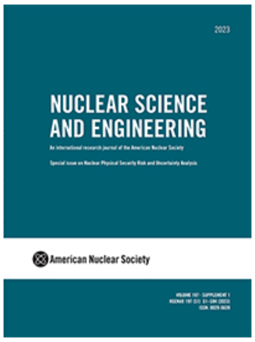


2023

NUCLEAR SCIENCE AND ENGINEERING

American Nuclear Society

Nuclear Science and Engineering

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/unse20

New Security Concepts for Advanced Reactors

Alan Evans, John L. Russell & Benjamin B. Cipiti

To cite this article: Alan Evans, John L. Russell & Benjamin B. Cipiti (2023) New Security Concepts for Advanced Reactors, Nuclear Science and Engineering, 197:sup1, S70-S79, DOI: 10.1080/00295639.2022.2112134

To link to this article: https://doi.org/10.1080/00295639.2022.2112134

NUCLEAR SCIENCE AND ENGINEERING · VOLUME 197 · S70–S79 · SUPPLEMENT 1 · 2023
DOI: https://doi.org/10.1080/00295639.2022.2112134

New Security Concepts for Advanced Reactors

Alan Evans,* John L. Russell, and Benjamin B. Cipiti

Sandia National Laboratories, Albuquerque, New Mexico

Received April 13, 2022
Accepted for Publication August 8, 2022

Abstract — *Advanced nuclear reactors have moved toward smaller, modular construction and will likely dominate the expansion of nuclear energy in the near future. These compact reactors need new physical protection approaches to reduce costs while still meeting regulatory requirements to allow nuclear to be competitive with competing sources of electricity. This paper presents new technologies and new physical protection approaches that can help optimize protection costs for new facilities. The deliberate motion algorithm for efficient intrusion detection and alternative response force strategies and options is presented.*

Keywords — *Security, advanced reactors, security by design, deliberate motion algorithm.*

Note — *Some figures may be in color only in the electronic version.*

I. MOTIVATION

The future of nuclear power facilities, including advanced, small modular, and microreactors, is based on improved economics that allow these reactors to be competitive with competing sources of electricity. One of the perceived ways to do this is to reduce the upfront construction and installation costs, as well as long-term operational and maintenance costs. Sandia National Laboratories (SNL) is conducting research on new physical protection approaches to improving security using emerging sensor technologies and the implementation of new sensor fusion algorithms. The results from this work will enable the development of new physical protection systems (PPSs) not previously viable and new security methodologies to help reduce the costs for advanced reactor (AR) deployment in the United States and internationally.

The work presented here uses generic designs representing a small, modular, integral light water reactor (LWR), small modular pebble bed reactor (PBR), and heat pipe–cooled microreactor. For this first step in the design process, the details of the reactor design are less important. What is more important is to protect the reactor core, safety equipment for reactor operations, and onsite spent fuel from a potential adversary. Current and future work will explore specific sabotage scenarios in more detail that will be specific to each AR class; those scenarios will be used to strengthen PPS designs in the future.

This paper focuses on how novel security technology, postures, and PPSs can be implemented across all AR types. Advanced PPSs that improve performance and decrease the capital cost and operation/maintenance costs can allow ARs to be more economically viable in the energy production market.

II. BACKGROUND

The next generation of nuclear power plants in the United States is being driven by private investment into

*E-mail: aevans@sandia.gov

This material is published by permission of Sandia National Laboratories, for the US Department of Energy's National Nuclear Security Administration under Contract No. DE-NA-0003525. The US Government retains for itself, and others acting on its behalf, a paid-up, non-exclusive, and irrevocable worldwide use in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

smaller, modular, and less capital-intensive designs that take advantage of enhanced safety systems. Public financial support is being provided to overcome the first-of-a-kind production and licensing costs associated with these reactor designs. In particular, the Advanced Reactor Demonstration Program[1] is providing cost-share support to several new reactor vendors to help meet U.S. carbon reduction goals.

One of the challenges AR vendors face is meeting physical protection requirements in a way that will be more appropriate to the smaller size of these reactors. Existing regulations were built around the large LWR fleet, but smaller reactors will need more efficient designs to stay economically competitive. The Advanced Reactor Safeguards (ARS) program area, funded through the Office of Nuclear Energy (NE) in the U.S. Department of Energy (DOE), provides research and development support to solve materials accountancy and physical protection challenges for ARs. A key thrust area of the ARS program is to provide PPS design alternatives that significantly reduce the PPS footprint or the number of onsite response force personnel.

II.A. U.S. Nuclear Regulatory Commission Requirements

The U.S. Nuclear Regulatory Commission (NRC) regulates the security, operations, and safeguards of nuclear power facilities and research reactors in the United States. The NRC is proposing new rulemaking language that will allow for a technology-inclusive and performance-based approach to regulate the security of ARs. The new options are meant to consider advanced technologies that allow for the improved detection, delay, and response of security incidents. This new shift in regulatory requirements is being developed in two stages, with the first being alternative physical security requirements[2] and the second being a risk-informed, technology-inclusive regulatory framework for ARs through a new licensing framework in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 53 (Ref. 3).

The alternative physical security requirements will ultimately be worked into the new 10 CFR Part 53. The changes include

1. Eliminating the requirement for a minimum number of onsite armed responders.

2. Eliminating all requirements for any onsite armed responders to interdict and neutralize the design-basis threat (DBT) in cases where reliance on offsite law enforcement or other offsite responders will be adequate to fulfil interdiction and neutralization capabilities.

3. Allowing alternative means for delay other than what is required in current regulations.

4. Allowing an offsite secondary alarm station, no longer considered a vital area.

These changes to the existing regulations will provide flexibility to AR vendors or operators in the design of the PPS.

II.B. Traditional PPS Design

Traditional PPSs have relied on a defense-in-depth strategy with multiple layers of detection, delay, and response. This has been a staple of PPS designs since the creation of the Design Evaluation Process Outline (DEPO) methodology (see Fig. 1) developed at SNL (Ref. 4).

The DEPO methodology was developed as a systems engineering approach to design and evaluate a PPS. The first step of the process is to define the PPS requirements

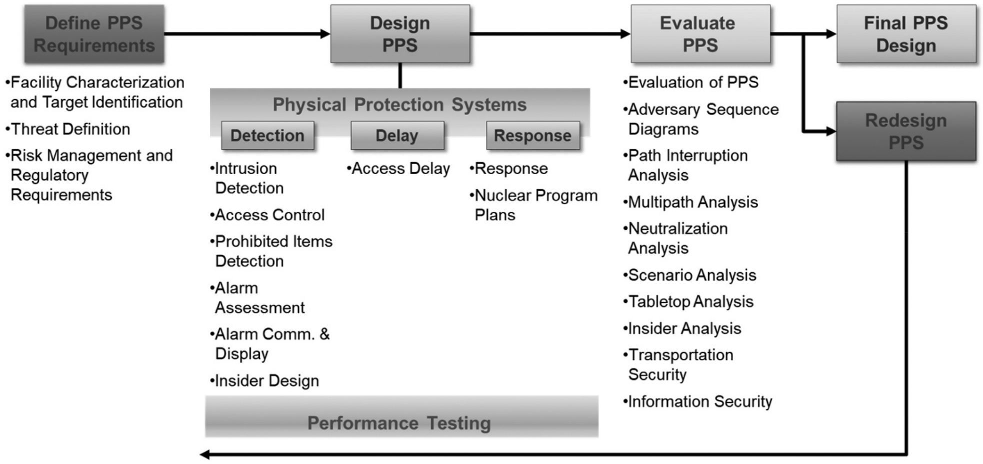


Fig. 1. DEPO methodology.[4]

and includes characterizing the facility. Facility characteristics may include hours of operation, climate, environment, buildings and building materials, ventilation systems, required vehicle access for deliveries, and personnel access for site operation and maintenance. This is an important step in the facility process that determines how the facility operates and identifies potential access points that need to be secured to mitigate a malicious attack at the facility.

This first step also requires the identification of targets. These targets could include nuclear material that could be stolen or sabotaged, or components and systems that are used to ensure the safe operation of reactors or the facility. Threat definition requires understanding the threat that the facility must defend itself against. Traditionally, the threat definition takes the form of a DBT, which should define the adversary's capabilities, motives, and intentions. The PPS needs to meet all regulatory requirements and not interfere with the safety and operations of the facility.

The second phase of the DEPO methodology is to design the PPS. The PPS consists of the three key areas: detection, delay, and response. Detection considers the identification by technologies or the direct observation and assessment of the malicious act to determine the cause of an alarm and the determination of a threat. The key areas considered in the design process here are external and internal intrusion detection, access control devices for authorized entry into the facility, prohibited item detection, and alarm communications to a central alarm station (CAS) that allow for an alarm communication and display system to assess the cause of an alarm.

Delay includes the use of barriers or physical spaces to increase the time it takes an adversary force to accomplish their goal at a facility. Delay can take the form of structural barriers (i.e., doors, walls, windows, floors, ceilings, etc.) or the form of more advanced delay features, such as active delay (i.e., smoke, obscurants). Delay elements are designed and implemented after detection occurs. This ensures that once an adversary force is detected and assessed, the delay barriers can be used to extend their task time and allow a response force enough time to interrupt and neutralize the adversary force.

The response aspects include designing an appropriate response force that has the capabilities to respond in a timely manner to interrupt and neutralize a DBT adversary force. Response includes the size of the response force, location, tactics, and training required.

The last phase of the DEPO methodology is evaluation, which may use multiple tools. Path analysis, neutralization analysis, and force-on-force exercises or simulations are used to determine the overall performance of the system. A performance-based PPS is based on the following equation:

$$P_E = P_I \times P_N \ ,$$

where P_E is defined as the system effectiveness defined as the probability that the PPS can both interrupt and neutralize a malicious act, P_I is the probability of interruption, and P_N is the probability of neutralization. The P_I is determined by conducting path analysis. The P_N can be determined by neutralization analysis, force-on-force simulations, tabletop exercises, or force-on-force exercises. SNL has developed novel computer-based programs for path analysis and force-on-force simulations: PathTrace© and SCRIBE3D© (Ref. 5). System effectiveness is determined here by multiplying the P_I 's and the P_N's.

The final step in DEPO is redesign until an appropriate system effectiveness has been reached. The design process is iterative and may continue on in the future in revaluating the system when new technologies or systems are implemented into the system, when a change in the DBT is made, or when regulatory requirements change.

III. SECURITY BY DESIGN

For AR facilities, costly retrofits and overdesigning security elements can result in deployment options that make ARs nonfeasible. Security-by-design (SeBD) has traditionally been discussed and described as conducting security design and analysis earlier in the design process of the facility (i.e., implementing the DEPO methodology during the facility design phase).[6] However, SeBD also includes implementing technologies and new PPS postures to decrease both the capital and long-term operating and maintenance costs of the system.

Security-by-design is highly recommended to current and future nuclear reactor vendors to avoid costly retrofits, reduce long-term operational costs, and enable assessment of the effectiveness of advanced security technologies. In addition, AR vendors need to consider safety, safeguards, and cybersecurity along with the security design to develop efficient overall plant monitoring systems.[7]

Security-by-design is in many ways built into the DEPO methodology described previously in the design iteration, but modeling tools can allow this design process to proceed more efficiently today. The security analysis for ARs should also consider reactor safety systems, including passive safety systems for reactor primary coolant and emergency reactor cooling. Passive safety systems may reduce the number of targets and target sets as compared to active safety systems. Reducing the number of targets and target sets would lead to decreased security systems that need to be protected, and therefore decrease the cost of a security system.

When designing a facility, path analysis software and techniques can be applied to determine credible adversary pathways into a facility. By considering these adversary pathways, facility designers and PPS engineers work together to develop reinforced walls or reinforced doors that increase adversary task times and improve PPS effectiveness. While conducting this path analysis, the designers may also determine detection technologies that ensure high probabilities of detection. Considering detection and delay when designing the facility may allow for increased probabilities of interruption, and therefore, higher system effectiveness levels.

In the design phase of the facility, PPS engineers can also consider the response force strategy and posture for neutralization of an adversary threat. These design choices may include response force routes or designing hardened fighting positions that increase response force safety and their effectiveness for neutralizing an adversary force. By considering improvements to the P_I and P_N, AR facilities may see improved system effectiveness. SeBD may also consider locating all reactors in one building below grade, rather than modularizing each reactor in its own building. As the number of buildings increases, the separation of targets and target sets increases. This causes more security features and systems to be put into place and creates a more complex response force strategy to protect the separated targets.

To summarize, SeBD presents an opportunity for AR designers to increase security system effectiveness by reducing the attractiveness of the reactor technology, designing security features into the reactor design, and designing security features and security postures into the consideration design of the PPS. The following sections provide new technologies and approaches that should be considered as part of a SeBD approach.

IV. ADVANCED PPSs

During the last 35 years, there have been tremendous advances in sensor technologies, communications, signal processing, and computational capabilities. Applied to PPS design, these technologies will likely play key roles in the development of next-generation physical intrusion detection systems; however, the technical challenges related to these technologies need to be solved for them to be considered as viable candidates. Four technologies are described here in more detail: radar; video analytics (VA); light detection and ranging, known as lidar; and artificial intelligence (AI)–based detection algorithms.

IV.A. Radar

The benefits of radar for intrusion detection systems include accurate range and bearing data associated with a target, working in fog and other weather conditions, and the ability to look directly at the sun without degradation in detection. However, historically radar-based intrusion detection systems have not attained mainstream acceptance in short-range (100 to 500 m) detection systems because of its high false positive alarm rate, commonly referred to as nuisance alarm rate (NAR). Radar sensors can be configured to reliably declare an alarm on an intruder, but without advanced algorithms the radar will also declare alarms on fences moving in the wind, moving foliage, and rainstorms. Testing of radar sensors in the last 10 years for ground-based intruders and unmanned aerial vehicles has shown that most radar sensors can produce 100 to 1000 nuisance alarms during a light rainstorm and from windblown foliage in less than 1 h. The NAR performance is an issue with radar that has not been satisfactorily addressed until recent advances in AI (Ref. 8).

Another historical challenge has been cost. Short-range radar units can cost $30 000 to $60 000 for a single unit, discouraging many security designers from incorporating radar technology into modern-day perimeter intrusion detection designs. However, recent advances in microelectronics incorporated into radar, primarily driven by the autonomous navigation industry, have significantly reduced their cost. For example, a radar currently used in vehicles for collision avoidance can be purchased for $300.

A combination of low-cost radar technology enhanced with advanced detection algorithms to reduce NAR and provide reliable detection will be instrumental in the creation of next-generation PPSs.

IV.B. Video Analytics

Video analytics is a relatively new technology compared to radar, having made its entry into the security sector in the early 1990s (Ref. 9). Today's VA systems attempt to use object detection to accomplish intrusion detection. Because of the need to reduce false positive alarms or nuisance alarms, there has been active research in computer vision, a subset of AI (Ref. 10). A host of different branches of AI and machine learning have been topics of very active research, including neural networks, deep neural networks, convolutional neural networks, and dynamic Bayesian networks, to name a few. Machine learning algorithms have been applied to VA with the goal of maintaining reliable detection and reducing nuisance alarms. However, VA by itself cannot meet the detection and nuisance alarm requirements of a high-security perimeter. The problem of excessive nuisance alarms still persists for VA.

A significant limitation of imaging technology is that it does not report the range to a target or object, so a drop of water running down the lens of a camera can look like a large object in the camera's far field. By adding the range data of radar, the data fusion of VA and radar may be a key technology that will lead to new PPSs that will be able to meet the stringent detection requirements of reliable detection and low NAR.

IV.C. Lidar

Lidar functions much like radar, except it uses reflected light instead of radio waves to measure the range to a target. Lidar can use visible, ultraviolet, or near infrared light, but today the most commonly used wavelength of light is near infrared. The ability to measure range to target very accurately complements the weakness of imager-based VA because imagers do not natively measure range to a target. Lidar units increase vertical angular resolution by increasing the number of beams used. Most of these lidar units can rotate 10 to 20 times per second, providing high angular resolution and range data and making this technology ideal for sensor fusion algorithms with both radar and VA (Ref. 11).

Lidar has several challenges it must overcome before it can be considered a viable technology for intrusion detection. One of the challenges is a limited operating temperature, which requires good heat dissipation or active cooling. Another issue is vibration of the sensor, which can cause the images to be blurred, degrading the angular and range resolution of the sensor. Because lidar uses light reflected from a target, it is susceptible to many of the same physics-based environmental limitations that imager-based VA experiences, including fog, rain, snow, and dust. The cost of lidar has been an issue in the past, but significant investments by smart phone technology and autonomous navigation technology are driving down the costs.

IV.D. Deliberate Motion Algorithm

One approach to solving the nuisance alarm problem is to combine complementary sensors.[12] This approach allows the strength of one sensor to augment the weakness of another. An effective deployment of complementary sensors requires two or more sensor detection envelopes to overlap, forcing an adversary to attempt to defeat two different sensor technologies at the same time. Implementing AI techniques by utilizing complementary sensors in software for the alarm decision process reduces nuisance alarms and strengthens detection.

The SNL Global Security Analysis and Simulation department, in collaboration with Management Sciences Inc., has taken a deterministic approach that identifies and scores features of intruder motion to distinguish alarms caused by intruders from nuisance alarm sources, i.e., weather, foliage, wildlife. This approach is called deliberate motion analytics (DMA). DMA is a multiple intelligence fusion algorithm for intrusion detection and tracking using a distributed, multilayer tracking and classification algorithm.[13] DMA's motion pattern recognition algorithms have demonstrated the ability to identify potential intruders inside and outside of the perimeter intrusion detection system (PIDS), issuing alarms against tracks with the correct motion features while filtering out background noise and nonthreatening tracks from weather, foliage, and background traffic.

The effective utilization of DMA enables individual sensor settings to be set at very sensitive detection thresholds, increasing the probability of sensing a stealthy intruder. Because individual sensors can be set to a high detection sensitivity, the individual sensors will generate numerous nuisance alarms. Test results to date have shown that the DMA algorithm is capable of effectively filtering out hundreds of thousands of nuisance alarms per day from individual sensors, yielding no nuisance alarms over a period of 1 day to 1 week. DMA has successfully demonstrated the fusion of complementary sensors including

1. radar and VA
2. radar and thermal radar
3. VA and a buried line sensor.

IV.E. New Security Concept and Cost Comparison with a Traditional Design

The following discussion is intended to show a comparison between a traditional design for a PIDS and a new security design concept. The new PPS introduced is made possible by the advances in sensor technology and the DMA sensor fusion technology discussed in the previous section.

IV.E.1. Traditional PIDS Design

Figure 2 shows a traditional PIDS design, including an inner fence and outer fence separated by 10 m, a triple-stack microwave as a single line of detection, fixed cameras, and 100-m sector lengths except for the sector covering the entry portal. The conceptual design assumes a square perimeter with 1600 m at the inner fence and 1680 m for the outer fence.

For simplicity, this conceptual design does not include a secondary alarm station, delay barriers, entry control details, or power coming into the site. Power and communications are shown emanating from the CAS to conceptually show that power and communications must be run to the perimeter to support cameras, sensors, and lights. Microwave sensors are used in this example because they are commonly used by many sites.

The estimated cost to design and build the traditional perimeter is $4 500 000. Several data sources for this cost estimate were used to estimate construction costs, including costs taken from the RSMeans[14] and taking construction costs from the internet. The inner fence length is 400 m on a side or 1600 m for the property protection area (PPA) boundary. The 1600-m PPA boundary equates to 5248 ft. In addition to the total cost to build a PIDS, a useful metric for cost analysis and comparison is the cost per foot. In this example, $4 500 000/5248 ft equates to $860 per foot.

IV.E.2. New PIDS Design

Figure 3 shows an example of a new PIDS that takes advantage of the new "enabling" technologies. The concept depicted is called the centralized radar–pan tilt zoom (CR-PTZ) module, and consists of a frequency-modulated continuous-wave radar, a bi-spectral PTZ, and the DMA algorithm. This design uses a radar capable of reliable detection out to 700 m. In the design proposed, the radar needs to provide reliable detection out to 240 m so the detection range needed in this design concept is well within the radar's detection capability of the radar.

The DMA algorithm, discussed in the previous section, allows the detection sensitivity of the radar to be increased to allow reliable detection of walkers, crawlers, and runners attempting to cross the 40-m clear zone, yet produce an estimated one nuisance alarm per 24 h or less. This concept also provides significantly improved detection of bridging attacks because the detection height of the radar is approximately 65 ft high at the perimeter boundary.

The bi-spectral PTZ imager is capable of imaging intruders day or night, negating the need for lights. The DMA-

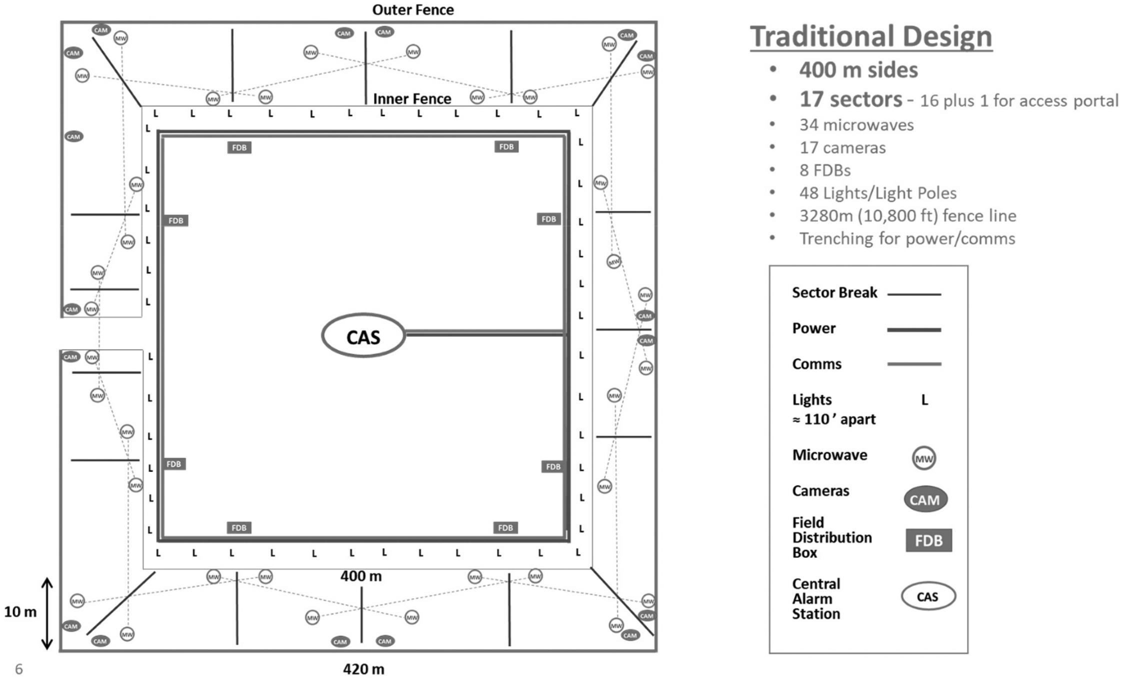


Fig. 2. Traditional PIDS design.

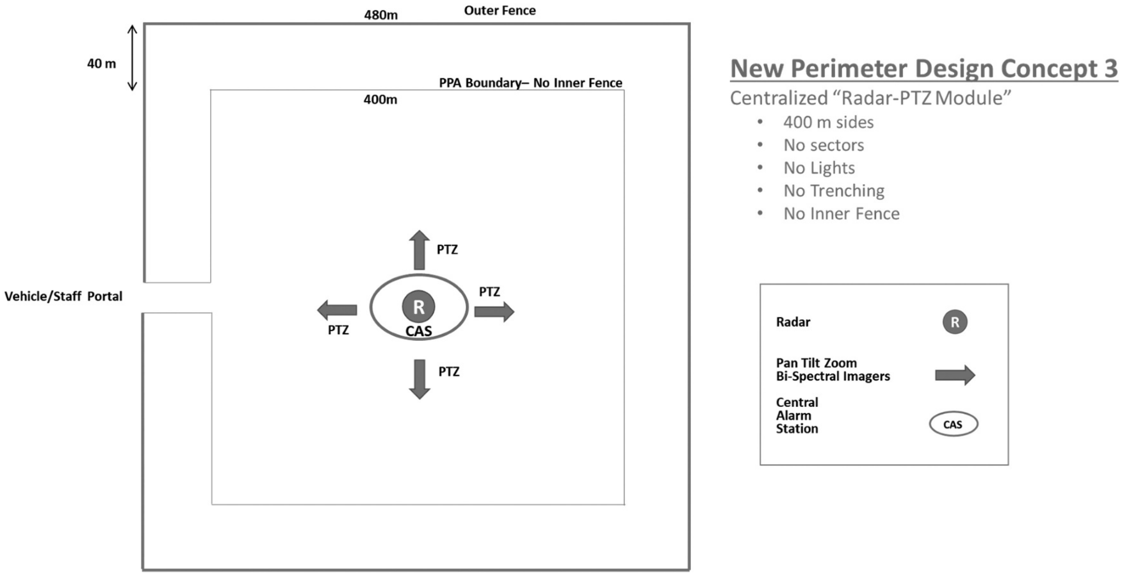


Fig. 3. New PIDS design.

enhanced radar will declare an alarm on an intruder making deliberate motion toward the site within the clear zone. When a DMA/radar alarm is declared, a switch closure is actuated, allowing the DMA to be integrated with existing monitoring systems. The DMA output will look like the output generated by a microwave or other commonly used sensors. Upon receiving a DMA/radar alarm, the DMA controller will move the bi-spectral PTZ imager to the DMA alarm coordinates and will continue to track the intruders as they traverse the 40-m clear zone, allowing the CAS operator to visually assess the cause of the alarm.

Preliminary testing of the CR-PTZ concept shows the ability to detect DBT intruders at 90% probability with a 95% confidence level, yielding less that one nuisance alarm per day. It is important to note that additional nuisance alarm data collected in different environments over extended periods of time are needed before a conclusive statement can be made. SNL is currently in the process of collecting more field test data to show this sensor system can provide reliable detection in harsh weather conditions, including hot, dry, windy conditions in the New Mexico desert; cold, snowy conditions on the shores of Lake Michigan in March; and hot humid conditions in Louisiana in July. After assessing the performance of the CR-PTZ concept, a follow-on report will be released with more conclusive results.

There are several notable differences between this design and the traditional design, including

1. No trenching is required to run power and communications to the perimeter.

2. No lights are needed for assessment.

3. No inner fence is needed (an outer fence is still required as a demarcation of a protected area allowing for appropriate posting or signage).

4. Minimal geotechnical changes are required; only rough grading is required to allow drainage and prevent pools of water forming in the clear zone.

5. The clear zone is 40 m as opposed to the 10-m clear zone in the traditional design. (The 1600-m dimension of the PPA boundary is the same.)

The estimated cost for the CR-PTZ concept is $2 650 000. The same references were used to estimate this cost as used to estimate the traditional cost. The inner-fence PPA boundary is 1600 m or 5248 ft. The cost per linear foot for the PPA boundary is $2 650 000/5248 ft or $502 per foot.

Table I summarizes the cost comparison between the traditional and the new CR-PTZ intrusion detection system, showing a 40% cost reduction for the CR-PTZ concept as compared to the traditional design. A detailed breakdown of the PID costs is not provided in this discussion, but it is worth noting that the differences described earlier are the key reasons for the cost reductions.

IV.F. Designing Security Systems with Advanced Technologies

Under the DOE NE ARS program, security system designs are being developed using hypothetical AR facilities that incorporate new technologies, such as the DMA. New technologies and new response force strategies (i.e.,

TABLE I

Cost Comparison Between Traditional and New PIDS Design

	PIDS Length	Estimated PIDS Construction Costs	PIDS Cost Per Foot
Traditional design	5280 ft	$4 544 000	$860
CR-PTZ	5280 ft	$2 654 000	$502

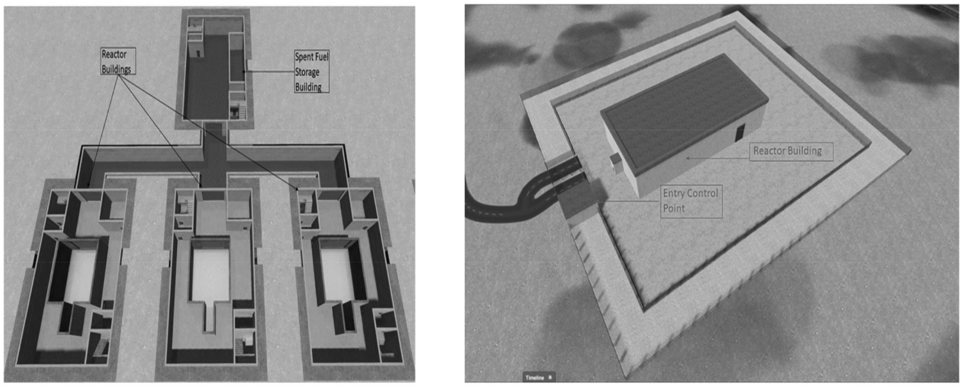
the use of an offsite response force) that would support AR licensing under the proposed limited-scope rulemaking from the NRC have been considered here. This work has focused on designing and analyzing security system designs for integral pressurized water reactors, PBRs, and microreactors.[7,15,16] These facilities have been designed to be generic to provide guidance to multiple vendors with design-specific information. The PBR and microreactor, respectively, can be seen in Fig. 4.

In these studies, advanced detection technologies, advanced delay features, and an offsite response force were designed and analyzed to determine their effectiveness in a PPS design. The offsite response force was considered with response times of 30 to 60 min to imitate various local law enforcement or offsite response force times. Due to the extended response force times, DMA technologies were used to extend the detection envelope beyond the security boundary of the site. Traditionally, this security boundary would be the protected area of the facility. This extended detection would allow for earlier detection of an adversary force and decreased costs compared to the traditional PIDS system that forms the protected area boundary. Additionally, to delay adversaries long enough for an offsite response force, active delay features were considered to increase adversary task times. These active delay features included fog and slippery agents (agents that can be sprayed or injected into an area to make it much more difficult for the adversary to use tools and carry out tasks). These features are called delay multipliers and are placed in front of locations that require an adversary to breach a barrier. By placing active delay features at fixed delay barriers, the task time to breach a barrier is multiplied. Figure 5 shows where some of these active delay features were placed in the PBR design.

In Fig. 5, active delay features are placed in front of the hardened doors to multiply the adversary task time to breach through the hardened doors. PathTrace was used throughout the design to add additional detection and delay barriers to improve the P_I and allow the response force to be more effective at neutralizing an adversary force.

Once a high P_I (95% or higher) was achieved, force-on-force simulations were developed and conducted using SCRIBE3D. In both cases, a range of adversary threats were analyzed against an offsite response force. The results of the analysis conducted using the PBR can be seen in Fig. 6.

As can be seen in Fig. 6, various scenarios were run. As the size of the adversary force increased, a decline in system effectiveness was seen. As the response time grew longer,



(a) (b)

Fig. 4. Hypothetical (a) PBR and (b) microreactor.

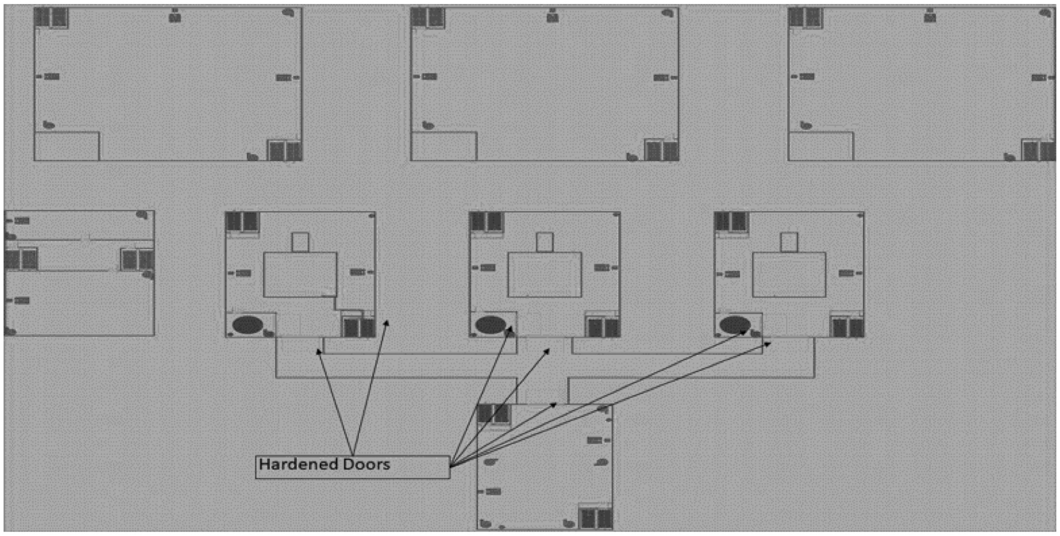


Fig. 5. Active delay in a PPS.

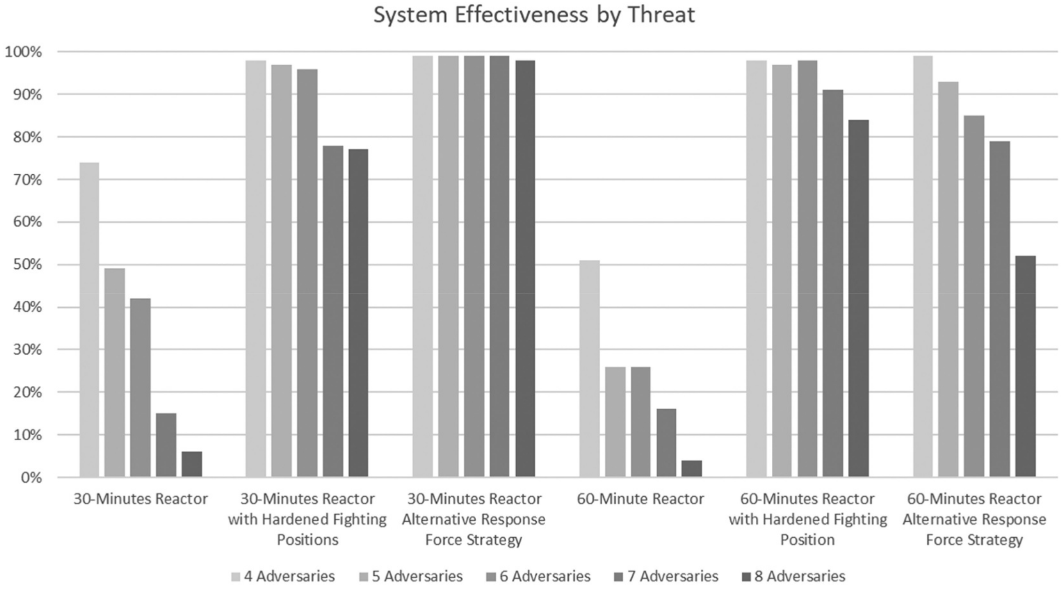


Fig. 6. PPS effectiveness for the PBR generic design.

system effectiveness decreased as well. This work analyzed two different response force paths into the facility to neutralize an adversary force. By using an alternative response path into the facility, the P_N improved significantly and created improved system effectiveness. This can be seen when comparing the “30-Minute Reactor” and the “30-Minute Reactor Alternative Response Force Strategy” data points.

The results from this work highlight the importance of using the SeBD approach to design PPSs. This work also identifies the importance of integrating advanced technologies and unique approaches into the design of security systems that improve their effectiveness. In the cases provided in this section, advanced technologies, novel approaches to delay barriers, and integrating an offsite response force led to improved effectiveness for the PPS.

V. CONCLUSION

The SeBD for ARs presents a unique opportunity to decrease the complexity, decrease the initial and long-term costs, and improve the effectiveness of a PPS. Advanced technologies may lead to drastic decreases in the construction costs of a subsystem of a PPS. The advantages of the

SeBD and the use of advanced technologies may be improved performance and system effectiveness compared to those of traditional PPS designs and technologies.

A decreased cost up to 40% using an advanced PIDS system, as discussed in this paper, is just one of the many technologies that could be incorporated into an advanced PPS. As new technologies are considered for securing AR facilities, they can be assessed within the entire PPS and better position AR vendors to design facilities that have higher system effectiveness at lower costs. The CR-PTZ concept shown here could represent a viable and cost-effective candidate for ARs, LWR sites, or other high-security sites.

The SeBD includes integrating advanced technologies and novel approaches into security systems that improve security system effectiveness. In the SeBD approaches described, integrating detection, delay, and response plays a major role in increasing system effectiveness to allow for the differing security approaches being proposed in the NRC's limited-scope rulemaking. Advanced detection technologies can be used to improve system effectiveness, reduce security system costs, and meet proposed NRC rulemaking requirements.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

ORCID

Benjamin B. Cipiti http://orcid.org/0000-0003-1721-4809

References

1. "Advanced Reactor Demonstration Program," U.S. Department of Energy, Office of Nuclear Energy; https://www.energy.gov/ne/advanced-reactor-demonstration-program (current as of Apr. 5, 2022).
2. "Rulemaking: Alternative Physical Security Requirements for Advanced Reactors," U.S. Nuclear Regulatory Commission Public Mtg., January 22, 2022.
3. "Part 53—Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors," U.S. Nuclear Regulatory Commission (October 4, 2022); https://www.nrc.gov/reactors/new-reactors/advanced/rulemaking-and-guidance/part-53.html (current as of Apr. 5, 2022).
4. M. L. GARCIA, *Design and Evaluation of Physical Protection Systems*, 2nd ed., Sandia National Laboratories (2008).
5. "Re-imagining Security Through Visualization," Sandia National Laboratories (2021); https://insetools.sandia.gov/ (current as of Apr. 5, 2022).
6. M. SNELL et al., "Security-by-Design Handbook," SAND2013-0038, Sandia National Laboratories (Jan. 2013).
7. A. EVANS et al., "U.S. Domestic Pebble Bed Reactor: Security-by-Design," SAND2021-13122 R, Sandia National Laboratories (Oct. 2021).
8. J. RUSSELL, J. ANDERSON, and C. STERN, "Video Motion Detector Fused Radar, the First Volumetric Ultra-Low NAR Sensor for Exterior Environments," SAND 2016-0083, Sandia National Laboratories (Jan. 2016).
9. F. SPLAIN, "The Evolution of Video Analytics: How AI Is Revolutionizing Security and Surveillance," March Networks (January 15, 2021); https://www.marchnetworks.com/intelligent-ip-video-blog/the-evolution-of-video-analytics-how-ai-is-revolutionizing-security-and-surveillance/ (current as of Jan. 15, 2021).
10. "Video Content Analysis," Wikipedia (September 8, 2022); https://en.wikipedia.org/wiki/Video_content_analysis (current as of Apr. 2022).
11. "Ouster OS2 Data Sheet," Ouster, Inc. (December 18, 2021); https://data.ouster.io/downloads/datasheets/datasheet-rev06-v2p2-os2.pdf (current as of Apr. 2022).
12. J. RUSSELL, "Complementary Sensor Selection for High Security Applications," presented at the Int. Nuclear Materials Management Conf., September 2012.
13. J. RUSSELL et al., "Deliberate Motion Analytics Fused Radar and Video Test Results," SAND2021-5413, Sandia National Laboratories (Apr. 2021).
14. "Building Construction Cost with RSMeans Data," 79th Annual Edition, Gordian (2021).
15. A. EVANS et al., "U.S. Domestic Microreactor Security-by-Design," SAND2021-13779 R, Sandia National Laboratories (Nov. 2021).
16. A. EVANS et al., "U.S. Domestic Small Modular Reactor Security-by-Design," SAND2020-9982 R, Sandia National Laboratories (Sep. 2020).