A Senstar Corporation White Paper

119 John Cavanuagh Drive
Carp, ON K0A 1L0
+1.613.839.5572
www.senstar.com

Securing The Power Grid
You Cannot Protect All Sites At All Times

By: Jim Mauk
October 2012

November 2, 2012

Contents

Background

Recent blackouts, such as the widespread outages experienced by the US and India, as well as other power-related incidents across the globe, have underscored the vulnerability of the electricity supply chain.

While the trigger of these outages can be relatively minor, such as a transmission station failure, the impact can sometimes be felt nationwide. Blackouts disrupt public services, interrupt business activity, halt transportation systems and even risk lives. As an example, the September 2011 Southwest US power disruption caused a 15-hour blackout with an estimated $100 million in losses.

The growing wave of anti-government protests, ongoing terrorist threats, vandalism, criminal activity and the recent trend of copper theft emphasize the need to physically protect the power grid across the entire supply chain. Continuous power supply is a basic necessity of any 21st century society, yet ironically it is relatively easy to disrupt. This phenomenon bears some resemblance to the events of 9/11 where, hostile activity by a small group caused massive and widespread damage.

Even the "minor" theft of a copper grounding line, let alone an intentional terror attack, can put a transmission station out of service, and eventually shut down significant parts of the

entire grid. For example, though a transmission station in South Africa was protected by an electric fence, a thief managed to dig under the fence and steal a thick copper grounding section. Although he may have earned a few hundred Rand by selling the copper, he caused direct damage of more than US$20M.

Entry point under an electric fence at a South African Transmission station

The challenge

Protecting a power grid represents a significant challenge, due to its overall size and vast deployment. Although technological solutions exist to detect intrusions close to the grid elements, a sufficiently rapid response to mitigate a detected risk is sometimes not realistic. As a result, the entire solution is often discarded.

As total protection is not feasible, it is more reasonable to prioritize the security solution based on risk assessment.

Senstar, with more than 30 years of experience in protecting power grids, is herby proposing a multi-dimensional model to analyze vulnerability of the power grid, examine solution applicability and accordingly optimize solutions and products.

The following parameters should typically affect the model:

- Potential **direct damage**, inflicted by a hostile action
- Potential **indirect damage**
- Expected **outage duration**
- **Security technology** applicability
- Availability of **first responders**

Critical factors to consider when prioritizing a solution

Direct damage represents the vulnerability of the system and the direct cost to rectify the damaged assets and restore full production. For example, blowing a main generator in a conventional power-plant can cost millions, in comparison to the cost of repairing a damaged transformer, which is significantly lower.

Indirect damage represents the potential indirect damage caused to customers. In general, this calculation takes into account the percentage of lost production, the criticality and size of the affected area, the level of dependency on power (e.g., high dependency of industrial areas), the economic implications, the risk to lives (especially in megacities), and other intangible factors such as political and prestige concerns. As an example, if a relatively small district is dependent on a single high voltage transmission station, then either an expensive redundant channel must be built or the transmission asset must be protected with a robust security system.

Outage duration represents the expected duration of the outage inflicted by the damage. The duration period takes into account the redundancy built into the power grid and the time to rectify the indirect damage, whether by

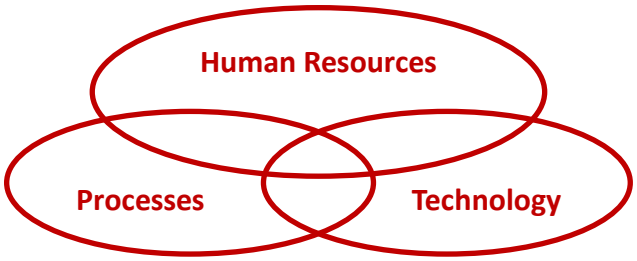
replacing the component or by securing an intermediate alternative.

Security technology represents the applicability of cost-effective security technology in protecting a system or an object. Theoretically, any asset can be protected in a manner that will significantly mitigate the majority of threats. However, in many cases, other constraints may eliminate such solutions. For example, protecting high-voltage transmission lines with physical smart barriers is not practical due to both cost and environmental concerns. On the other extreme – nuclear power plants are relatively small and easy to protect by off-the-shelf Perimeter Intrusion Detection Systems (PIDS).

First responders represent the probability of the human element's capacity to respond to a threat in an acceptable period of time. It will always be simpler and quicker for a first responder team to address a threat within a power plant than along a lengthy transmission line, simply due to the sheer geographical constraints, especially in rural areas.

The linkage between technology and first responders

The availability of technology and first responders are closely linked. An integrated security solution must combine three critical inter-related elements, as illustrated below:



The reliance on implemented technology vs. human resources is essentially a tradeoff. In third world countries, where labor cost is low, human guards can be the backbone of the "system", supported by minimal technology. Elsewhere, human labor is being replaced by sophisticated technology. Nevertheless, on some level, the human element is always required in an effective security solution. Automatic shooting robots are still science fiction, and not at all realistic in a civil environment, where a power grid is deployed.

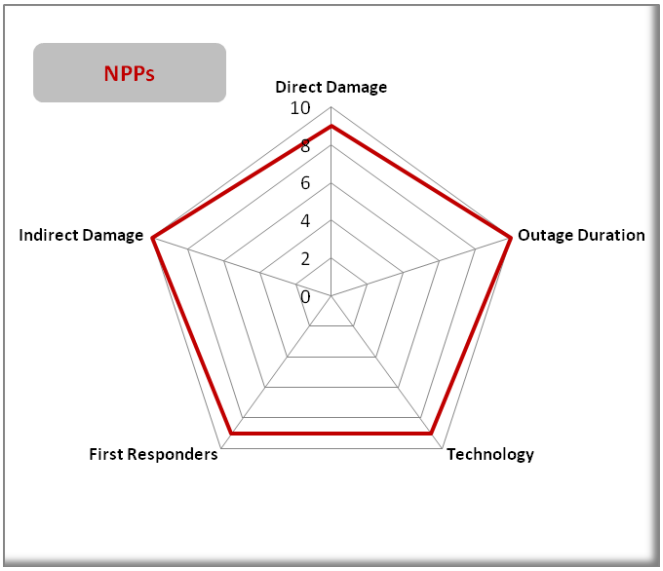
The reaction time of first responders is critical because it will directly affect the chosen technology. If the response time is expected to be lengthy, the security solution should provide the required built-in delay to allow for detection, verification, deployment of the responders, travel time and interception of the intruder.

Another critical technology component used for protecting the power grid is the Physical Security Information Management (PSIM). PSIM automates and glues together physical security, process and personnel.

Prioritization for securing power grid elements

Based on the proposed model mentioned above, the following is a review of some key elements in a power grid. Each parameter is scaled 1 (low) to 10 (high), representing its relative importance. Naturally, the real values are subjective and depend on the market, layout, threats, etc.

Nuclear Power Plants (NPPs) require a high level of protection; any direct damage may have a catastrophic, lasting and long-range effect on both the environment and on lives. In addition, any disruption will likely affect a significant portion of the power generation capability due to its gigawatts capacity. Fortunately, NPPs typically have a small footprint. Security personnel are always available on site; therefore NPPs are easy to secure via advanced technology supported by a small mobile unit of first responders.

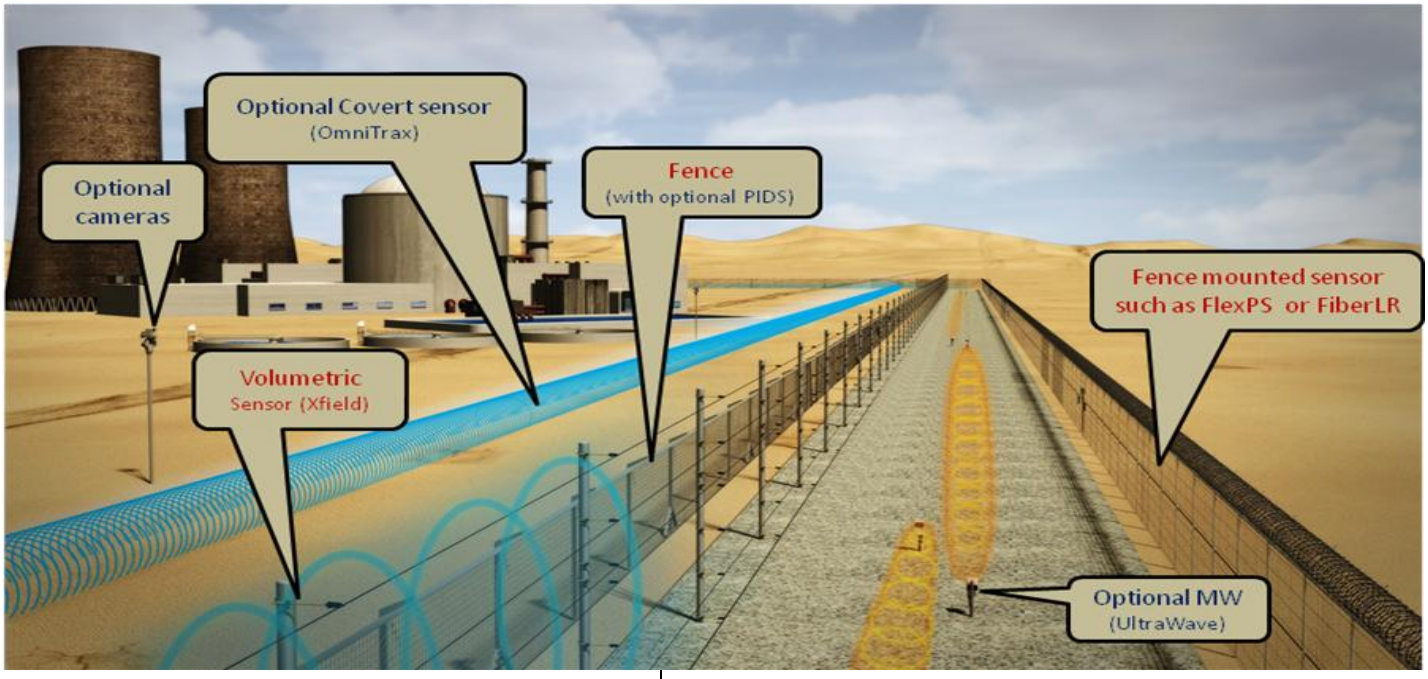


The security at NPPs is highly regulated by governments. A typical solution will include at least two layers of fences/barriers with at least two independent detection layers. North American NPP will typically include:

- A smart fence with a fence-mounted sensor, such as the FlexPS system as a deterrent and a 1st detection and delaying layer.
- A sterile zone in between fences
- A high (typically ~6 meters) terrain-following volumetric sensor as a 2nd layer, such as XField. XField also has a deterring effect, as it looks like an electric fence.
- A second fence/barrier as a final delaying layer, which should provide the adequate extra delay to ensure interception by the security staff.

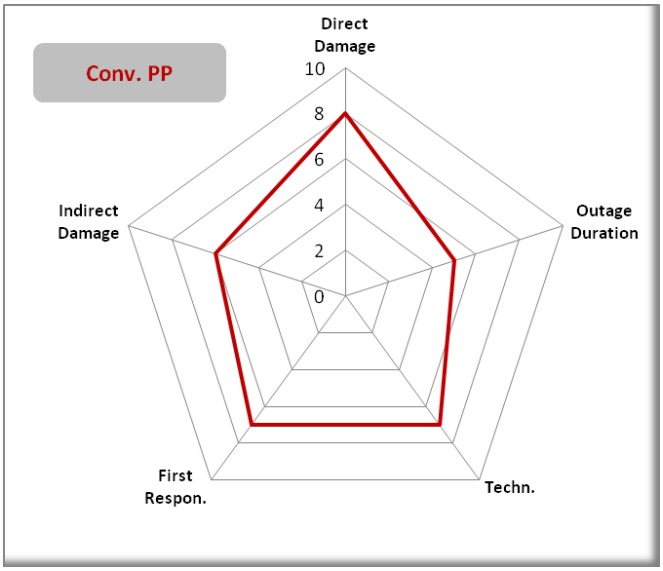
Sometimes the solution can be augmented by additional layers such as:

- A microwave sensor located in the sterile zone – as an additional detection layer, a gap filler, or as a virtual fence when gates are open
- A covert detection layer such as Omnitrax to detect the accurate location of intruders
- Surveillance cameras, which may be used for verification and tracking both during and post intrusion



A typical multi-layer PIDS' layout of NPPs

Conventional power plants have a lot in common with NPPs. Technology implementation is typically more challenging due to the larger footprint of these sites. The sites often include storage for coal/oil or may have pipeline routes to transport massive amounts of fuel. The larger size lengthens the typical response time.

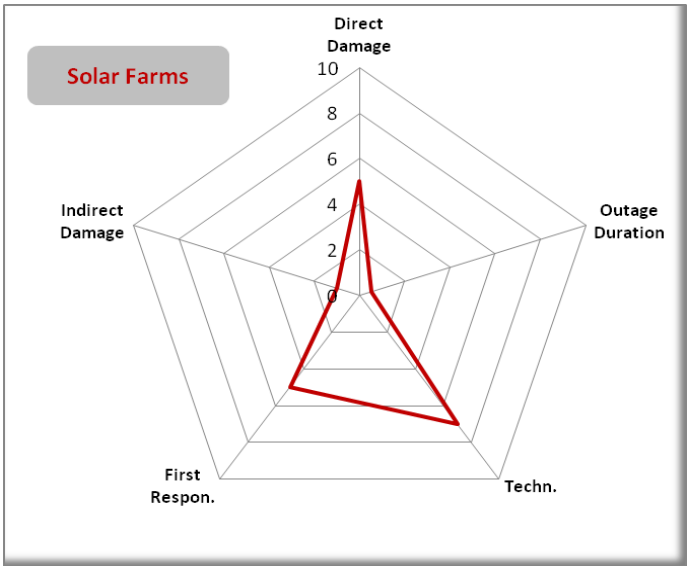


Ideally, conventional power plants should be secured by two layers:

- An external robust smart barrier embedded with sensors, such as taut wire, for maximum deterrence, guaranteed probability of detection (POD), with minimal false alarm rate, and maximum delay time. Due to the unique environmental conditions within such plants, Senstar's taut wire fence is an ideal solution because of its inherent EMI resilience.
- A second layer of fence in order to extend the delay. In between the two fences there is a clean "sterile" zone, which can significantly improve the verification and threat assessment process.
- A secondary detection and/or surveillance cameras for verification, filtering out false alerts, and ensuring almost 100% POD. This detection level can be made of a fence-mounted sensor such as FlexPS. If the perimeter is long enough, FiberLR would be an optimal and cost-effective solution due to its accurate location capability, ease of installation and inherent RFI/EMI immunity.

A multi-layer power plant security scheme with outer taut wire and inner microphonic fence-mounted sensors

Solar farms are very different from power generation plants mentioned above. Large solar farms, the so-called "Concentrated Solar Power Plants," constitute an interesting entity. If the core production plant is damaged, the direct damage is quite significant. However, the overall impact on power outage is limited because the reliance on solar energy is still limited, plus solar plants always have alternate power sources for cloudy days. Therefore, the main driver to secure these farms is economical protecting the large investment in equipment.



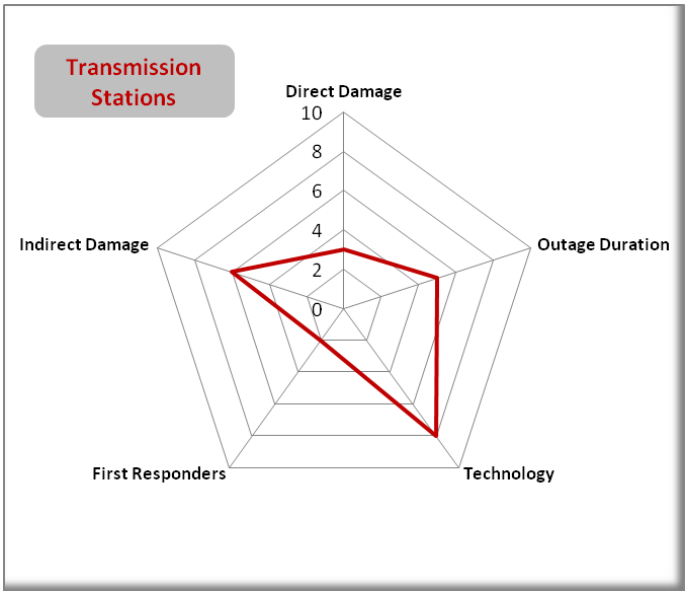
Large solar farms typically use:

- A PIDS backbone consisting of a smart-welded mesh or chain-link fence, supported by a fence-mounted sensor. For very large farms, FiberLR is a very cost-effective solution. For smaller sites, simpler zone sensors would be more economical.
- PTZ surveillance cameras must augment the solution in order to eliminate false or nuisance alarms. Without them, the small team of first responders may experience burnout due to the size of the protected site and the frequency of false alarms.
- The core power plant is relatively small, but nevertheless very expensive to replace. Therefore, a focused second layer of protection would be a cost-effective investment.

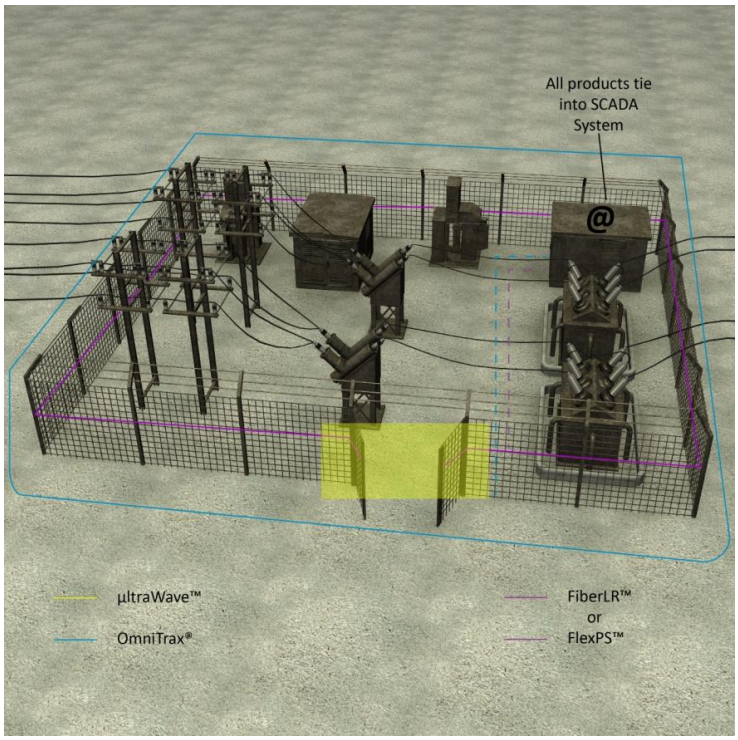
High-end solar farm, typically protected as part of the insurance package

Transmission stations provide grid redundancy and load balancing, especially in the case of supply problems, making them an important and somewhat tricky since in some scenarios, the main transmission stations may constitute a single point of failure.

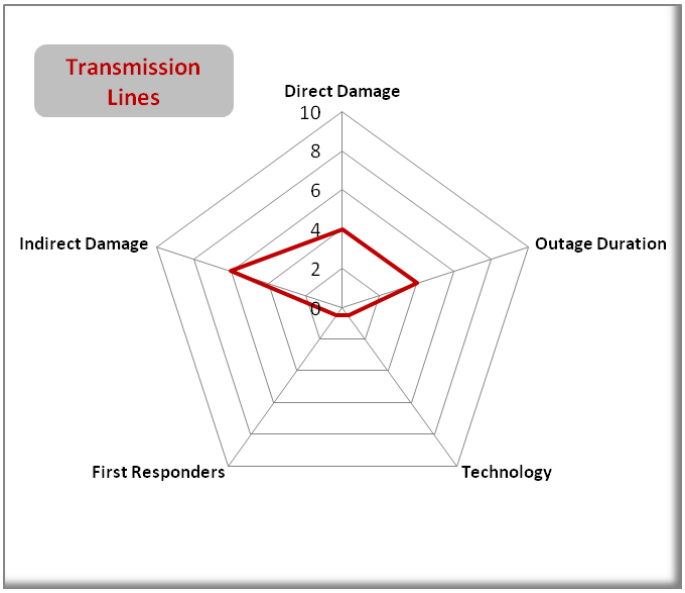
In addition, most of the stations are not attended round-the-clock and therefore the response time can be lengthy, especially for stations located in rural areas. Fortunately, these stations occupy a small enough footprint to enable technology deployment at an affordable cost.



The large and critical transmission stations should always be protected by a reliable detection system as a first line of the PIDS. As these stations are unattended, the detection system must be fully automatic, with very low false and nuisance alarm rates (FAR/NAR). A significant physical barrier would be required as a second line of defense to allow the first responder's time to react. Typical solutions consist of an integrated barrier and sensors such as a FlexPS sensor mounted on a chainlink fence, supported by surveillance cameras, connected to a regional Command and Control center managed by a PSIM system.



Transmission lines present a complex security challenge. Even though the main lines are critical, they are very hard to protect both from the technology perspective and the required availability of first responders. Therefore, in most cases they are not protected.



PSIM importance

A PSIM system is vital and critical for national power grid protection, as it maintains the entire security solution and significantly improves the overall effectiveness and efficiency of the integrated security system (ISS). The PSIM improves almost every component of the ISS. The key benefits of an advanced PSIM include:

- Real-time collection and integration of all sensors, to ensure enhanced POD and more rapid rejection of FAR/NAR
- Geographical (GIS-based) presentation of the entire network to improve situational awareness and enhance the verification process through data fusion
- Predefined and embedded checklists to improve the decision cycle and ensure compliance throughout the entire process
- Complete communication integration for rapid and efficient communication with first responders from the initial dispatch until the successful interception of the intruder
- Real-time location and display of the mobile responders to enable efficient force allocation, guidance and event handling
- Bi-directional data sharing (maps, video, etc.) to streamline coordination between all the security players and particularly mobile forces

Which PIDS technology is best?

Many security experts will claim that there are no bad sensors, just bad applications (and on occasion, bad installers). Finding a ***knowledgeable consultant***, system integrator and/or ***PIDS supplier*** with verifiable ***PIDS references*** and access to a wide array of PIDS technologies is probably the best way to ensure a successful outcome. Nevertheless, the main sensor technologies that are commercially available are listed below:

Taut wire – A hybrid system of sensors weaved into a barbed wire fence. This fence offers guaranteed performance in all weather conditions. It has demonstrated a high POD and almost zero FAR/NAR. Although it is costly, it is relevant for high security, where deterrence and delay must be achieved on top of uncompromised detection.

Fence-mounted sensors – These sensors are affordable and ideal add-ons to existing fences. A second security measure, such as CCTV, is recommended as a verification tool to manage FAR/NAR.

Buried cable sensors – A ***virtual fence*** implemented by smart cables, buried less than 9 inches underground. These cables create an ***invisible*** electromagnetic field, capable of detecting any intruder entering the narrow virtual corridor. The buried cable sensor is a perfect solution for locations where a fence cannot be installed for ***aesthetic or environmental*** reasons, such as concrete platforms where movement must be enabled only during active parts of the day. As a concealed, terrain-following sensor it is almost ***undefeated by intruders***. Therefore, in many places it is used as a second layer – sometimes outside of a fence, but more commonly as an inner detection layer. As virtual fences do not impose any delays on intruders, accurate ***location (ranging)*** of intruders (rather than rough zoning) is essential to enable their effective interception.

Microwave – Another type of ***virtual fence*** that creates an invisible electromagnetic beam. It is also used as a standalone detection layer – either on ***top of walls*** or as ***sterile zones*** between barriers. It is also used for ***virtual gates***, where the "gate" must be open for traffic during the day but must be shut down at off-times, such as nights, weekends or during temporary construction, when the "virtual gate" must be easily installed and removed later.

Tailored robust grids – These are designed to cover critical holes in perimeter security such as ***canals, pipes, open tunnels or drains***.

Long-range fiber – An innovative new technology, using a fiber sensor as a wall/fence or buried detector. It is especially cost-effective for large sites with lengthy perimeters.