (If the alarm is triggered, the EDG room is filled with smoke upon entry, provided the smoke generator does not fail due to random failures.)

If Adv is delayed sufficiently, RF may arrive in time.

If Adv is detected here, SPO may respond in time.

Adv out of SPO's range

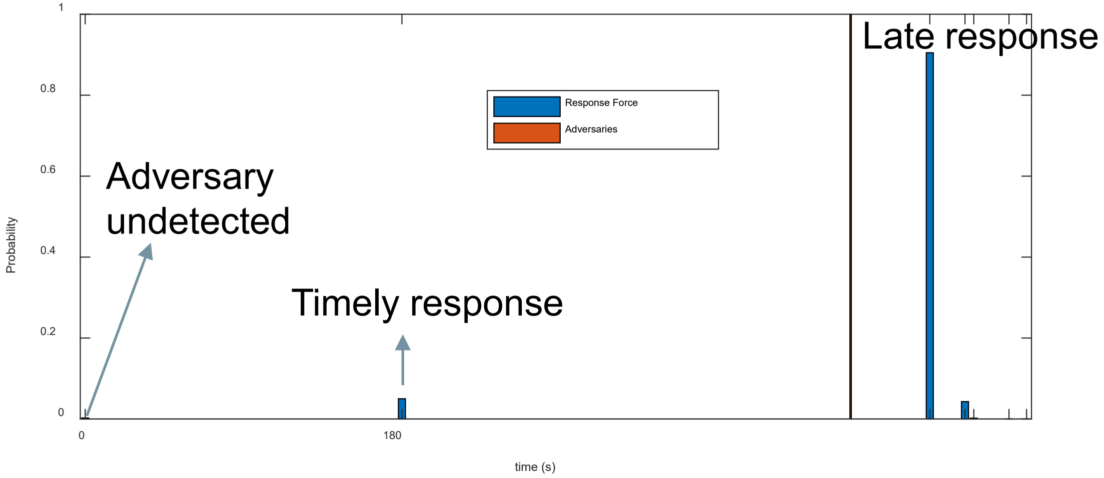
<u>Future effort</u>: Use dynamic HRA to evaluate the scenario's dynamics

Results

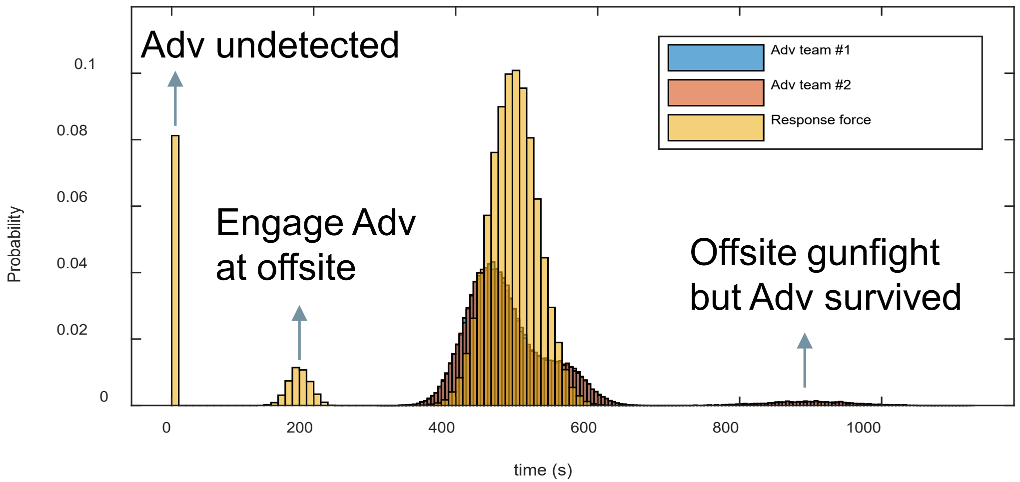
	Static (DEPO)	(Dynamic) EMRALD
Sabotage events	SBO without TDPs, P = 0.9947 LOOP without TDPs, P = 5.3E-3	SBO without TDPs, P = 0.79 LOOP without TDPs and 1 EDG, P = 0.18 LOOP without TDPs, P = 3E-2
CCDP (sabotage outcomes coupled with plant PRA)	5.4E-1	4.3E-1

Dynamic modeling reveals additional benefits to PPS system

Static time distribution



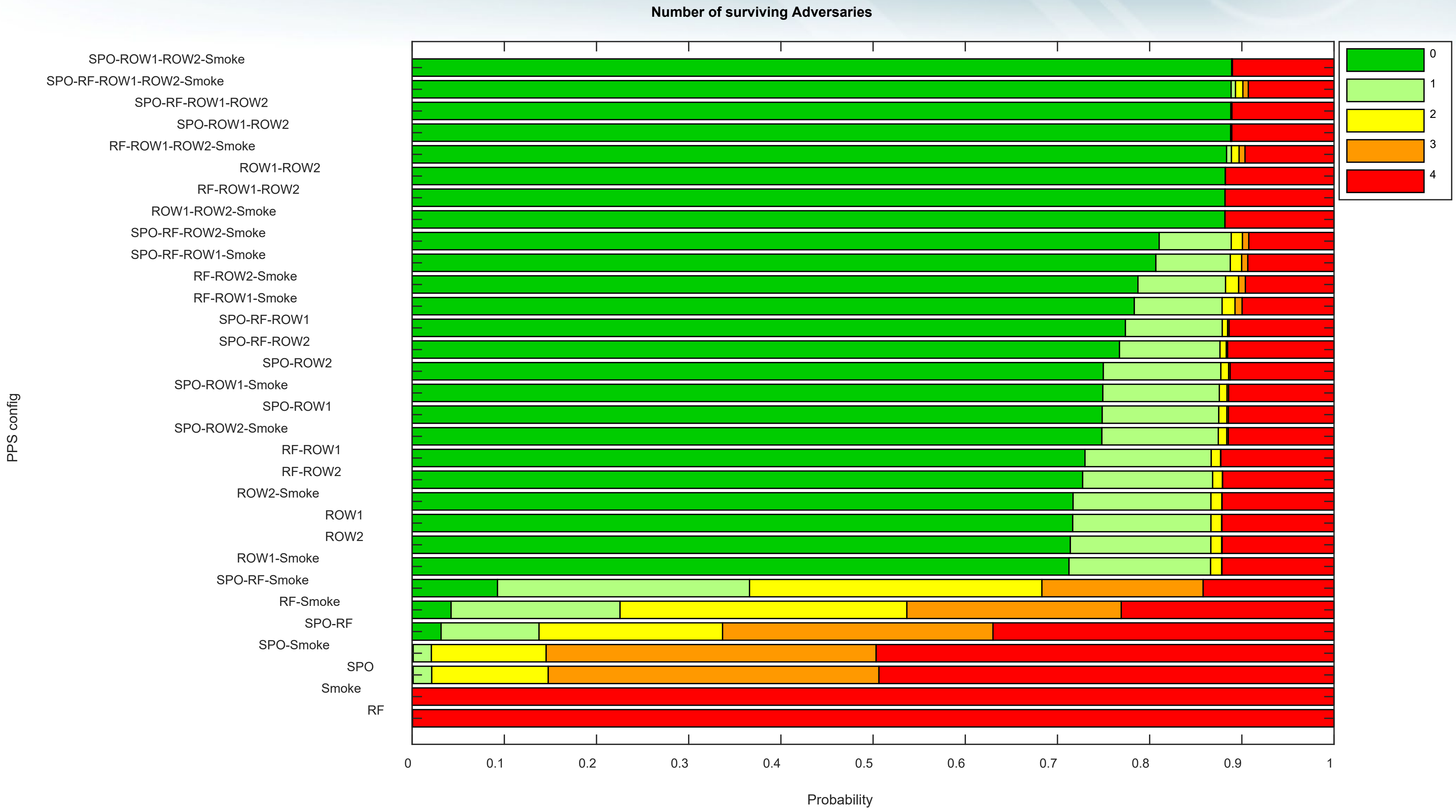
Dynamic time distribution

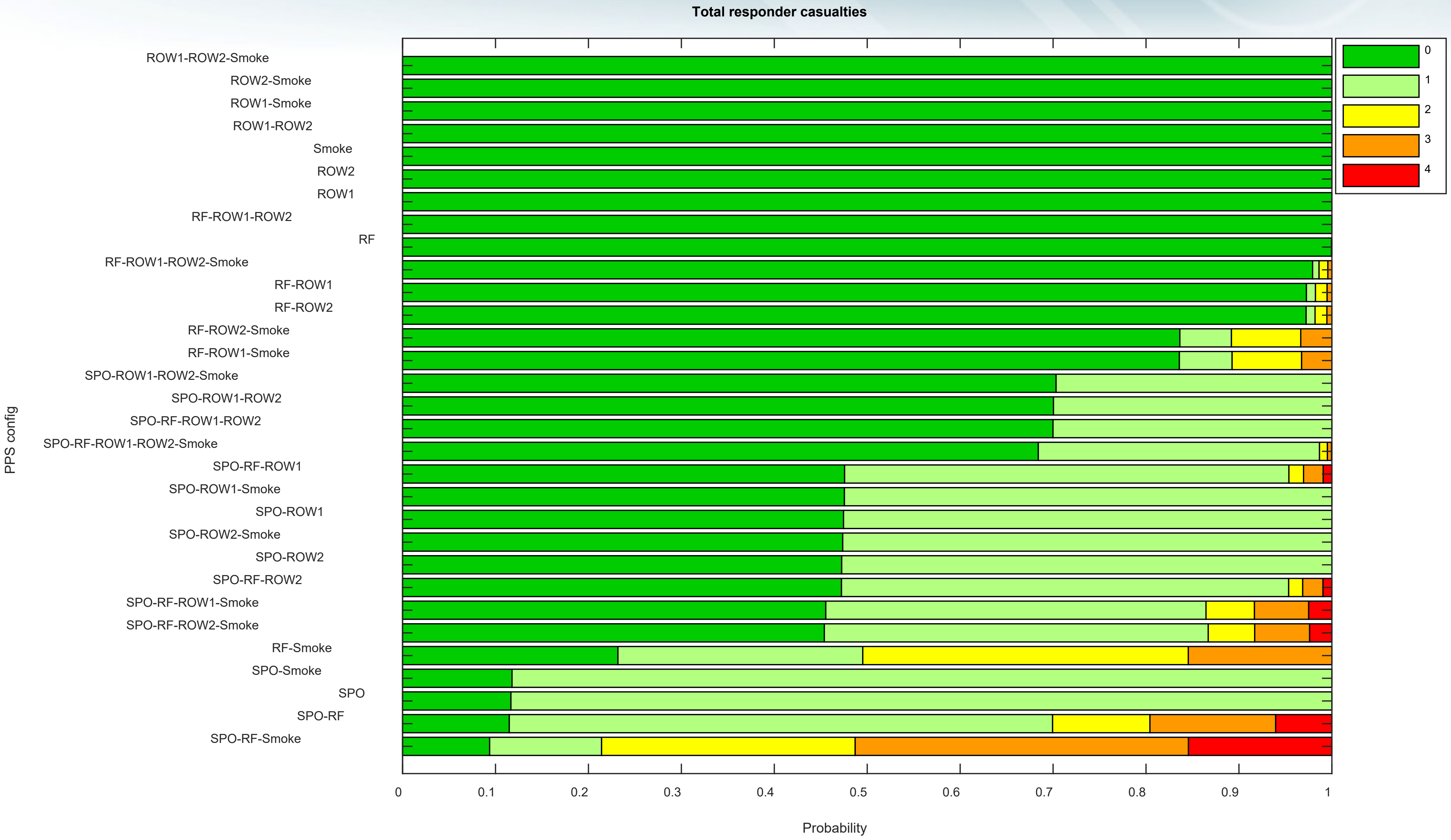


Case Study 2: PPS Design Comparison

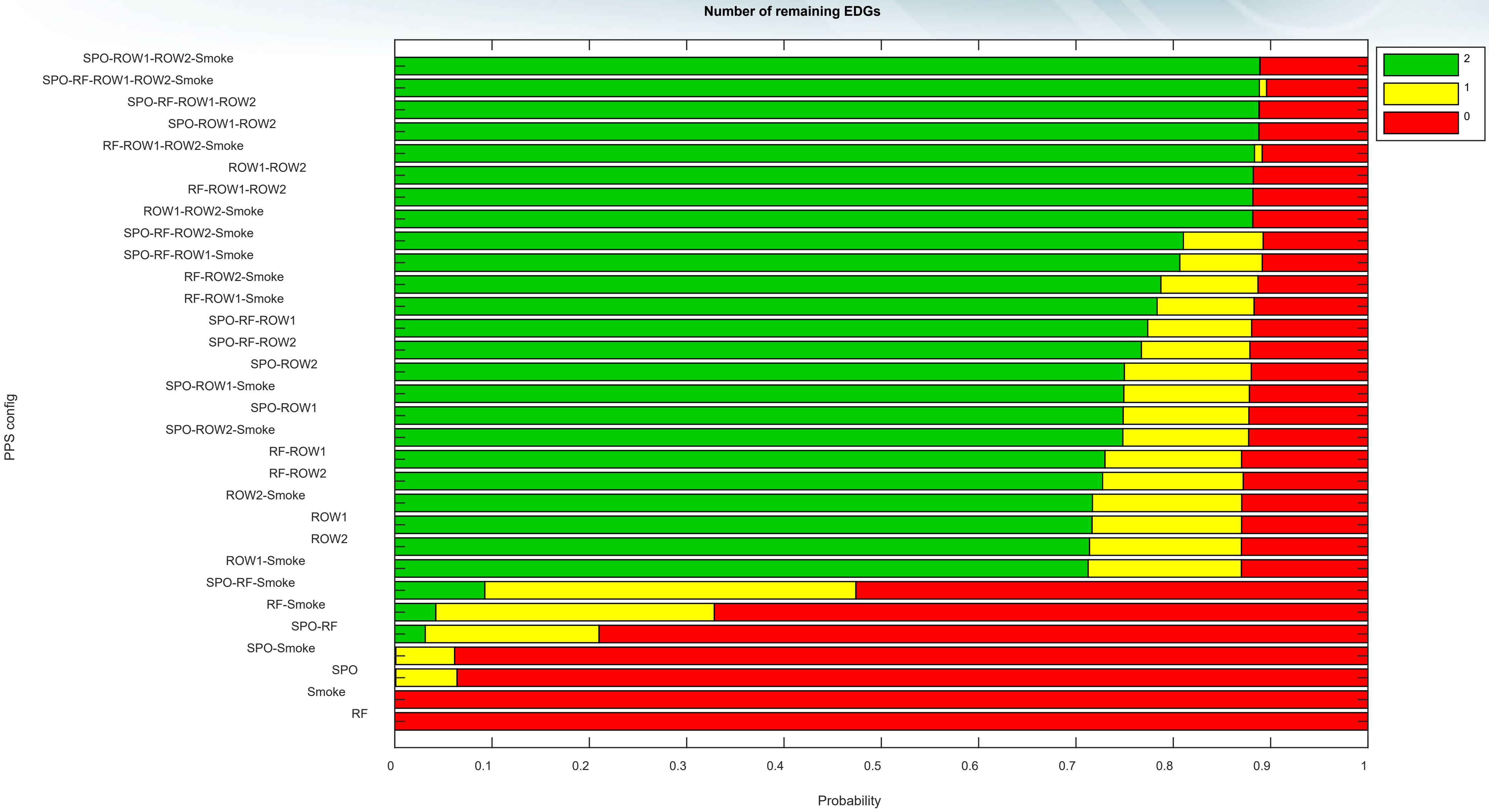
- Enumerate combinations of these elements in EMRALD:
  - SPO guards
  - Mobile tactical Response Force (RF)
  - Smoke generator as an indoor delay element
  - Two Remote Operated Weapon Systems (ROWS)

  Total of 2^4-1 = 31 combinations

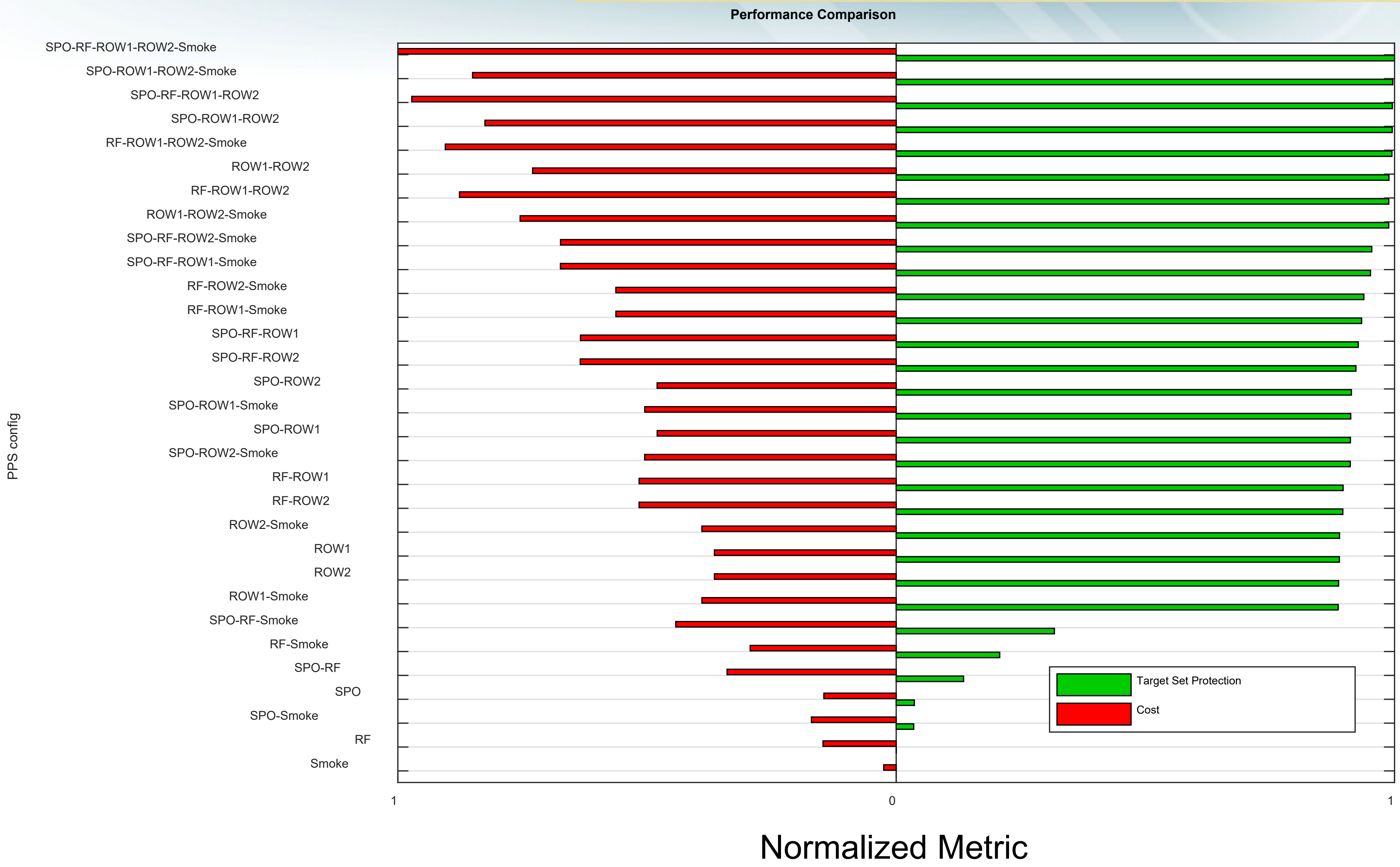

Number of surviving Adversaries
PPS config
SPO-ROW1-ROW2-Smoke
SPO-RF-ROW1-ROW2-Smoke
SPO-RF-ROW1-ROW2
SPO-ROW1-ROW2
RF-ROW1-ROW2-Smoke
ROW1-ROW2
RF-ROW1-ROW2
ROW1-ROW2-Smoke
SPO-RF-ROW2-Smoke
SPO-RF-ROW1-Smoke
RF-ROW2-Smoke
RF-ROW1-Smoke
SPO-RF-ROW1
SPO-RF-ROW2
SPO-ROW2
SPO-ROW1-Smoke
SPO-ROW1
SPO-ROW2-Smoke
RF-ROW1
RF-ROW2
ROW2-Smoke
ROW1
ROW2
ROW1-Smoke
SPO-RF-Smoke
RF-Smoke
SPO-RF
SPO-Smoke
SPO
Smoke
RF
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Probability
0
1
2
3
4



Total responder casualties
PPS config
ROW1-ROW2-Smoke
ROW2-Smoke
ROW1-Smoke
ROW1-ROW2
Smoke
ROW2
ROW1
RF-ROW1-ROW2
RF
RF-ROW1-ROW2-Smoke
RF-ROW1
RF-ROW2
RF-ROW2-Smoke
RF-ROW1-Smoke
SPO-ROW1-ROW2-Smoke
SPO-ROW1-ROW2
SPO-RF-ROW1-ROW2
SPO-RF-ROW1-ROW2-Smoke
SPO-RF-ROW1
SPO-ROW1-Smoke
SPO-ROW1
SPO-ROW2-Smoke
SPO-ROW2
SPO-RF-ROW2
SPO-RF-ROW1-Smoke
SPO-RF-ROW2-Smoke
RF-Smoke
SPO-Smoke
SPO
SPO-RF
SPO-RF-Smoke
0
1
2
3
4
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Probability



Number of remaining EDGs
PPS config
SPO-ROW1-ROW2-Smoke
SPO-RF-ROW1-ROW2-Smoke
SPO-RF-ROW1-ROW2
SPO-ROW1-ROW2
RF-ROW1-ROW2-Smoke
ROW1-ROW2
RF-ROW1-ROW2
ROW1-ROW2-Smoke
SPO-RF-ROW2-Smoke
SPO-RF-ROW1-Smoke
RF-ROW2-Smoke
RF-ROW1-Smoke
SPO-RF-ROW1
SPO-RF-ROW2
SPO-ROW2
SPO-ROW1-Smoke
SPO-ROW1
SPO-ROW2-Smoke
RF-ROW1
RF-ROW2
ROW2-Smoke
ROW1
ROW2
ROW1-Smoke
SPO-RF-Smoke
RF-Smoke
SPO-RF
SPO-Smoke
SPO
Smoke
RF
2
1
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Probability



Performance Comparison
SPO-RF-ROW1-ROW2-Smoke
SPO-ROW1-ROW2-Smoke
SPO-RF-ROW1-ROW2
SPO-ROW1-ROW2
RF-ROW1-ROW2-Smoke
ROW1-ROW2
RF-ROW1-ROW2
ROW1-ROW2-Smoke
SPO-RF-ROW2-Smoke
SPO-RF-ROW1-Smoke
RF-ROW2-Smoke
RF-ROW1-Smoke
SPO-RF-ROW1
SPO-RF-ROW2
SPO-ROW2
SPO-ROW1-Smoke
SPO-ROW1
SPO-ROW2-Smoke
RF-ROW1
RF-ROW2
ROW2-Smoke
ROW1
ROW2
ROW1-Smoke
SPO-RF-Smoke
RF-Smoke
SPO-RF
SPO
SPO-Smoke
RF
Smoke
PPS config
Target Set Protection
Cost
1
0
1
Normalized Metric

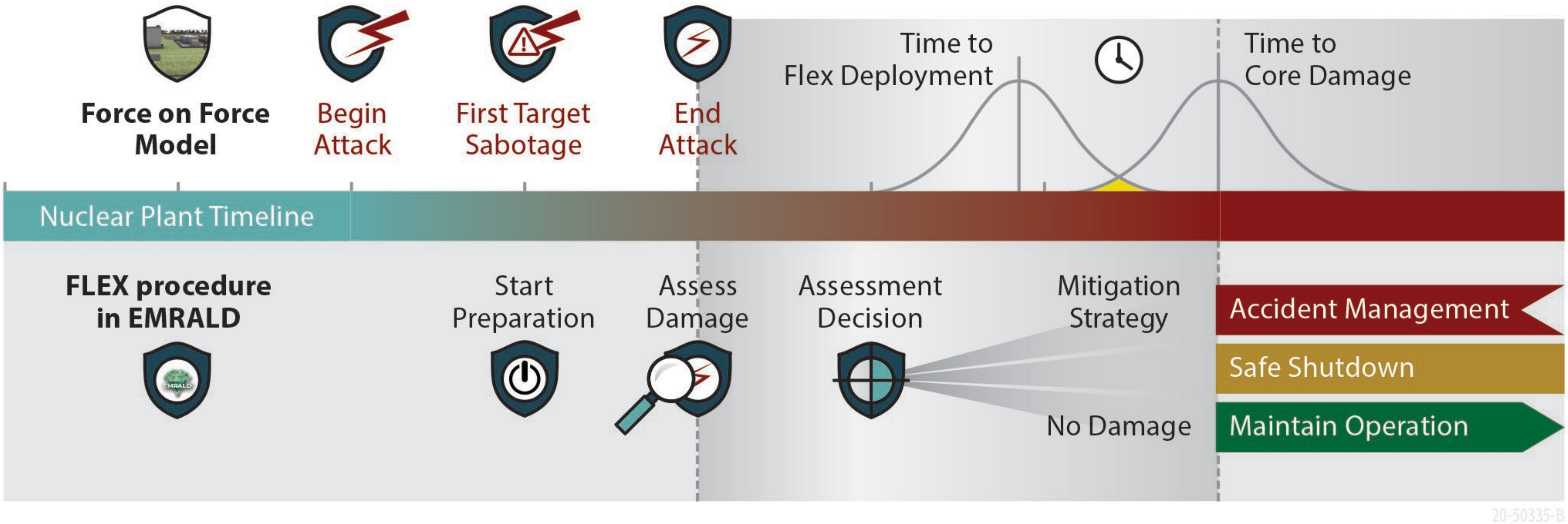
Case Study 3: Crediting Backup Safety Equipment

Diverse and Flexible Mitigation Strategy (FLEX)

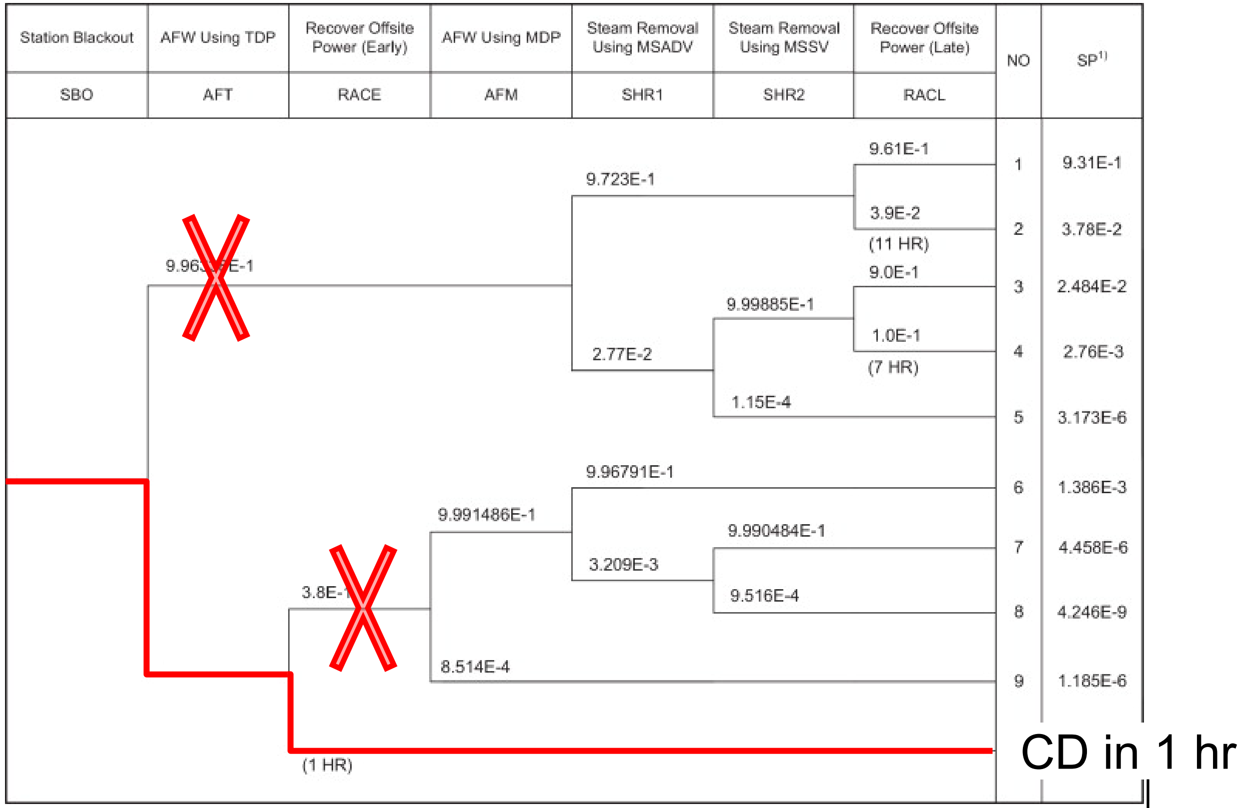
Backup equipment can be brought from offsite to any U.S. nuclear power plant within 24 hours. (Photos of equipment at National Response Center.)

Portable pumps and generators provide water and power to maintain key safety functions. (Photos of pumps and generators at the Diablo Canyon nuclear power plant.)

FoF-FLEX Timeline Model



Time Window to Execute FLEX Strategy



Conservative time limit

Realistic limit > 1 hr

- RELAP5 TH analysis with uncertainties*:
  - Operator action timing

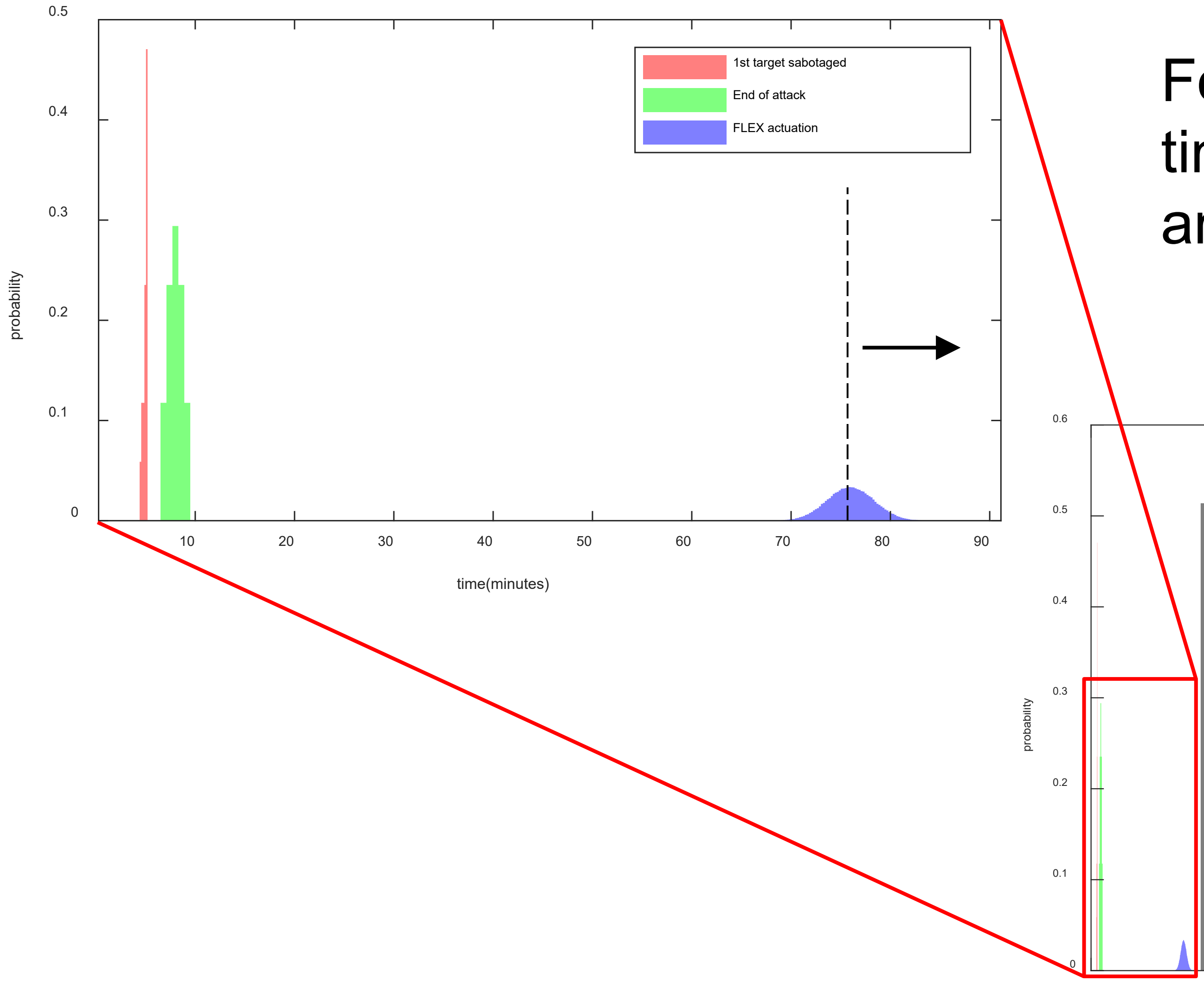
Task	Average(s)	Std dev (s)
Average performance time of standard post-trip actions	196.2	72.8
Event diagnosis time data for SBO	251.7	78.6
Minimizing the leakage from RCS	395.4	61.0
Preventing the over-pressurization of main condensers	410.8	76.5
Restoring AC power	515.6	89.7

  - Component failures:

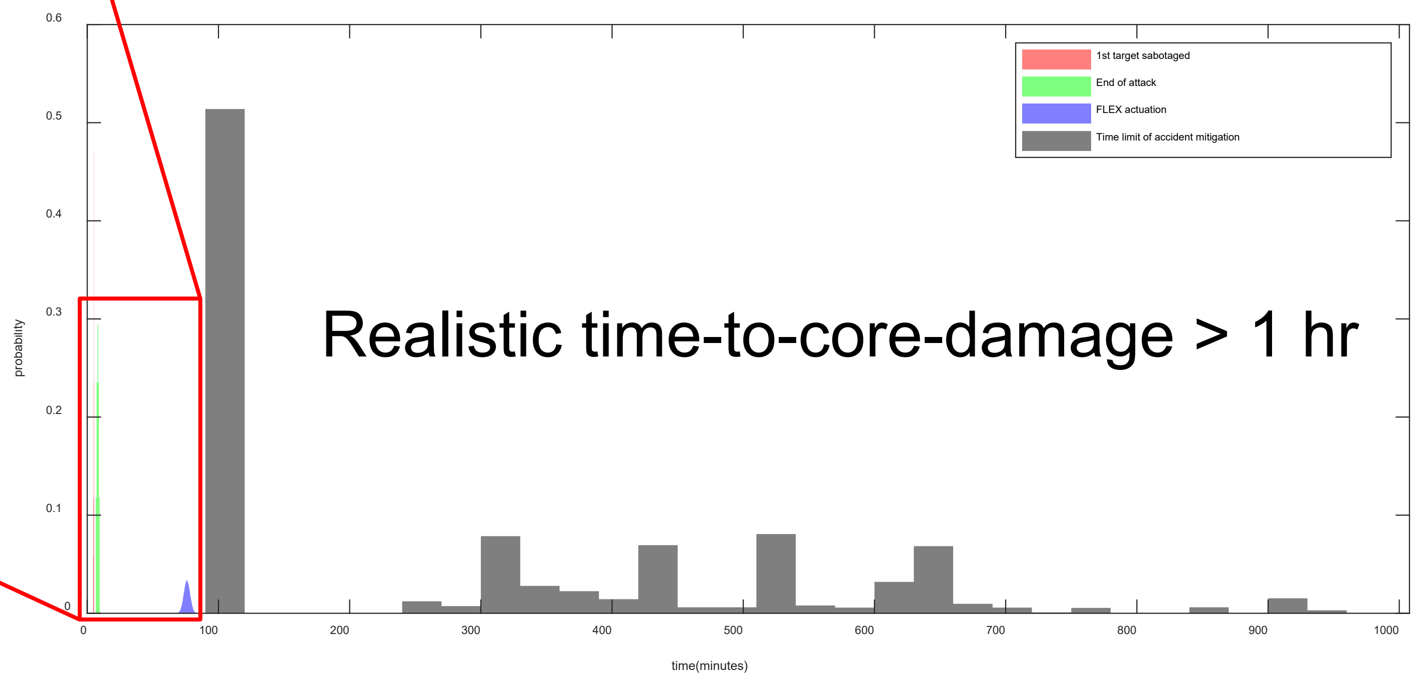
Variable	Distribution
Number of AFWs (MDP/TDP) available	Bernoulli (P_f=6.57E-3 / 1.46E-2)
Initiation timings of AFWs	Normal (μ=196.2, σ=72.8)
Offsite power recovery (hr)	Lognormal (μ=0.793, σ=1.982)
Operation of secondary depressurization	Bernoulli (P_f=2.31E-3)
Initiation timings of secondary depressurization	Gamma (α=28.83, β=14.28)
AFW pump (MDP/TDP) fail to run (hr)	Exponential (λ=3.59E-3/2.21E-3)
Reactor coolant system (RCS) depressurization operation	Bernoulli (P_f=5.69E-3)
Initiation timing for bleed operation	Gamma (α=4, β=0.03178)
Number of high-pressure safety injection pumps	Bernoulli (P_f=6.66E-4)

*Shah, A.U.A.; Christian, R.; Kim, J.; Kang, H.G., "Coping Time Analysis for Chromium coated Zircaloy for Station Blackout Scenario based on Dynamic Risk Assessment", Proceedings of The 15th Probabilistic Safety Assessment and Management Conference (PSAM 15), Venice, Italy, November 2020.

Realistic Time-to-core-damage



FoF-TH coupled simulations show enough time to actuate the FLEX strategy following an attack scenario



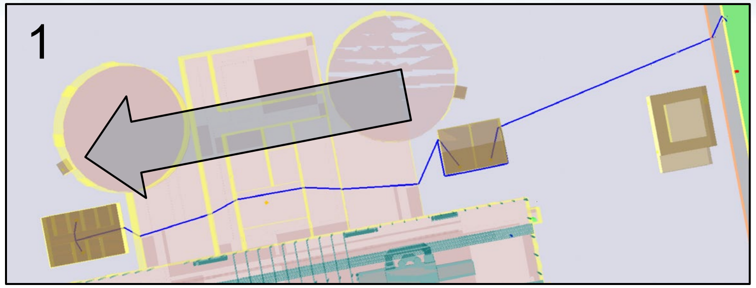
Realistic time-to-core-damage > 1 hr

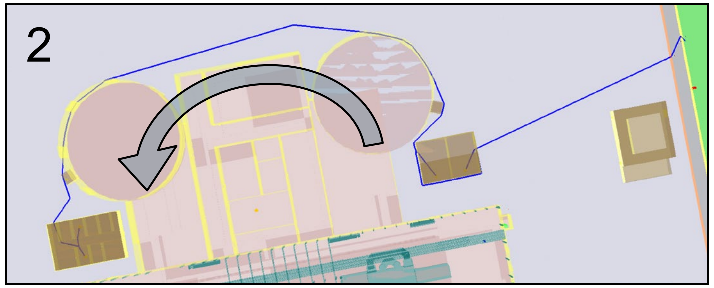
Results Comparison

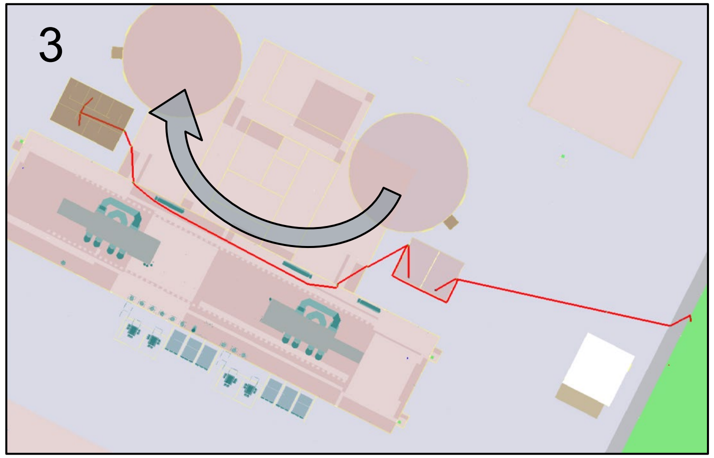
- Simulation of the three attack paths @ 100 runs

No.	System availability			Mitigation strategy	Probability	P(CD) without FLEX	P(CD) with FLEX
	Offsite power	EDG	TDP				
1	✓	✓	✓	N/A (Continue operation)	0	0	
2	✓	✓	✗	Non-transient shutdown	0	0*1E-4	
3	✓	✗	✓	Non-transient shutdown	0	0*1E-4	
4	✓	✗	✗	Non-transient shutdown	0	0*1E-3	
5	✗	✓	✓	LOOP ET	280/300 = 0.933	0.933*1E-3	
6	✗	✓	✗	LOOP ET	0	0*5E-3	
7	✗	✗	✓	**FLEX** EDG strategy within 11 hours	17/300 = 5.67E-2	5.67E-2*4E-2	5.67E-2*1.54E-4
8	✗	✗	✗	**FLEX** ELAP strategy within 1 hour	3/300 = 0.01	0.01*1	0.01*1.83E-4
Total					1	1.32E-2	9.44E-4

FLEX strategy reduces Core Damage Probability







Other Case Studies

- Evaluating whether guards in towers may take bathroom breaks

- EMRALD simulation results:
- 1E6 simulations → 560 attacks → 39 times (7%) guards not ready

- Optimizing the location of guard towers

- EMRALD manages FoF simulations with various tower locations, and post-processes the results.

Summary

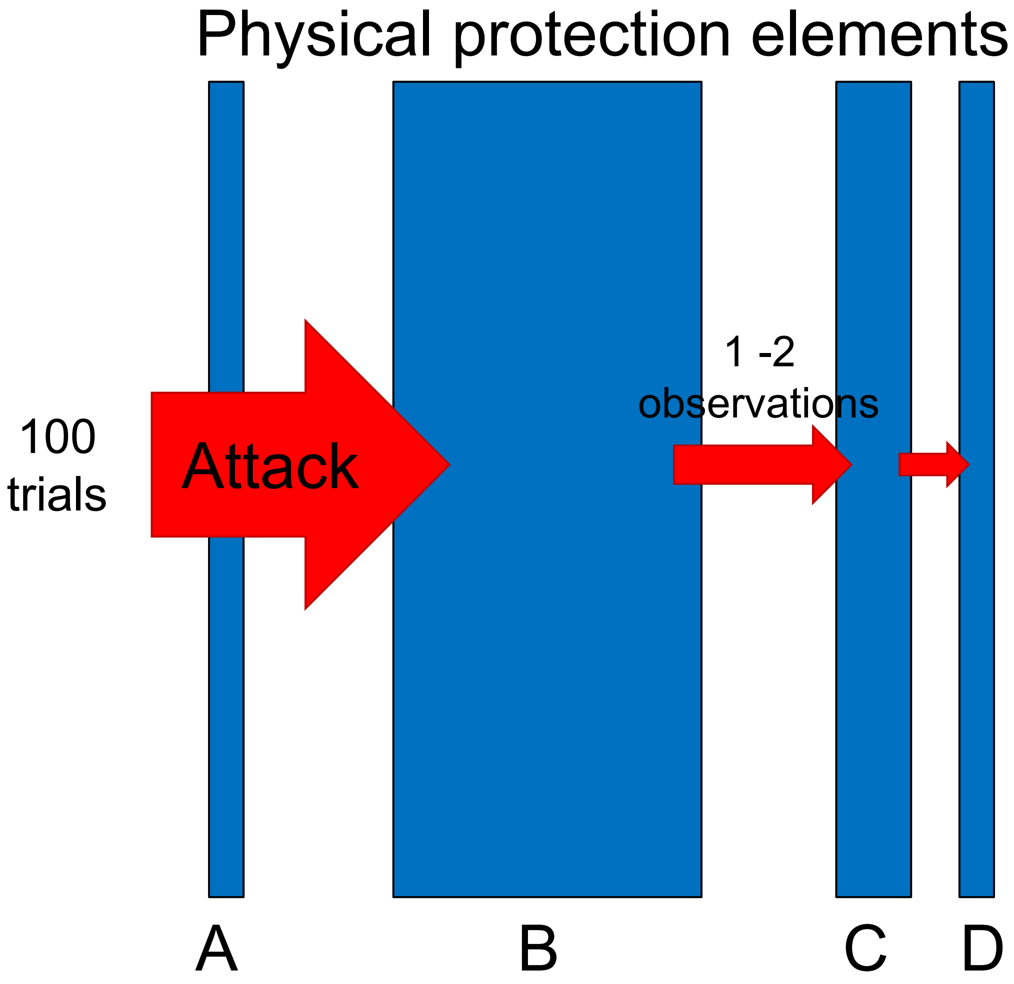
- The current physical protection evaluation method is static and conservative.
- The dynamic modeling method using INL's EMRALD may reduce PPS design conservatism and cost.
- Existing measures in NPP, i.e. FLEX and Design-Basis safety actions, may be credited towards NPP's compliance regarding the physical protection's objective. This approach affords NPPs more flexibility to optimize their PPS design.

Thank you

Research team:
Shawn St. Germain
Vaibhav Yadav
Steven Prescott
John Weathersby
Pralhad Burli
Robby Christian

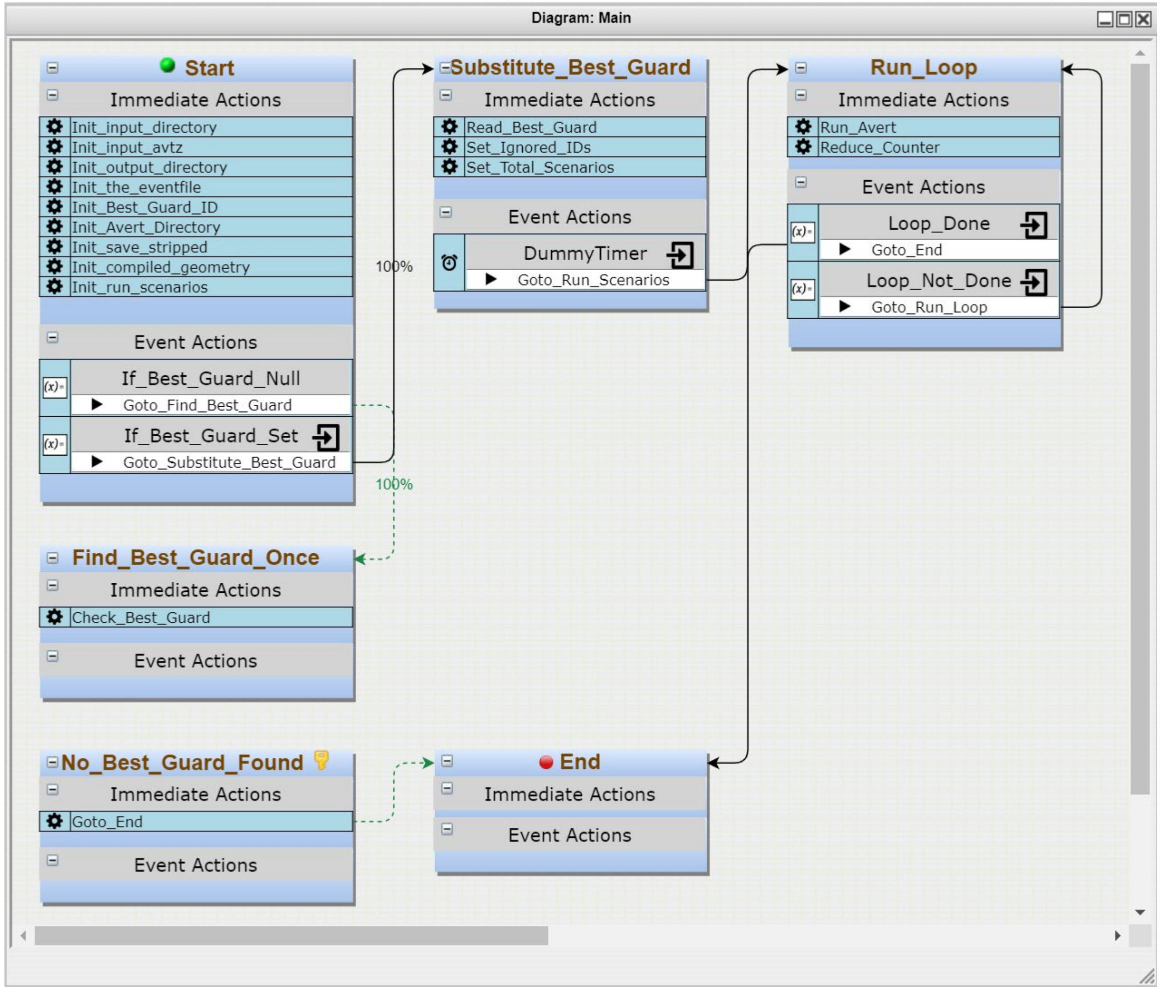
Extra Slides

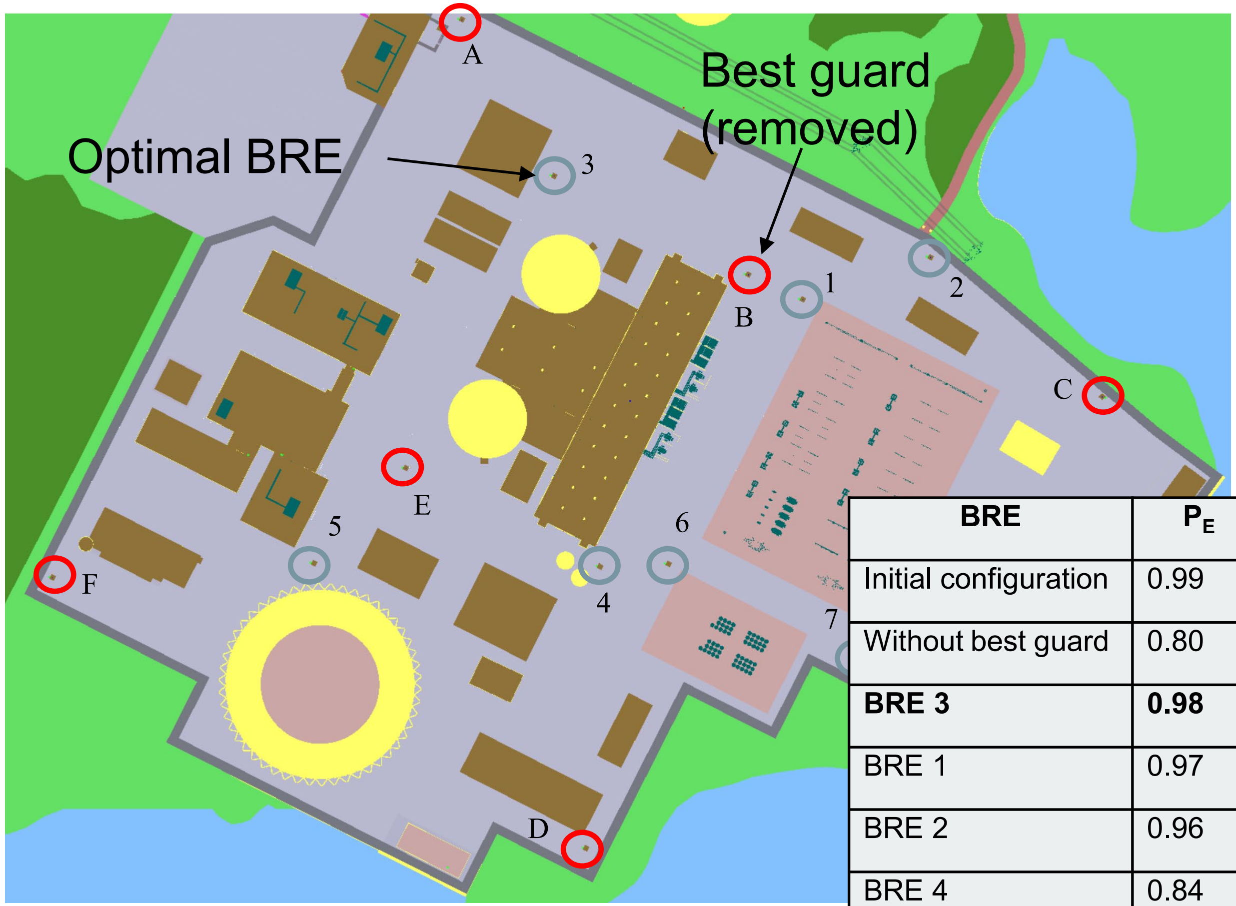
Case Study 4: BRE Placement Optimization



- Problem: Computational challenges in FoF simulations when optimizing physical protection's Defense-in-Depth (e.g., BRE tower location)
- Solution: Use of EMRALD as an automation tool
  - Run initial FoF simulations
  - Process FoF results, identify and remove the most effective guard
  - Re-run FoF simulations with various tower locations
  - Compare P(E) results

Results



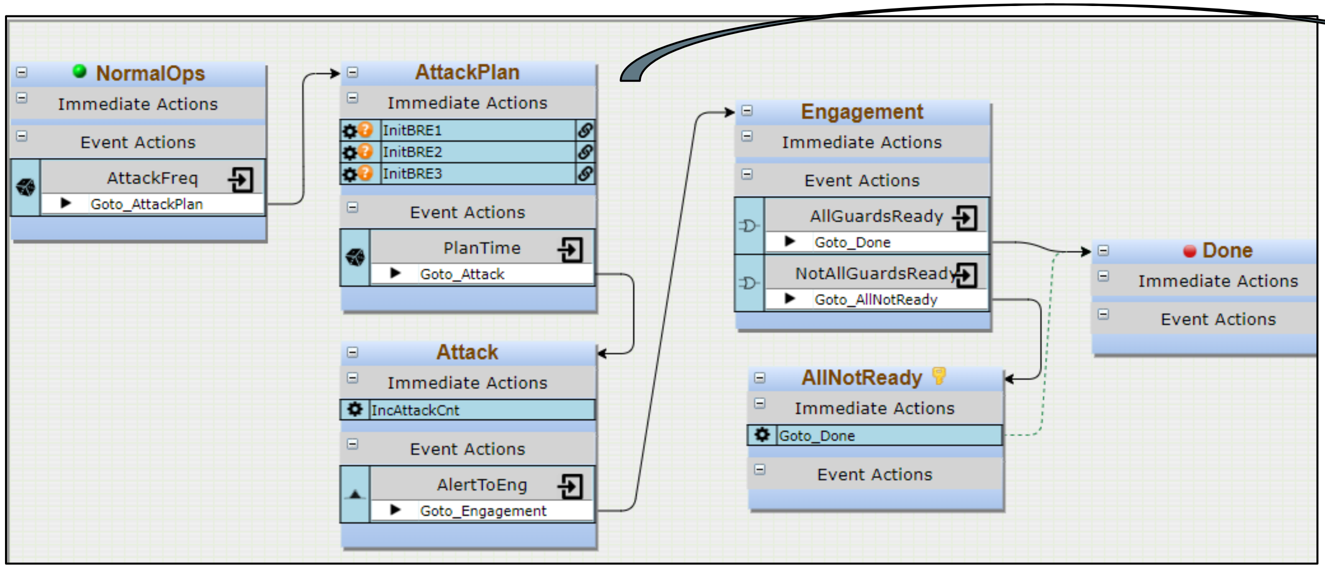


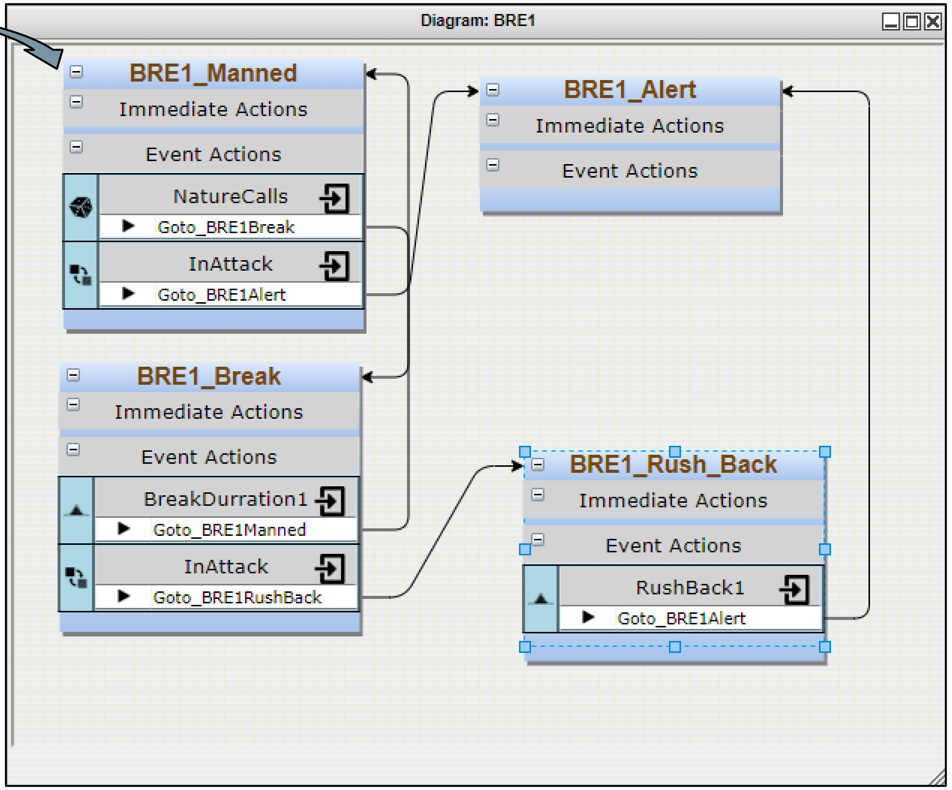
BRE	P_E
Initial configuration	0.99
Without best guard	0.80
BRE 3	**0.98**
BRE 1	0.97
BRE 2	0.96
BRE 4	0.84
BRE 6	0.87
BRE 7	0.82
BRE 5	0.82

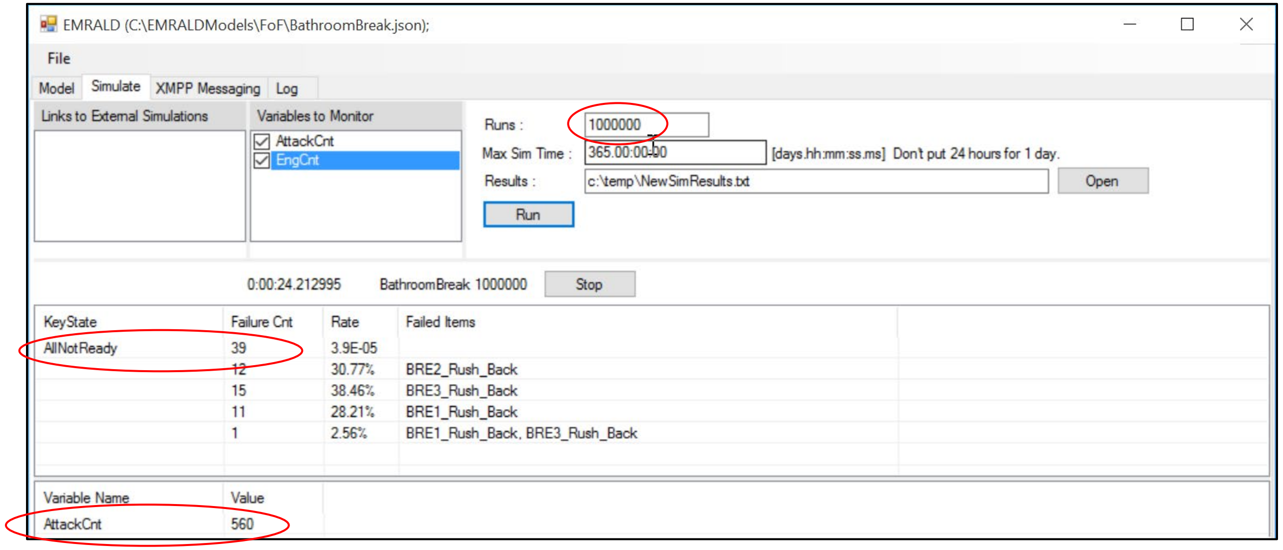
Case Study 1: Bathroom Breaks

Bathroom breaks for guards in bullet-resistant enclosures (BREs)

EMRALD Model: Bathroom Break







1E6 simulations → 560 attacks → 39 times (7%) guards not ready