SAND2022-8024C

ADVANCED REACTOR SAFEGUARDS

3S-Informed Security for Next Generation Nuclear Facilities

ANS Annual Meeting

PRESENTED BY

Ben Cipiti & Alan Evans

June, 2022

SAND 2022-xxxC, 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.

Sandia National Laboratories | U.S. DEPARTMENT OF ENERGY

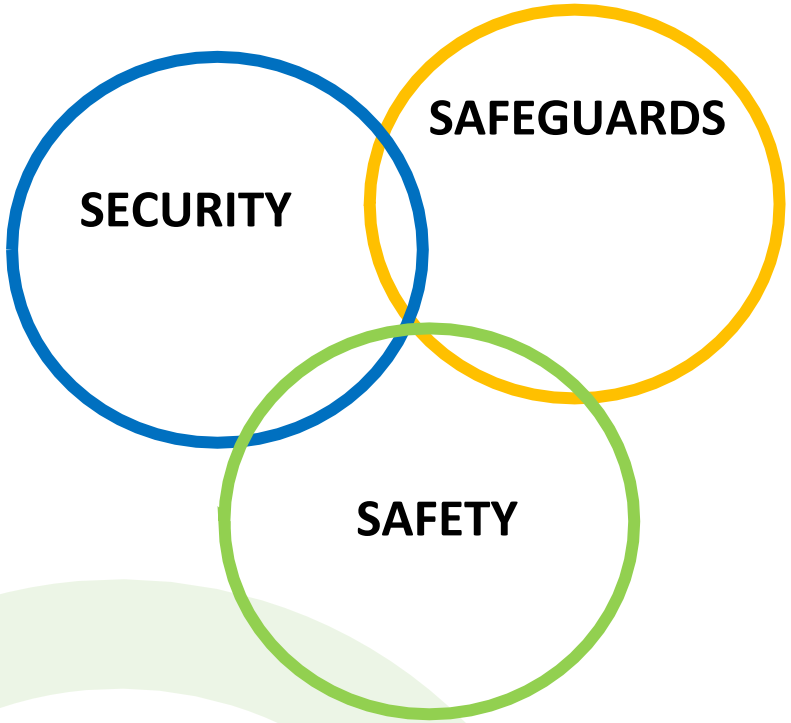
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

3S-Informed Engineering

- Next generation nuclear reactors and fuel cycle facilities are being developed with particular attention to Safety, Security, and Safeguards (3S) by Design.
- These reactors (and potentially fuel cycle facilities) are compact, utilize modular construction, and take advantage of enhanced safety.
- These compact facilities require 3S-informed approaches and more integrated thinking between the domains to develop efficient security designs.
- Early consideration of design requirements will help the nuclear industry avoid costly retrofits in the future.

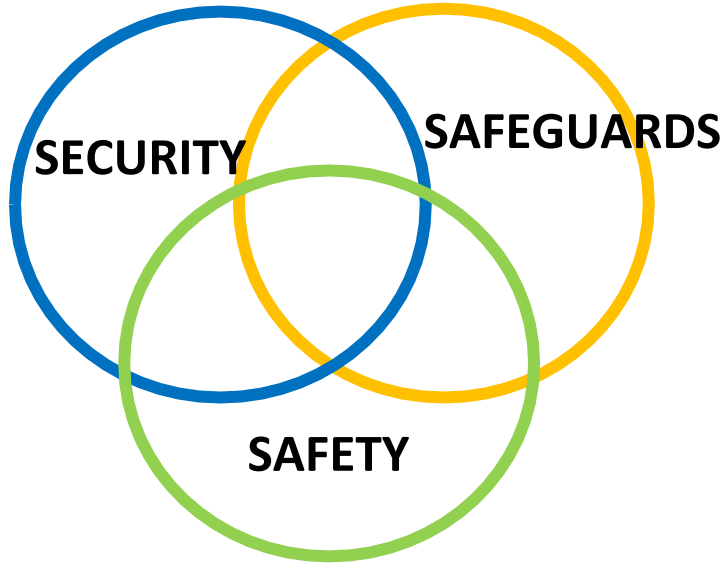
What's Different with Today's Designs?

Traditional Large LWRs



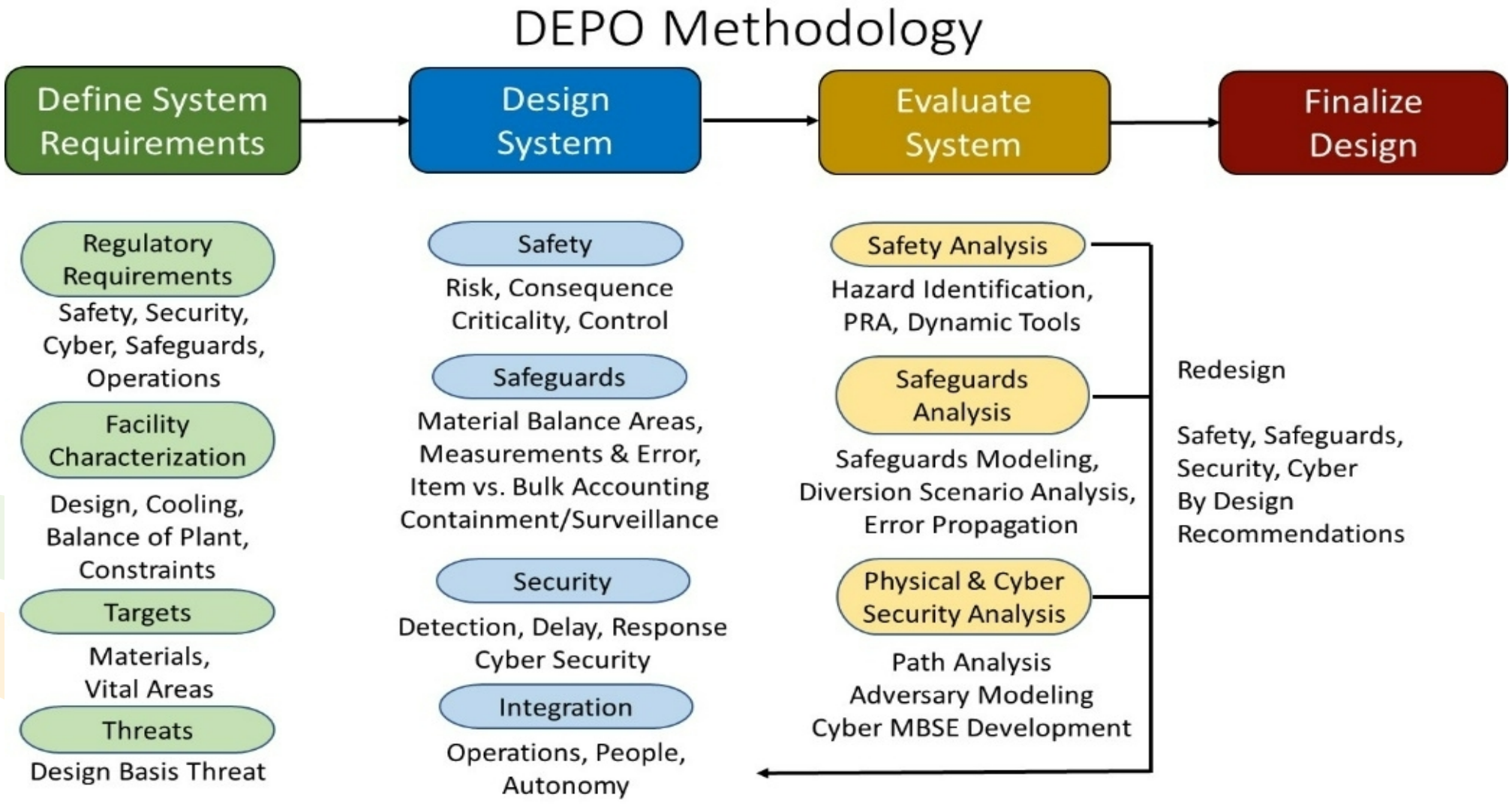
- The existing large LWRs are very large sites.
- There is greater physical separation of vital areas.
- Security was added later in the process.
- Less need for integrated safeguards with fixed assemblies.

Advanced Reactors



- Very compact designs and site layouts.
- Smaller physical separation of vital areas
- Safety systems extend timeline of accident/sabotage
- Different fuels require new MC&A approaches
- Security costs must be reduced to be competitive

Design and Evaluation Process Outline



NRC Rulemaking

- Keep the requirements of 73.55 to protect against sabotage but set out additional guidance in 73.55(s) for advanced reactors which can establish a performance-based approach
  - Relieved of 73.55(k)(5)(ii) **minimum number of armed responders**
  - Relieved of 73.55(e)(9)(v) and 73.55(i)(4)(iii) requiring that the **secondary alarm station, including if offsite, be designated and protected as a vital area**
  - Sites must still have two onsite alarm stations per 73.55(i)(2), but a designated secondary alarm station may be offsite. It is not required to be a vital area, nor is its associated secondary power supply required to be.
- One of the most significant NRC comments is the allowance for the use of local law enforcement rather than licensee security personnel to interdict and neutralize the DBT
- The NRC is proposing to amend security requirements based on three **eligibility criteria** specified in a new 73.55(a)(7).
  - Dose limits in 10 CFR 50.34 and 52.79 are not met after a radiological event involving loss of engineered safety features and physical structures.
  - The DBT cannot compromise plant features necessary to mitigate an event, which prevents the release from reaching values in the CFR sections.
  - The reactor and facility includes inherent safety features which would maintain the dose below consequences above if a target set is successfully sabotaged.

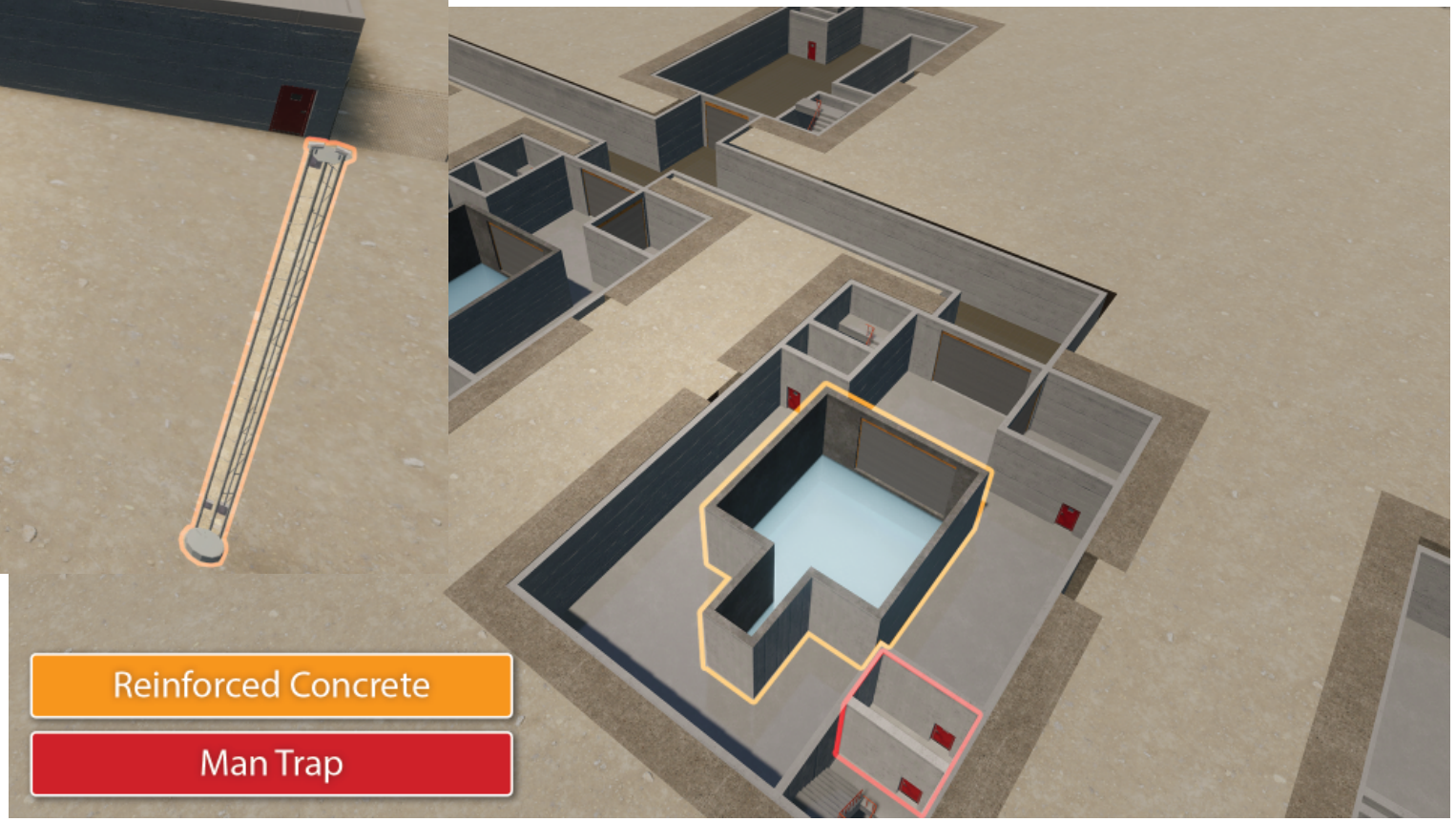
3S-Informed Physical Protection Design

- The goal of the ARS program is to provide physical protection system (PPS) design alternatives for vendors to consider that will meet the new rulemaking with a more efficient (yet robust) approach.
- Generic reactor designs are being modeled to develop multiple PPS options to consider based on location, company views, and economic considerations.
- Currently, iPWR, PBR, and microreactor models exist with future plans to expand into SFR and MSR designs.
- Options will include with reliance on off-site response and without, as well as with Remote Operated Weapons Systems (ROWS) and without.

Reliance on Off-Site Response Security Approach

Sensor towers that make use of the Deliberate Motion Algorithm provide 2π detection with reduced footprint and cost.

Enhanced delay features increase time to breach key targets allowing reliance on off-site response

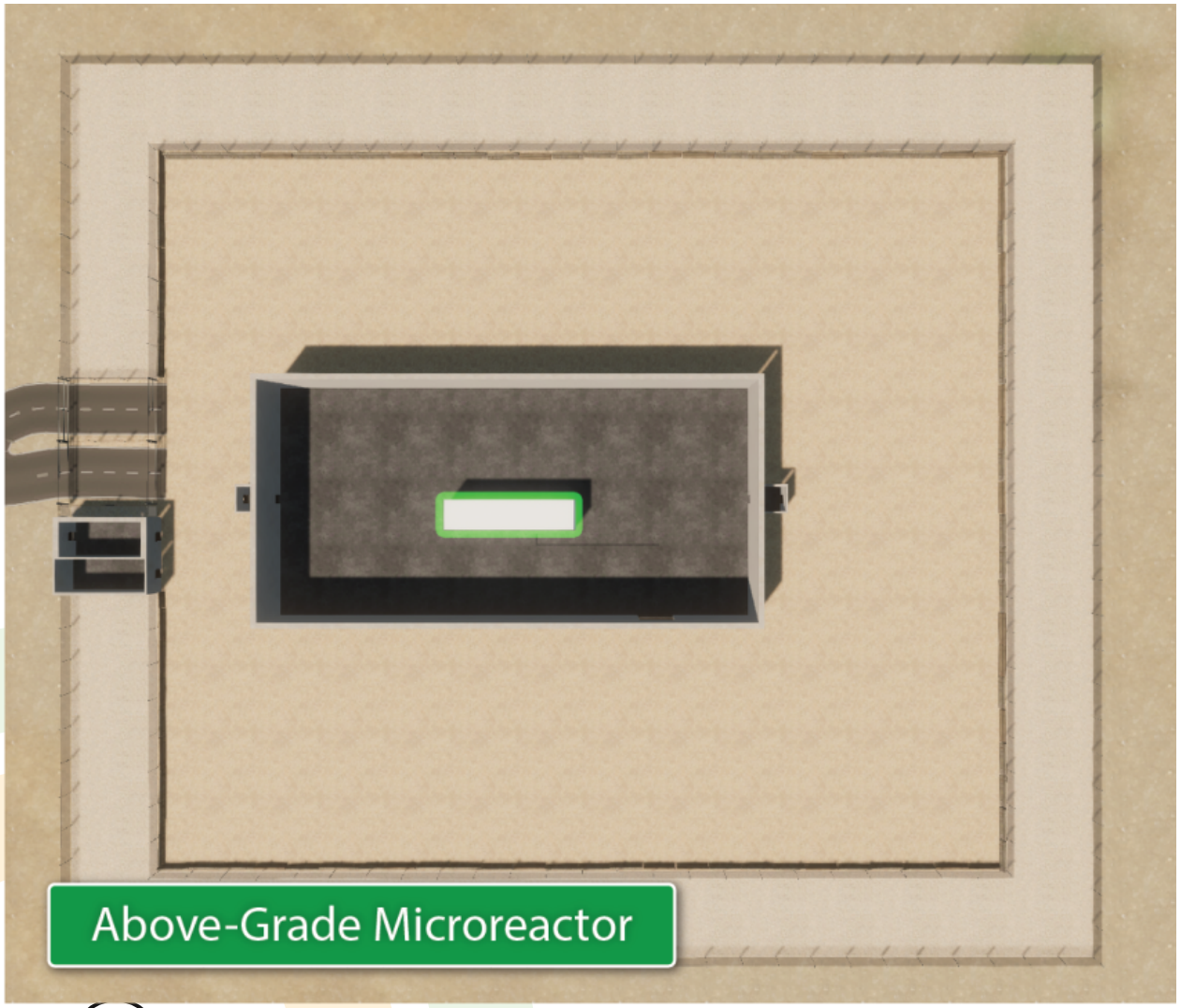


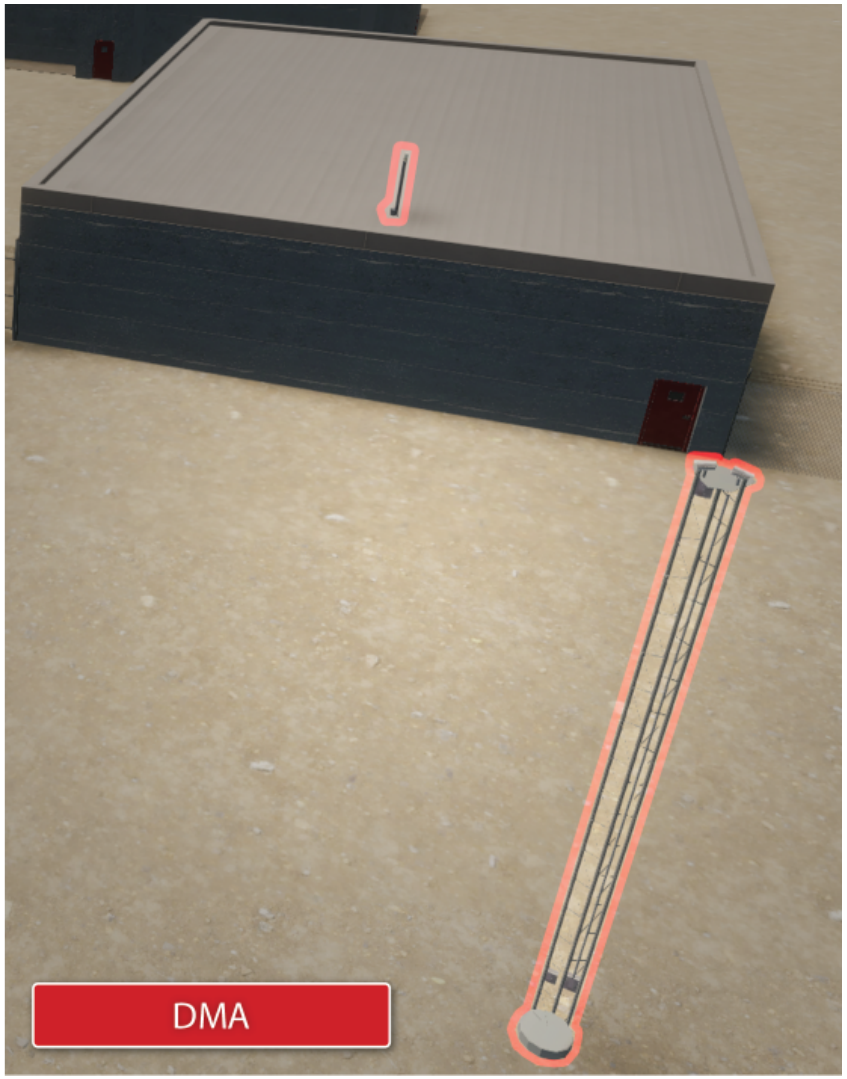
Reduced On-Site Response

Exploring design options with reduced on-site response to respond to a DBT threat with much less on-site response.

Note that locating critical targets (reactors and spent fuel) together helps to optimize the size of the response force.

Above Grade Microreactor Security Approach





Safety-Informed Security Approach

- We’re exploring options that rely on a denial strategy for the most critical targets (reactor and spent fuel), but take advantage of enhanced safety systems for additional attack scenarios.
  - For example, with minimal on-site response near the key targets, there may not be staff on site to respond to a stand-off attack
  - A standoff attack that interrupts decay heat cooling likely will not lead to problems at the plant for several hours to days.
  - Off-site responders could then interdict in these situations.
- So ultimately the reactor building itself is a hardened bunker, but with an efficient and small on-site response. Off-site responders (either a centralized response from the operator or SWAT type response) would be required for another set of scenarios. The timing of these scenarios becomes important.

Discussion

- The unique features of the next generation of advanced reactors requires more integrated thinking between the domains of Safety, Security, and Safeguards.
- The design process for materials accountancy, physical protection, and cyber security have many overlaps that should be exploited by the designer.
- Various PPS design options are being considered per reactor class to provide options to vendors depending on site-specific needs.
- Future work will expand the design classes being examined and look more closely at the cyber-physical interface.