CORPORATE AND CRITICAL INFRASTRUCTURE SECURITY OPTIMIZATION

CFO WHITE PAPER

EXECUTIVE SUMMARY

In today's environment, the corporate C-Suite is faced with the challenging task of preserving operating margins in the face of economic headwinds resulting from the ongoing global pandemic. Chief Financial and Operating Officers are faced with the difficult task of optimizing cost structures within their businesses to sustain bottom line performance, ensuring business continuity and positioning for growth in a post-pandemic economic recovery period. While most executives realize that operational efficiencies and cost reductions can be realized through the deployment of advanced technology solutions, many still struggle with the decision to invest in technology automation. Although Return-on-Investment (ROI) justifications seem to make sense conceptually, actual ROI uncertainty leads to hesitation or indecision with respect to making actual investments and implementing the operational changes that the adoption of technology often requires. What executives need most is assurance that technology driven change can be successfully be implemented and will produce the expected efficiency gains and ROI.

OBJECTIVE

Reduce Operational Costs, Minimize Capital Expense and Realize immediate ROI while concurrently Increasing Organizational Security Posture

EXECUTIVE SUMMARY CTD.

The use of technology to increase automation, improve manufacturing/production yields, manage staffing more efficiently and allow for remote workers has played a key role in operating margin improvement for enterprises that have made the leap. Despite these efficiency gains achieved through the use of advanced technologies, one area of operations that remains woefully unautomated and therefore non-optimized is Corporate/Enterprise Security. The global security market is approaching US$300B in annual spend with approximately 50% related to on-site security staffing. The balance is spent on deploying and maintaining new technology to include security cameras, access control, throughput detection, other sensors and command and control systems. Companies and Government Agencies spend tens of millions of dollars on security for their corporate offices and manufacturing/production facilities to mitigate potential events such as active shooter, improvised explosive devices, theft, executive harassment and personnel security.

Corporate Security Executives, most of whom are ex-military or law enforcement officials, have significant field experience with security operations but often lack available technology based tools that would facilitate increased security while concurrently lowering operational costs. These Security Executives are inundated with new technology products such as smart cameras and sensors, a kinetic threat environment, fixed or shrinking budgets and often rely upon outside Subject Matter Experts (SMEs) that typically have exceptional operational experience but lack familiarity with available risk assessment, validation, optimization and training tools. Corporate Security Executives need technology tools that enable them to proactively architect new facility security systems and/or assess existing security infrastructure to increase protection while concurrently minimizing costs. The C-Suite relies upon in-house security expertise and outside SMEs for recommendations and needs verifiable evidence of the predicted outcome of these recommendations prior to committing to investment.

Given the realities stated above, current Corporate and Critical Infrastructure security systems are far from optimized for cost and security effectiveness. ARES Security Corporation (ARES) has completed over one hundred site security assessments across Corporate Offices/Campuses, Ports, Transportation Hubs, Transmission and Power Generation Facilities, Sports and Entertainment Complexes and Manufacturing Plants using our proven AVERT® technology. Without exception, all ARES projects have resulted in identified cost savings while maintaining or improving security effectiveness. By engaging with ARES, these clients were able to realize cost savings ranging from 10-50% of onsite security staffing and 20-70% of planned capital expenditures. Through the use of advanced 3D digital twin facility modeling and simulation software tools, security system effectiveness can be quantitatively validated, optimized and cost reduced. These significant savings can be identified in ANY organization and are not limited to only high security facilities. Security Executive and C-Suite stakeholders can reduce their reliance on outside SMEs and evolve from qualitative to quantitative decision making to improve security and decrease expense.

Based on experience, ARES is so confident in its tools and methodologies that it will provide a written guarantee that you will achieve agreed upon ROI targets and recoup your investment in less than 1 year. ARES challenge to each C-Suite executive who is responsible for the efficient operations and management of risk inside their global organizations is to take advantage of the opportunity to understand, test and optimize your security systems and practices through the deployment of ARES AVERT technology. Your company will not only enjoy the benefit of significant savings without risk but will also provide your employees and communities with a safer workplace.

The remainder of this white paper will be dedicated to an overview of the ARES AVERT technology, specific use cases and ROI examples that can be expected from the use of AVERT technology.

A NEW PARADIGM IN SECURITY

Historical Corporate Security Concepts of Operations (CONOPS) include detection systems (cameras and other sensors), delay systems (barriers, access controls and check points) and security personnel. These legacy CONOPS are designed manually utilizing the combined expertise of existing Security Personnel, outside SME's or perhaps even the expertise of outsourced guard forces from organizations like G4S or Securitas to determine the types of systems, sensors and number of guards required to "secure the facility". Although this approach is experience based and well intentioned, current risk profiles, rapidly advancing adversary technologies (i.e., Drones and UAS), and available toolsets to assess risk are well beyond the capacity of any individuals to fully comprehend let alone optimize and verify without the assistance of technology tools.

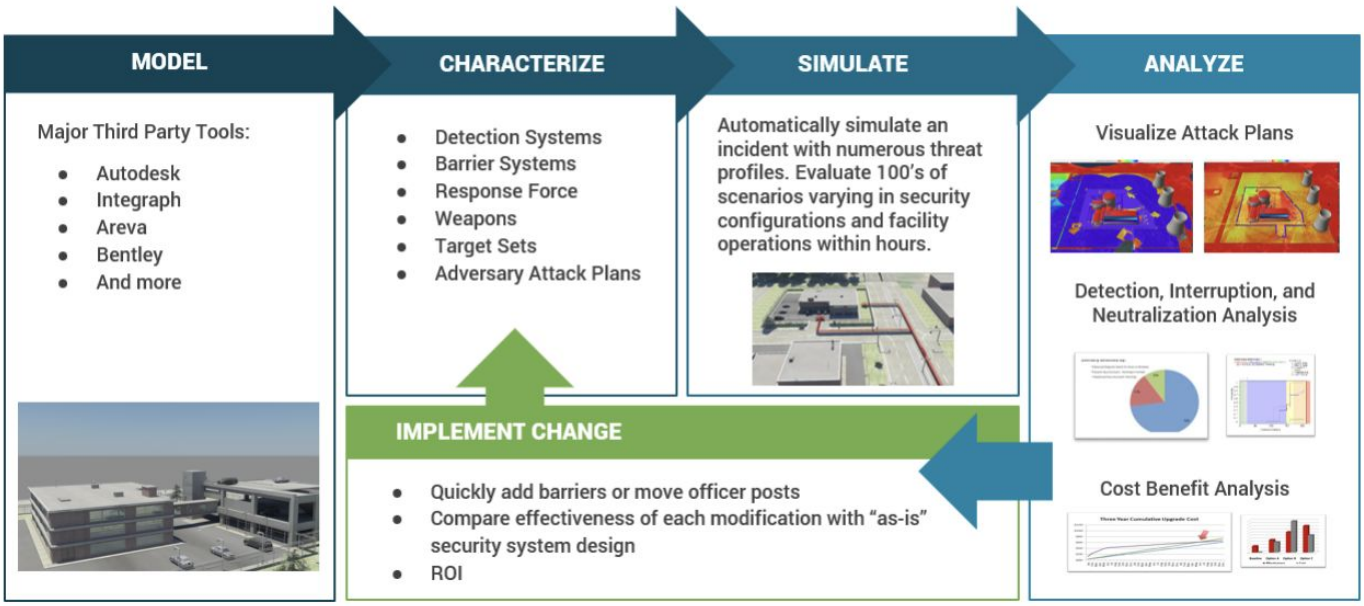
Security systems today may be comprised of hundreds of cameras, interlocking access control, shot detection and multiple response layers including existing guards and offsite (Police) response. The threats are wide ranging from active shooter, Improvised Explosive Devices (IEDs), theft, vandalism or nuisance intrusion. Building Information Management Systems (BIMS) are also part of the monitoring ecosystem which can affect the environmental risk profile depending on corporate or social situations. Stated simply, too much is expected from existing security experts and the numerous permutations of system configurations have become too complex to accurately assess and evaluate.

To overcome this complex environment, ARES has developed a software suite to support Security Professionals and optimize/automate security operations. The AVERT software suite includes tools for assessing physical security, performing tabletop exercises, training and a fully integrated command and control system. ARES AVERT Physical Security software provides a proven advanced simulation and modeling environment that rapidly generates a high resolution, 3D digital twin model of a designated site.

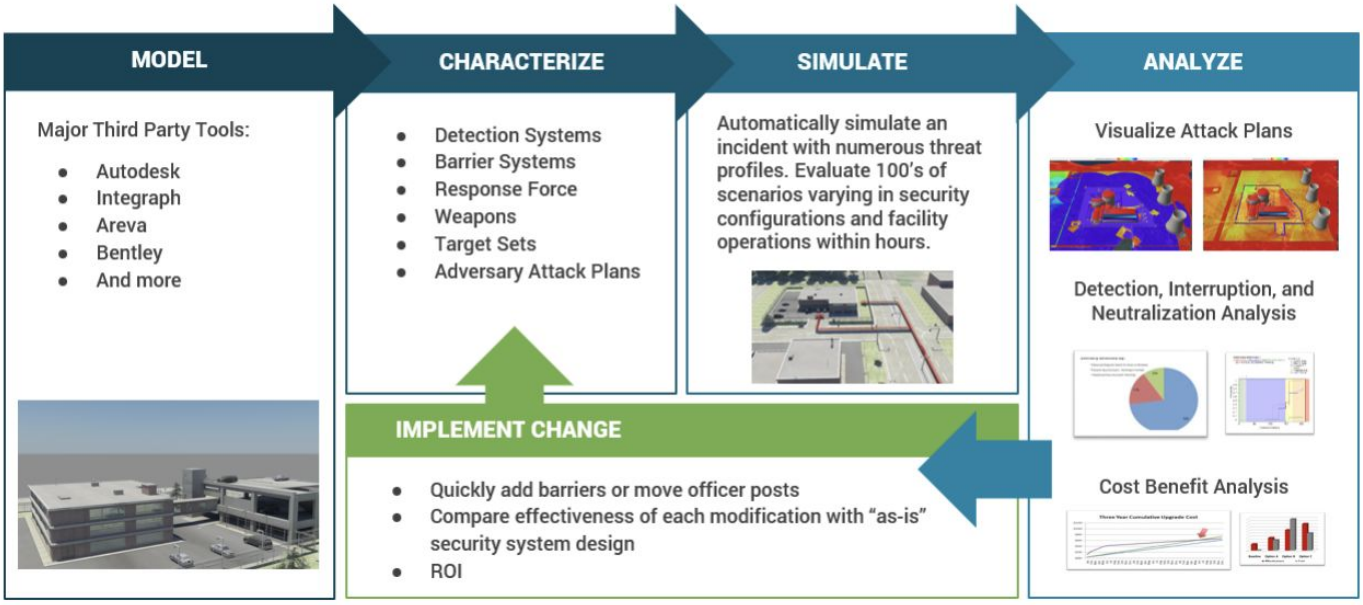
These 3D models provide a high-fidelity virtual representation of site security CONOPS which allow organizations to test both their existing capabilities and any planned changes for security effectiveness resulting in better insight and optimization. AVERT Physical Security is also the best available Department of Homeland Security Safety Act Certified solution on the market thereby limiting your liability while providing a level of assurance that Corporations and their staffs are implementing cutting edge measures to ensure safety and risk mitigation.

TECHNOLOGY DESCRIPTION

AVERT Physical Security is a unique security risk assessment (SRA) software tool that is used to visualize and quantify the performance of **any** physical security threat against critical assets and response plans. AVERT's holistic and integrated approach, delivers accurate, repeatable and quantified assessments of physical security design and operations. The AVERT software provides security analysts with the capability to make security decisions based on quantitative, 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. AVERT provides leadership insight into security plans and the objective data required to initiate security modifications in those areas that yield the greatest benefit and largest improvements to security effectiveness. AVERT allows security professionals and executive management to answer "why" security upgrades are required and justifies projects based on improved security effectiveness. This greatly improves objectivity in security design decisions. CONOPS changes and emerging threats can also be "tested" through thousands or tens of thousands of simulations prior to a real incident. In effect, the security solutions are optimized and verified before they are implemented. The following diagram depicts how AVERT is used in the physical security assessment process:



TECHNOLOGY DESCRIPTION CTD.



- MODEL: Develops an accurate 3D model of the facility, site or region that includes buildings, terrain, elevation, infrastructure, delay systems, detection technology, response forces and security plans. AVERT Physical Security guides the user through this virtual representation of their site using a wizard.
- CHARACTERIZE: Details each modeling element based upon detailed performance data from the AVERT Library which contains data on most security systems, platforms, weapons, and detection and delay systems. SMEs contribute data about guards, law enforcement responders and their level of proficiency. The site's security plan is also added to the system and includes target sets, adversary attack plans, tactics and objectives.
- SIMULATE: Conducts a comprehensive analysis to identify the best path for each adversary to access the facility or site based on their objective. The software then runs exhaustive simulated attacks for each of these vulnerabilities to determine overall security effectiveness.
- ANALYZE: Produces visualizations, charts, graphs and metrics to give users insight into the performance of security and operations. These powerful reports clearly and objectively justify new security system configurations or modifications to procedures.
- OPTIMIZE: Users can optimize their overall physical security system configuration and procedures with AVERT Physical Security assessments by evaluating numerous combinations of tactics and security system configurations and comparing security effectiveness with the operational and capital costs.

TECHNOLOGY DESCRIPTION CTD.

Thousands of Characteristics Modeled

ARES Security's Characteristic Library contain an extensive collection of validated performance characteristics. For instance, AVERT Physical Security knows the time it takes for a trained attacker with a 15 lbs weapons kit to run 100 meters up a 30-degree grade hill and cut through a 12' triple concertina wire fence. The following is just a small sampling of the threats, defenses, and sensors that AVERT has modeled:

- Video, Night Vision
- Eyes, Ears, Scent
- Public Reports
- BMS, Radar

- Fences
- Gullys, Mounds
- Bollards, Jersey Barriers
- Concertina Wire

- 2WD/4WD Vehicles
- Helicopters, Drones
- Boats, Humvees
- Foot Patrols

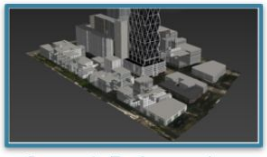
- Rifles, Shotguns, SMG's
- Mortars, Grenades
- Machine guns, Mini guns
- Explosives, IED's

AVERT Physical Security models security effectiveness to the fidelity of reality. This starts with the use of Commercial-off-the-Shelf (COTS) 3D modeling tools to rapidly capture terrain data and a 3D footprint for buildings, doors, passageways, barriers and location of communications and detection systems such as cameras, radar, IOT, communications technology and other sensors. Textures can be applied to building for visual reference. High fidelity modeling of specific locations can be captured if critical to the mission.

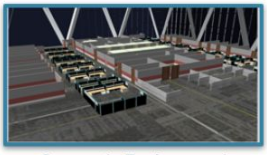
AVERT has a library of over fifty-five thousand elements that provide performance characteristics for the security elements in the model. This means that nearly any camera, sensor or weapons system that would be used at your site can be modeled. If a needed component is not included in the existing library, it can easily be added.

Massive amounts of quantified statistics are generated during an AVERT simulation. The overall site security probability of effectiveness is a rolled-up summary of the details which capture each event across thousands of simulations. As an example, heat maps which represent the coverage of detection devices, can be useful in evaluating how to create additional delay between the adversary and the target. Likewise, visual playback of each threat scenario and simulation can provide insight to vulnerable pathways, points of detection, shots fired and casualties.

AVERT Physical Security is a powerful modeling and simulation product that is easy to use and proven to have the robustness to provide quantitative security vulnerability assessments for critical assets. Without AVERT Physical Security, even the best subject matter experts would find these questions extremely challenging. This is exactly why AVERT Physical Security was developed and why many agencies within DOD, DOE, Commercial Nuclear, Critical Infrastructure and Corporations have found AVERT to be extremely valuable. ARES has validated the AVERT technology works and delivers on its optimization value proposition across many industries and project sizes. The AVERT screen shots below capture just some of the many examples where AVERT has been used to analyze threats and response plans from iconic public venues in New York City to highly secured sites focused on the protection of critical assets.



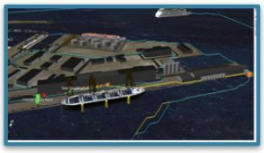
Corporate Environment
Exterior



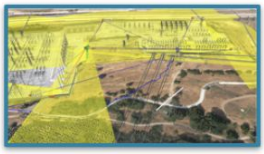
Corporate Environment
Interior

Public Venues

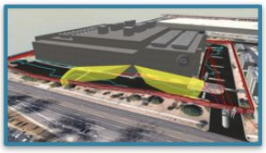
Transportation
Mass Transit



Transportation
Air/Seaports



Electric Grid



Data Centers

Law Enforcement

HOW DOES AVERT SAVE MY COMPANY MONEY?

ARES has conducted security assessments and optimized projects across hundreds of domestic and international sites. Below are examples of ARES AVERT Physical Security deployments with realized ROIs.

EXAMPLE 1: ANY PERIMETER DETECTION SYSTEM (CORPORATE OR PRIVATE)

The first example shows the use of AVERT to provide an optimized Perimeter Detection System design. This example (a real design project) is similar to **ANY** security camera project design that is being evaluated to provide additional coverage for parking lots, manufacturing sites, public or corporate campus or venues where perimeter detection is desired.

In this example, effectiveness of a security system design to protect the perimeter of a secure site is being assessed. Three designs are being analyzed:

1. A Baseline Design that represents a typical SME camera design (provided to ARES);
2. Alternative Design #1; and
3. Alternative Design #2 (both created by ARES).

All three designs include the same fencing, fence detection system and at least 20 Perimeter Protection Forces (PPF) on target at the fence line. The analysis, therefore, was focused on the camera coverage, camera types/design and the Probability of Detection P(d) of the cameras along the fence line. The alternative designs included evaluation of other camera systems that were part of the "approved for use" technology. A top-level summary of the options and the P(d) results are shown in the table above:

By deploying ARES AVERT technology, each design was verified in terms of effectiveness for the desired purpose (in this case the selected assessment criteria was chosen as Probability of Detection). In both additional options that were evaluated, the P(d) exceeds that of the baseline case at a lower cost of implementation. The decision to move past the baseline option to one of the options analyzed became obvious based on the chosen criteria. This also provided management with verifiable data in which to make the final design decision. In this case the increased effectiveness (and cost) of Design Option 3 versus Option 2.

The investment to gain this information through the implementation of AVERT Physical Security was approximately US$50K for a one-week assessment project which resulted in US$641K cost savings.

Design Scenario	Fixed Cameras	PTZ [1] Cameras	Number of Poles	P(d)
Baseline	40	0	40	86.4%
Option 1	24	4	15	90.1%
Option 2	33	4	17	99.7%

(1) Pan/Tilt/Zoom

	Option 1	Option 2
AVERT® Costs[1]	$50,000	$50,000
AVERT® Based Savings	$641,000	$573,000
ROI	1182%	1046%
Payback Period	Immediate	Immediate

(1) Includes AVERT® Project Software License and implementation costs.

EXAMPLE 2: LARGE SECURE MANUFACTURING FACILITY

ARES has modeled numerous highly secure manufacturing facilities. Because these facilities have very complex security systems and legally mandated requirements, security effectiveness must be assured. Sample clients would be Commercial Nuclear, Department of Defense, or high security manufacturing sites. ARES has conducted dozens of these assessments and optimizations which include detailed modeling of "as is" conditions, defense-in-depth analysis and "what if" assessments. These more extensive assessments may take up to 6 months to complete at an average cost of US$750K for the Physical Security assessment.

Although seemingly expensive, these assessments have resulted in **annual** savings from a minimum of US$1M up to US$5M. These savings are mainly generated from reductions in site security personnel and the associated infrastructure and equipment ranging between 15 and 50% depending on the site. In each case security effectiveness was maintained or improved. Savings can often be much more, as an example one site saved more than $17M in planned capital **and** the anticipated average annual savings. The AVERT Physical Security large scale implementation cost of US$750K includes the purchase of a **perpetual** AVERT Physical Security Software license that would be owned by the client and deployed within the client's ongoing operations for continuous cost savings from future security staffing savings as well as design analysis for capital improvements.

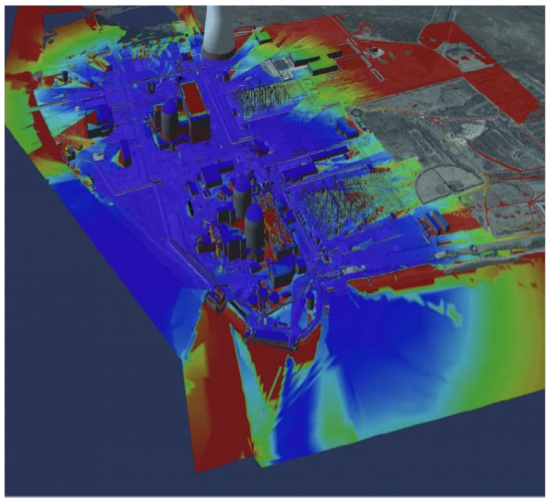
ARES maintains multiple technology sales models to best fit the client's needs from project only licenses to software lease and Software as a Service (SaaS) models that significantly reduce the upfront investment required. In the table shown, the investment ROI is based on the purchase of an AVERT Physical Security perpetual license, all hardware to support secure modeling, with three years of software maintenance. Additional savings (security reductions) beyond year 1 are not included in the projected ROI but would be expected in practice to further increase the above ROI results.

Below is a firepower heat map (blue is good, red is bad) of one of the sites that was modeled. The "after" captures shows improved coverage despite a 14 post (approximate 55 person) reduction in security personnel.

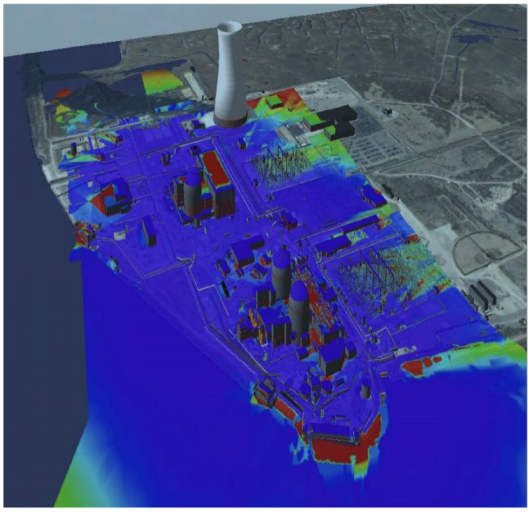
Since many manufacturing or operational facilities such as pharmaceutical, aerospace, airport, ports or other critical infrastructure sites have simpler but critical security systems, ARES cost scales downward as does the time required to complete the assessment. This linear correlation has been found to essentially maintain the same level of ROI/Payback period of more secure sites but at lower invested cost.

The investment to gain this information through the implementation of AVERT Physical Security was approximately US$930K for a six month assessment project which resulted in US$9M of annual cost savings.

Not Just Cost Savings: Improved Effectiveness



BEFORE: Post Reductions



AFTER: Post Reductions

EXAMPLE 3: CORPORATE SECURITY

ARES recently conducted an assessment on a large Corporate Campus. This model was utilized to analyze active shooter events in key locations including the call center, lunchroom and executive suite of offices. During the implementation phase while the virtual 3D model was being developed, it was determined that there were numerous previously planned security upgrades including the addition of shot detection technology. This technology was to be rolled out in phases. Phase I was already approved and included upgrades inside their key buildings at a capital investment cost of US$2.5M. The entire capital investment project for the campus was estimated to be approximately US$7.5M. ARES was able to determine that the impact on security effectiveness of this investment was **ZERO.** Based on the configuration of the site's security and response plans, it was determined that shot detection provided **NO** benefit during response scenarios. It was also determined that improvements in response time were required to mitigate the modeled active shooter attack. Most of these improvements required a much lower or no capital expenditure.

Scenario Average Time Post Detection to Scenario End	Time in Seconds	Estimated Fatalities
Security Officers with Current Weapons (Pistol)	137	95.9
Security Officers with Upgraded Weapon to 5.56mm (Rifle/Pistol)	128	89.6
Security Officers with Upgraded Weapon to 5.56mm (Rifle/Pistol) also with Segway's to increase response speed (12 - 15 mph)	37	25.9

The table shown above represents the original timelines, and recommendations that were made by ARES to further mitigate the impacts of the event.

The cost of this project was approximately US$300K, and the effort required was about 90 days. The resulting savings from cancellation of the "shot detection" project was $2.2M. Additional savings of $1.5M per year were achieved from the replacement of existing guards with high throughput badge scanners which were identified as an option due to the limited impact on effectiveness of these guard positions.

EXAMPLE 4: UTILITY ELECTRIC DISTRIBUTION SUBSTATIONS

ARES, in partnership with one of the largest power companies in the United States, modeled and provided a risk assessment of the client's fleet of 41 High Voltage Substations. These substations, which fell under NERC-CIP-14-02, were identified for a significant security upgrade. Using AVERT technology, the ARES team reduced the planned capital investment across these substations by approximately US$61.5M. The analyses allowed all factors such as offsite response time, terrain, sensors packages and non-lethal deterrents through multiple options to be evaluated for improved site security at minimum capital investment. Each substation model was conducted virtually and took approximately two weeks per substation. As an added benefit, the completed "3D digital twin" models remain available for future assessments or re-evaluation of changes in threats or risks to the substations.

The investment to gain this information through the implementation of AVERT Physical Security was approximately US$1.2M which resulted in US$61.5M cost savings.

	Project Implementation [1]
AVERT® Costs	$300,000
AVERT® Based Savings [2]	$6,700,000
ROI (3 Years)	2133%
Payback Period	Immediate

(1) Includes AVERT® Software (for the Project Implementation Period) and Implementation Services.

(2) Initial Savings of $2.2M for Capital Investment avoidance plus 3 years savings from guard replacement.

	Project Implementation [1]
AVERT® Costs	$1,200,000
AVERT® Based Savings [2]	$61,500,000
ROI	5025%
Payback Period	Immediate

(1) Includes AVERT® Software (for the Project Implementation Period) and Implementation Services.

(2) Savings of $1.5M per substation (41) total.

SUMMARY AND CLOSING

Driving operational efficiencies and lowering costs while maintaining or improving security effectiveness is no longer an impossibility with today's technology advances. ARES AVERT technology is simple to deploy and user friendly to utilize for current operations or future assessments or training. C-Suite Executives who have historically balked at technology based capital improvement investments due to ROI ambiguities or uncertainties can now make those investments with confidence. ARES Security's AVERT technology provides a PROVEN method to assure ROI. **ARES will guarantee that any Clients adopting this technology will realize a minimum 100% ROI and a maximum payback period of one year.** Although every client will be unique in their operations and savings potential, ARES technology can play a significant role in driving increased security while concurrently lowering operational and capital expense thereby increasing profitability.

Ben Eazzetta – CEO
ARES Security Corporation

For more information visit www.aressecuritycorp.com
or email contactus@aressecuritycorp.com