INL/MIS-23-73355-Revision-0

Methodology and Tool for the Physical Security Analysis of Micro and Advanced Reactors

July 2023

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-23-73355-Revision-0

Methodology and Tool for the Physical Security Analysis of Micro and Advanced Reactors

Robby Christian

July 2023

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

National Nuclear Security Administration

United States
Department of Energy
National Nuclear Security Administration

International Nuclear Security

Methodology and Tool for the Physical Security Analysis of Micro and Advanced Reactors

Robby Christian

July 10, 2023

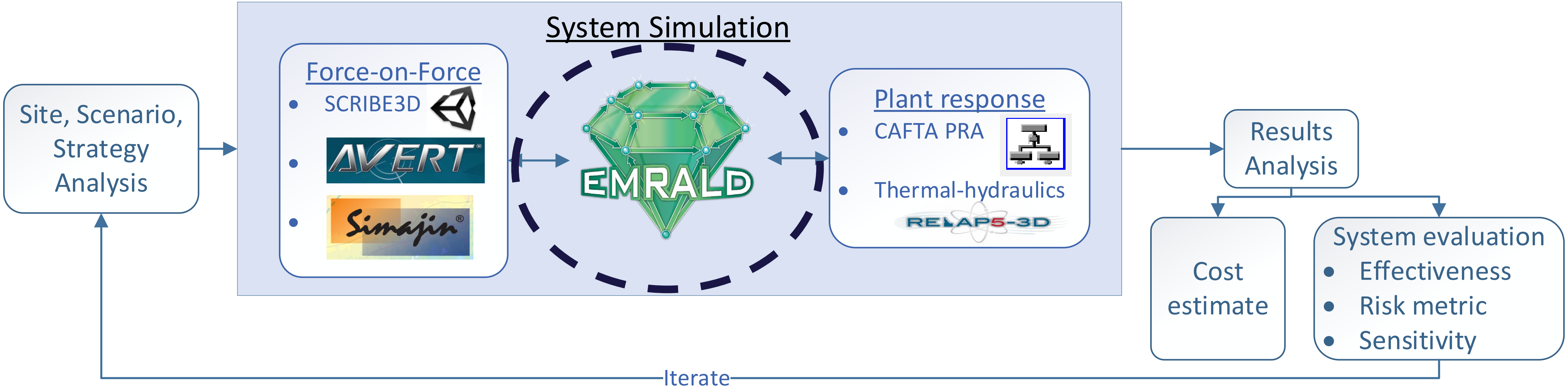
INL/MIS-23-73355

International Nuclear Security
Reducing Risk of Nuclear Terrorism

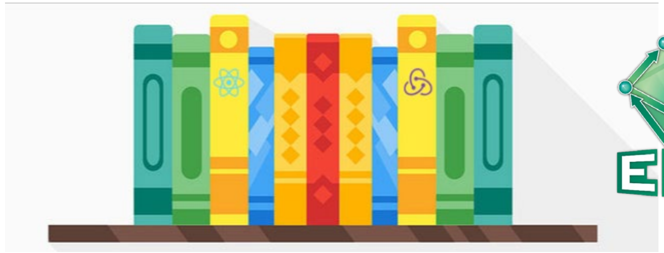
Overview

- Develop a **dynamic methodology** to evaluate physical security
  - Allow dynamic scenarios with timing uncertainties
- **Leverage existing work** for light-water reactors (LWRs) using Event Modeling Risk Assessment using Linked Diagrams (EMRALD) tool
  - Include preventive safety procedures and analysis
  - Allow rapid scenario assessments using templates
- **Relevance to INS**: enables stakeholders to design and/or analyze A/SMR security risks using ModSim by considering safety and security features

Methodology



EMRALD Libraries



Barriers

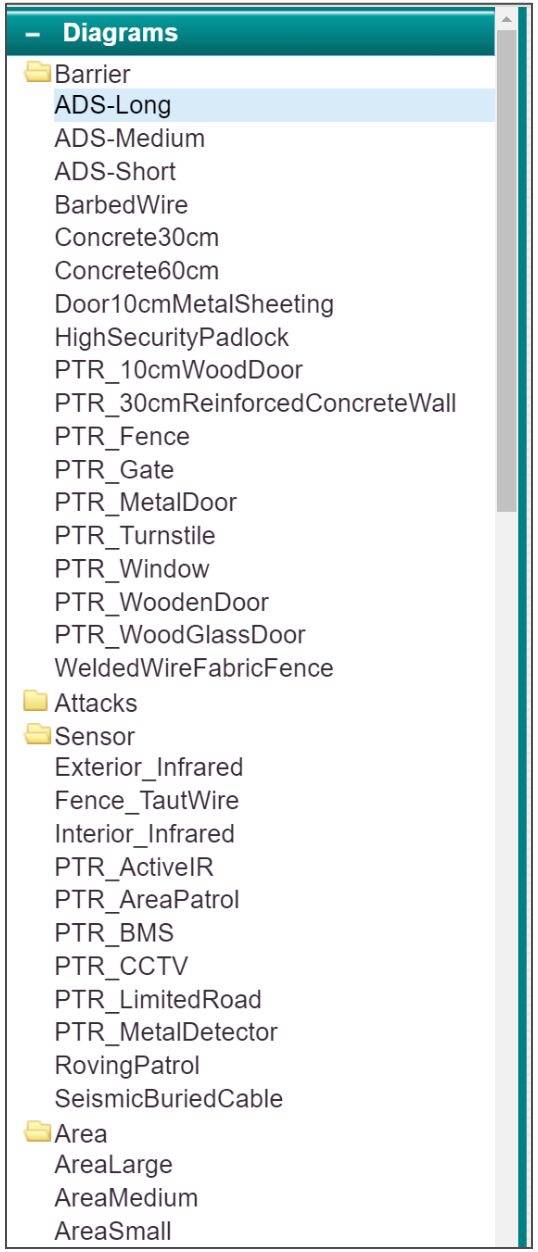
- Fences
- Sticky Foam
- Concrete Walls
- Security Doors
- Active Delay Systems
- Etc.

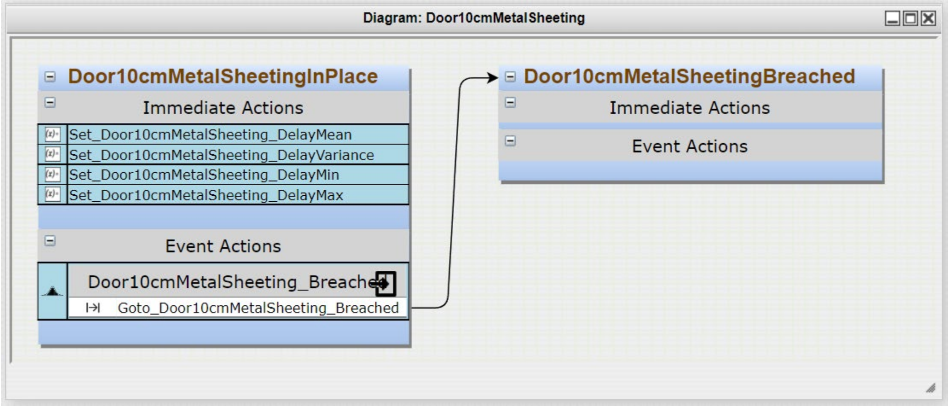
Properties

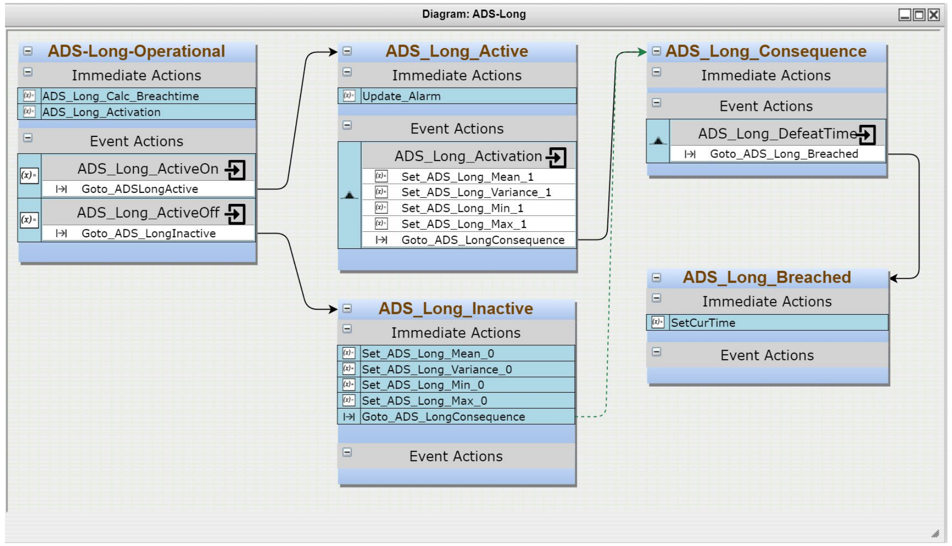
- Delay Time
- Equipment Requirements
- Detection Probability
- Etc.

Specific reactor design features

- Above / below grade
- Flood reactor area
- Passive safety systems
- Etc.







International Nuclear Security
Reducing Risk of Nuclear Terrorism

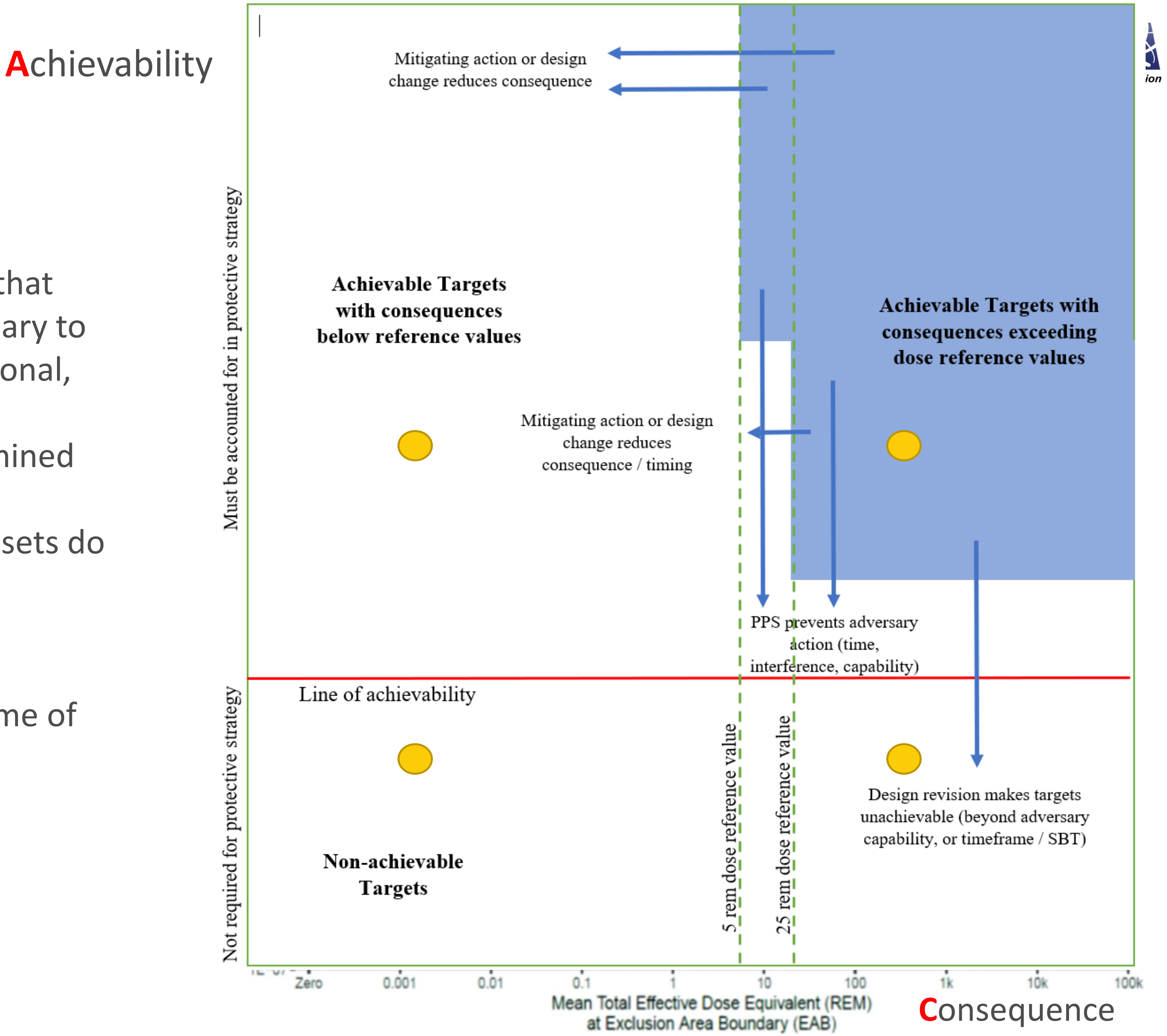
National Nuclear Security Administration

A/C Output

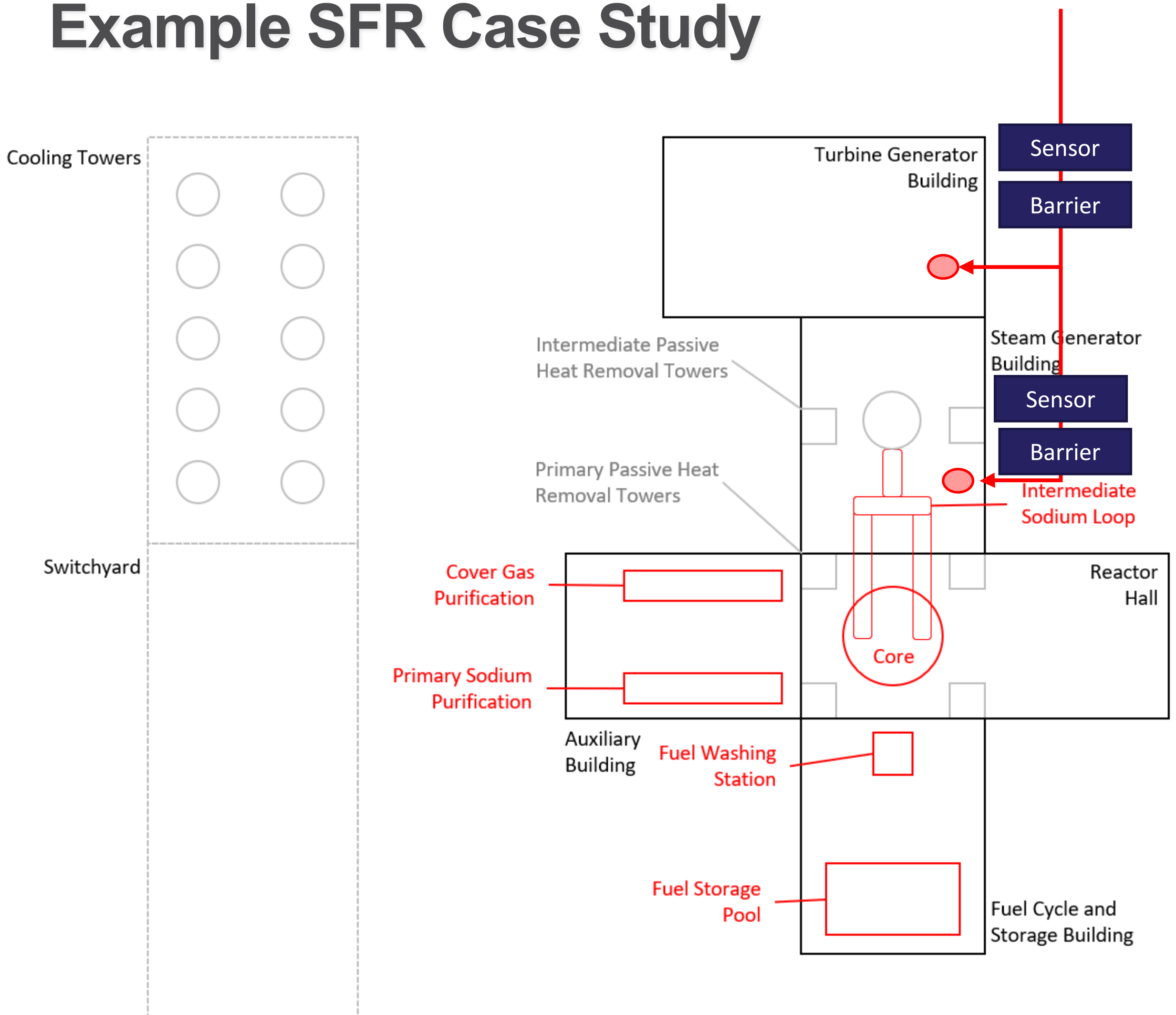
From RG 5.81 Rev 1:

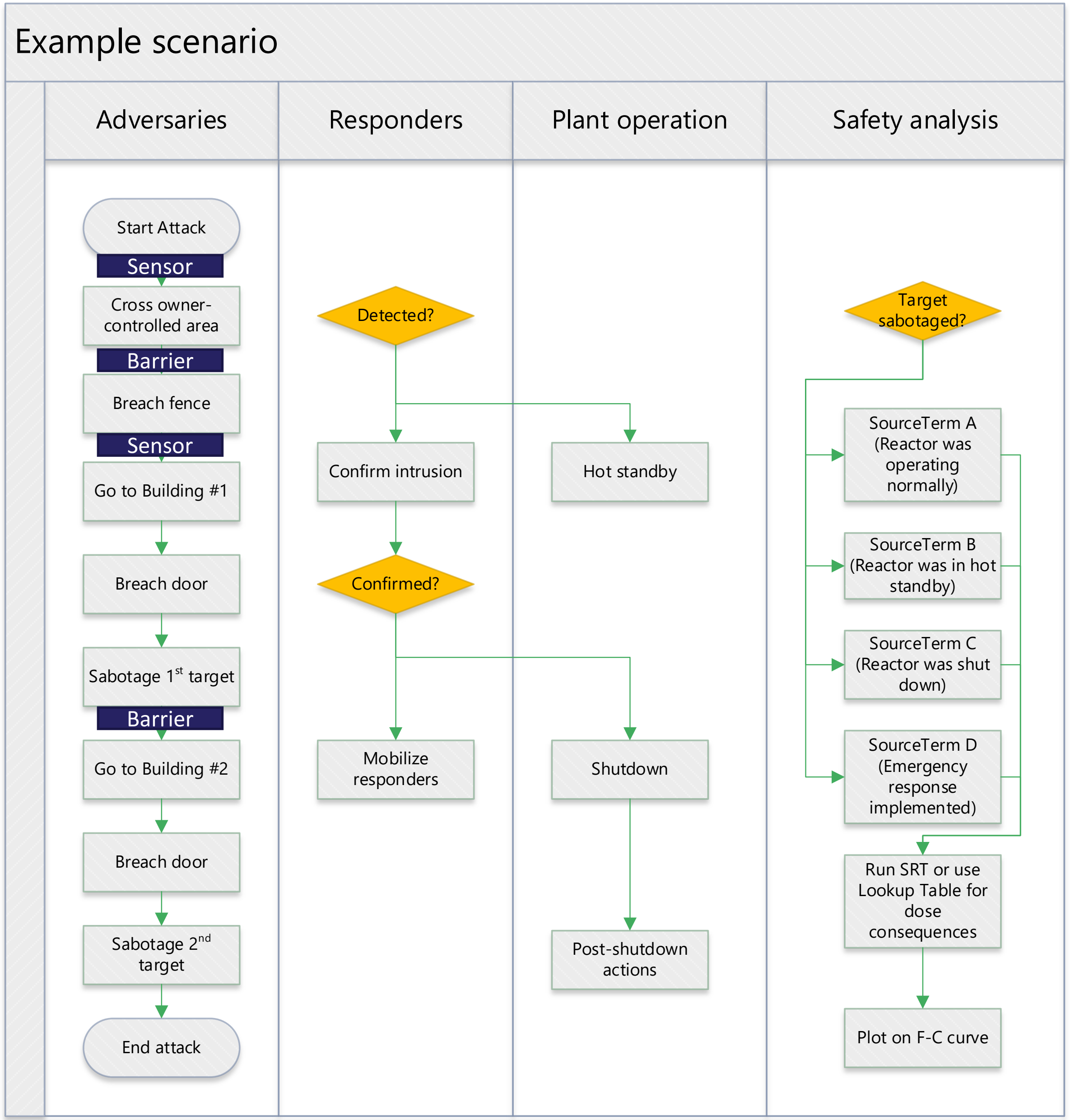
- Achievable target set elements are those that are within the capabilities of a DBT adversary to compromise, destroy, or render nonfunctional, independent of response strategy.
- Achievable target set elements are determined by the capabilities of the DBT adversary.
- The definition and development of target sets do not consider the success of the security organization.

We also use a SBT / RAPT to define a timeframe of achievability.



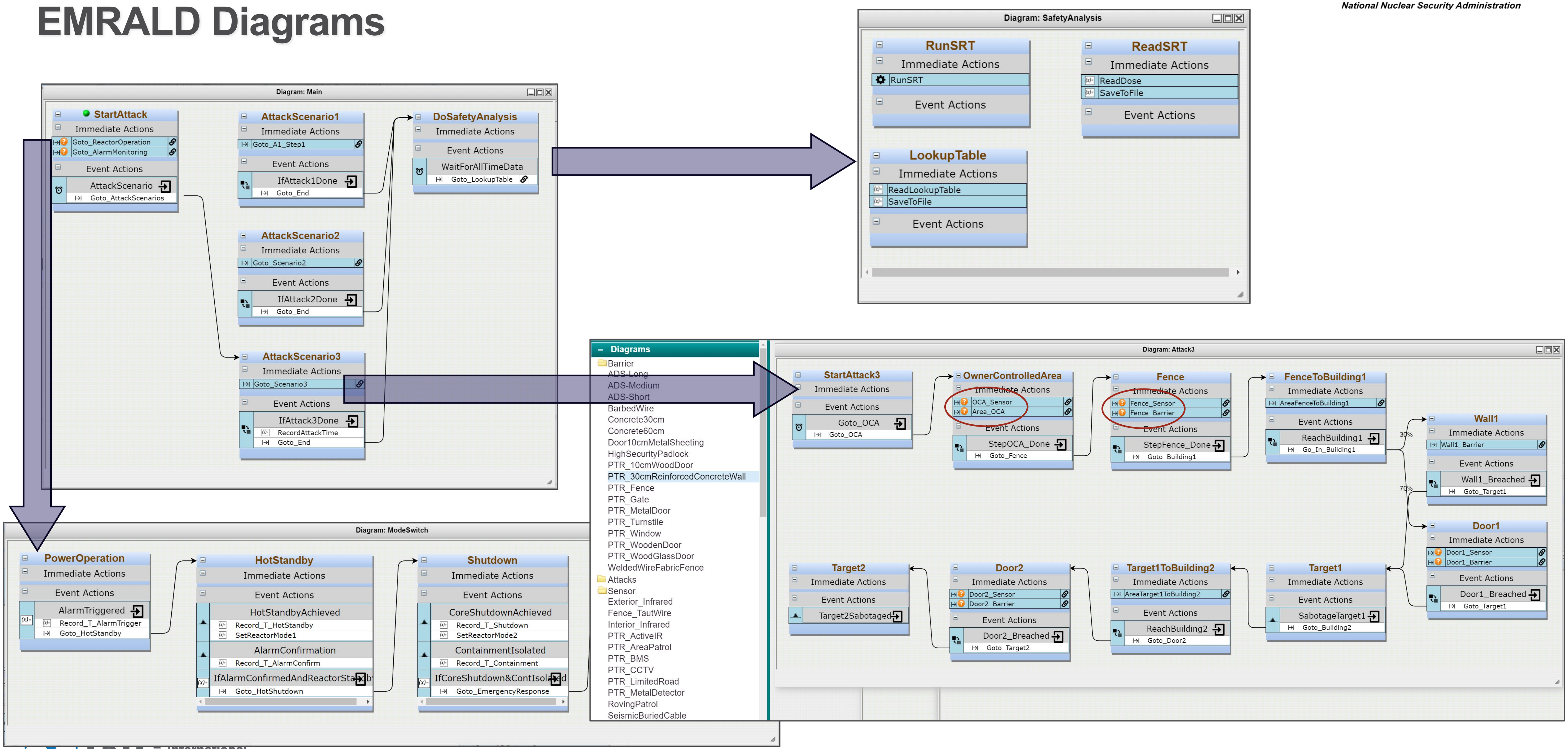
Example SFR Case Study



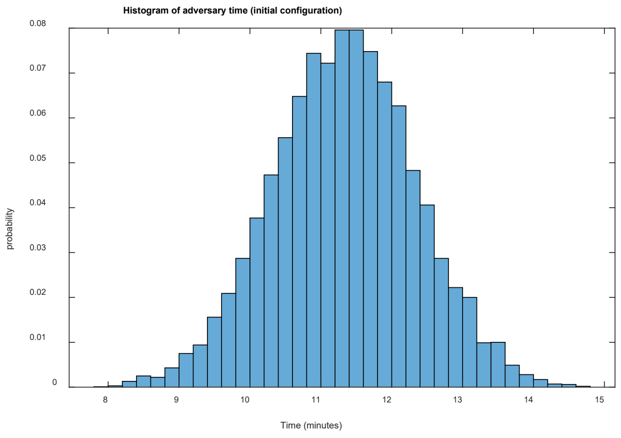


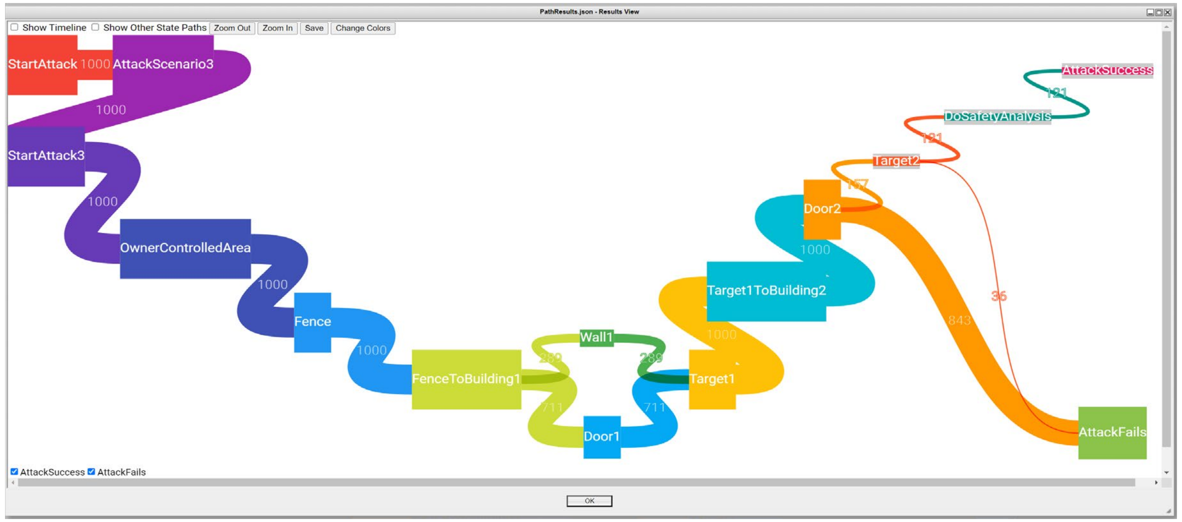
Disclaimer:
Facility drawing, targets, and scenario are hypothetical, and do not represent any actual nuclear power plant.

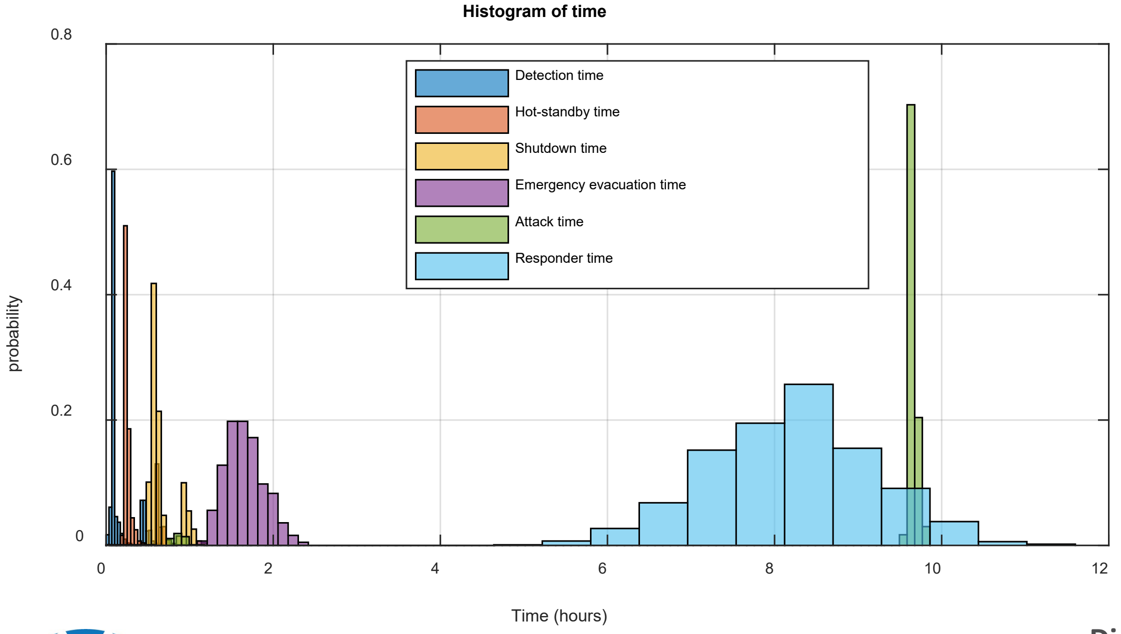
EMRALD Diagrams

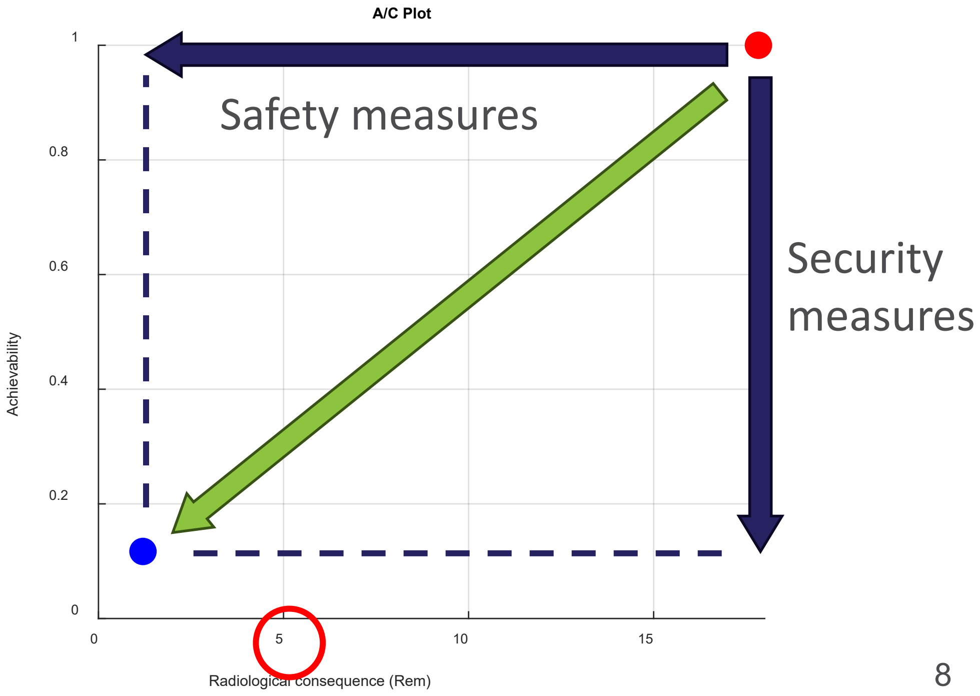


Results









Disclaimer
Results are from a hypothetical case study, and do not represent any actual nuclear power plant.

Conclusion

- Proposed a security-safety (2S) methodology to assess A/SMR security risks
- Added new capabilities to EMRALD to support rapid estimation of A/SMR security risks
- Continue work into FY24 to run scenarios on example SFR and HTGR models, tweak and/or add templates, & gain insights
- Work will benefit A/SMR vendors during the design iteration phase

Research Team

- INL: Robby Christian, Steve Prescott, Christopher Chwasz, Shawn Germain, Vaibhav Yadav
- ANL: Dave Grabaskas, Matthew Bucknor
- X-Energy (non-funded SME)

Appendix Slides

- These slides are just for backup

National Nuclear Security Administration

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

SFR Preventive Actions

Stages of Intrusion	Sources of Radioactivity					
	Core	Primary Sodium Purification System	Cover Gas Purification System	Fuel Washing Station	Fuel Storage Facility	Intermediate Sodium Loop
Detection[1]	• Power runback (or Hot Standby)	• Closure of isolation valves • Shutdown of system	• Closure of isolation valves • Shutdown of system	• Cessation of any fuel washing activities	• Cessation of any fuel movement activities	(see core)
Confirmation[2]	• Reactor Shutdown • Containment Isolation • Transition to passive heat removal system (shutdown of BOP)	• Cell HVAC isolation • Cold trap cooling switched to emergency power	• Cell HVAC isolation • Decay bed cooling switched to emergency power	• Washing station HVAC isolation	• Facility HVAC isolation • Spent fuel pool cooling power switched to emergency power (or passive cooling)	• Shutdown of intermediate sodium pumps
Sabotage[3]	• Remote control room activation • Emergency response implementation[4]	• Emergency response implementation[4]	• Emergency response implementation[4]	• Activate emergency mercury flood system • Emergency response implementation[4]	• Emergency response implementation[4]	• Activate intermediate sodium loop drain • Emergency response implementation[4]

[1] Assumption that detection has certain level of confidence (*i.e.*, multi-sensors, etc.).

[2] Confirmation of site intrusion.

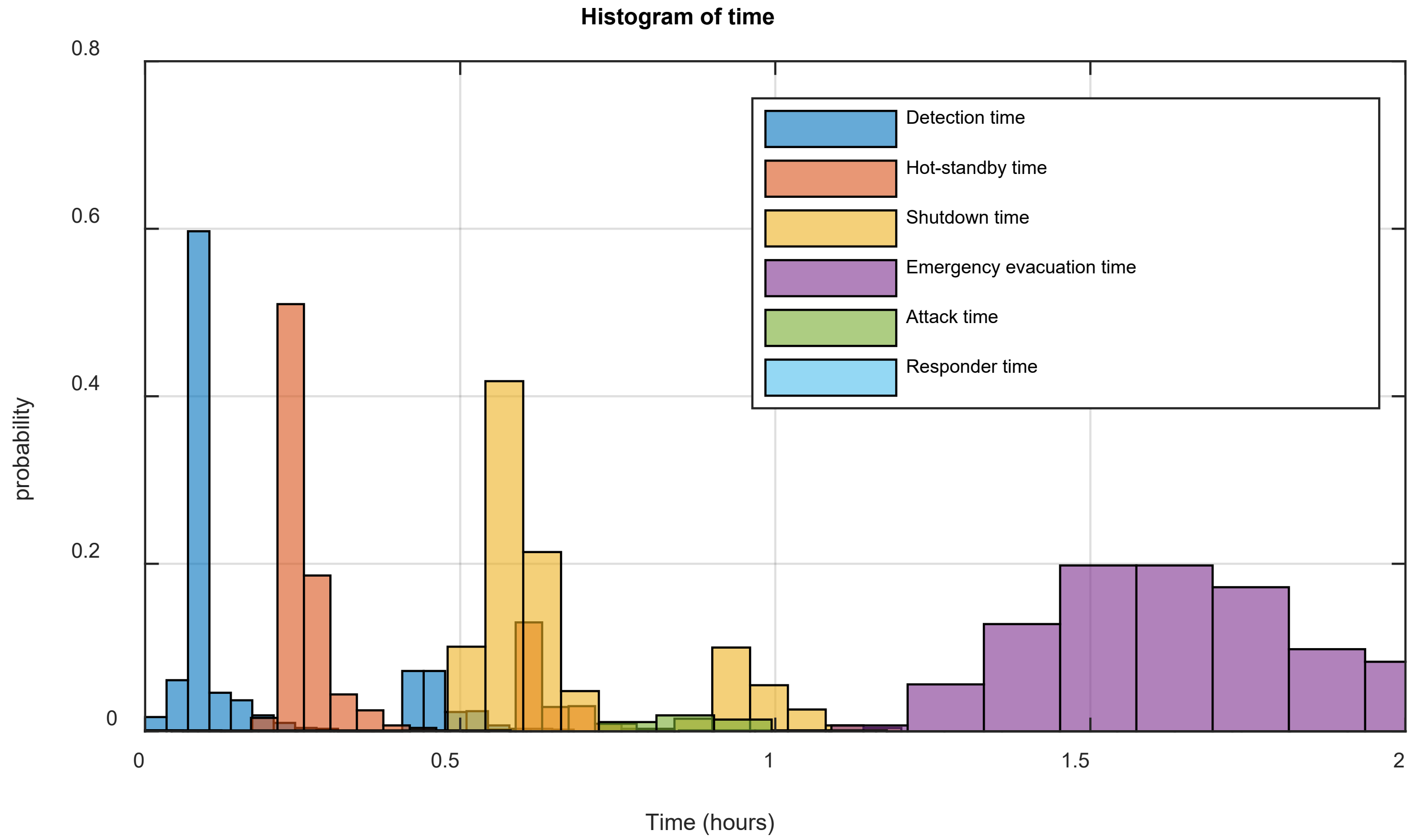
[3] If sabotage is related to the designated radionuclide source.

[4] As described in the plant's emergency plan. Includes protective actions and other emergency response measures for workers and public.

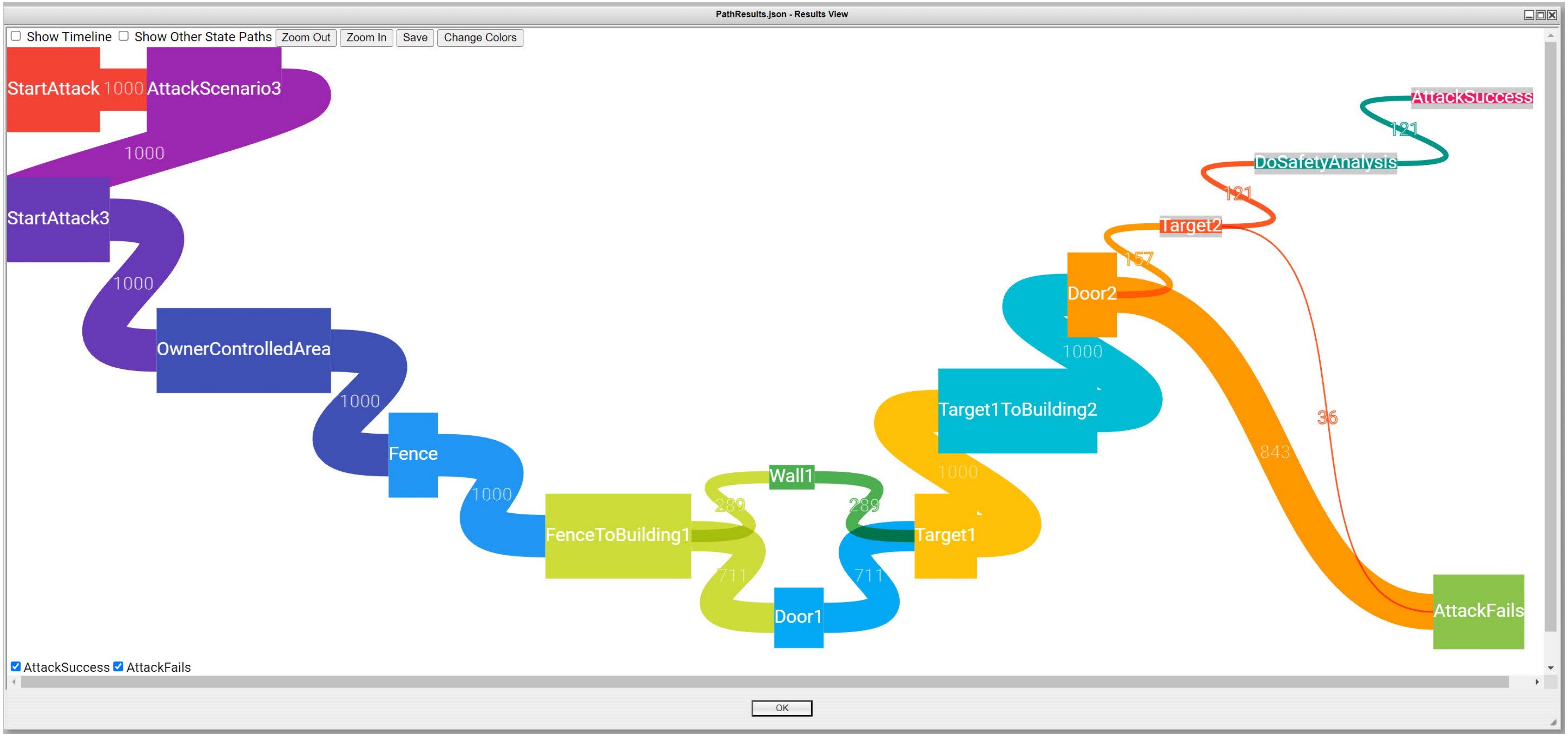
Case Study Results

Attack Outcome		Reactor State	Probability	Radiological Consequence (Rem)
Attack fails due to timely interruption		Reactor full power	88.3%	0
Attack successful	Sabotage completed after preventive actions	Reactor is shut down, and nearby population is evacuated	7.2 %	2E-2
	Sabotage completed before preventive actions	Reactor is shut down	3.6 %	2.07
	Sabotage completed before detection was confirmed	Reactor hot standby	0.9%	7.1
	Sabotage goes undetected	Reactor full power	0 %	17.83

Histogram up to 2 Hours



Scenario Flow Diagram



INS International Nuclear Security

Reducing Risk of Nuclear Terrorism