WHITE PAPER / **SECURITY SYSTEM PILOTS**

METHODOLOGIES FOR ADOPTING NEW SECURITY TECHNOLOGIES

BY Brock Josephson, PSP

As new security risks and standards emerge, electrical utilities are relying more heavily on technology to deter, detect and deny a variety of threats. Utilities that traditionally have limited physical security technologies are now investing in advanced intrusion detection, surveillance and deterrence systems. Yet adopting the correct technologies presents a challenge for many utilities.

CHOOSING THE TECHNOLOGY

The market is flooded with security technologies that accomplish the same thing in different ways, so it can be difficult to select and implement the most effective systems. Investing in technologies that do not meet performance requirements can result in wasted capital on operations and maintenance (O&M) expenditures, frustrated security officers and managers, and increased security vulnerabilities.

Developing an effective technology strategy prior to the deployment of electronic security systems is crucial to avoid these outcomes. Such a strategy should include a methodology of identifying and eliminating problematic technologies. This can be accomplished by introducing a process that includes the following steps:

- Develop clear and measurable performance metrics for each security system.
- Identify technologies that meet performance metrics (on paper) and shortlisting a viable number of testable options.
- Test potential technologies for performance, robustness and ability to integrate into your security system.

Each of these three topics will be examined further in the following sections. Discussions will include justifications for why the steps are important, as well as descriptions of tools that should be developed to assist with implementation.

DEVELOPMENT OF PERFORMANCE METRICS

The most recent North American Electrical Reliability Corporation (NERC) CIP-014 standards require utilities to develop and implement a physical security plan to protect critical substations. Most utilities consider technology upgrades a significant component of that plan. Once the decision is made to introduce technology, there is a tendency to start researching viable technologies immediately. But doing so before defining the performance metrics the technology should meet is a lot like going house shopping before creating your wants and needs list: You're likely to end up with technology that showed well but doesn't meet your needs or is too expensive.

To be effective, performance metrics need to be developed in accordance with as many stakeholders as possible. Stakeholders may include substation engineers, systems and security operators, compliance, law enforcement, information technology, cybersecurity and security consultants, executives, and shareholders.

COMMON PERFORMANCE METRICS

Performance metrics may include functionality, environmental, usability, communication, costing, and viability metrics. These are not metrics for specific technologies; rather, they are metrics for the system as a whole. They may change from site to site based on surroundings, criticality of the site and proximity to response resources. Examples of the common performance metrics that may be considered are listed below.

Functionality metrics may include:

- Distance from the site for detection of an intruder
- Probability of detection of an intruder
- Identification of an intruder at specific ranges
- False alarm rate

Usability metrics may include:

- Ease of use of the technology
- Ease of installation of the technology
- Ability to integrate with existing security infrastructure
- Time and effort required to operate the technology
- Time and effort required to train new personnel on the technology

Communication metrics may include:

- Supported communication protocols
- Data encryption standards
- Maximum bandwidth requirements
- Storage requirements

Environmental metrics may include:

- Minimum ingress protection ratings
- Minimum and maximum temperature ratings
- Mean time between failure rates

Costing metrics may include:

- Purchase price
- Cost of installation
- Ongoing maintenance costs
- Training costs
- Total cost of ownership

Viability metrics may include:

- Manufacturer's years in business
- Manufacturer's financial health
- Minimum number of units deployed in similar environments
- Minimum technologies
- Readiness level

UNCOVERING TECHNOLOGY GAPS

Before investigating new technologies, you should determine if any existing technologies can be used to meet your new security standards by comparing them to the metrics outlined above. The goal should be to minimize the number of technologies implemented to reduce the overall complexity of installing and maintaining your system. In other words, using the same technology for multiple applications, when it fits the needs, is desirable.

To evaluate your existing technologies' ability to meet the new security requirements, create a matrix that compares each existing technology against requirements.

Consider the following example for a fictitious sample utility. The utility decides to implement a new standard for perimeter detection out to 100 meters beyond the perimeter for Tier 1 substations. The utility determines there are two technologies currently deployed by the utility — microwave and video analytics — that may be able to detect potential intruders out to 100 meters. The technologies are assessed based on their ability to meet each of the performance metrics outlined in Figure 1.

	Video Analytics	Microwave Sensors
Functionality (detect intruders out to 100 meters beyond the fenceline)	Yes	Yes
Usability (deploy in less than 1 week)	Yes	No
Communication (communicate alarms to the access control system)	Yes	Yes
Environmental (IP66 or greater)	Yes	Yes
Costing (cost less than $100,000 per site to deploy reliably around the entire site)	No	No
Viability (technology has been successfully deployed at other major utilities)	Yes	Yes

FIGURE 1: *Identify technology gaps.*

In this example, both technologies can functionally perform the task but do not meet the costing and/or usability requirements. From this the utility can infer that new technologies must be researched, evaluated and implemented in order to fulfill the performance requirements. If a technology already deployed by the utility meets all the performance requirements, then there is no need to continue with evaluating other technologies.

IDENTIFYING AND SHORTLISTING TECHNOLOGIES

At this point, you are ready to research viable products to meet your new performance requirements. The list of security technology providers is too long to allow testing of every potential solution. So, before investing significant resources in any level of design or testing, the list of potential products must be narrowed significantly.

DEVELOPING QUALIFYING QUESTIONS

To reduce the list of potential solutions to a manageable level you will need to create a list of qualifying questions that can be answered with minimal time researching specific products. The questions should reflect the performance metrics outlined earlier. An independent security consultant can assist in the process of developing the questionnaire and shortlisting technology if needed.

In our previous example — a perimeter intrusion detection technology able to detect 100 meters beyond the fence line — the yes/no questionnaire might look something like this:

1. **Functionality**: Is the technology able to detect humans beyond 100 meters in all lighting conditions?
2. **Usability**: Is the technology able to integrate with your existing cameras and video surveillance systems?
3. **Communication**: Can the technology communicate via the necessary protocols?
4. **Environmental**: Is the technology environmentally rated to IP66 or greater?
5. **Cost**: Is the cost of deploying the technology prohibitive? (Assign specific budget limit.)
6. **Viability**: Has this technology been successfully deployed in similar environments?
7. **Viability**: Has the company been in business for at least five years?

Once the list of questions and answers has been developed, any technology that fails to satisfy even one of the criteria should be removed from further consideration.

Next, develop a scoring matrix (Figure 2) to rank technologies that pass the yes/no questionnaire. The matrix should incorporate all performance metrics already discussed and may be constructed using either a pure ranking system or a weighted point system based on which criteria has the highest priority for your organization. Regardless of how the scoring system is constructed, the result will lead to a justifiable ranking of each candidate technology.

Completing this matrix should not require in-person testing or evaluations of each technology but may require engaging with the manufacturer by phone. Accordingly, rankings in some fields may be based on the security professional's past experience with other utilities and sense of how certain technologies would perform, rather than on verifiable data. If the number of viable vendors is too exhaustive to engage each one, then additional yes/no questions should be used to reduce the number of candidates.

TESTING TECHNOLOGY PERFORMANCE

The next step in the process is to conduct an on-site test or pilot of the top two or three technologies in your ranked list. The pilot serves several purposes. The first and most obvious purpose is to determine if the technology or technologies can really do what it has been promoted to do. The technology needs to operate in its designated environment as expected. If it doesn't, it may be a waste of time and money to implement. Worse, it may increase, rather than decrease, a facility's overall vulnerability.

The pilot should also assess system integration, ease of installation and operation, and the false alarm rate, as well as the system's ruggedness and maintenance requirements.

Metric	**Tech A**	**Tech B**	**Tech C**	**Tech D**	**Tech E**
Detection Coverage	5	3	2	4	1
False Alarm Rate per Site	2	1	4	5	3
Integration with Cameras	3	2	5	1	4
Environmental Rating	1	4	3	2	5
Cost per Site	2	3	4	5	1
Deployment at Similar Sites	3	2	1	5	4
Company Viability	2	1	4	5	3
Totals	**18**	**16**	**23**	**27**	**21**

FIGURE 2: *A sample ranking matrix. A "5" represents the highest performance in the category while a "1" represents the lowest.*

PERFORMANCE TEST

In addition to evaluating the functionality of the system, an effective test plan must address how the technology works. For instance, in our previous intrusion detection technology example, Utility X sought to understand how potential technology solutions detect intrusion. (A summary of common types of intrusion detection technologies is provided in Appendix A.)

Understanding how the technology works allows you to write a procedure that tests strengths and weaknesses. Every technology has weaknesses, so revealing a limitation should not preclude a technology from use — identifying the weakness will help you anticipate the need for supplementary technologies and procedures to mitigate the risks presented by the weakness of the technology.

When planning the tests to be performed to defeat a technology, you should consider as many methods as practically possible. For testing a perimeter intrusion device this may include approaching the sensor from different angles, positions and speeds, using a blanket to hide heat signatures, or using acoustic or seismic devices to mask your presence. Once a list of methodologies has been created, test procedures can be written to test the system's ability to detect the various methods of defeat.

The testing procedures should include multiple repetitions of each test, and the results should be averaged to reduce the risk of results being skewed by outliers. If adjustments are made to the system during testing, previous tests should be run again to see that the results do not change.

Finally, conduct tests in a setting similar to the deployment setting. For example, if the system will be deployed at a substation, the test should occur at a substation. Tests should also account for as many environmental factors as possible. While testing in every possible weather condition may be unfeasible, testing in various lighting conditions should be completed if the technology under consideration is light-dependent.

Include within each testing procedure a description of the technology being tested, how it is to be deployed for the test, how each test phase will be performed and a checklist to record the results for each phase. Once performance testing is completed, a matrix can be used to compare how each of the tested technologies performed.

BURN-IN

After performance testing is complete, implement a more in-depth burn-in test to evaluate environmental factors and additional functionality. A burn-in test entails long-term testing for false alarm rates and ability to withstand the elements. If possible, burn-in phases should test the system's ability to perform during both the hottest and coldest months of the year. Running performance tests during periods of extreme weather, including heavy rain, snow and fog, is also advised. Comparing the results of tests conducted in fair and bad weather will reveal the performance degradation of the system in difficult conditions.

The burn-in phase is also a time to closely monitor false and nuisance alarm rates. False alarms in this context are defined as alarms that were triggered by an unverifiable source. Nuisance alarms are defined as alarms triggered by a verifiable but nonthreatening source. These are often caused by animals or authorized activity in or around the substation.

Before the pilot, you'll need to determine your acceptable threshold of false and nuisance alarms. Occasional nuisance alarms may be beneficial, as they keep operators active and give them the experience of responding to alarms. However, if the false alarm rate is too high, alarms will soon be ignored.

Alarm ID	Date	Time	Cause	T/F Alarm?
12114	6/5/18	2:41 AM	Deer crossed into the sensor FOV	True
12137	6/5/18	9:45 AM	Unknown	False
12187	6/5/18	7:21 PM	Person walking	True
12189	6/5/18	7:47 PM	Tree blowing in the wind	False
12222	6/6/18	5:42 AM	Unknown	False

FIGURE 3: *A record of the alarm activity.*

Once the acceptable false alarm rate is determined, a process for recording the alarm should be established. This process should include an alarm ID (if available), time, date and cause of the alarm. This data may be recorded directly in the access control or video management system, or in a simple table as shown in Figure 3.

After a few weeks of data have been collected, you can calculate an average false alarm rate. You may also need to modify sensitivity settings or make other adjustments before the system is tuned correctly. If this is the case, note how much time is spent making these adjustments and how many times the system must be adjusted during the pilot. This information will be useful later, when planning for the effort required to tune each system after it is installed.

Recording any times during the pilot that the system does not perform as expected — for example, if it does not detect something that it should have detected — is important. This will become critical information in the decision-making process.

INTEGRATION

Integration is essential to seamless operation whenever you're dealing with multiple technologies. Whether the integration is a simple relay trigger from the sensor to the access control software, or a software integration bringing geospatial data into a map interface and triggering different events based on criteria defined during programming, the integrated system should be tested as part of the pilot.

As part of the integration testing, confirm alarms are coming in consistently and correctly. Confirming that alarms are coming into the monitoring software does not mean the alarms are coming in correctly every time. During the pilot, consider monitoring alarms at both the sensor level and the system level and comparing to make sure all alarms are making it through. If the alarms logged on the piloted technology do not match the alarms on the operator interface, it will be important to determine why. Common reasons include the following:

- Software filters are limiting the alarms passed from the sensor to the software.
- Network connections are dropping between the sensor and head-end software.
- Times between the sensor and head-end are not in sync.

To make the matching of alarms between the sensor and the operator interface easier, be sure the times on the two systems are synced. This can be done by syncing both systems to a common NTP server.

A table similar to Figure 4 may be used to monitor alarms at both the sensor level and the operator interface level.

If some alarms exist only at the sensor level or only at the interface level, the discrepancy should be investigated and resolved. If a custom software plug-in is being developed for the integration, the comparison between sensor and system alarms is especially important to make sure all potential alarm scenarios are accounted for.

Sensor Alarm ID	Date and Time	Interface Alarm ID	Date and Time	Sensor Only/ Interface Only/Both
124	6/9/18 5:42 AM	3542	6/9/18 5:42 AM	Both
196	6/10/18 2:22 PM			Sensor Only
		3674	6/11/18 4:21 AM	Interface Only

FIGURE 4: *Monitoring sensors and operator interface alarms.*

SCALE TESTING

Scale testing of the system should be done to the greatest extent possible. This will confirm the load-bearing capability of the software, as well as identify functionality issues that may not present themselves with just a few units. Scale testing also helps uncover issues that may occur when many systems are integrated into the interface simultaneously.

Setting up sufficient hardware to run a full load test can be difficult, especially when it is necessary to deploy the system at many sites. To simplify this process, sensor software and sensor alarms can often be simulated on the software level at minimal cost. A simulated system should consist of five to 10 times as many sensors as planned for the full scale of the project in order to identify potential issues that may occur as the system is scaled.

TRAINING

Training on system operation is a key part of the implementation strategy that is often overlooked until after the decision to implement has already been made. Conduct training for operators as part of the pilot. During this time, give operators the opportunity to experiment with the technology interface and provide feedback on how the system works. Many technologies have been purchased and installed only to be abandoned shortly thereafter because they were too complex to operate, produced too many false alarms or the operators were never trained properly.

Depending on the size and skill of your operating group, you may consider assigning only a few operators to train on and test the technology. If the same operators test multiple technologies, ask them to provide feedback on which they prefer and why. Then, incorporate that information into your overall scoring matrix.

By the time the pilot is complete, the technology should be fully functioning within the larger security system architecture and the transition from pilot to full implementation should have minimal hiccups.

CONCLUSION

Developing an effective technology strategy prior to the deployment of electronic security technology is crucial. When utilities take time to define clear and measurable performance metrics, identify and thoroughly vet technologies that meet those metrics, and conduct comprehensive testing of the two or three best candidates, the odds of successful product selection and implementation are greatly increased.

By incorporating a strategy for continual adoption of new technologies into your existing security technology strategy, you can garner long-term success. Ultimately, these efforts made on the front end of the project will provide benefits later on, such as faster and more predictable implementation and improved overall functionality of the integrated security system.

BIOGRAPHY

BROCK JOSEPHSON, PSP, is a physical security specialist at Burns & McDonnell. His work includes helping utility clients assess and mitigate their physical security vulnerabilities, as well as plan out their electronic security systems. Brock has extensive, firsthand experience in physical security system installation management with more than eight years of experience in the full spectrum of substation security upgrades, including system implementation and commissioning for substations ranging from distribution substations to transmission substations. He has also worked on numerous NERC CIP upgrade projects, including CIP-014.

APPENDIX A

TYPES OF INTRUSION DETECTION TECHNOLOGIES

Acoustic sensors use microphones to listen for specific types of audio signatures, such as gunshots or human voices. The performance of these sensors typically is limited in noisy environments and tuning the system may require significant time and effort.

Contact status sensors measure the status of a door, window or gate. Because contact monitors provide only the status of the contact, which typically has just two states (open or closed), they work well for monitoring points of entry, like doors, windows or gates, where the status is either open or closed.

Passive infrared (PIR) sensors create an infrared beam or field that triggers an alarm when disrupted. PIRs have limited areas of coverage and, in the case of PIR break beam sensors, can be easily circumvented by going over or under the beam. They also are susceptible to false alarms created by animals or blowing clutter.

Radar transmits a radio wave and then measures the time it takes for the wave to bounce off an object and return. Based on the time and phase of the returned signal, software can then infer movement and, in some cases, measure distance and angle to a target. Because Doppler systems look for change in range of an object relative to the sensor, areas where there is a lot of movement or where line of sight is very limited typically are not effective applications for radar.

Seismic sensors detect vibration in the earth around the sensor. Their detection ability varies significantly based on the type of earth around the sensor and the magnitude of vibration caused by the moving target. Some have the ability to predict the type of target based on the vibration patterns created.

Video analytics look for changes in pixel color across a series of images to infer the movement of an object within frames of the video. One significant benefit of this is analysis is the ability to combine video for verification purposes with detection. However, video analytics typically do not perform well in areas where there are constant pixel changes, like looking over water, or where pixel changes are minimal or non-existent, like looking into a dark area with a color camera.

RF sensors detect RF signals between devices that communicate wirelessly. RF sensors have become particularly relevant in the detection of drones. Advanced RF sensors can provide locations for the drone and the pilot and, in some cases, provide details about the information passing between the two. RF sensing is not effective at detection when direct communication between the pilot and drone is not present.