Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting August 23-26 & August 30-September 1, 2021

Using AVERT Physical Security (AVERT-PS) to optimize physical security effectiveness at the South Texas Project Electric Generating Station

Jim Raines
ARES Security Corporation

Kip Rowh
South Texas Project Electric Generating Station

Joel Edwards
ARES Security Corporation

ABSTRACT

ARES Security Corporation (ARES) flagship product, AVERT, is an established suite of all-encompassing software solutions for the entire physical security life cycle from design to operations. AVERT transforms physical security planning and assessment from a dependence on the qualitative judgement of subject matter experts to a science based on a 3D digital twin, physics-based quantitative modeling, simulation, and artificial intelligence. The AVERT software suite is actively used by 65% of the USA commercial nuclear plants, along with industrial, corporate, and government organizations and has a proven track record of effectively assessing and optimizing security systems and identifying subsequent cost savings. One member of the AVERT software suite, AVERT Physical Security (AVERT-PS) is unique Security Risk Assessment (SRA) software used to perform a facility Vulnerability Assessment (VA) along with providing the capability to visualize, quantify, assess and optimize security posture. This solution's holistic and integrated approach, delivers accurate, measurable, and repeatable assessments of physical security design and operations. AVERT-PS provides security analysts with the capability to make security decisions based on quantitative, physics and probabilistic risk-based models and provide decision makers with a detailed understanding of the effectiveness of their physical security systems and operations against evolving threats. The South Texas Project (STP) has been actively using the AVERT-PS software to assess and optimize security posture since 2018. In 2019, the South Texas Project (STP) initiated a program to optimize their security posture using AVERT-PS as a tool to support these activities. This paper will present in a high level, non-SGI generic format the types of changes implemented along with the improvements to security posture and resulting cost savings.

INTRODUCTION

Developing, implementing and refining a nuclear facilities physical security posture requires a large amount of expertise and experience. Ensuring public safety is the responsibility of the maintenance, operations and security departments at nuclear facilities. This paper will describe the activities performed by the STP security department leveraging the use of conventional and cutting edge modeling and simulation technology.

SOUTH TEXAS PROJECT (STP)

The South Texas Project (STP) nuclear facility is a 2700 MW dual unit Westinghouse Pressurized Water Reactor (PWR) electric generating station located in Bay City, Texas about 90 miles southwest of Houston, Texas. The STP Unit #1 was issued an operating license on March 22nd, 1988 and renewed on September 28th, 2017 for an additional 20 years of operation with that renewed license expiring August 20th, 2047. STP Unit #2's operating license was issued on March 28th, 1989 and like Unit #1 renewed their license also extending operation to at least December 15th, 2048.

The following aerial view of the STP facility provides an overview of the site's owner controlled area (OCA) and Protected Area (PA).

The OCA and PA security zones each carry their own physical security requirements. The STP physical security posture is established to prevent the threat of radiological theft or sabotage at the facility. This will assure the general public will not be subject to undue risk due to radiological or other risks.

The STP physical security posture was developed, established and is actively maintained through a well-developed process that has evolved and improved over the years. The process is in compliance with all of the U.S. Nuclear Regulatory Commission (NRC) rules and regulations. To briefly summarize the process, a nuclear power facility security posture is established to assure mal intentioned individuals, or more commonly called adversaries, are not permitted to compromise or steal radiological assets that could be used to subject the public to undue risk.

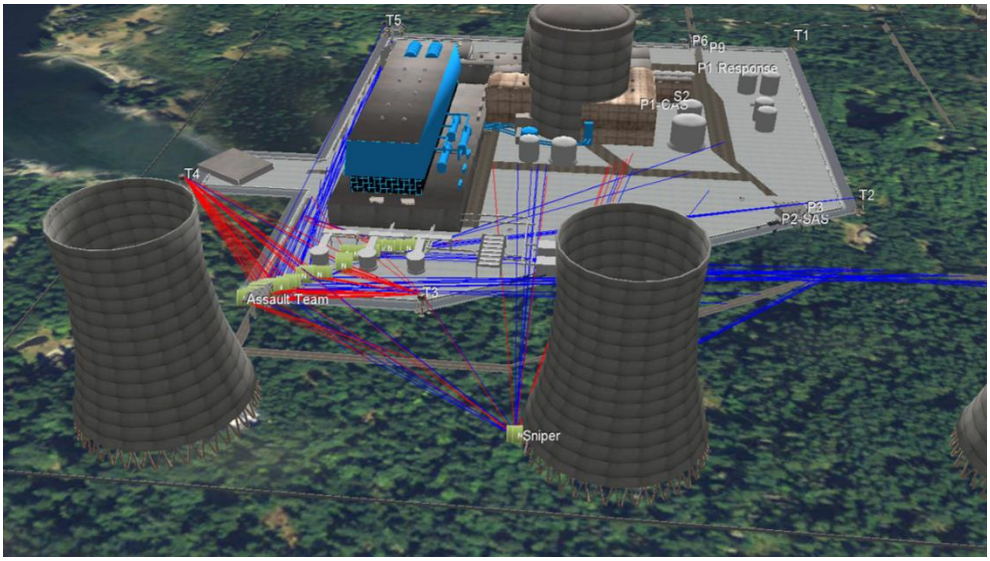
Security posture is similar to the tactics employed a sporting event, for example a football game. The security posture includes both offensive and defensive tactics and like football, nuclear security includes an enormous amount of training and exercises to hone effectiveness. Physical security defensive tactics includes items such as fences, barriers, video cameras, sensors and many others. In regards to physical security offensive tactics, these includes items such as armed security officers, patrols, and strategies designed to interdict and/or neutralize a threat prior to, and many others.

With the mission of nuclear power facility security being the protection of the general public from a radiological release, the critical assets that require protection need to be defined and then procedures, programs, equipment, training and exercises need to be established to fulfill the mission statement. Within security, the critical assets combine to create a "Target Set". A Target Set identifies a given set of components that together, if compromised or destroyed could have a detrimental effect on the safety of the plant and potentially resulting in radiological consequences. An example of a Target Set could be an emergency cooling pump, controls and instrumentation that is essential for maintaining the plant in a safe state. Once defined, the security posture is then developed, trained upon, implemented and continually refined to fulfill the security mission statement.

The establishment and refinement of a site's security posture is a complicated process that includes both offensive and defensive tactics. Until recently, nuclear power facility physical security have relied on subject matter experts (SME) judgement to define a set of measures deemed to fulfill the security mission statement. In 2018, STP adopted the ARES Security Corporation (ARES) AVERT Physical Security (AVERT-PS) software to build upon the knowledge and tools already in use at the site.

AVERT Physical Security (AVERT-PS)

AVERT-PS is unique Security Risk Assessment (SRA) software used to evaluate physical security posture, perform Vulnerability Assessments (VAs) and facilitate training of the facility along with providing the capability to visualize, quantify, assess and optimize security posture. This solution's holistic and integrated approach, delivers accurate, measurable, and repeatable assessments of physical security design and operations. The AVERT-PS software system provides asset owners and security analysts with the capability to make security system investment decisions based on quantitative, probabilistic risk-based models. The following is a generic representation of an AVERT-PS simulation for a hypothetical nuclear power plant



AVERT-PS's intuitive user interface can quickly create a realistic 3D Digital Twin model of the facility that includes interior and exterior features or structures, access points and entrances, natural features, and the placement of both defensive tactics (i.e., active and passive barriers and detection tools) and offensive tactics (i.e., guards and deterrence systems). Once the site is modeled, the solution uses proven Modeling and Simulation technology along with Monte Carlo simulations in order to evaluate the comprehensive security design. AVERT-PS utilizes an

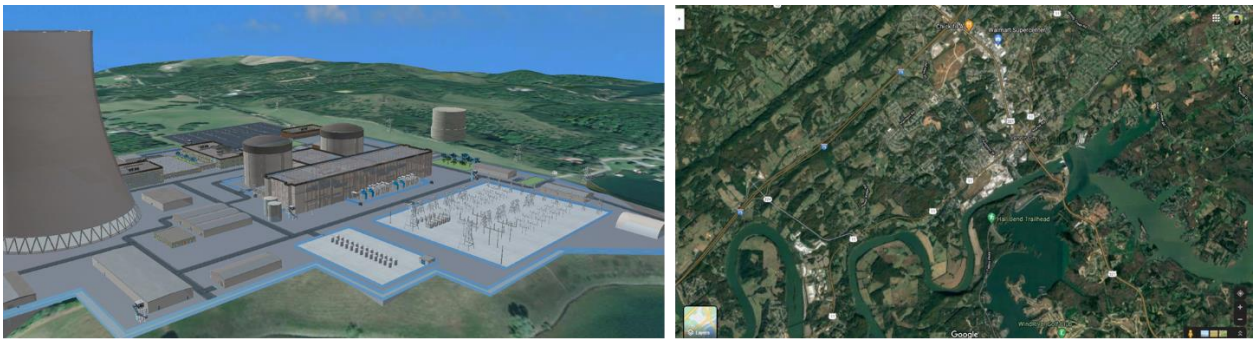
ARES exclusive automated pathing algorithm to determine the various pathways of adversaries, responders, and even natural hazards. The design of the AVERT PS software easily allows the ability to perform thousands of simulations and multiple variations within a compressed timeline. Through the use of enhanced reporting and output tools, all of the generated data can easily be mined and presented in easy to use and understandable reports.

The AVERT-PS assessments provide the organization with a complete understanding of the facility's security posture and response to address vulnerabilities and optimize configurations for both effectiveness and costs. The parameters can easily be changed within the model to address a wide range of security system configurations, threats and targets. Once the vulnerabilities and pathways have been identified and analyzed, a baseline assessment can be established. This baseline assessment can then be compared to variations of the security posture such as changing and testing newly modeled sensors, systems, and procedures. Through the evaluation of various "what ifs", a quantified assessment of a site's existing and potential new/revised security posture can be performed. This quantitative approach provides a cost-effective means to continually assess risks and optimize your security's effectiveness against your budget. Thus resulting in a thorough understanding of a site's return on investment. AVERT-PS clients have identified a wide range of cost savings, while maintaining or improving security posture.

The most common cost reduction that AVERT-PS has identified through this process is reducing existing security posts. The industry average cost to maintain a security post is approximately $575K per year (with a cost range of $375K-$1200K per year). Assuming an average facility lifetime of 25+ years, a single post reduction can result in an overall NPV of $6M or more. Typically, multiple Post reductions are identified during an AVERT-PS assessment project. Post reductions of 1-3 posts, with limited capital investment, and upwards of 14 posts with capital investment have been achieved. In such cases where capital investments are used to generate additional staff reduction, AVERT-PS is used in the design and justification of the capital investments to ensure minimum spending and optimizing design while improving or maintaining effectiveness.

Fictitious Lenoir NPP model

The following is a brief overview of the fictitious Lenoir nuclear plant that will be used in this paper for demonstration purposes. As shown in the following images, the Lenoir plant has all the same components and security posture as an operating nuclear power plant, without the restrictions of containing nuclear safeguards information (SGI). So it is very convenient to use for demonstrations.



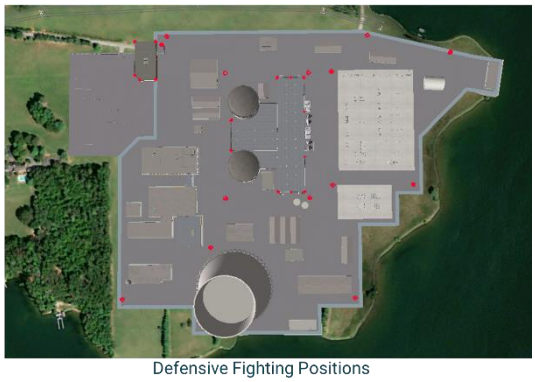
Lenoir nuclear power station - Fictitious plant sited in Lenoir City, TN

Aerial view of the Model

The Lenoir model includes detailed building interiors so that security response within buildings can be modeled.

Detailed Building Interiors

Like all nuclear facilities, strategic defensive fighting positions are established and manned accordingly to protect the plant's critical assets. These positions are shown in the following image by the red spots within the plant.



Defensive Fighting Positions

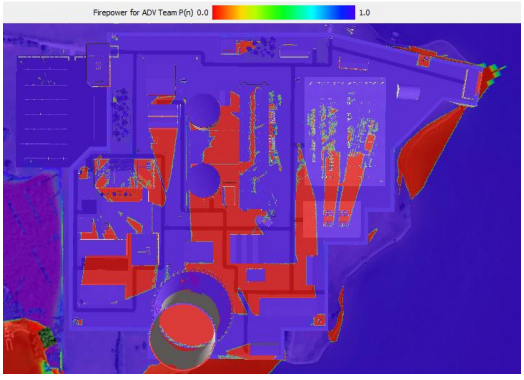
Each plant has several types of delay systems deployed to maintain a secure environment. These delay systems include items such as walls, fencing, razor wire and others. The following image presents the delay systems modeled and highlighted in red.

Delay Systems

Along with delay systems, each plant has several detection systems to identify when an adversary is trying to enter the plant's protected area (PA). These systems include items such as perimeter intrusion detection system (PIDS), video surveillance and others. The following image presents the Lenoir detection system by the maroon coloring on the plant overview image.

Detection Capabilities

The following image is an AVERT-PS generated heat map that provides the entire site probability of neutralization, based upon the various guards located around the Lenoir facility. In this image the color coding changes from red to blue as the probability increases for 0 to 1.0. For this heat map, the color red represents a 0 probability of neutralization (i.e., areas outside line of sight of guards) and the color blue represents a 100% probability of neutralization. It should be noted, the AVERT-PS software provides quantified results for all of the information generated and that information can be expanded to justify any changes to security posture. The ability to quantify and examine security posture modifications is a key attribute that is used to evaluate and justify security changes.

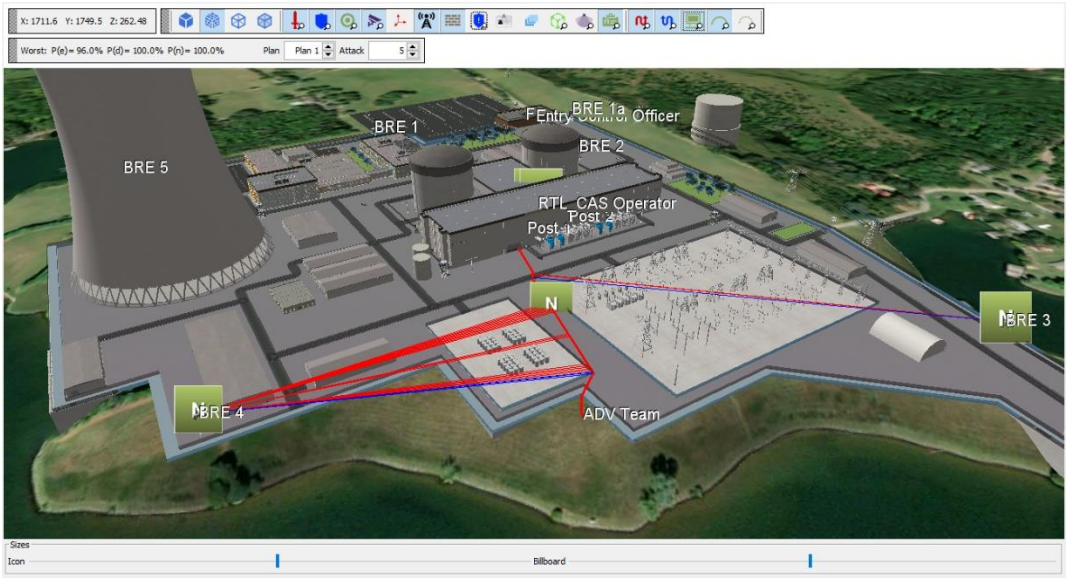


STP's use of AVERT-PS

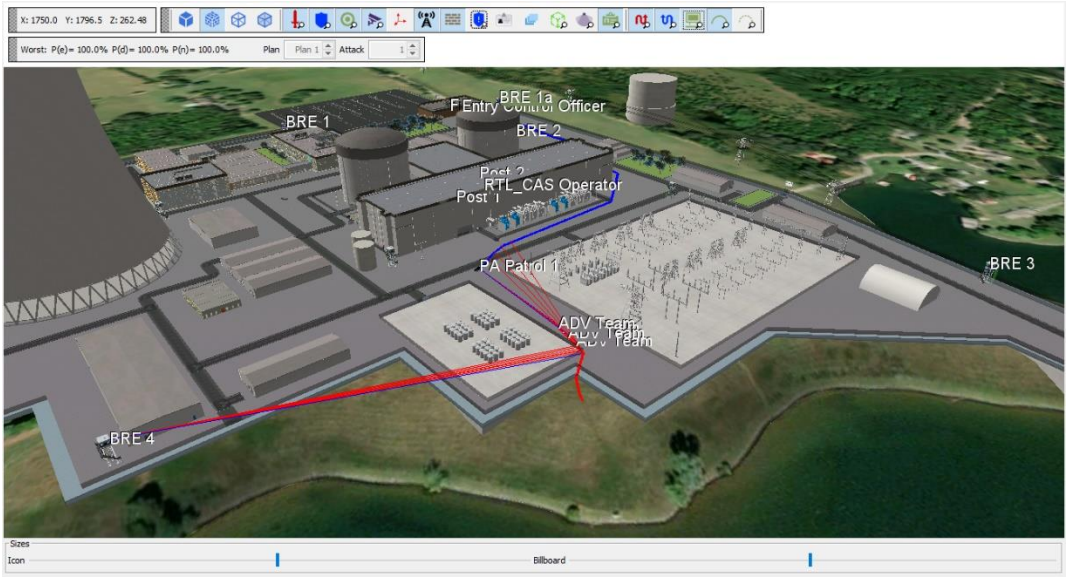
As previously mentioned, STP has been using the AVERT-PS software since 2018. In 2019, STP initiated a large physical security modification program. Since nuclear power security involves the use of Safeguards Information (SGI), the specific details of the activities performed at STP cannot be publicly presented. So for this paper, generic modifications and assessments that could have been performed during the STP project will be presented, described and discussed. In addition, along this same tact, for the information presented in this paper the STP plant will not be used but rather the fictitious Lenoir nuclear power plant, will be utilized for all illustrations.

AVERT-PS has unlimited possibilities to evaluate security elements to determine both their security effectiveness and cost efficiency. For this paper, we will present a few sample applications using the fictitious Lenoir nuclear plant. It needs to be kept in mind, that physical security is a very complicated process with many moving parts. For the purposes of this paper, the examples presented will be simple illustrations of the capabilities that AVERT-PS provides to understanding and optimizing physical security. The results from the simple examples alone should not be used to make security posture decisions. But together in the integrated AVERT-PS simulations each of the interacting components are address resulting in a highly quantified physical security assessment.

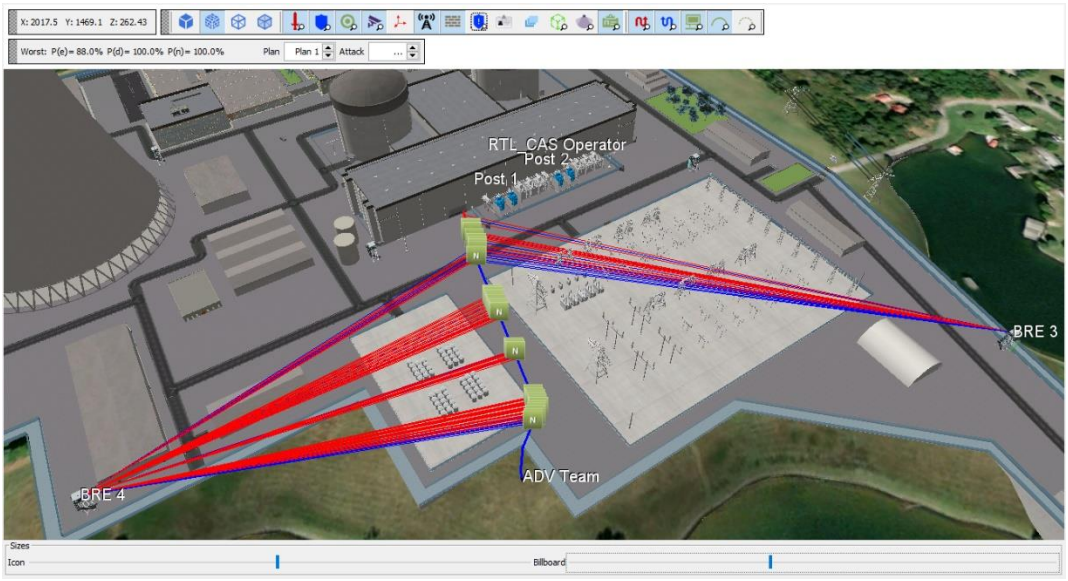
The use of roving security vehicles is a response that is deployed at nuclear plants. For these assets there are numerous questions to be answered: how many rovers, what interval should they patrol, how should they be equipped, etc. One of the basic questions to be asked is how does a roving patrol car effect the overall site Physical Security system effectiveness [P(e)]. An AVERT-PS simulation was run to compare the use of fixed security posts, elevated bullet resistant enclosures (BREs) compared to the removal of one of the site's BREs and replacement with a roving patrol car. The first image presented shows the site P(e) for the BRE only utilization at 96%



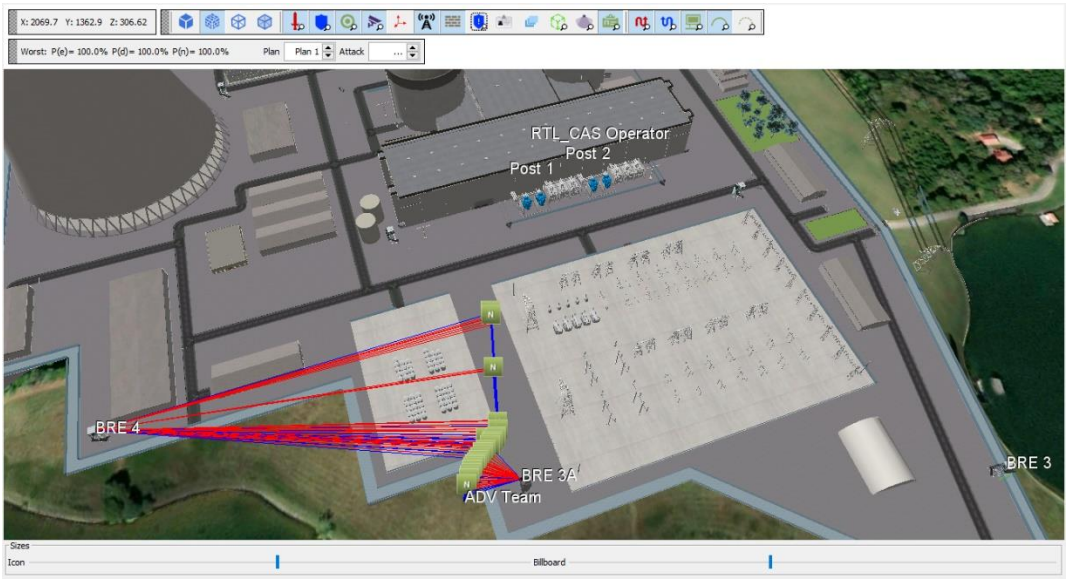
That same simulation was then evaluated but in this case the BRE3 post was disabled and replaced with a roving patrol car. The following image shows an improved P(e) of 100%.



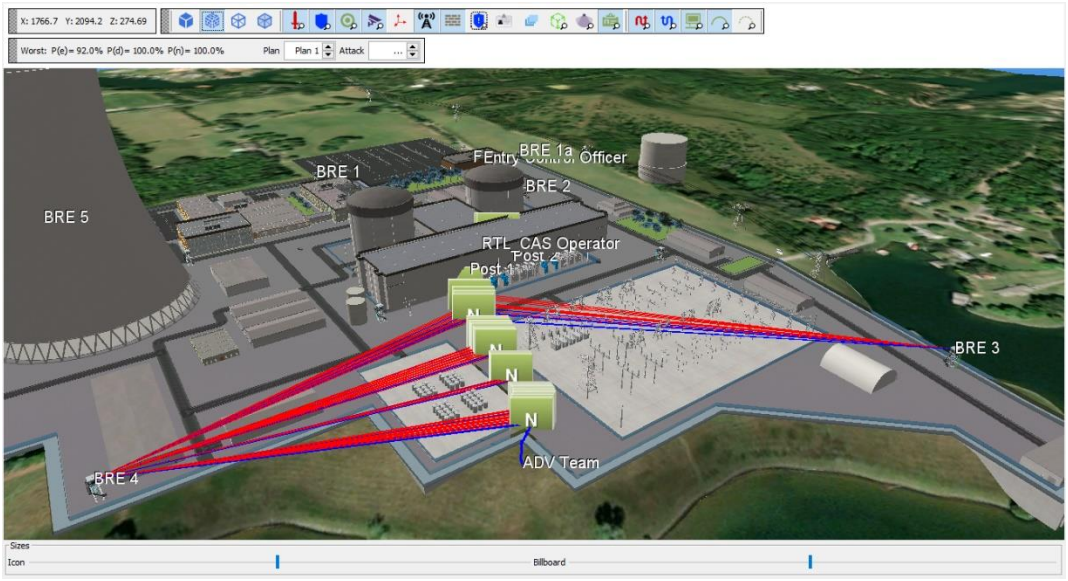
The next example is the addition of a new elevated BRE at the site. The first image illustrates the location and positioning of elevated BREs can make a significant impact on overall system effectiveness.



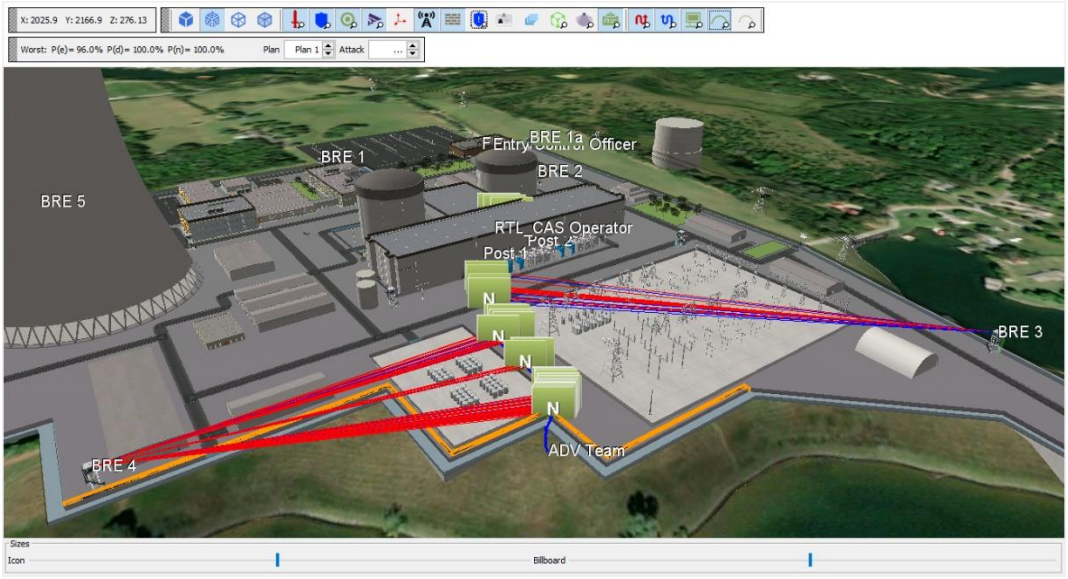
For this example BRE4 has limited and BRE3 has no sight of the attacking adversary team. The system effectiveness is calculated by AVERT-PS to be 88%. With the addition of a new elevated BRE (BRE3A) the system effectiveness increases to 100%.



The last example illustrates the effectiveness of barriers. Without interior barriers, the system effectiveness is 92% as shown by the following image.



With the incorporation of an inside fence barrier (highlighted in orange), the physical security effectiveness increases to 96%.



CONCLUSION

The use of the AVERT-PS modeling and simulation tool has expanded the capabilities of the STP security team by providing an industry acknowledged software tool that can evaluate potential future security modifications for both physical security effectiveness and cost efficiency, prior to any construction. STP has been able to optimize security and generate cost savings all while maintaining or improving security posture.