Opportunities for the Application of Artificial Intelligence in Physical Security Risk Assessment

Matthew Zerphy
Assistant Dean for Operations, College of Engineering
Professor of Practice, Ken and Mary Alice Lindquist Department of Nuclear Engineering
Nuclear Security Education Program – University Park and Penn State World Campus
Affiliate - PSU Law, Policy, and Engineering
Advisor - PSU Chapter, Institute of Nuclear Materials Management (INMM)
mxz206@psu.edu

WORLD INSTITUTE FOR NUCLEAR SECURITY

Introduction to the Role of Artificial Intelligence in Strengthening the Security of Nuclear Facilities
06 February 2024 - 08 February 2024
Vienna, Austria

Ken and Mary Alice Lindquist
Department of Nuclear Engineering

PennState
College of Engineering

Nuclear Security Risk Assessment

- Risk is the potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences (NSS No. 24-G).
  - Risk is a function of the Threat, the Vulnerabilities, and the Consequences
  - It is common practice to assume that threats will materialize at some time and result in an attack ($P_{attack} = 1$)
- Threat
  - A person or group of persons with motivation, intention and capability to commit a malicious act (NSS No. 13)
- Vulnerability
  - A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat (NSS No. 24-G)
- Consequences
  - Potential negative impacts on people, property and the environment resulting from a nuclear security event

https://www.wins.org/document/2-6-assessing-and-communicating-nuclear-security-threats/

Nuclear Security Threat Attack Vectors

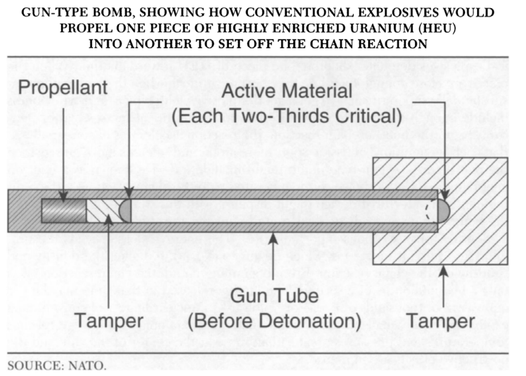
- Attack/Sabotage
- Theft (for subsequent attack)

NFK: Nuclear Facility Kinetic

SND/BND: Stolen/Bought Nuclear Device

"SADM"

IND: Improvised Nuclear Device



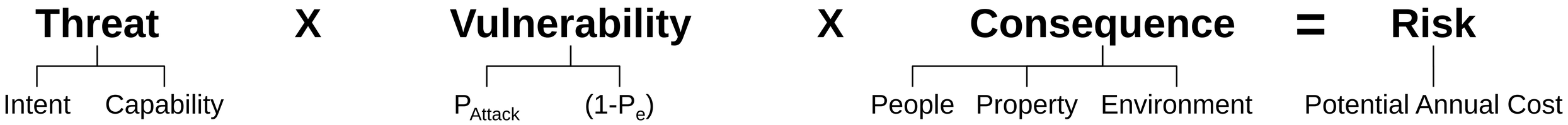
INSIDER THREAT

NFC: Nuclear Facility Cyber (primary or enabling)

RED: Radiation Exposure Device

RDD: Radiological Dispersal Device ("Dirty Bomb")

Nuclear Security Risk Assessment

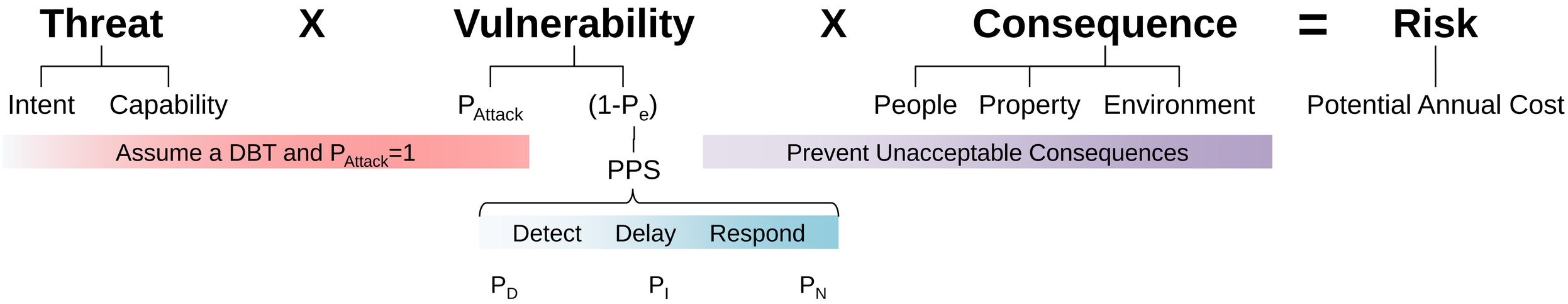


- **Risk**
  - The potential for an unwanted outcome resulting from a nuclear security event as determined by its likelihood and the associated consequences.
  - *Risk is a function of the Threat, the Vulnerabilities, and the Consequences.*
- **Risk Assessment**
  - The overall process of systematically identifying, estimating, analysing and evaluating risk for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, Implementing Guide, IAEA Nuclear Security Series No. 24-G

Developing a National Framework for Managing the Response to Nuclear Security Events, Implementing Guide, IAEA Nuclear Security Series No. 37-G

Nuclear Security Risk Assessment



Nuclear Security Risk Assessment

Threat (Intent, Capability) **X** **Vulnerability** (P_{Attack}, $(1-P_e)$) **X** **Consequence** (People, Property, Environment) **=** **Risk** (Potential Annual Cost)

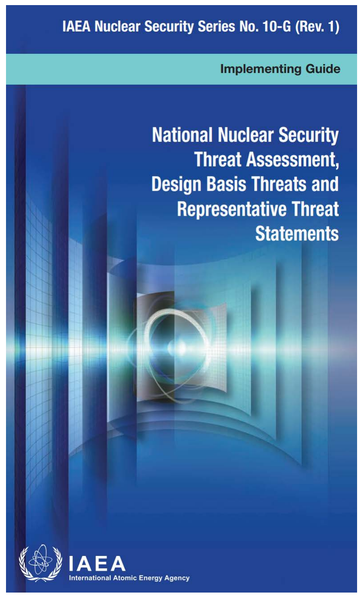
Assume a DBT and $P_{Attack}=1$

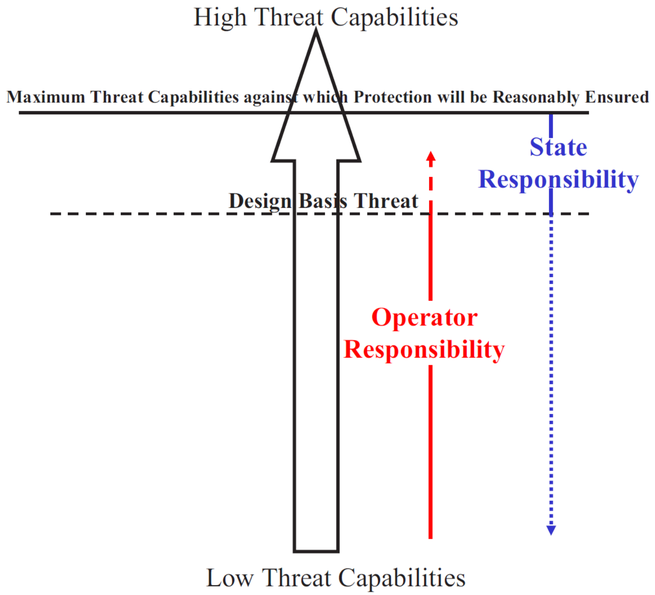
PPS: Detect, Delay, Respond

P_D P_I P_N

Prevent Unacceptable Consequences

- Design Basis Threat (DBT) - The attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated.



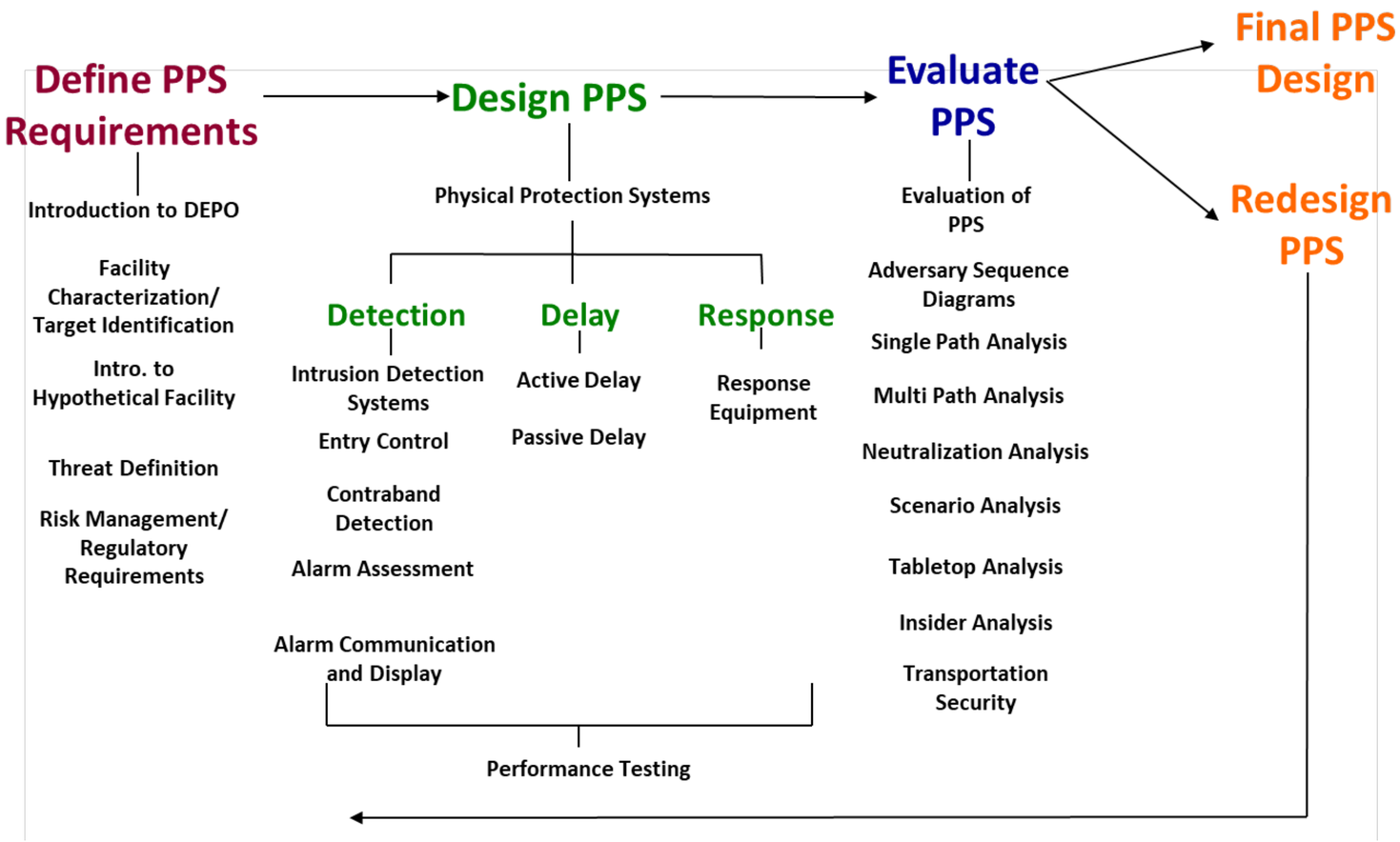


Simulation of tank attack via main entrance to Zaporizhzhia NPP, similar to Russia attack 03Mar2022.

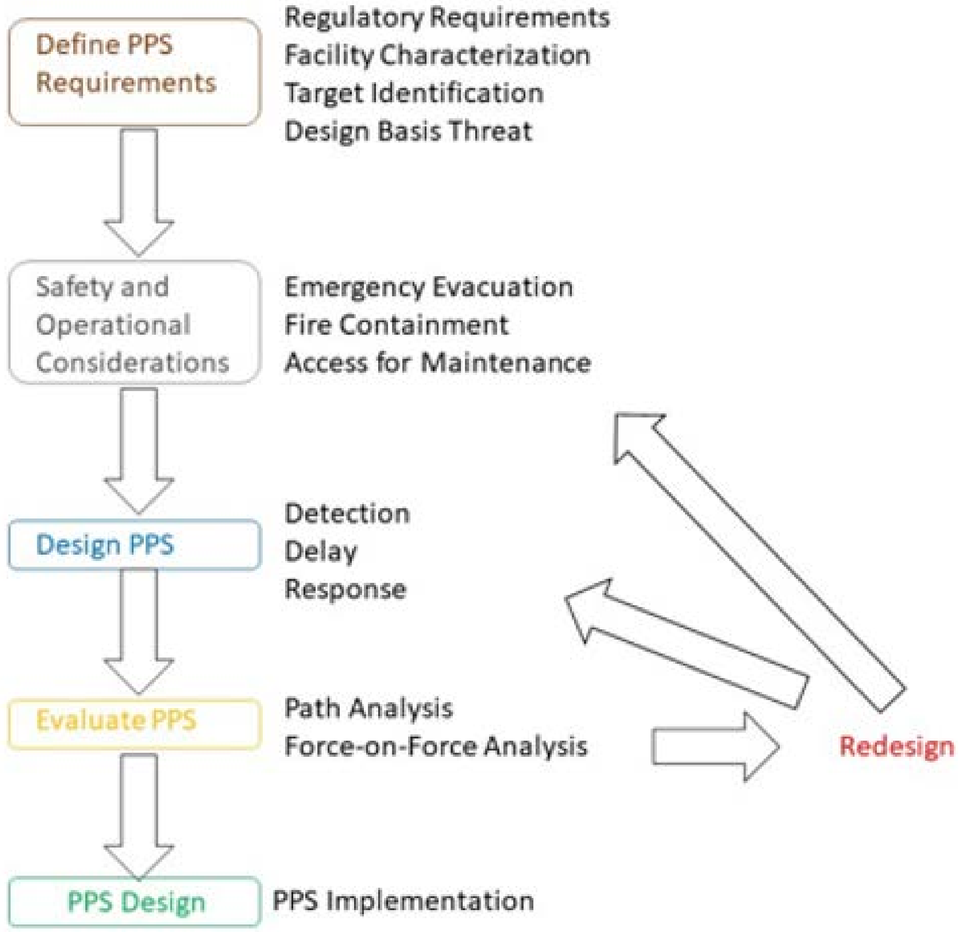
Force-on-Force (FoF) exercise with security guards at the FirstEnergy Davis-Besse reactor near Toledo, OH train with laser weapons simulators.

Protesters demonstrate against atomic energy in front of the nuclear plant in Biblis, western Germany, on April 29, 2006, on the 20th anniversary of the Chernobyl nuclear plant accident. Thomas Lohnes/DDP/AFP VIA Getty Images

Design and Evaluation Process Outline (DEPO) and Security-by-Design (SeBD)



Design Evaluation Process Outline (DEPO) Methodology developed by Sandia National Laboratories.



Modified DEPO Methodology for Security-by-Design. "U.S. Domestic Sodium Fast Reactor: Security-by-Design." Evans, A. Sandia National Laboratories. SAND2023-09146R

Nuclear Security Risk Assessment

Threat X **Vulnerability** X **Consequence** = **Risk**

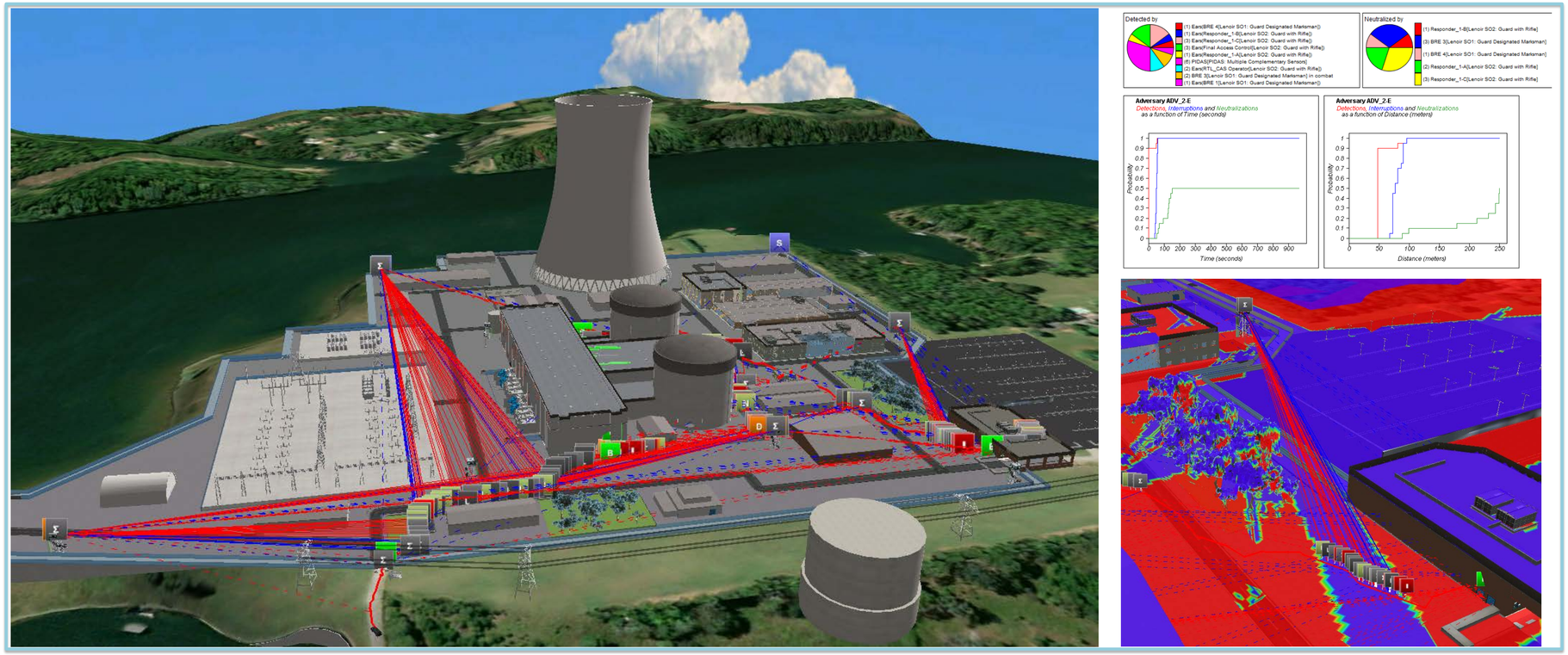
- Threat: Intent, Capability
- Vulnerability: P_{Attack}, $(1-P_e)$
- Consequence: People, Property, Environment
- Risk: Potential Annual Cost

Assume a DBT and $P_{Attack}=1$

Prevent Unacceptable Consequences

PPS: Detect, Delay, Respond

P_D P_I P_N



J. Raines, M. Zerphy, C. (Yeager) Eveland, and P. Zahnle, "AVERT 4 Universities (A4U) Program Support to The Pennsylvania State University," in Proceedings of the INMM & ESARDA Joint Annual Meeting (2021), https://resources.inmm.org/system/files/annual_meeting_proceedings/a359.pdf.

Nuclear Security Risk Assessment

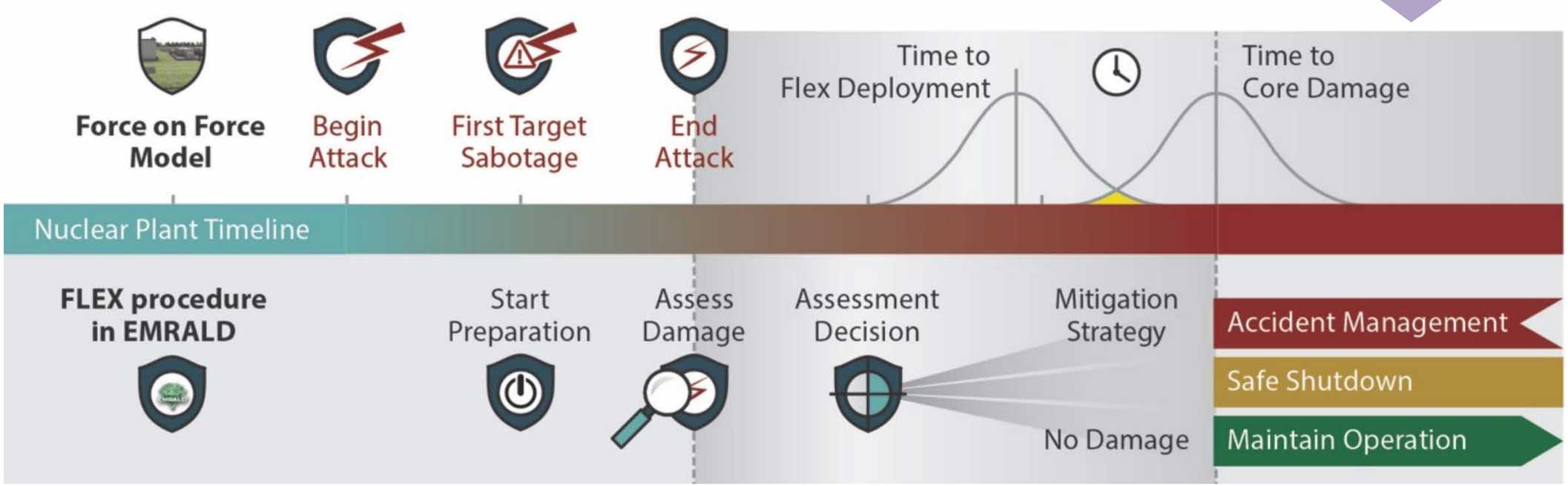
Threat X **Vulnerability** X **Consequence** = **Risk**

Intent, Capability | P_{Attack}, $(1-P_e)$ | People, Property, Environment | Potential Annual Cost

Assume a DBT and $P_{Attack}=1$

PPS: Detect, Delay, Respond

Prevent Unacceptable Consequences



- Figure 9. FOF-FLEX integration framework using AVERT-PS and EMRALD
  - Christian, Robby, Yadav, Vaibhav, St Germain, Shawn W, Weathersby, John H, and Prescott, Steven R. 2020. "Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling". United States. https://www.osti.gov/servlets/purl/1670433.

Nuclear Security Risk Assessment

Threat X **Vulnerability** X **Consequence** = **Risk**

Intent, Capability | P_{Attack}, $(1-P_e)$ | People, Property, Environment | Potential Annual Cost

Assume a DBT and $P_{Attack}=1$

AI could enable consideration of a range of potential threats.

AI can enable real-time I&W.

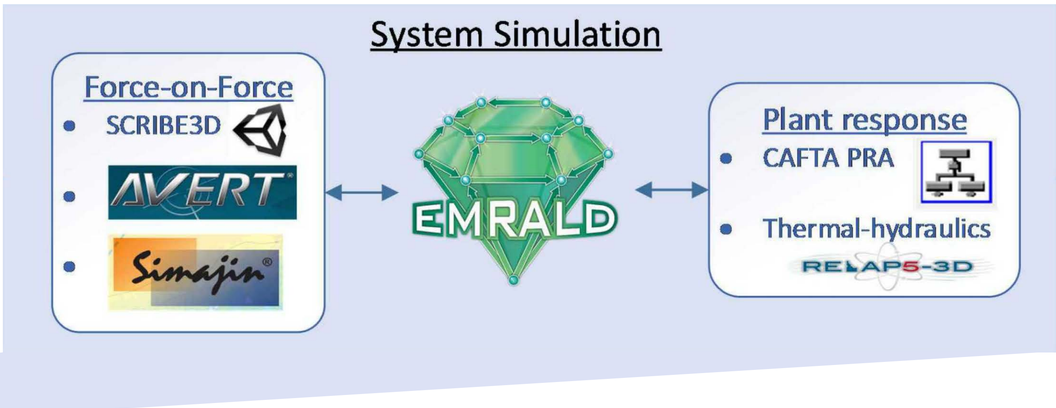
PPS

Detect Delay Respond

P_D P_I P_N

Excellent AI work in this area – AI to integrate into PPS mod/sim.

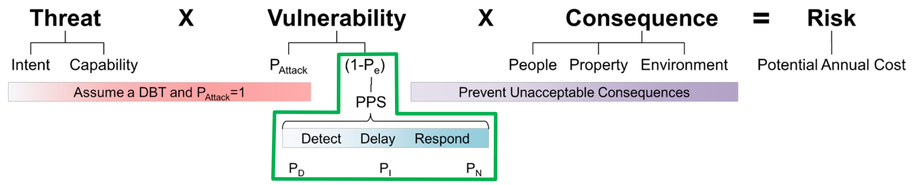
Prevent Unacceptable Consequences

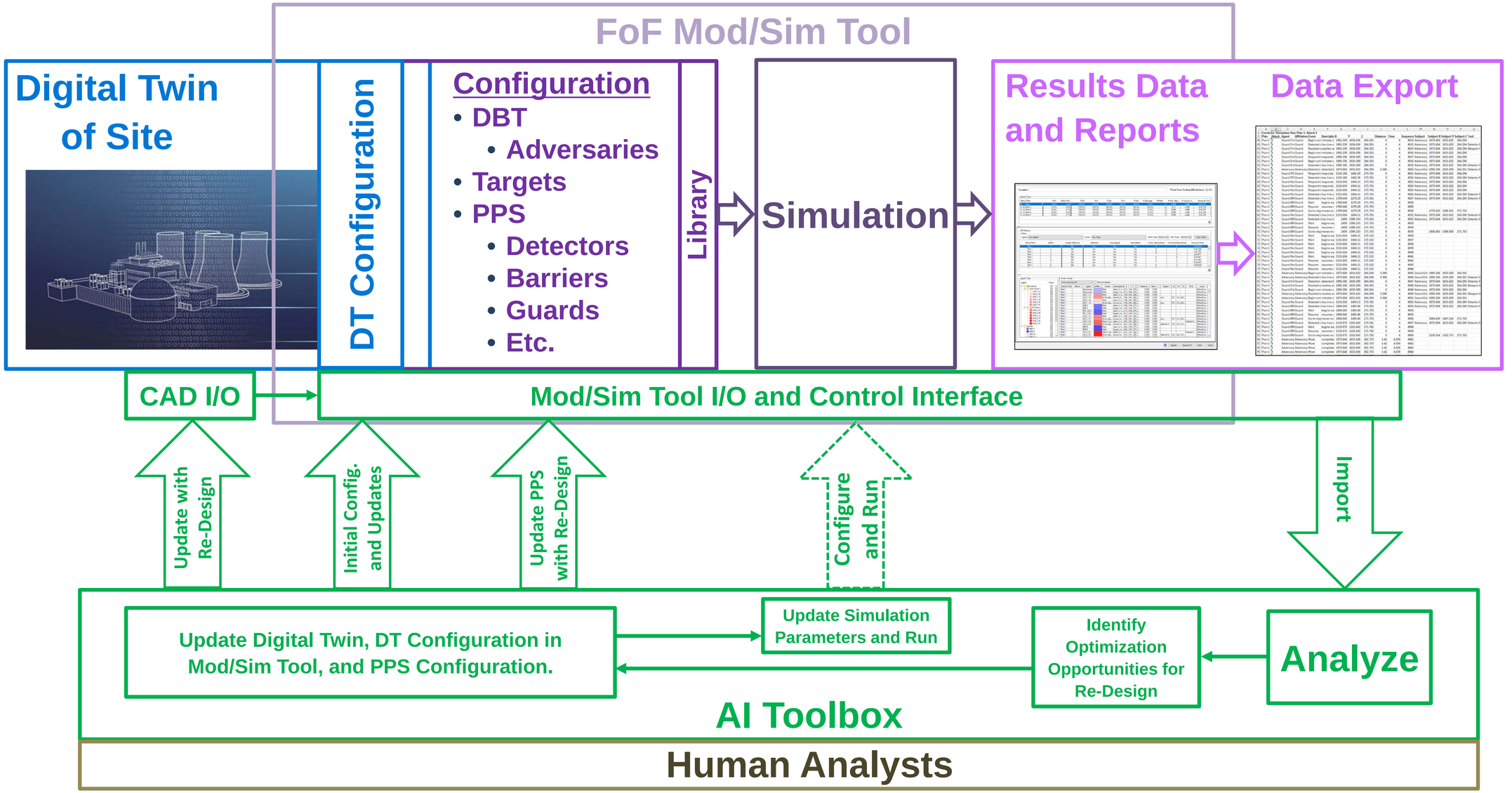


Digital Twin of Site	Automate import and configuration (topography, site, and plant)
Agents (Guards and Adversaries)	Analyze and recommend (e.g., Guard placement, armament, ROE, etc.)
Algorithms	Algorithms (enhanced agent advanced behaviors)
Library	Library (add new items and analyze parameters)
Results Data and Reports	Results Data and Reports (analysis and optimization feedback)
Reactor Simulator	Integration and analysis of new designs (e.g., microreactor)

Opportunities for AI Support to PPS Mod/Sim

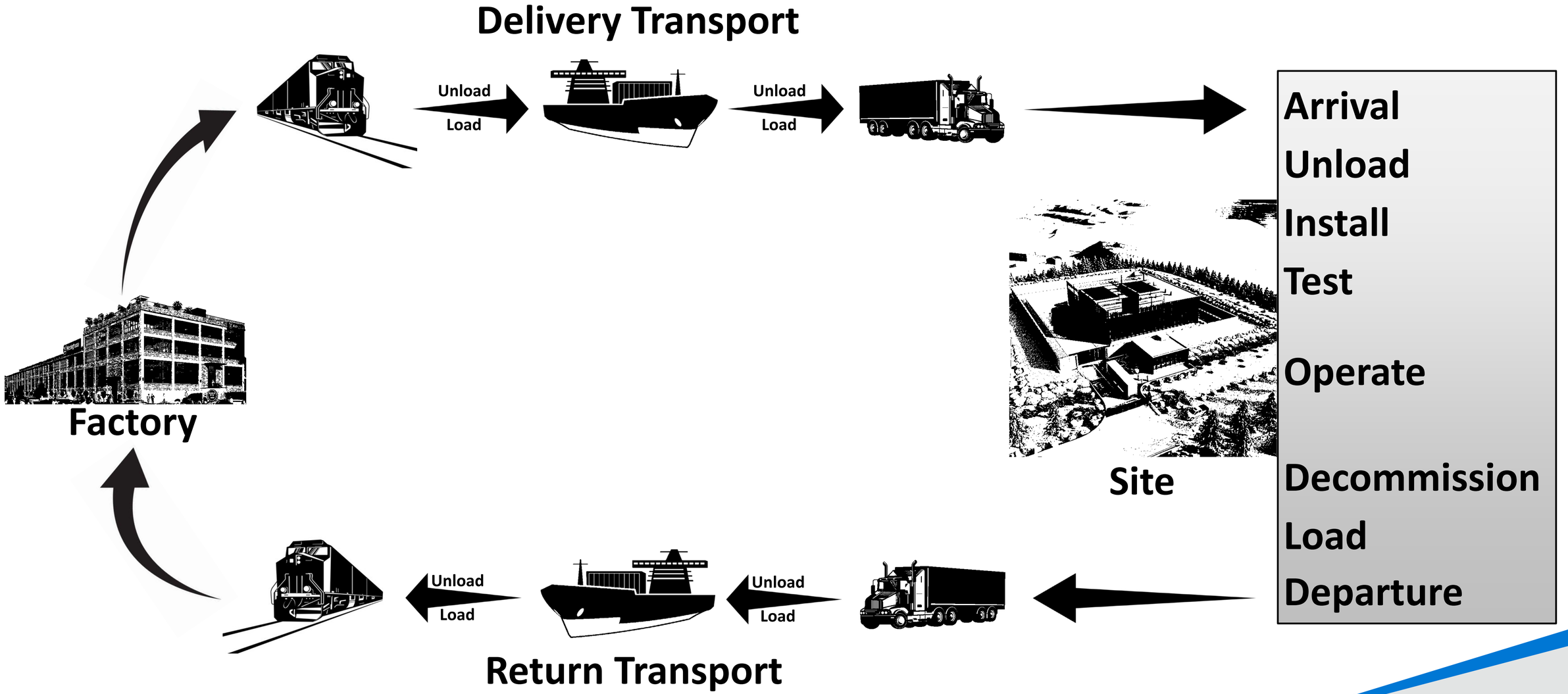
AI Tools Applied to Proven FoF Mod/Sim Tools





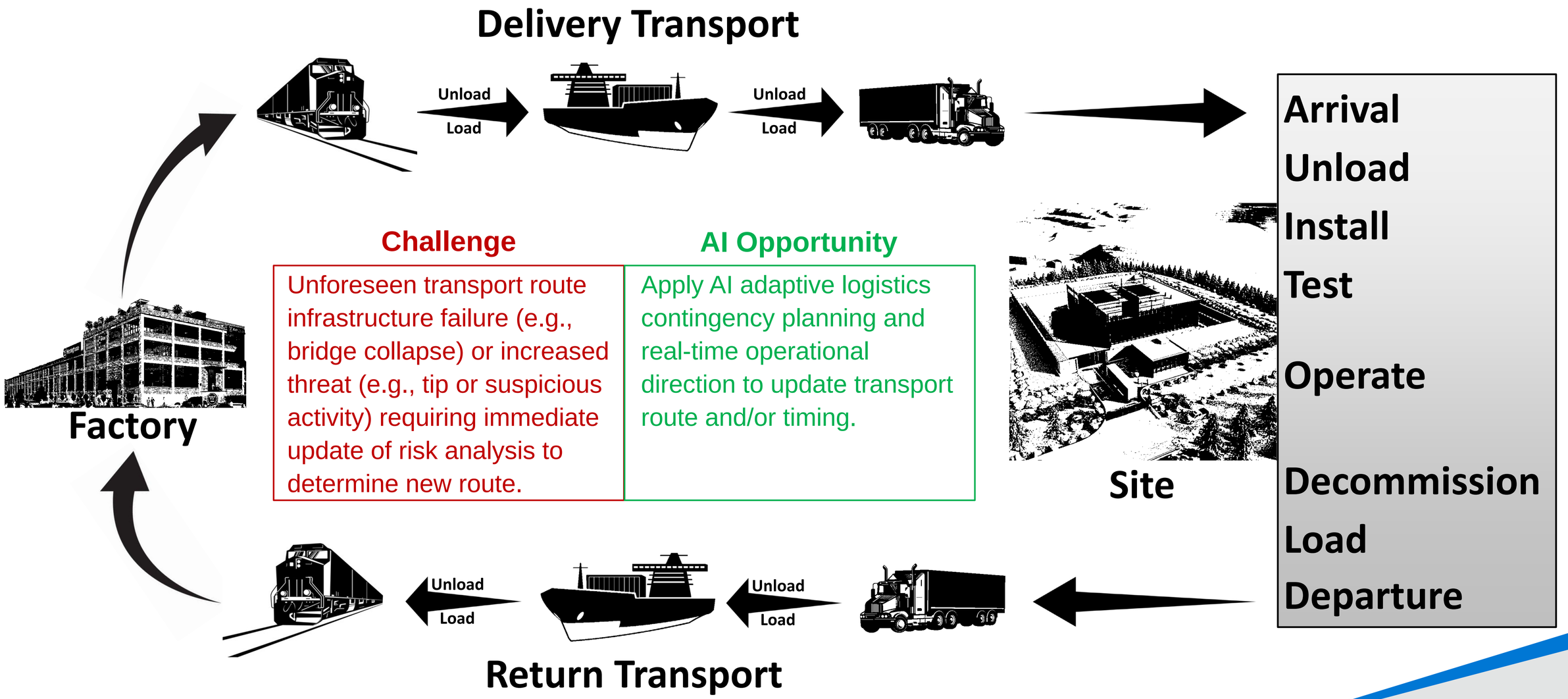
Microreactor Deployment Lifecycle Risk Assessment

- At least 20 separate physical security analyses for this example.
- Compounded by variety of MR designs, site configurations, deployment types/locations



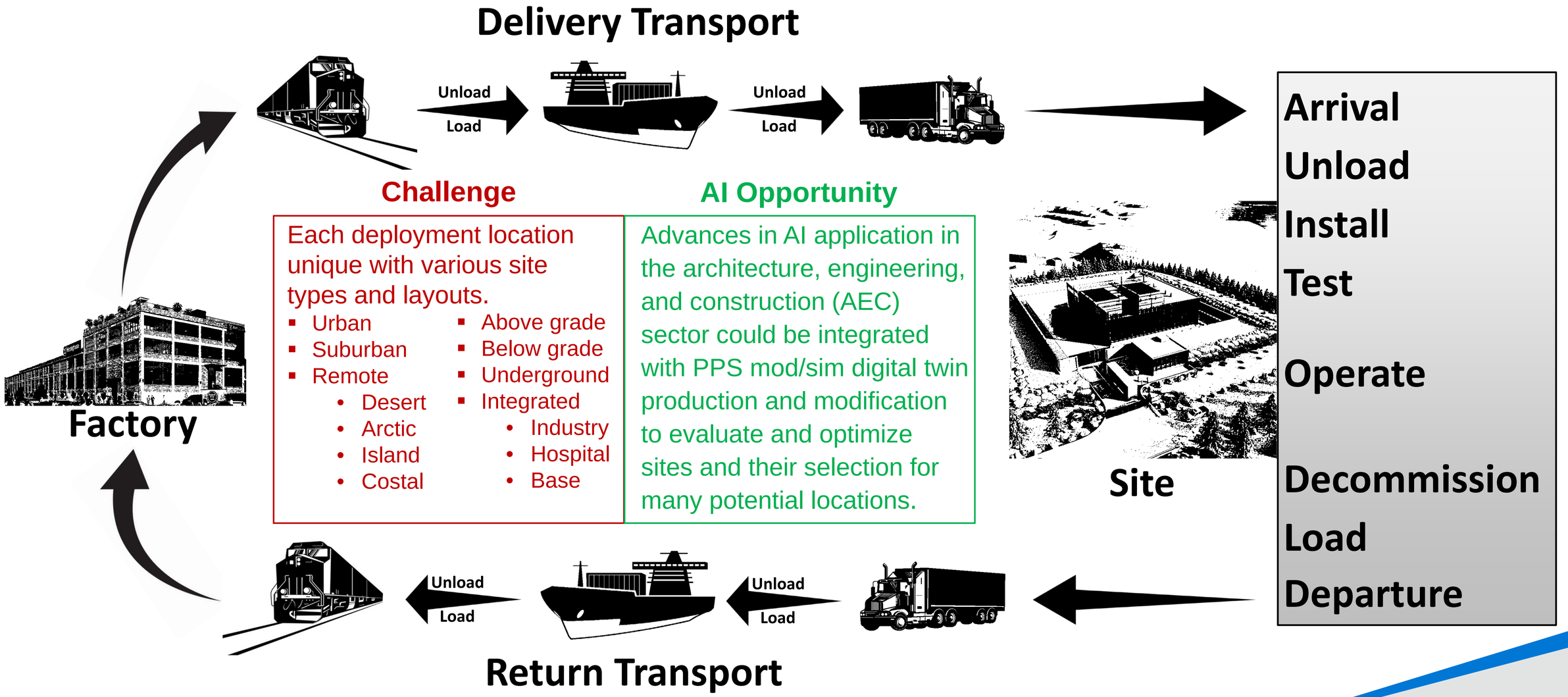
Microreactor Deployment Lifecycle Risk Assessment

- Delivery transport could involve MR with fresh or irradiated fuel.
- Spent MR remains on site while ‘new’ MR is delivered for continuous site operations.



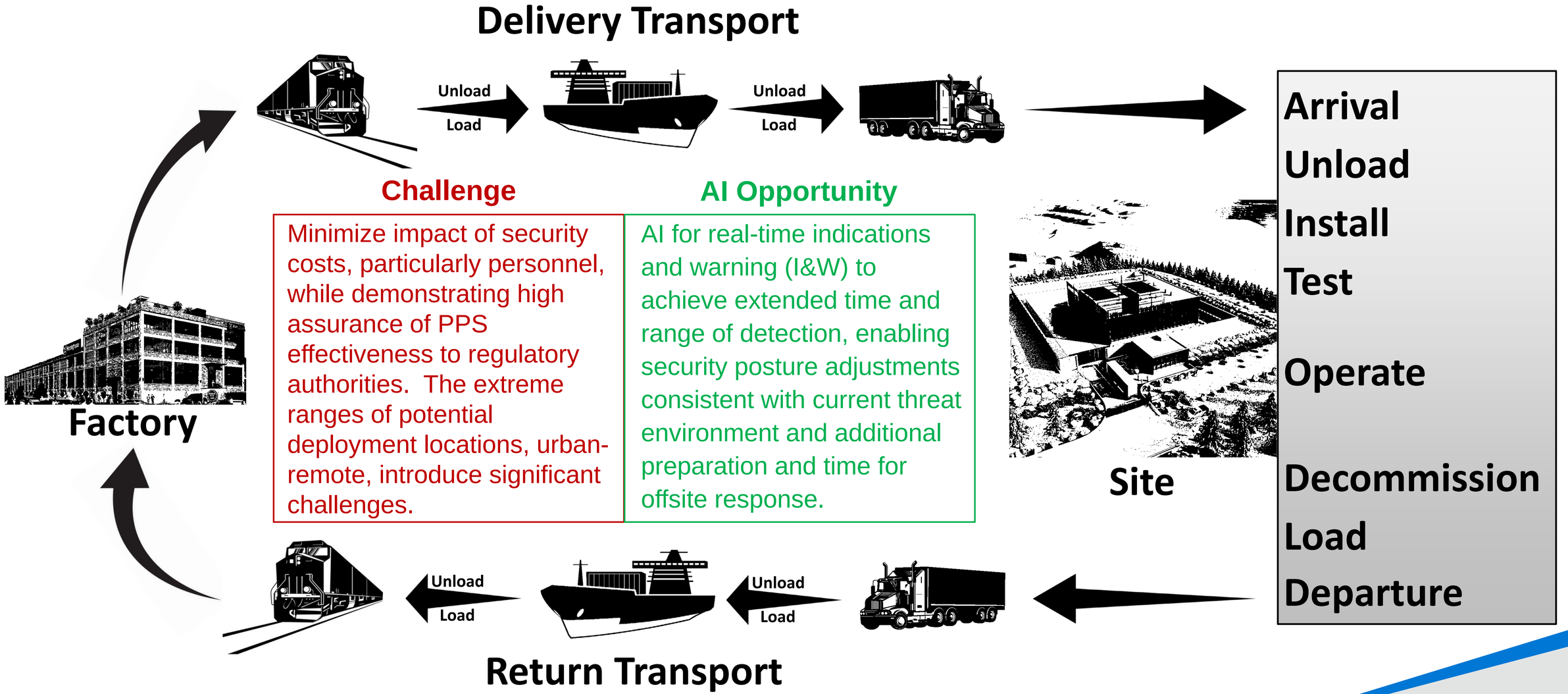
Microreactor Deployment Lifecycle Risk Assessment

- Deployment at-scale with many MR designs deployed to a variety of locations for a range of uses requires the ability to perform many risk assessments quickly for regulatory review/approval.



Microreactor Deployment Lifecycle Risk Assessment

- Minimize security costs throughout a wide range of deployment variables.



Applying AI to Nuclear Security Risk Assessment

- There are many opportunities to apply AI across all variables of nuclear security risk assessment.
- AI support to existing, proven methodologies and tools can:
  - Enable more comprehensive risk assessments
    - Analysis across the full range of risk variables
  - Reduced the time to perform analyses
    - Particularly helpful to support:
      - Advanced reactor deployments at-scale
      - Rapidly evolving security situations such as armed conflict
  - Discovery of previously unseen vulnerabilities and opportunities
    - Keep pace with evolving technologies (threat, response, and new designs)
  - Maintain ability of regulatory authorities to review and approve security plans
    - Mitigate AI ‘black box’ concerns
- Successful AI support to analysis in other disciplines and industries can be applied.
- Security of information must be maintained.
  - In most cases, AI tools should independently operate on host systems.

Questions for Discussion

- Where does AI benefit security risk assessments the most?
- What are the regulatory considerations for using AI in security risk assessments?
- Can artificial intelligence provide better inputs for analyzing nuclear security risk than traditional methods?