RESEARCH

The Use of Security Risk Assessment (SRA) Tools for Nuclear Power Plant Security Assessment

USA Nuclear Report 2020-06

June 2020

Developed and Authored by USA Nuclear for **ARES Security Corporation**

1. Abstract

Security Risk Assessment (SRA) tools have been used for more than forty years to assist in the assessment of security for nuclear facilities, including extensive use by the Department of Energy (DOE) and the Department of Defense (DoD). These two agencies have found SRA tools to be helpful in determining security effectiveness, evaluating changes or upgrades to physical protection systems, and assessing potential compensatory measures. Given the complexity of the facilities and the protection strategies, the agencies find it necessary to apply sophisticated simulation and modeling tools to ensure a thorough and structured assessment of security at major nuclear facilities.

For the DOE and DoD, the primary security challenge is the theft of a nuclear weapon or special nuclear material for use in an improvised nuclear device. The number of targets that need to be breached are limited, albeit heavily protected. However, at NPPs the primary security challenge is radiological sabotage (i.e., release) and not theft. NPPs are designed and operate with multiple independent, physically separated redundant safety systems to assure confinement of radiological material and prevent radiological release. Hence the number of targets that must be breached to cause a radiological release at an NPP are considerably more than those at a DOE and DoD facility.

Until recently, commercial utilities were not using SRA tools to assess security at NPPs, relying instead on subject matter experts' (SME) judgement to establish a set of measures deemed to be adequate. It takes one or more adversaries to access and accomplish required tasks of all targets within a target set to achieve successful radiological sabotage. The targets that comprise each target set will generally be found in several locations throughout the plant. Given the extreme complexity of NPP security programs, as well as their interfaces with even more complex safety systems, a structured approach leveraging computer modeling would provide much better assessments of security effectiveness than expert judgement.

2. Current State of the Nuclear Power Industry

The plants that comprise the commercial nuclear power enterprise are relatively old. The oldest operating reactor in the world is the Beznau Nuclear Plant in Northern Switzerland. In the USA, Nine Mile Point, in upper state New York, is only a few months younger than Beznau, having been commissioned in December of 1969, making it over fifty years old. The average reactor in the USA is just under forty years old.

Reactors were originally designed and licensed to operate for a period of forty years. These plants have a proven track history of generating clean, green, reliable energy and have been operating safe and efficiently through the years. As such, many plants have gone through the regulatory licensing process and obtained license renewals that now permit them to operate to sixty or eighty years.

Within the USA, at the industry's peak, there were 112 operational NPPs. At the current time, there are 96 operating NPPs. However, the generating capacity is substantially the same due to power uprate programs which have been implemented over the years. There are two large light water reactors currently under construction in the USA and many more around the world. This number is much lower than the approximately thirty that were forecast as part of the 'Nuclear Renaissance.' In addition, there are prospects for new classes of reactors to be built and licensed: small modular reactors, advanced reactors, and micro-reactors.

Almost all of the NPPs were built and initially licensed with security requirements that were in force prior to the terrorist events of September 11, 2001. Before that date, there had been limited increases in security requirements for NPPs for decades. After that date, the NRC issued orders, as well as new regulations and changes to the design basis threat (DBT) that dramatically increased the requirements for security at NPPs. The utilities bought up land to enable earlier detection, added fencing and barriers, and significantly increased the size of protective forces to comply with the new requirements. As a result, NPPs are among the most highly protected facilities within the critical infrastructure of the United States.

Approximately fifteen years ago in the USA, there were indications of a Nuclear Renaissance, leading to the construction of approximately thirty new large light water reactors. However, other sources of energy for electrical generation saw significant price drops. In particular, with the increased use of fracking to obtain natural gas, the price of natural gas dropped significantly relative to nuclear fuel. In addition, government subsidies for wind and solar have also adversely impacted the commercial viability of nuclear power. This change in pricing, along with the financial challenge of constructing new reactors that cost billions of dollars each, led to a collapse of the Nuclear Renaissance, with only two reactors likely to see construction completed. In addition, with increased security costs combined with more expensive relative costs of nuclear fuel, smaller NPPs are facing even more challenges in being financially viable. Many have shut down and have entered decommissioning. Some have been rescued by new support from state governments.

3. Traditional Approach to Physical Protection of NPPs

Virtually all of the current fleet of NPPs were constructed and began operation more than a decade before the terrorist events of September 11, 2001. As a result, significant security upgrades have been put in place throughout the industry in order to meet the changing security requirements imposed by the Nuclear Regulatory Commission (NRC). These enhancements have been implemented using expert judgement of plant security personnel and approved using expert judgement by NRC licensing staff, as opposed to implementation using a structured analytical approach. Many of the enhancements were also implemented to preclude the possibility of security force failures during a force-on-force (FoF) exercise.

As a result of the major increase in security requirements, plants have been retrofitted to comply with the new requirements. Many of the requirements were implemented as directed, such as stand-off distance, barriers, security patrols, security training, and access requirements, which are prescriptive in nature. In addition, there were more performance-oriented requirements such as an increased focus on defense-in-depth, and the conduct of FoF inspections to test against the DBT. To comply with the new requirements and address the more performance-related requirements, billions of dollars were spent across the fleet.

4. Current Challenges in NPP Security

As with any complex system, there are numerous challenges and many ways to address them. The NPP security issues being discussed include how to address compensatory measures, FoF exercises, how to credit FLEX equipment, and how to credit local law enforcement agency (LLEA) response. In addition, how do we better understand the risks associated with adversary attacks and the plants' ability to defend against them? All of this in a difficult market environment with increased alternatives requiring improved cost efficiency to remain commercially competitive.

Without the aid of SRA tools, the only answer had been to let the SMEs decide. However, no two groups of SMEs will consistently reach the same conclusion, as everybody has a unique view and is only capable of factoring in a relatively small part of the interactions that take place in an attack and a response, given the complex nature of plants and their associated safety and security systems. Most often in the past, the answer that all could agree on was that more guards, responders, and equipment would help solve the problem.

4.1 Compensatory Measures

As with any complex set of systems, parts and subsystems do fail and/or can be removed by maintenance for a period of time. When this happens, the plant is required to implement compensatory measures. Most often, the approach is to throw manpower at it. There also is the question of how quickly one must implement the measure, given the adversary would not immediately know that a portion of the system was out of service. The use of SRA tools provide quantitative insights to address compensatory measures allowing NPPs to determine if security effectiveness is compromised and if compensatory measures are required.

In regard to acceptable maintenance outage time intervals, that question will have to be negotiated between the utility and the regulator to determine what is reasonable given the regulatory framework. But even that can be aided by SRA tools. At a minimum, many NPPs today use SRA tools to effectively model temporary buildings and configurations to assure effectiveness.

Understanding what compensatory measure is appropriate given what has failed or is undergoing maintenance, along with how long it may be out of service can be modeled and alternatives can be assessed. For systems that may be out of service for an extended period, technical solutions may be the better answer. DoD and DOE have programs to develop such technical solutions, such as a portable Perimeter Intrusion Detection and Assessment System (PIDAS). For system elements that may be more prone to failure, the modeling approach may be able to provide insights into whether the technical solution is cheaper and possibly more effective. SRA tools can also provide insights as to whether the compensatory measure maintains the security effectiveness of the overall system.

4.2 Force-on-Force Exercises

FoF exercises serve an especially useful purpose. However, they are often misinterpreted, and their results can be misused. FoF exercises are a form of simulation and modeling. However, they cover a single scenario and many artificialities can lead to challenges of their results. In particular, the exercises help understand how the parts of the system work together and how people may react to certain circumstances. SRA tools allow many more scenarios to be evaluated, simulated, and quantified, then modified and re-evaluated, providing a much better indication of system effectiveness. At a minimum, SRA tools and the corresponding tabletop tools, should provide a method to plan, test and train for upcoming FOF exercises. Caution should be exercised as the simulation

will run as modeled. If elements of the security system are not functioning properly, the model should be adjusted as appropriate.

There is ongoing discussion as to how the regulatory framework should proceed with FoF exercise programs. Should the numbers be reduced? How should the results be handled and reported? In the end, FoF exercises and SRA tools should both be used in the assessment of security system effectiveness.

4.3 FLEX Equipment

In response to the Fukushima reactor event in Japan, all NPP sites have a supply of FLEX equipment that is available to help mitigate or prevent radiological releases due to a sabotage or safety event. If the site personnel can gain access to this equipment and deploy it in a timely fashion, the effects of a sabotage event would be mitigated or eliminated. The SRA is a useful tool in the process. Without it, SMEs would have to agree on whether the operators can access the FLEX equipment in a timely fashion and deploy it. Using SRA tools, the plants can assess how soon the FLEX equipment will be available to the operators and whether it provides sufficient time to mitigate the potential consequences. In addition, if attacking adversaries either target or impede access to FLEX, those tactics can also be addressed using modeling and simulation.

4.4 LLEA Response

Virtually all NPPs have agreements in place with LLEAs. These agreements identify how the LLEA will respond and support the facility in the event of an attack. However, there are questions about the speed of the response, and what the LLEA officers will be able to do. Have they trained at the facility? Will they perform support beyond traffic control? Will they take a leadership role? Without computerized tools, plant SMEs will have to negotiate with NRC licensing staff to assess how much credit, if any, can be provided for as a result of an LLEA response. SRA tools will allow the plant to better understand the range of response times and how much that impacts support the LLEA can provide to the site. It is even conceivable that modeling could be used to incorporate the activities of LLEAs in response efforts, such as protecting operators that may deploy FLEX equipment. This information can prove useful in the discussions with NRC staff on credit allowances, allowing these discussions to be backed with meaningful data across many scenarios.

NRC and stakeholders have discussed this issue for several years as system bounding time or coping time. Can the adversary be held off for sufficient time for an LLEA to arrive and provide necessary support to defeat the adversary and/or assist operators in deploying FLEX equipment and applying other

measures to mitigate any potential consequence? The SRA can predict this behavior.

5. New Technology and Emerging Issues

New technologies are constantly arriving on the scene and are rapidly evolving. This is true with respect to technologies available to the adversary, technologies available to the protective force, and new reactor technology.

5.1 New Technology Available to the Adversary

Adversaries are continuously seeking new technology to aid in attacks against NPPs and other critical infrastructure. Understanding how they might attack an NPP, how it might be defended, and the potential consequences are important considerations for the plant. A good example of this is the use of drones/unmanned aerial systems (UAS). It is a topic that is in the news, discussed by politicians, and rapidly evolving.

The NRC has recently started assessing the need to include UAS as part of the adversary characteristics in its DBT. Due to a lack of risk-significant vulnerabilities at NPPs and the inability of NPP security forces to do anything to counter the UAS, it is not included at this time. However, a pledge was made to continuously monitor the evolution of the technology and work with other Federal agencies to establish a legal and regulatory framework to allow for the defense of NPPs from potential adversary attacks using UAS. As a result, it is incumbent upon NPP security organizations to monitor the evolution of the technology as well as the progress in legal and regulatory changes to support the development of counter-UAS technology.

SRA tools can assist NPP security organizations in better understanding how evolving UAS technology might be used by adversaries in attacks. In addition, software can enable a better understanding of how different counter-UAS technologies can be used to detect and defend NPPs from attacks, so that if NPPs become legally allowed to defend against UAS, they will be able to select a counter-UAS technology and deploy it.

5.2 New Technologies Available to Protective Forces

New technologies to protect facilities are being developed on a continual basis. NPP security organizations are considering many new technologies, including the use of UAS and remotely operated weapons systems (ROWS).

NPP security managers are overwhelmed with companies trying to sell these technologies. Some may be beneficial and provide cost-savings to the NPPs in the long-run. However, without the ability to effectively evaluate how these new technologies might integrate into existing security programs, making an appropriate business decision can be challenging. Using expert judgement in decision making will likely give an indication of whether existing elements of the program could be replaced by the new technology. However, it is difficult to evaluate whether there would be any significant change in system effectiveness. In the end, this approach would make changing security plans to incorporate the new technology more challenging. Using SRA tools can provide a measure of system effectiveness using the current protection program, as well as a measure of effectiveness with the new technology incorporated into the protection program.

Several NPP organizations have demonstrated significant savings utilizing SRA tools to simulate significant changes to security programs. The commercial success of these SRAs are best recognized through the success of SRA users. For example, in 2018, Public Service Enterprise Group (PSEG), headquartered in Newark, New Jersey was recognized for their outstanding work using ARES Security's AVERT Physical Security SRA. PSEG Nuclear employees were recognized with Top Innovative Practice (TIP) awards during the annual Nuclear Energy Assembly, hosted by the Nuclear Energy Institute (NEI). The TIP awards celebrate industry leaders for new practices, enhanced processes, and improved technology, and is widely considered one of the most prestigious awards an energy utility can receive. This is one of many examples of ARES Security's commercial success with AVERT.

It is important to account for both routine and non-routine operations when considering the incorporation of new technologies into existing security programs. For UAS, considerations must be given for maintenance of the UAS, weather conditions that preclude the use of UAS, and what measures are taken when a UAS observes anomalous activities. For ROWS, it is important to consider maintenance of the ROWS, whether there are different operational profiles for day vs. night or varying weather conditions, as well as whether the ROWS should be used in the same manner during operations and outages. Taking these issues into account and assessing potential degradation in security performance is quite difficult using SMEs. However, SRA tools can be easily employed to make these evaluations and assessments.

5.3 New Reactor Technologies

We are entering a new era of reactor technologies. There are design innovations under development for small modular reactors (SMRs), advanced reactors, and

micro reactors. These new reactors are much smaller than the typical large light water reactors that make up the current NPP fleet in the US and the world. As a result, even if attacked by adversaries, these new reactors may not have large enough source terms within the core to result in radiological sabotage as specified in NRC regulations. In addition, engineered safety features in the reactor designs may respond to adversary attacks with a safe shutdown that precludes radiological release.

As a result, security for these reactors may be substantially different than security at large light water reactors. The design basis threat (DBT) might be met by the fact that a significant radiological release cannot be achieved, rather than by having a protective program from precluding an adversary from achieving a release through an attack. The response force may be appropriately replaced by LLEA response. Many elements of the protection program may be different.

At this time, the NRC is in the process of a rulemaking for security of advanced reactors, to include SMRs. The intent of this rulemaking will be to remove or replace prescriptive requirements in current regulations with performance measures. The intent is to reduce the number of exemption requests that might be required for these new reactors.

If this rulemaking is successful, it will be necessary to have an approach to measure the effectiveness of a variety of security measures. Traditionally, this has been done using an agreement between judgements of SMEs (plant and NRC). However, an SRA tool that provides a consistent and structured approach to assessing security measures against some level of required performance would be a significant improvement.

Prior to the rulemaking being approved, or if the rulemaking is not approved by the Commission, differences between protection programs and specific regulatory requirements will require approval of exemptions or alternate approaches. As above, this would require some level of consensus between SMEs or through the use of SRA tools that are able to measure whether the proposed security measures perform as the regulations would intend them to perform.

6. Regulatory Challenges

NRC recognized the need to revamp its regulatory process to deal with all of the challenges and new technologies that are evolving around it. NRC has initiated a transformation program to become a modern regulator that promotes and adopts innovative approaches to achieve its mission. NRC desires to become a "modern, risk-

informed, regulator." The NRC has been a world leader in the development and use of modeling and simulation to support safety regulation. Modeling and simulation in safety and security have many similarities and apply many of the same technical approaches. It seems that with a major initiative to transform its regulatory process, a major element of that process can move in the direction of using similar technologies to assess safety and security and to encourage the use of these technologies in the security regulatory process.

In order to become a modern, risk-informed regulator in the security arena, the NRC must take advantage of technological tools that can provide more insight into the risks associated with security and provide a structured approach to assessing security performance. This structured approach will provide assurances that potential vulnerabilities at facilities are not slipping through the cracks. This approach has served NRC and its stakeholders well in the safety arena. There is no reason that it cannot do the same for security.

There is a current, ongoing discussion between NRC and the stakeholder community regarding how to best risk-inform security. The discussion focuses on individual elements of the security program. This approach leads to an inefficient use of resources. It would be better to look at the overall risk for facilities and the licensed community; SRA tools can provide this understanding. Once the overall risk is better understood, selection of elements to better risk-inform can be made. This would allow NRC and its stakeholders to focus on areas that have the highest likelihood of payback from the process.

6.1 Current Regulatory Structure

Much of the NRC's security regulations are prescriptive in nature and based on requirements from decades ago and have not been restructured into performance-based requirements. Others were put into place to address the new world of terrorism, emanating from post-9/11 orders; these too were not implemented using performance-based measures. However, many performance-based measures exist in the regulations, most importantly, the DBT.

The most obvious application of modern SRA tools is to support an assessment of whether the DBT requirement is met by licensed facilities. Over the previous decades, most people have looked to FoF exercises to provide that assessment. However, FoF exercises have some weaknesses. They look at a single scenario and have notable artificialities, many of which are hampered by safety restrictions. Facility personnel are aware that an exercise is about to happen and are primed and ready. In addition, certain SRA solutions allow for alternative attack path and defense-in-depth assessment assuring that the complex nature of the NPP security systems is well understood. Augmenting the assessments

with modeling and simulation could yield a much better process; more scenarios can be addressed, and multiple runs of individual attack paths can be assessed without having the impact of safety restrictions. Additionally, the use of a combined approach (FoF and SRA tools) would lead to more effective enhancements to address security deficiencies. Typically, if a site fails a FoF exercise, the security organization looks for a quick fix to address the deficiency; however, the fixes generally provide only marginal improvements. Whereas, if SRA tools were part of the process, a better overall assessment could be performed. This would lead to security enhancements that improve the overall effectiveness of the system and are implemented using a cost-effective approach.

SRA tools can also be used to support evaluation of the other performance metrics specified in the regulations. Such use would augment limited scope performance testing that tends to be relied upon for these assessments.

The bigger challenge is to address prescriptive elements of the regulations, which are either met or not. However, this is contrary to the transformation initiative of the NRC. In order to transform these prescriptive requirements into more of a risk-informed, performance-based approach, it is necessary to identify what metric is expected to be achieved as a result of implementing the prescriptive requirement. Once the objective of the requirement is understood, it would be possible to consider a variety of performance metrics that could be submitted as alternative measures or exemptions for approval by the NRC. SRA tools could help identify potential metrics and support the development of alternative measures or exemptions that would be submitted. In addition, these tools can assist the utility and the NRC in evaluating the performance of the utility against the performance metric.

6.2 Necessary Guidance/Manuals/Training

Guidance documents and manuals will need to be developed for NRC staff and utilities to take advantage of these modern tools and help fulfill the NRC's transformation objectives. Utilities will need to understand how to use the tools to support regulatory submissions. NRC licensing staff will need to understand how to factor insights gained from these tools into their licensing decisions. Regional inspectors will need to understand how to assess the use of the tools and whether reality at the plants is properly reflected.

These guidance documents and manuals will need to address the scope of information necessary for completeness in the regulatory process. What level of engineering analysis should be included? What is the balance between performance testing and modeling and simulation that is appropriate? How

much performance testing is enough? How many simulation runs should be performed? No model is expected to be perfect without having weaknesses, deficiencies, and biases. How should regulatory submissions compensate for this? Given the scope and complexity of these models, where should NRC's regulatory oversight focus?

These SRAs tend to be overly complex. There are many tools available to utilities and the NRC, including both commercially available tools and those developed at national laboratories. They produce different types of reports, may use different terminology, have different user interfaces, have differences in how they handle and display data, and have different inputs and technical approaches to perform the modeling and simulation. Even with these differences, the use of SRAs is critical to support security professionals in assessing the complex security systems at NPPs.

7. AVERT by ARES Security Corporation

Since 1999, the most widely used security SRA tool in the commercial nuclear sector is the AVERT software suite, developed by ARES Security Corporation. The AVERT Physical Security software is used by 65% of the commercial USA NPP fleet. It has proven to be effective in evaluating security system performance and has been critical in restructuring protective strategies to make them more cost effective, without reducing overall system effectiveness.

7.1 AVERT Software Suite

AVERT is a suite of software products focused on the Physical Security Life Cycle which includes Design, Assessment, Training, and Response. With initial product development starting in 1999, the suite of ARES Security products extend the physics-based models first developed during the security design and assessment process into a virtual tabletop and virtual reality training environment for security professionals to train on responses to threats and incidents. AVERT C2 completes the lifecycle through the integration of alarms, video, and security systems into a Common Operational Picture and Situational Awareness for real time security operations.

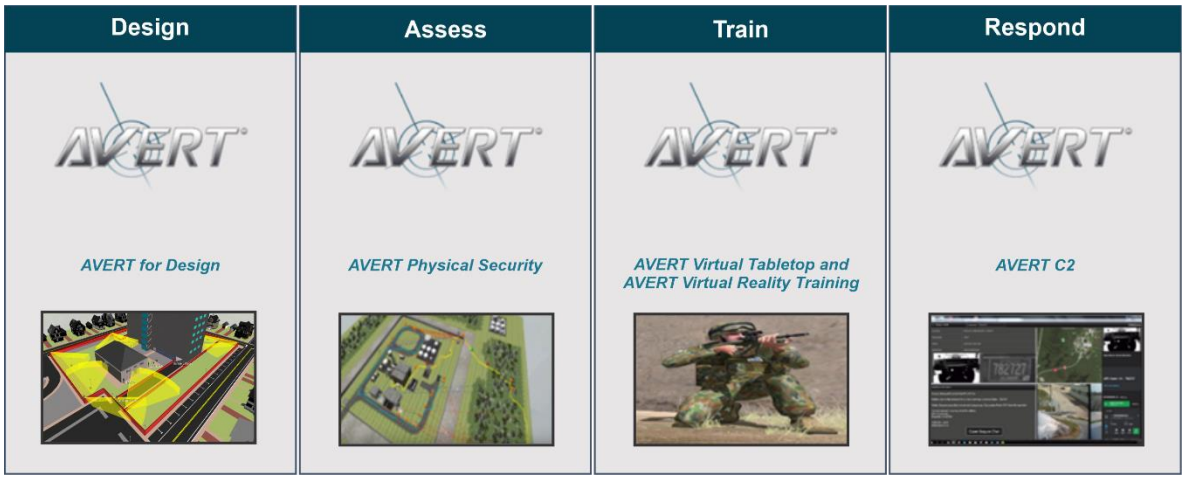

Figure 1: AVERT Software Suite

Using the AVERT SRA in the performance of evaluation, NPP Security SMEs are able to analyze data from thousands of simulated attacks to make improvements and gain efficiencies. ARES Security has helped users increase security effectiveness while saving millions of dollars in reoccurring costs. The average return on investment associated with security optimization in the commercial nuclear market is less than one year, and savings consistently achieve net present value between $15M and $50M per plant.

7.2 Client Cost Savings

The following examples provide insight as to how various utilities have been using the AVERT Physical Security software to improve their use of security expenditures. AVERT analyses were used, or are being used, to support NPP changes to their security plan (without decreasing physical security plan effectiveness) as permitted in 10CFR.50.54 (p). In addition, AVERT can also be used as primary or supporting information as part of these submissions.

Public Service Enterprise Group (PSEG) used AVERT Physical Security to assess whether its deployment of protective force was optimal at Salem-Hope Creek. Xcel Energy used AVERT to identify capital improvements that would allow for a reduction in operations and maintenance (O&M) costs for long-term cost-savings at the Monticello NPP. Dominion Energy used AVERT to perform a two-phased analysis to address both of the above issues.

Over the years, PSEG had periodically added response posts to address perceived weaknesses in preparation for FoF exercises. Prior to the use of AVERT, PSEG had not conducted an overall evaluation of its security system performance as part of upgrade decisions. PSEG questioned whether all response positions were making true contributions to the protection of the facility. The AVERT Physical Security analysis used many of the analytical capabilities of the software, including the ability to remove fighting position posts and other defense-in-depth measures,

resulting in the determination that not all positions were making significant contributions to the protection of the plant. Examples of these savings are outlined later in this document. As a side benefit, the analysis provided additional insights. One of the most useful ones related to the question of training versus flaws in the poor design. Prior to the use of the tool, if a member of the protective force was “killed” in a FoF exercise, PSEG required the individual to be retrained. However, the AVERT analysis identified the same individual as being “killed” by the adversarial force. Since the model assumes that the protection system is performing as designed, it was clear that these were not training issues. Rather, they were a result of an improper design of the protection system. In the end, PSEG was able to reduce the number of response position posts.

Xcel Energy had different issues at Monticello. The question of what constituted an optimal number of response position posts within the protective force was high on the list. Another issue arose out of a recalculation of the 100-year flood levels. As a result of the recalculation, the plant had to make some interim changes in its positioning of protective force officers. Rather than continue over the long term with the interim measures, Xcel Energy opted to do a complete assessment of its protective program using AVERT. The assessment considered numbers of responders, the positioning of responders, fencing and other barriers, as well as the location and heights of towers. In the end, Xcel energy opted to implement a significant capital improvement program, using AVERT Physical Security and AVERT Advanced Behaviors add-on module, that reduced O&M costs and reduced the overall security costs at Monticello over the long term, without adversely impacting the overall security system effectiveness.

Dominion Energy, also an AVERT Advanced Behaviors user, implemented a two-phase initiative to seek O&M cost savings at three of its Dominion Energy sites utilizing the AVERT software to optimize security resources while maximizing overall response effectiveness. The first phase operated under the assumption that no physical modifications would need to be made to the plant to achieve the projected savings. Phase 2 will take the next step and seek cost savings accompanied with capital improvements. The goal for this effort was an annual savings of $1.1M for each phase, due to post eliminations in conjunction with strategy modifications which would result in savings of approximately $9.9M over a 10-year period across the Dominion fleet.

Phase 1 was completed at two sites without physical modifications to the plants. These program adjustments were made using multiple tools (tabletops, SMEs, verification drills, historic data from FoF exercises/focused drills, etc.) and validated using AVERT computer modeling. This resulted in an annual savings of approximately $734,000. Using AVERT, Dominion Energy determined that the

third site was not able to make any changes to the protective strategy without accompanying physical modifications to the plant.

Phase 2 is under way and considers plant modifications. AVERT modeling was used to validate the conceptual plant modifications for each site prior to seeking funding to support the changes. Plant modifications have been identified at one site and work has begun. The analysis for the second site is approximately 50% complete and the third site is about 90% complete. AVERT modeling was used to determine the minimal physical modification(s) that would be needed to meet the savings target, while optimizing the protective strategy effectiveness.

AVERT Physical Security has a history of allowing commercial utilities to transform their protection of NPPs. In addition to security assessment, AVERT also has demonstrated value in the design process. It is important for NRC and the industry to work together to develop an approach that allows these SRA tools to be used seamlessly in the regulatory process.

7.3 Increased Cost Savings

An AVERT Physical Security assessment is the entry point for cost savings. As presented above, an AVERT Physical Assessment project has, on an average, eliminated 1-3 security posts or equivalent savings per site. This results in an average cost savings of $0.5 - $1.5M/year.

ARES Security is confident in the cost savings effectiveness of AVERT Physical Security. If a client pursues an AVERT Physical Security assessment project (software purchase and assessment), and ARES Security cannot identify the reduction of 1 security post, or the equivalent in cost savings per year, the client will have an option to only be charged for the assessment and can return the software at no charge.

The AVERT 3D Digital Twin model is a key deliverable of an AVERT Physical Security assessment project. The 3D Digital Twin model is the common thread for the entire AVERT software suite ecosystem. Using the 3D Digital Twin model, additional cost savings have historically been validated for:

- Advanced Assessments – Through the use of the AVERT Physical Security add-on module Advanced Behaviors, clients have been able to eliminate additional site security posts and reap additional cost savings. By using Advanced Behaviors, clients have eliminated up to 18 security posts while improving overall security.
- Design – Through the use of AVERT for Design, significant savings can be realized by quantifying and optimizing security designs during the design process, prior to any procurement or installation.

- Training – AVERT Virtual Tabletop and AVERT Virtual Reality Training tools have shown increasing promise to add capability and reduce the required manpower and associated expenses while increasing awareness and reality for exercises (i.e., FoF) and training. Since these tools run in a distributed client/server environment, they have the potential to effectively address remote or isolation requirements, such as those associated with COVID-19 social distancing requirements. These capabilities bring significant additional and long-term value to the 3D Digital Twin model created during the SRA assessments outlined above.
- Command and Control – The AVERT C2 software automates the security system, provides a tool to predict future "what if" scenarios and incorporates the latest technological components including robotic sentries, UAS and ROWS. ARES Security is dedicated to creating the next generation C2 system for use in US NPPs. ARES is currently working with DOD (USAF) in the development of next generation systems.

8. Conclusions

It is clear that a consistent use of a structured and integrated assessment of the security of NPPs must become an integral part of the regulatory process. This can only be done using sophisticated SRA tools for security, similar to the software that is commonly used to perform probabilistic risk assessments (PRAs) at NPPs around the world. Consistent use of SRA tools to assess security at NPPs will lead to more cost-effective application of security at these plants. It will enable effective deployment of compensatory measures when elements of the security system fail or go into a maintenance mode. It will also provide for more effective security during outages and decommissioning. The future direction of these technologies also appears to offer significant future savings. These are all lessons that can be learned from the experiences of DOE and DoD at its nuclear facilities.

The NRC and the industry need to work closely together to better integrate these tools into the regulatory process, so that both the regulator and the industry are comfortable with how the tools are used.

FOR QUESTIONS AND ADDITIONAL INFORMATION

Jerud E. Hanson, CEO

+1-202-730-2505 | info@USANuclear.org

USA NUCLEAR

USANuclear.org

ARES SECURITY

TO LEARN MORE ABOUT AVERT

Jim Raines, Vice President

+1-630-956-0519 | JRaines@ARESSecurityCorp.com

ARES Security Corporation

AresSecurityCorp.com