SAND2022-1380C

3S-Informed Security for Next Generation Nuclear Facilities

Ben Cipiti & Alan Evans

Sandia National Laboratories, 1315 Eubank SE, Albuquerque, NM 87185, bbcipit@sandia.gov

[leave space for DOI, which will be inserted by ANS]

INTRODUCTION

The next generation of nuclear power in the U.S. is being driven by advanced and small modular reactors. These reactors are compact, utilize modular construction, and take advantage of enhanced safety. Accompanying this next generation of reactors will be fuel cycle facilities to support enrichment, fuel fabrication, reactor manufacturing facilities, and waste processing. Next generation nuclear facilities are being designed with particular attention to Safety, Security, and Safeguards (3S) by Design in order to develop a safe, secure, and economically competitive nuclear fuel cycle. These compact facilities require 3S-informed approaches and more integrated thinking between the domains to develop efficient security designs. This paper describes a 3S-informed security approach to next generation nuclear facility design.

3S-INFORMED ENGINEERING

3S-informed engineering means that safety, safeguards, and security (including cyber) are considered as part of the design of any particular system. Depending on the facility, it may not always be appropriate or required to consider all S's at once, but efficient designs require more integrated thinking and working on the interfaces of the different S's. Early consideration of design requirements will help the nuclear industry avoid costly retrofits in the future.

The large light water reactors of the past are physically large facilities with significant separation between vital areas. The move toward small modular reactors and microreactors leads to more compact sites with much more overlap between the different systems, especially since different fuels will require new accountancy approaches (see Figure 1). Compact reactors that seek to take advantage of enhanced safety systems will see much more integration between safety and security. Cybersecurity is woven throughout advanced reactors as designs move toward more digital systems and autonomous operations.

Future fuel cycle facilities may also move toward smaller, modular designs for the same reason reactors have moved in that direction: smaller facilities are easier to finance and can be built up in a more modular fashion. Again, economical facility design will depend on developing efficient approaches that consider 3S-informed design early in the process. In addition, bulk handling facilities traditionally have additional safeguards requirements that require a 3S-informed design.

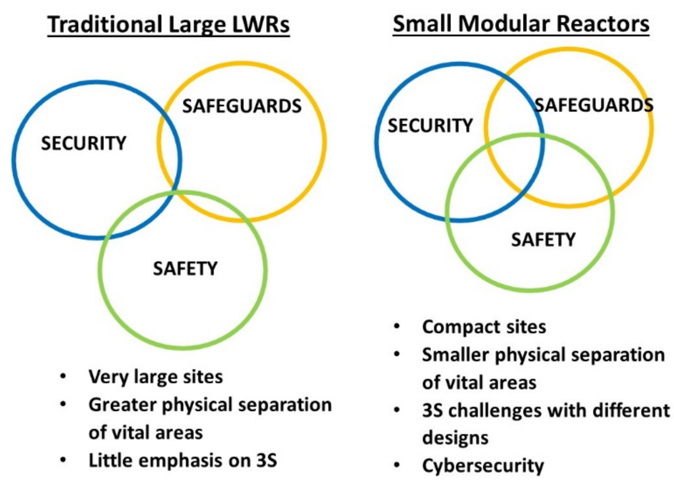

Figure 1: The Need for 3S-Informed Engineering

DEPO Methodology

The Design Evaluation Process Outline (DEPO) [1] is a systems engineering methodology that has been used for many years for the design of physical protection systems (PPS). The process flow, in a general sense, is used for the design of safety, safeguards, and cybersecurity as well. There are many common themes including beginning with defining the system requirements, designing the system, evaluating the system, iterating until acceptable performance metrics are achieved, and then finalizing the design.

Figure 2 shows how the different systems may map to the DEPO methodology. The definition of the system and requirements is common to the design of all systems and includes identifying regulatory requirements, characterizing the facility, identifying targets or materials, and determining the threat.

The design step has more differences between the systems. Safety focuses on active control, passive systems, and process monitoring. Safeguards focuses on material measurements, design of material balance areas, and containment/surveillance. Physical security focuses on elements for detection, delay, and response. Finally, cybersecurity includes protection of digital systems.

The evaluation step is similar in end goal but will utilize different tools, models, or analyses to determine performance metrics. All systems will then iterate on the design until performance goals are achieved. As the figure shows, there are plenty of areas where a 3S-Informed approach can take advantage of overlap.

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.

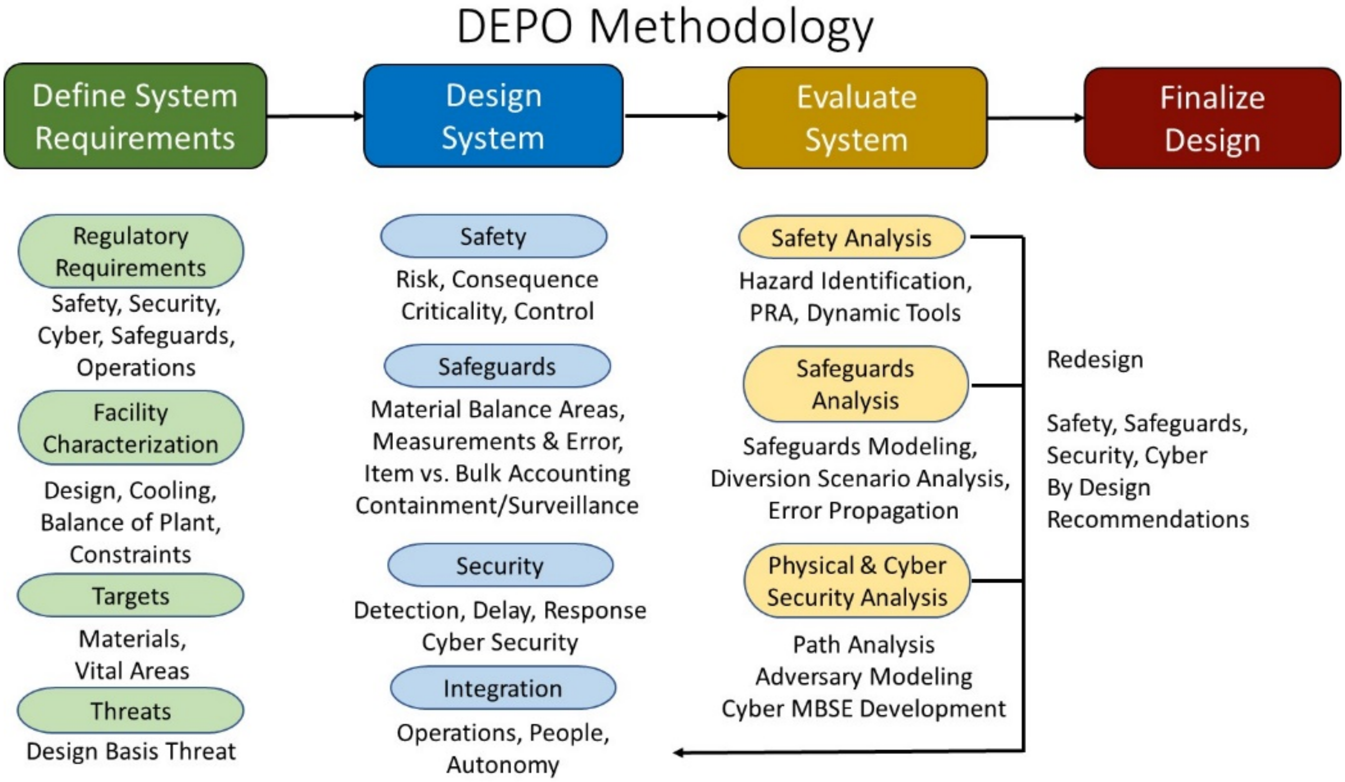

Figure 2: Design Evaluation Process Outline

PHYSICAL PROTECTION DESIGN

The key challenge advanced reactor vendors face with physical protection is developing PPS designs that are effective but also appropriate to the size of the facility. The Nuclear Regulatory Commission (NRC) is currently going through rulemaking to improve licensing efficiency, cover different types of reactor designs, and provide additional options for meeting protection requirements [2,3]. This rulemaking provides the vendors with additional options for reducing the PPS footprint including reducing the minimum number of armed responders, allowing for an off-site secondary alarm station, and allowing reliance on off-site response to interdict and neutralize threats. Advanced reactor vendors may take advantage of enhanced safety systems in evaluating new approaches.

The Advanced Reactor Safeguards program area, funded through the Department of Energy, Office of Nuclear Energy, is evaluating multiple physical protection options for advanced reactors [4,5,6]. These options all utilize a 3S-Informed approach, but the research area is still maturing. Of particular importance is integration between safety and security which is needed to allow vendors to take advantage of enhanced safety. The options are broken down into reliance on off-site versus on-site response.

Reliance on Off-Site Response

One option nuclear vendors may consider is more reliance on off-site responders in order to reduce on-site security personnel. This could be a dedicated off-site response force that an owner may deploy for multiple facilities or local law enforcement agencies. There can be a significant range in capabilities of local law enforcement depending on location, proximity to larger cities, and state and local laws.

This physical protection option assumes that advanced delay features will drastically extend the timeline of adversary attack in order to provide enough time for offsite response. Both 30-minute and 60-minute response force times were considered. The delays utilizing hardened doors and walls, mantraps, fog and slippery agents, ankle breaking rocks, etc to increase the delay time of the adversary. Additionally, advanced detection technologies such as deliberate motion algorithms were utilized to detect nuclear security events earlier [4,5,6]. Designs were considered for both small modular reactors and microreactors. While performance results showed that high system effectiveness could be achieved, there are several challenges with this approach including whether these response times are achievable and whether the PPS upgrades will be worth the additional cost. Microreactors will be sensitive to an added physical protection footprint since it could impact cost more drastically than reactors that produce more power.

Reliance on On-Site Response

The second option is still being evaluated but may provide an alternative if off-site response is not feasible. The approach considers two options: one that utilizes remote operated weapons systems (ROWS), and one that does not. ROWS may provide a significant advantage for reactor vendors looking to provide adequate protection of assets with reduced staffing. For both options, the goal is to minimize on-site responders to a small number (2-4) while still providing adequate protection against the design basis threat.

The use of on-site response may be more attractive to operators, but there may be attack scenarios for which off-site responders will still be needed. For example, a standoff attack that removes decay heat cooling capabilities will likely only cause a problem for the reactor after several hours or days have passed. This type of scenario can probably be handled with off-site response or local law enforcement since the on-site responder strategy is only focused on keeping people out of the facility. Detailed analysis of the safety systems and accident sequence timelines will be required to prove this response strategy, which requires a 3S-Informed approach to physical protection design.

Future work will evaluate the 3S-Informed approach in more detail and against analyses for the different classes of reactors. This work will need to take into account various sabotage pathways which will be unique to each reactor class. Parallel work in the Advanced Reactor Safeguards program is evaluating both sabotage scenarios and timeline analysis, pulling from the safety domain [7].

ADDITIONAL EXEMPLARS

The following examples highlight the need for 3S-Informed Security in the design of future nuclear fuel cycle facilities and provide an indication of the required future work to support vendors with efficient physical protection designs. All of these examples highlight the interfaces between the 3S's and how existing tools and methodologies must work together.

Pebble Bed Reactors

Pebble Bed Reactors (PBRs) contain fuel in graphite pebbles, and the pebble handling system is one of the more important areas from the standpoint of process control, physical security, and materials accountancy. The pebbles will be removed from the core at a frequency of about 30-60 seconds. Pebbles will need a burnup measurement and likely an integrity check.

The burnup measurement is mainly needed for process control so that all pebbles can be recirculated as much as possible before a burnup limit is reached. This measurement can benefit the materials accountancy system in estimating actinide content in the core and in spent pebble canisters. However, the amount of fissionable material per pebble is very small—it takes many thousands of pebbles to acquire significant quantities of material. Therefore, from a materials accountancy standpoint, pebbles will be tracked on a per canister basis.

On the other hand, an individual pebble needs to be protected from theft of radioactive material, which could be a target for a radioactive dispersal device. Containment and surveillance, as part of the PPS, will be used to ensure pebbles are not removed from the system. As this example describes, the process monitoring, MC&A system, and PPS can work together to develop a 3S-Informed approach to protection.

Molten Salt Reactors

Molten Salt Reactors (MSRs) include a wide range of design parameters. For simplification, liquid-fueled MSRs are considered here. A liquid-fueled MSR is closer to a bulk processing facility since the nuclear material is not contained in solid, discrete fuel assemblies. MSRs have a strong reason to consider a 3S-Informed approach since design considerations span the 3S landscape.

Recent work has found that the amount of fissionable material in a MSR will lead to high absolute measurement error, even if the measurements achieve below 1% uncertainty [8]. As a result, MSRs will need to also rely on containment and surveillance to control nuclear material. MSRs may have an advantage in the fact that the nuclear material is in a difficult form (molten salt), large quantities would be required (~100s of kg), and the material will have a very high radiation field. Again, a 3S-Informed approach will be required to develop an efficient PPS.

Sabotage Scenarios

The current NRC rulemaking allows advanced reactors to take credit for smaller source terms, enhanced safety, and possibly longer accident sequences. It is important to point out that passive safety does not equate to passive security since an adversary can initiate various sabotage scenarios. If advanced reactor vendors want to take credit for smaller source terms, they will need to evaluate an integrated safety-security analysis.

The analysis will require understanding potential sabotage targets and scenario progression timelines after those events occur. This must be evaluated in conjunction with path analysis to determine if on-site or off-site responders will be able to neutralize the threat in time to prevent an off-site dose below a threshold value. While reactor vendors do not need to follow this approach, it may be a route to reducing security staffing on site. These types of analyses require adequate modeling tools and represent a new approach, so research and development are needed to assist vendors in proving these concepts.

CONCLUSIONS

A 3S-Informed approach to nuclear facilities is required for efficient and robust physical protection design. There are many overlaps in the design process for safety, safeguards, and security (including cyber) that can and should be exploited to develop state-of-the-art protection strategies for the next generation of nuclear reactors and fuel cycle facilities. While current research is evaluating a 3S-Informed approach on a case-by-case basis, future work will need to better integrate modeling tools to streamline the approach. Future nuclear facilities need to consider these design requirements early in the process to save costs and help ensure that nuclear will be competitive in the future.

ACKNOWLEDGEMENTS

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. SAND2021-8058C.

REFERENCES

1. M.L. GARCIA, "Design and Evaluation of Physical Protection Systems, 2nd edition," Sandia National Laboratories (2008).
2. "Rulemaking for Physical Security for Advanced Reactors," NRC Docket ID: NRC-2017-0227, Nuclear Regulatory Commission (2019).
3. "Preliminary Proposed Rule Language: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," NRC Docket ID: NRC-2019-0062 (2020).
4. A. EVANS et al., "U.S. Domestic Small Modular Reactor Security by Design," SAND2021-0768, Sandia National Laboratories (2021).
5. A. EVANS et al., "U.S. Domestic Pebble Bed Reactor: Security by Design," SAND2021-13122R, Sandia National Laboratories (2021).
6. A. EVANS et al., "U.S. Domestic Microreactor Security by Design," SAND2021-13779R, Sandia National Laboratories (2021).
7. C. SMITH et al., "Treatment of Uncertainties for Security-Related Design Aspects of Advanced Reactors when using a Risk-Informed Licensing Approach," INL/EXT-21-64565, Idaho National Laboratory (2021).
8. N. SHOMAN & M. HIGGINS, "Considerations for NMA of Molten Salt Reactors," American Nuclear Society Summary (2021).