INL/CON-22-67660-Revision-0

A Risk-Informed Approach to Linked Safety-Security Modeling

June 2022

Changing the World's Energy Future

Shawn W St Germain, Vaibhav Yadav, Steven R Prescott, Robby Christian

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-22-67660-Revision-0

A Risk-Informed Approach to Linked Safety-Security Modeling

Shawn W St Germain, Vaibhav Yadav, Steven R Prescott, Robby Christian

June 2022

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

A Risk-Informed Approach to Linked Safety-Security Modeling

Shawn St. Germain

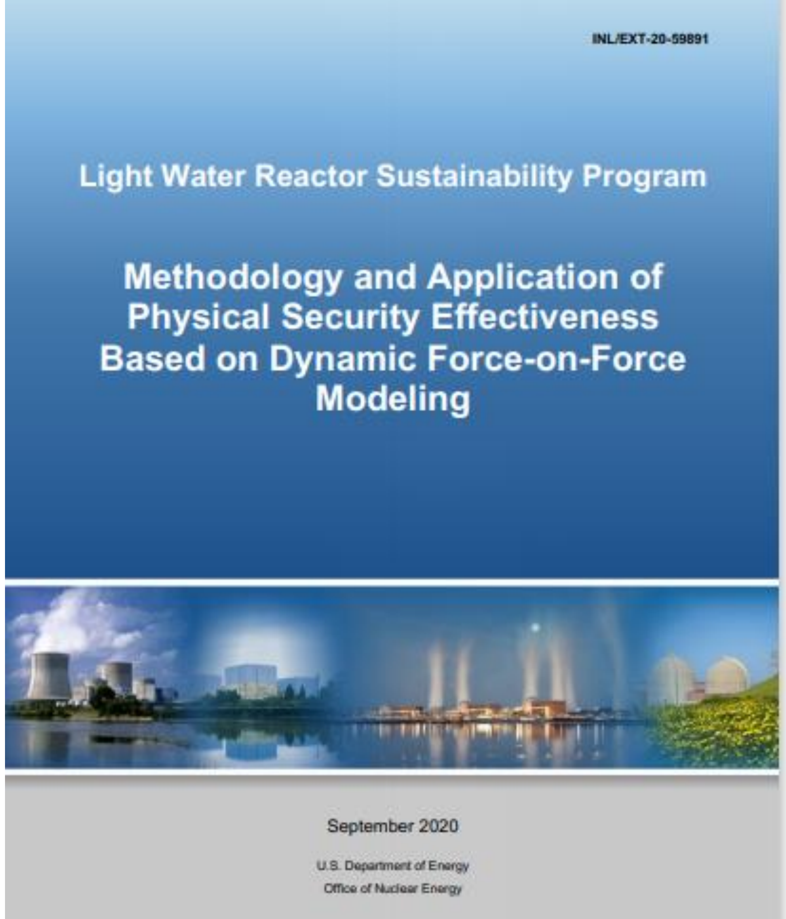
June 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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. SAND2022-5526C

Overall Proposed Approach

- Develop and demonstrate tools for a risk-informed physical security method by integrating dynamic risk methods, physics-based modeling and simulation, operator actions, and flex equipment, which should extend the adversarial timeline for response force success. The tools will enable commercial utilities to incorporate increased realism in their force-on-force models, take credit for operator actions and flex equipment, and move towards greater use of quantitative measures of performance in security posture and the technical basis for physical security at power plants.

FY 2020 Reports



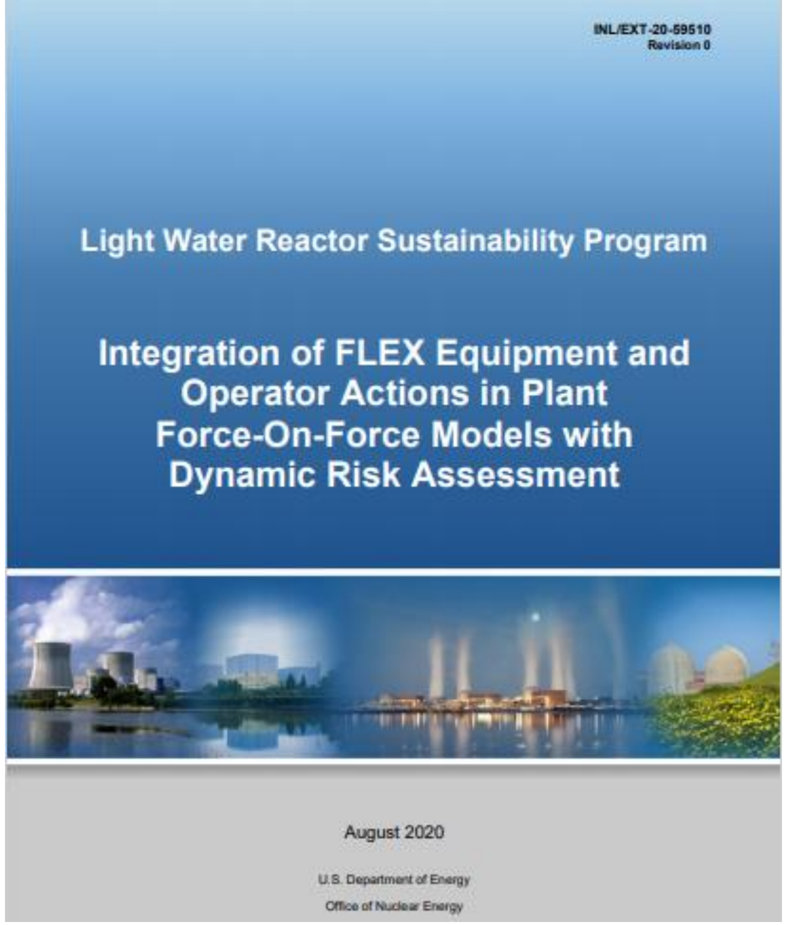
INL/EXT-20-59891

Light Water Reactor Sustainability Program

Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling

September 2020

U.S. Department of Energy
Office of Nuclear Energy



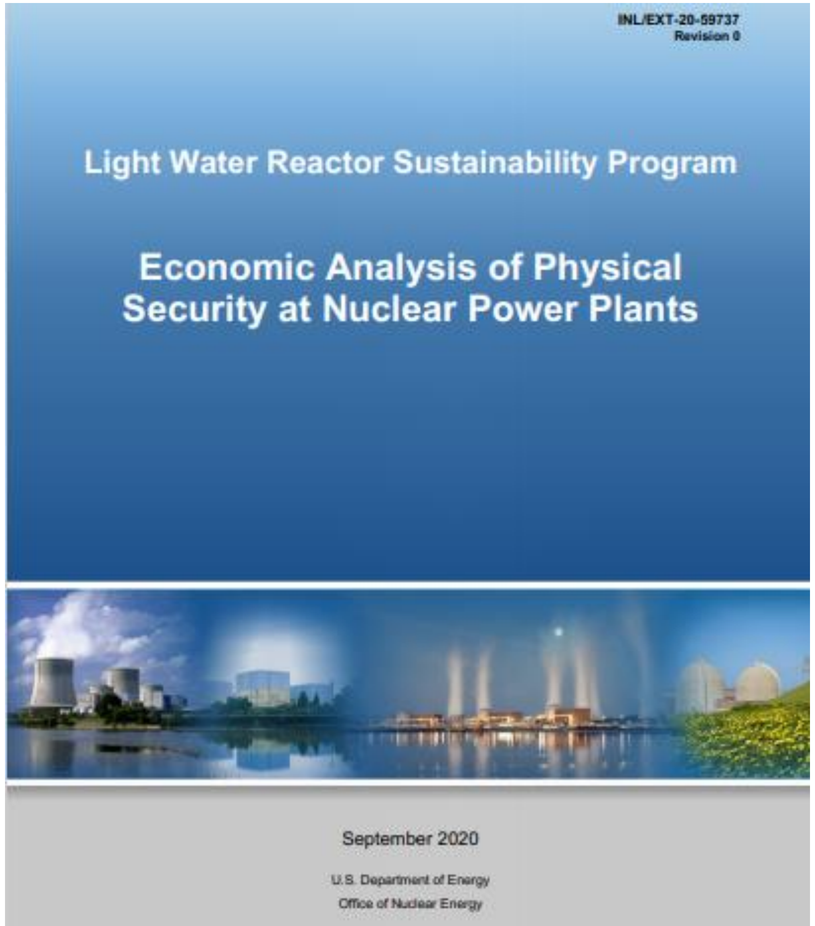
INL/EXT-20-59510
Revision 0

Light Water Reactor Sustainability Program

Integration of FLEX Equipment and Operator Actions in Plant Force-On-Force Models with Dynamic Risk Assessment

August 2020

U.S. Department of Energy
Office of Nuclear Energy



INL/EXT-20-59737
Revision 0

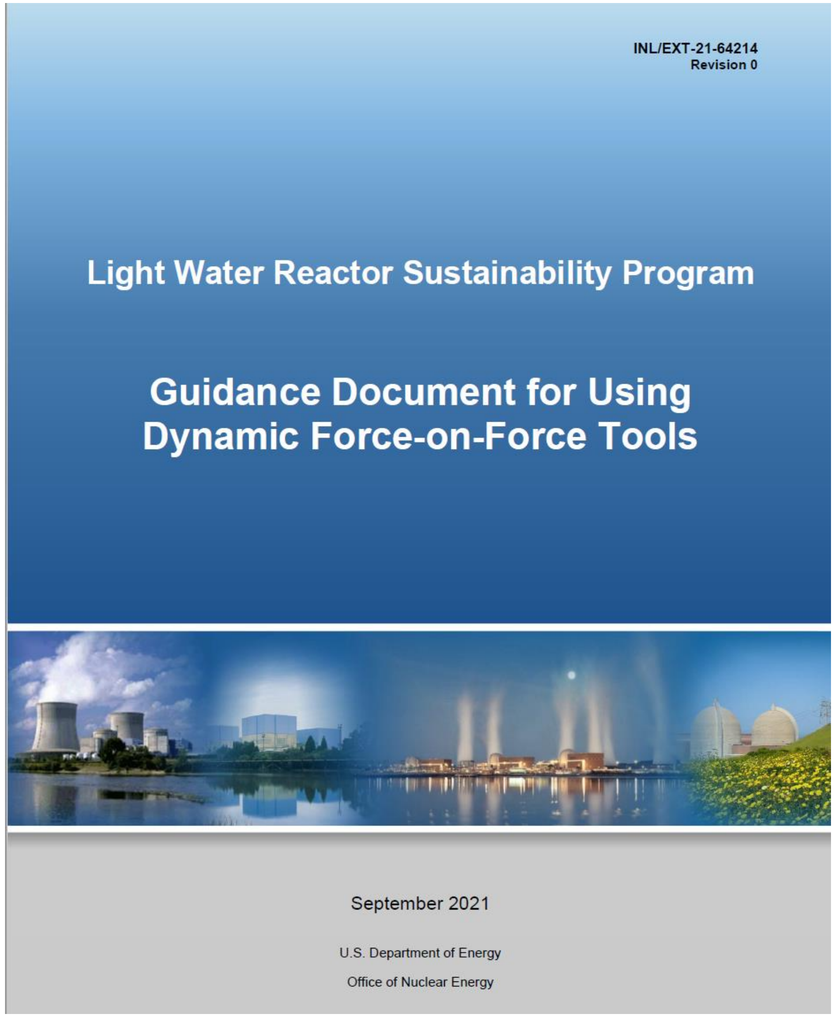
Light Water Reactor Sustainability Program

Economic Analysis of Physical Security at Nuclear Power Plants

September 2020

U.S. Department of Energy
Office of Nuclear Energy

FY 2021 Reports



INL/EXT-21-64214
Revision 0

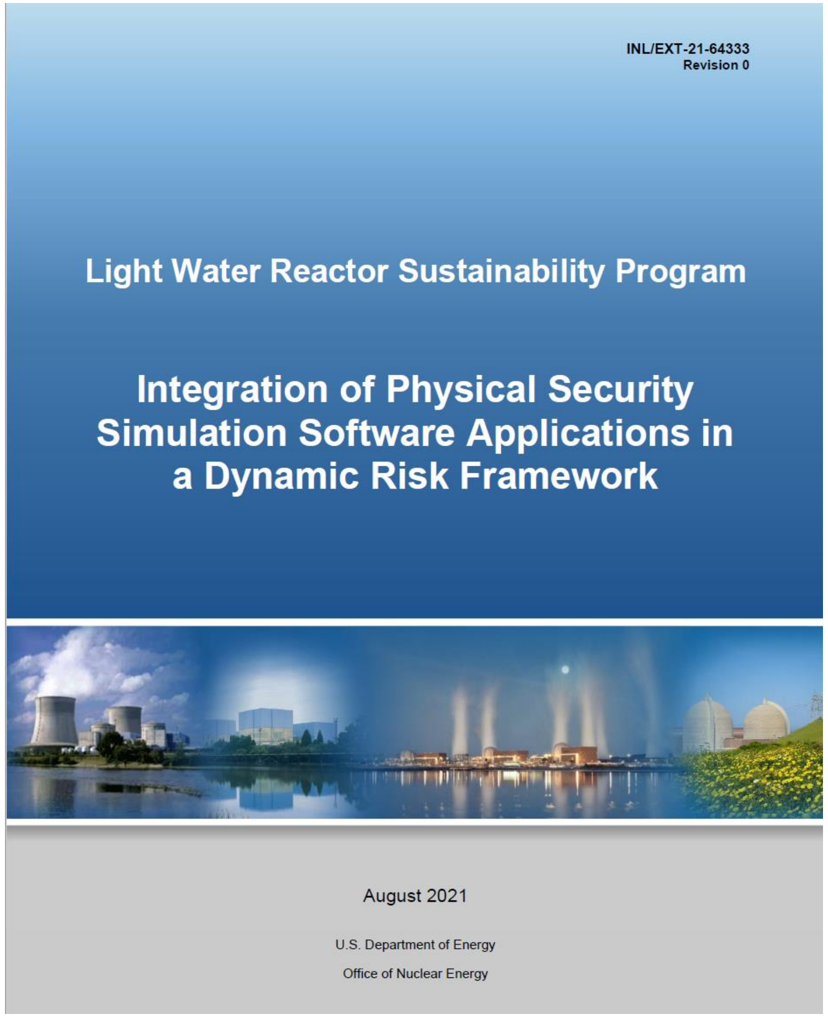
Light Water Reactor Sustainability Program

Guidance Document for Using Dynamic Force-on-Force Tools

September 2021

U.S. Department of Energy

Office of Nuclear Energy



INL/EXT-21-64333
Revision 0

Light Water Reactor Sustainability Program

Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework

August 2021

U.S. Department of Energy

Office of Nuclear Energy

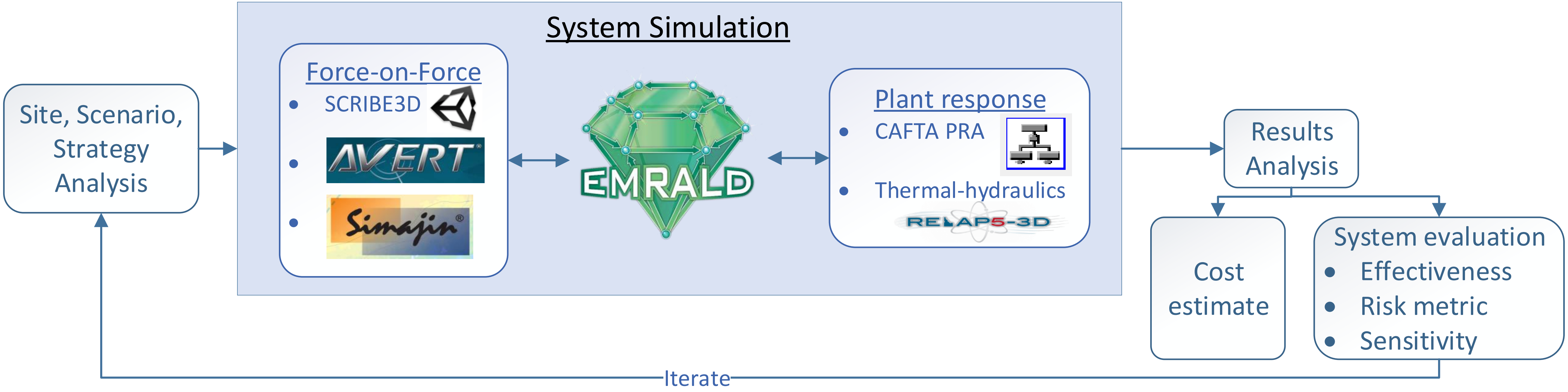
FY 2021 Reports

- **Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework**
  - Describes integration of Simajin simulation application into the Dynamic Risk Framework
  - Includes refined treatment of Defense-in-Depth Analysis
  - Includes refined treatment of post effectiveness evaluation
  - Includes refined treatment of human action modeling
- **Guidance Document for Using Dynamic Force on Force Tools to Support Physical Security Optimization**
  - Provides instructions for physical security modelers to implement the Dynamic Risk Framework
  - Describes the various tools that may be used
  - Describes how to set up EMRALD to support dynamic physical security risk modeling
  - Describes integration of common physical security simulation software applications in the Dynamic Risk Framework
  - Describes methods for evaluating and interpreting results

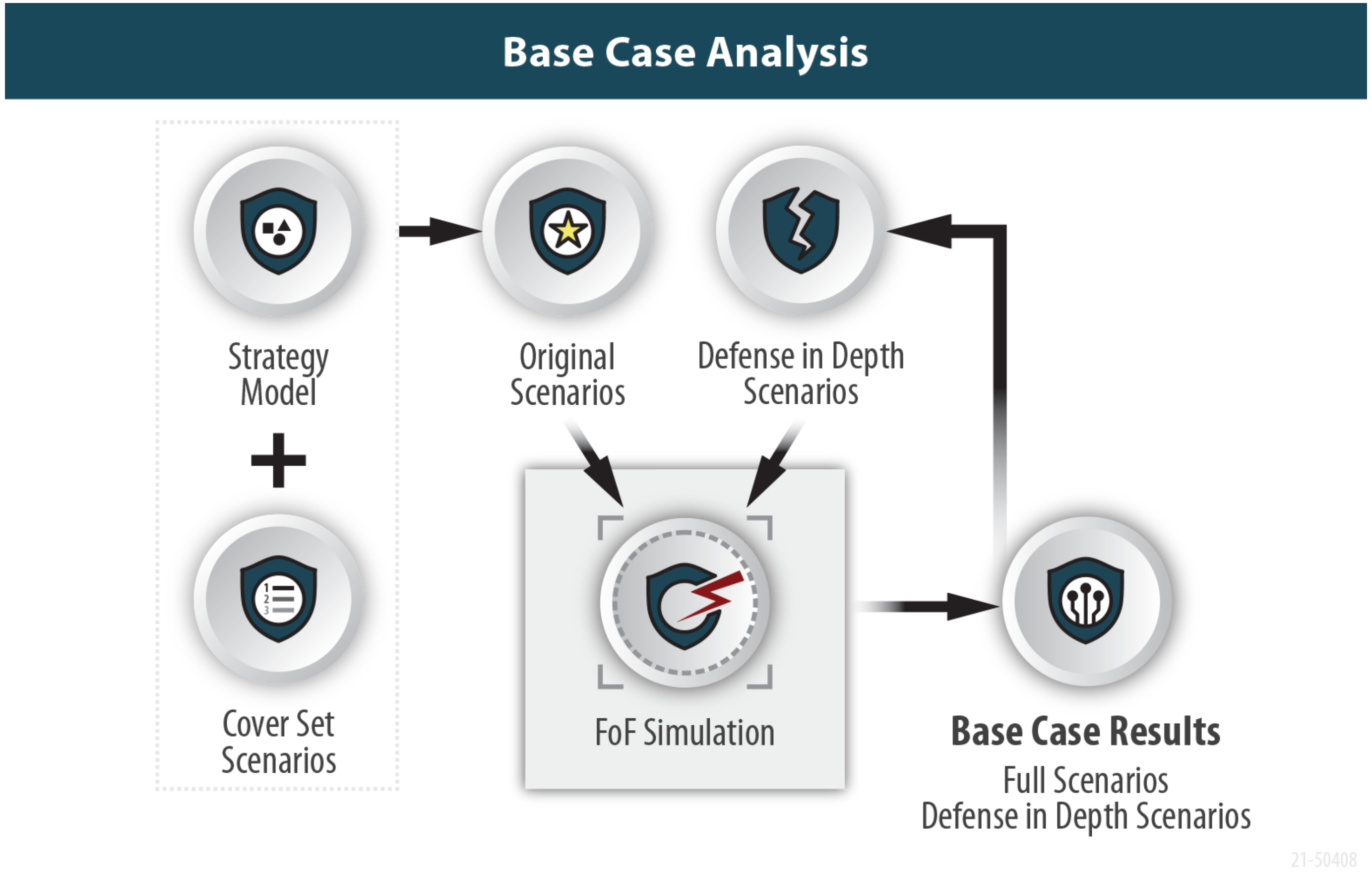
FY 2021-2022 Tasks

- Develop guidance documents in collaboration with stakeholders to support the use of the dynamic risk tools by industry security staff with support of nuclear utility PRA staff.
- Integrate additional force-on-force simulation software platforms and refine metrics for evaluation of effectiveness.
- Document the Physical Security Pathway human reliability needs for the RISA pathway's work package. Develop dynamic modeling tools to incorporate Force-on-Force and nuclear utility site operator actions into static and dynamic risk assessment models.
- Support the LWRS Program Physical Security Pathway Program Manager in providing input to the Physical Security Pathway program plan and support program meetings including stakeholder meetings.
- Demonstrate methodology with actual plant data to refine methods and validate assumptions.

Proposed Framework



Initial Plant Modeling



Base Case Analysis

Strategy Model

+

Cover Set Scenarios

Original Scenarios

Defense in Depth Scenarios

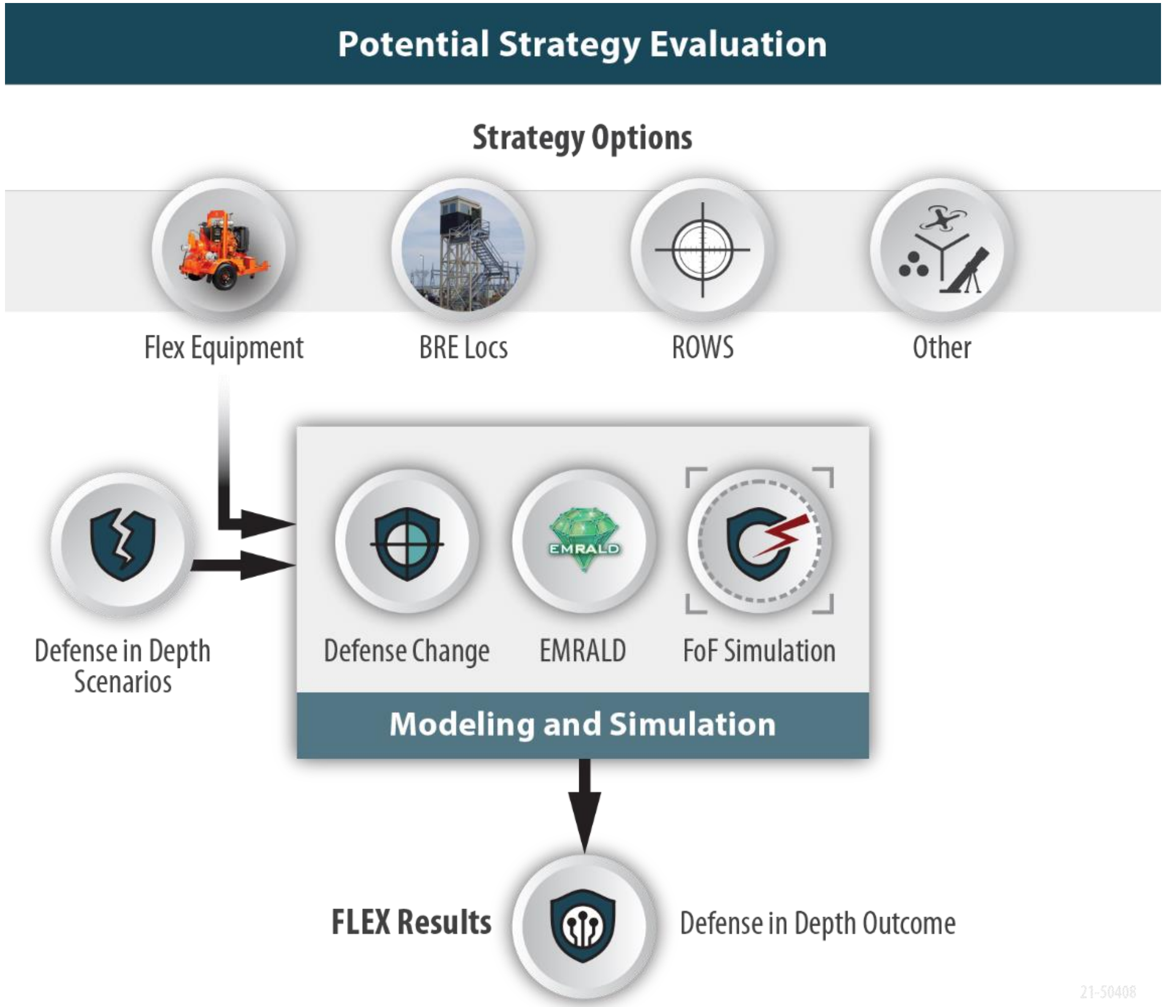
FoF Simulation

Base Case Results

Full Scenarios

Defense in Depth Scenarios

Modeling Potential Alternative Strategies



Potential Strategy Evaluation

Strategy Options

Flex Equipment

BRE Locs

ROWS

Other

Defense in Depth Scenarios

Defense Change

EMRALD

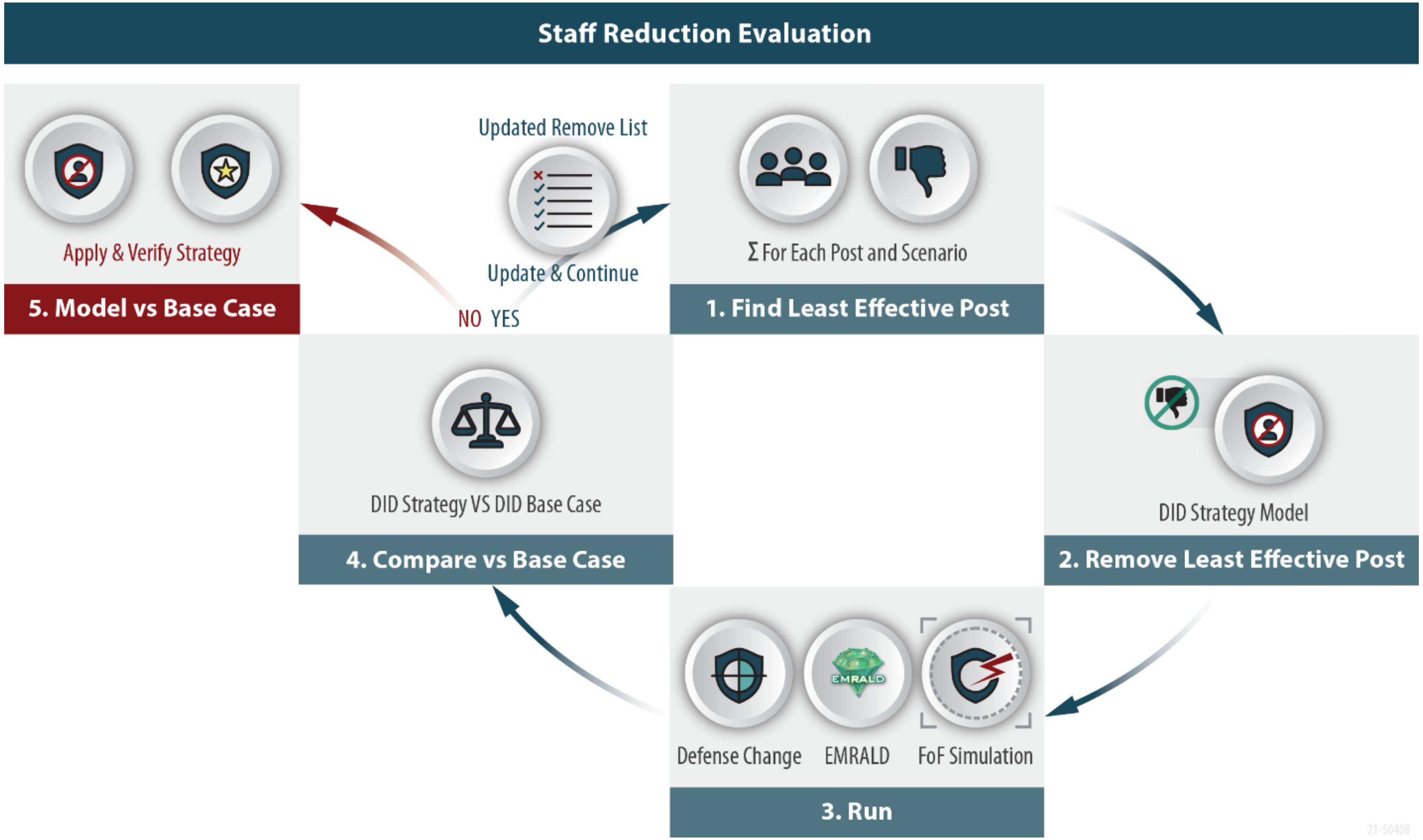
FoF Simulation

Modeling and Simulation

FLEX Results

Defense in Depth Outcome

Evaluate Potential Cost Savings



Staff Reduction Evaluation

Σ For Each Post and Scenario

1. Find Least Effective Post

DID Strategy Model

2. Remove Least Effective Post

Defense Change

EMRALD

FoF Simulation

3. Run

DID Strategy VS DID Base Case

4. Compare vs Base Case

NO YES

Update & Continue

Updated Remove List

Apply & Verify Strategy

5. Model vs Base Case

21-50408

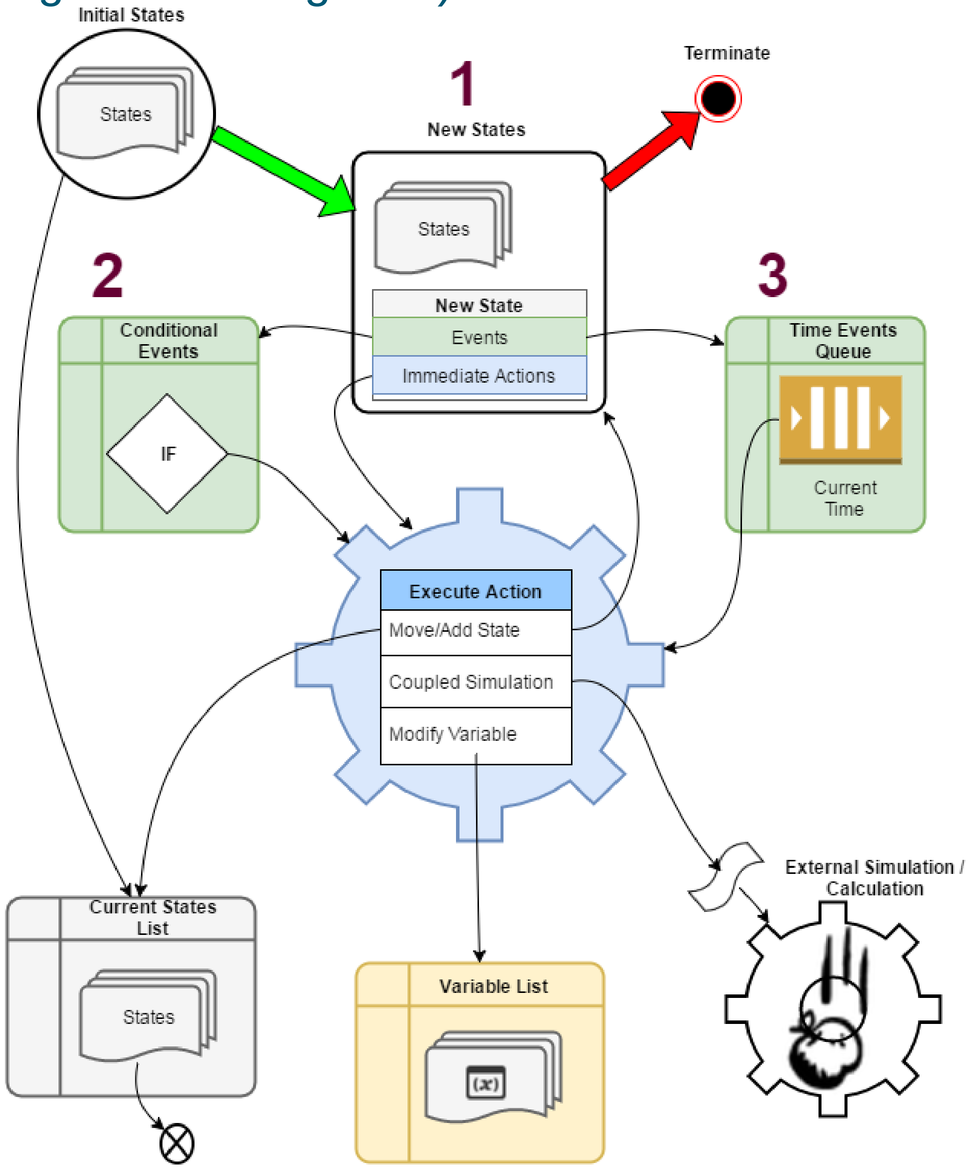
EMRALD

(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 Current and New States List.

1. While 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 criteria is met.
   - Execute that events action/s.
   - (Go to Step 1)
3. Jump to the next chronological event.
   - Process that event’s actions.
   - (Go to Step 1)



EMRALD Modeling

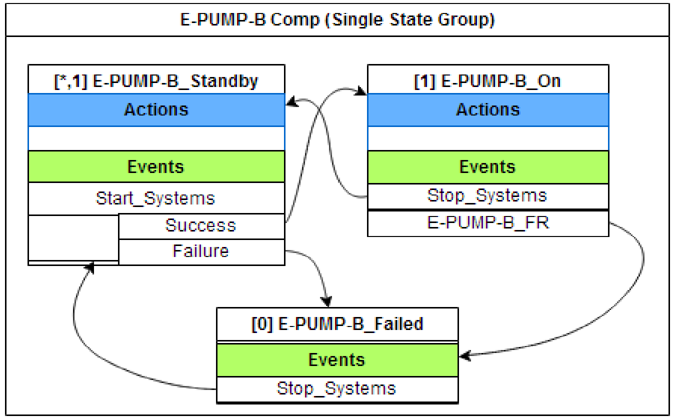
States

- 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



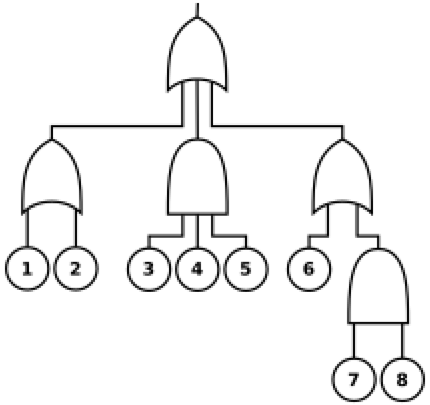
E-PUMP-B Comp (Single State Group)

[*,1] E-PUMP-B_Standby
Actions
Events
Start_Systems
Success
Failure

[1] E-PUMP-B_On
Actions
Events
Stop_Systems
E-PUMP-B_FR

[0] E-PUMP-B_Failed
Events
Stop_Systems

Logic Trees



Variables

External Links

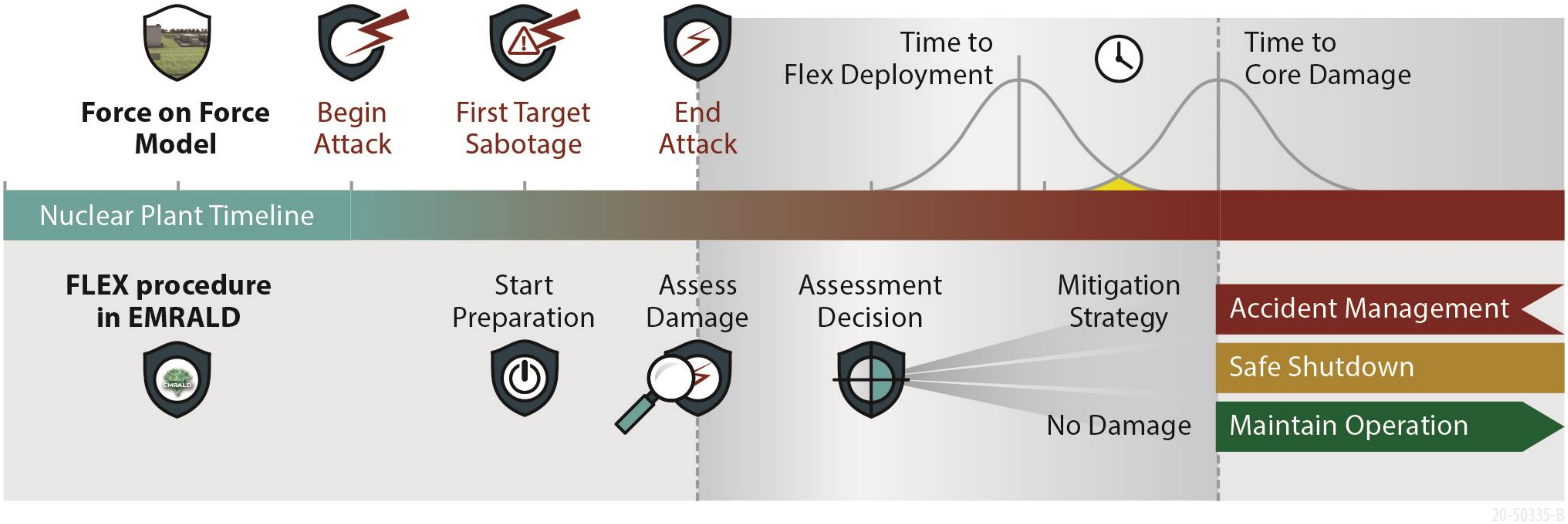
Case Study: Crediting FLEX Equipment

Diverse and Flexible Mitigation Strategy (FLEX)

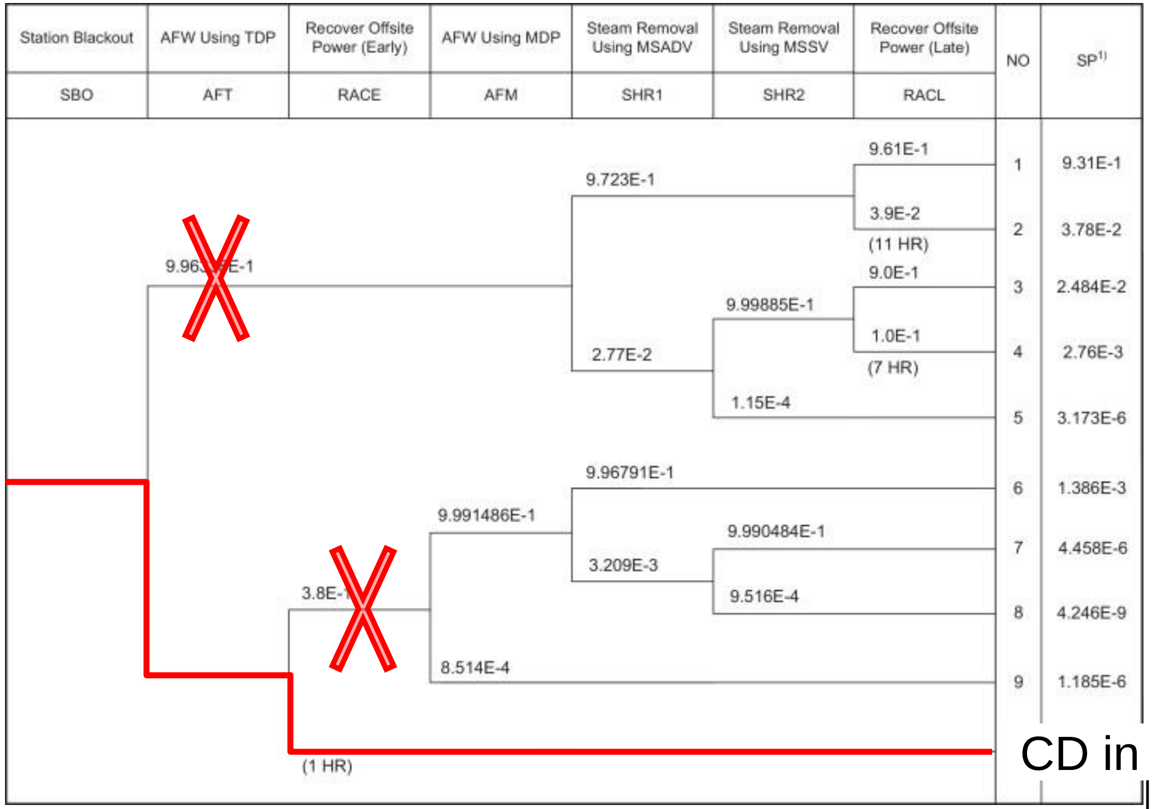
Backup equipment can be brought from offsite to any U.S. nuclear power plant within 24 hours. (Photos of equipment at National Response Center.)

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



CD in 1 hr

Conservative time limit

Realistic limit > 1 hr

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

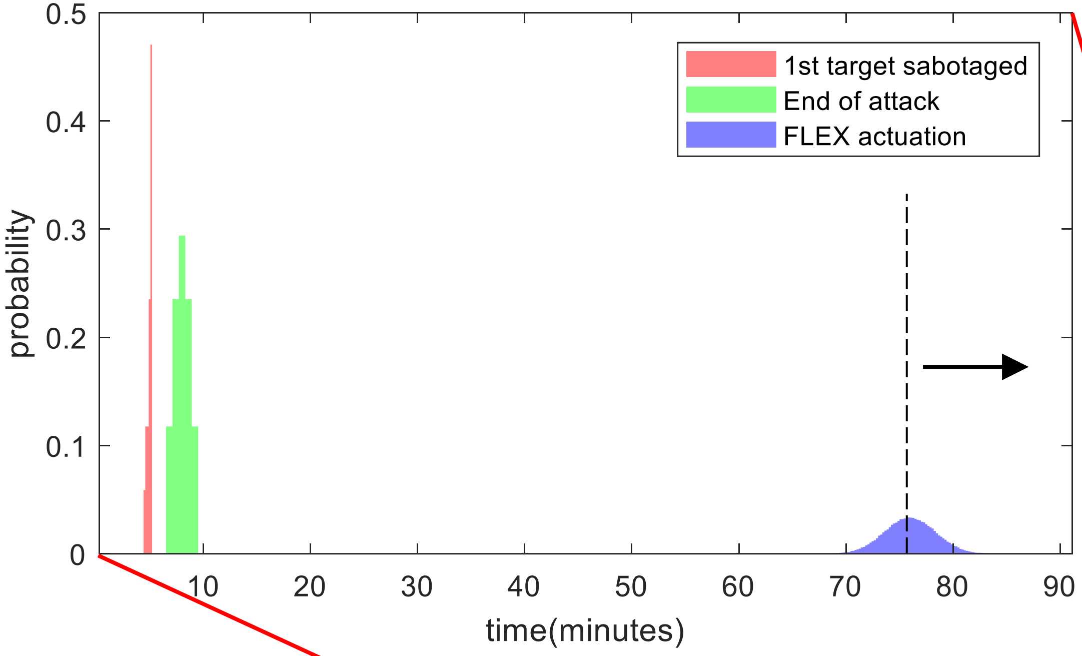
Task	Average(s)	Std dev (s)
Average performance time of standard post-trip actions	196.2	72.8
Event diagnosis time data for SBO	251.7	78.6
Minimizing the leakage from RCS	395.4	61.0
Preventing the over pressurization of main condensers	410.8	76.5
Restoring AC power	515.6	89.7

  - Component failures:

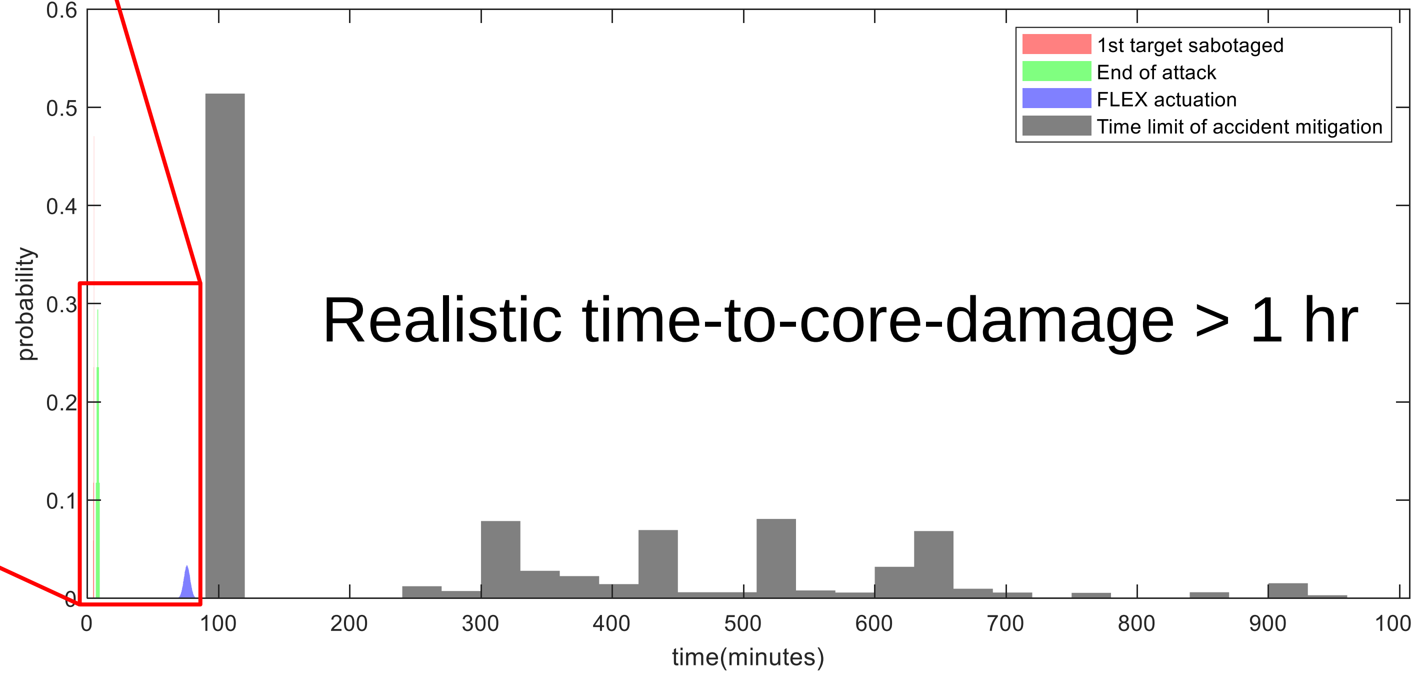
Variable	Distribution
Number of AFW (MDP/TDP) available	Bernoulli (P_f=6.57E-3 / 1.46E-2)
Initiation timings of AFWs	Normal (μ=196.2, σ=72.8)
Offsite power recovery (hr)	Lognormal (μ=0.793, σ=1.982)
Operation of secondary depressurization	Bernoulli (P_f=2.31E-3)
Initiation timings of secondary depressurization	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.

Option 2: Realistic core damage time



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



Realistic time-to-core-damage > 1 hr

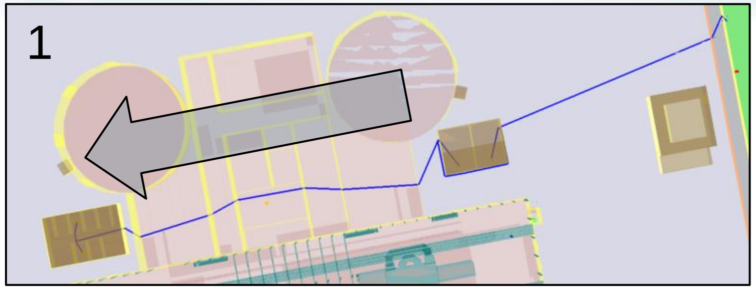
Results Comparison

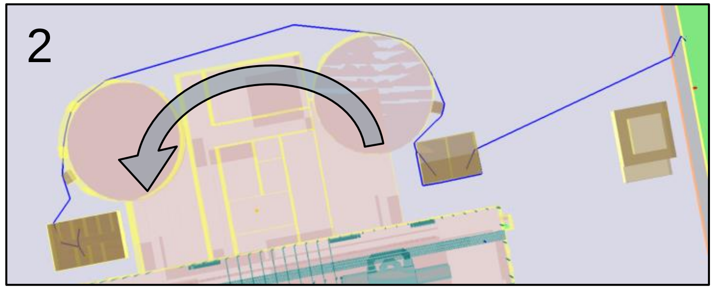
- Simulated 3 attack paths @ 100 runs

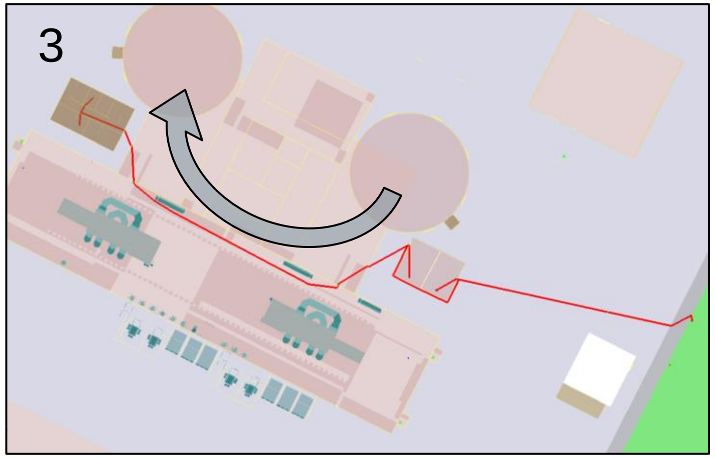
No.	System Availability			Mitigation strategy	Probability	P(CD) without FLEX	P(CD) with FLEX
	Offsite power	EDG	TDP				
1	✓	✓	✓	N/A (Continue operation)	0	0	
2	✓	✓	X	Non-transient shutdown	0	0	
3	✓	X	✓	Non-transient shutdown	0	0	
4	✓	X	X	Non-transient shutdown	0	0	
5	X	✓	✓	Loss-of-Offsite-Power Event Tree	280/300 = 0.933	0.933 * 1E-3	
6	X	✓	X	Loss-of-Offsite-Power Event Tree	0	0	
7	X	X	✓	DG FLEX Strategy	17/300 = 5.67E-2	5.67E-2 * 1	5.67E-2 * 0.1
8	X	X	X	DG & Pump FLEX Strategy	3/300 = 0.01	0.01 * 1	0.01 * 0.2
Total					1	6.76E-2	8.6E-3

FLEX strategy reduces Core Damage Probability

Assumption: Failure probability for each FLEX equipment is 0.1







Modeling Human Action Time Distributions

- Collaborated with the LWRS Risk Informed Systems Analysis Pathway Team to create a method for assigning time distributions to human actions for modelling flex procedures
- Created a simple method and worksheet that allows security risk analyst to interview flex implementation SME to assign a time distribution to key actions
- The worksheet guides the analyst to collect information about the task location, challenges, average time to complete, best case time to complete and worst-case time to complete
- The method then assigns a log-normal distribution with associated uncertainty parameters to use in EMRALD
- The method also allows for combining the input from several SMEs
- Future work will collect and provide representative time values for common FLEX actions based on industry data collection

Collecting Timeline Data

1. For an average operator performing this task and working as quickly and efficiently as possible under ideal conditions, please provide the minimum amount of time in which this task could be performed.

2. For an average operator performing this task and working as quickly and efficiently as possible under normal conditions, please indicate how long it would take, on average, to complete the task.

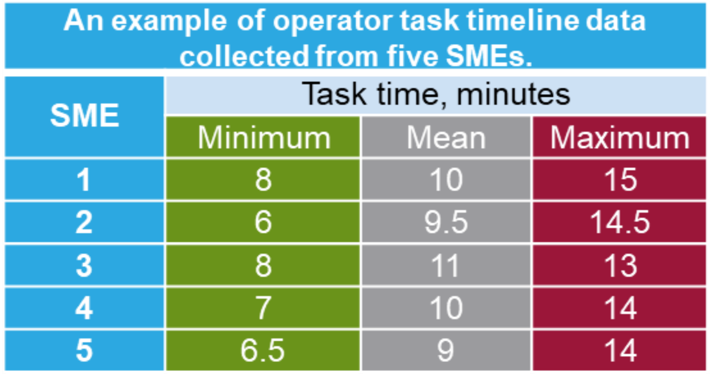
3. For an average operator performing this task and working as quickly and efficiently as possible under challenging conditions, please provide the maximum amount of time necessary to perform this task.

4. Gather additional information about the nature of the task (can inform estimating a shaping or weighting function for the time distribution).
   A. Will FLEX equipment require relocation? If yes,
      - How will the equipment be moved? (e.g., forklift, truck, by hand)
      - How far will the equipment be moved? (e.g., distance in yards,)
      - Over or through what terrain and barriers?

   B. Is this an individual or team task? If a team task, how many are on the team?

   C. For this task, what are the typical challenges the team will face?

   D. How physically challenging is this task?
      - High exertion (e.g., lifting heavy equipment, climbing ladders or stairs, etc.)
      - Medium exertion (e.g., moving or repositioning valves, electrical connections, etc.)
      - Low exertion (e.g., manipulating switches, opening doors, etc.)



An example of operator task timeline data collected from five SMEs.

SME	Task time, minutes		
	Minimum	Mean	Maximum
1	8	10	15
2	6	9.5	14.5
3	8	11	13
4	7	10	14
5	6.5	9	14

Statistical Distribution from Collected Data

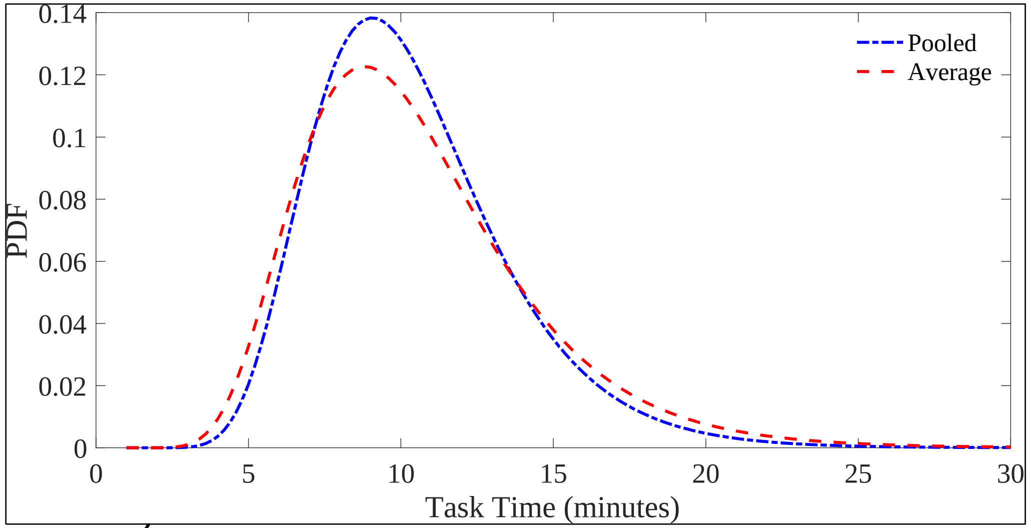
- Time data for human actions follow Lognormal distribution LN(μ, σ)
- Using maximum likelihood estimate
  - $\mu = \frac{1}{N}\sum_{i=1}^{N} \ln x_i$ and $\sigma^2 = \frac{1}{N-1}\sum_{i=1}^{N}(\ln x_i - \mu)^2$
- We use two approaches
  - **Average:**

$$\mu_A = \frac{1}{n}\sum_{i=1}^{n} \mu_i \; ; \; \sigma_A^2 = \frac{1}{n}\sum_{i=1}^{n} \sigma_i^2$$

$$\mu_i = \sum_{j=1}^{m} \ln x_{i,j} \; ; \; \sigma_i^2 = \frac{1}{m-1}\sum_{j=1}^{m}\left(\ln x_{i,j} - \mu_i\right)^2$$

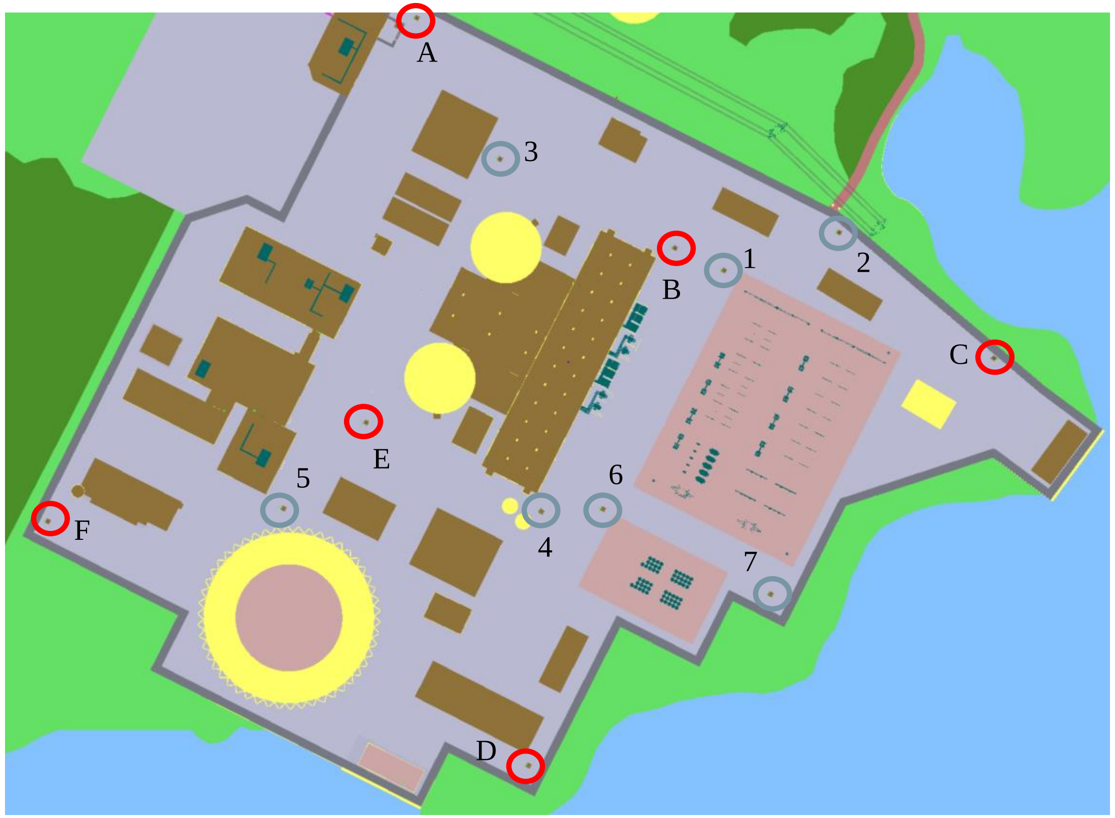
  - **Pooled:**

$$\mu_P = \frac{1}{n+m}\sum_{i=1}^{n}\sum_{j=1}^{m} \ln x_{i,j} \; ; \; \sigma_P^2 = \frac{1}{n+m-1}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(\ln x_{i,j} - \mu_P\right)^2$$



Other Case Studies

- Optimizing the location of guard towers



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

Summary

- 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 (FLEX and DB safety actions) may be credited towards NPP’s compliance on the physical protection’s objective. This approach provides NPP with more flexibility to optimize their PPS design.

Thank you

Research team:
Shawn St. Germain
Vaibhav Yadav
Steven Prescott
Pralhad Burli
Robby Christian
Chris Chwasz