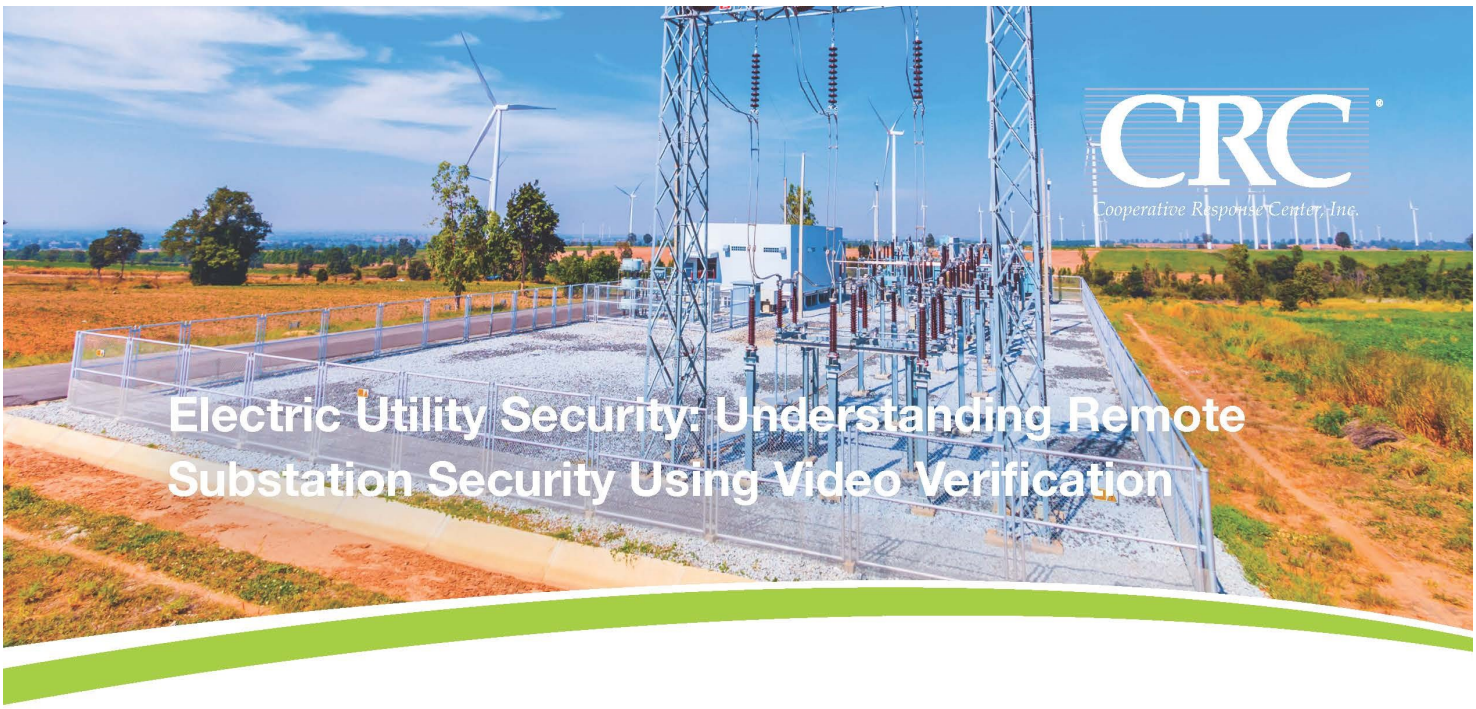

Electric Utility Security: Understanding Remote Substation Security Using Video Verification

Reports of remote asset vandalism, copper theft, and the threat of terroristic acts have continually increased over the past decade as it pertains to electric utility infrastructure. Awareness of risks and ramifications of remote asset threats and measures that can be taken to minimize those risks are critical for electric utilities to consider when making informed decisions regarding the safety and security of those assets, employees and service territory. This paper reviews the considerations electric utility providers should make when creating a security strategy for remote substations and outdoor assets.

Impact of Compromised Assets

Consequences of substation vandalism are far reaching and impact more than the infrastructure repair or replacement costs. In addition to the impaired service to the end user and lost revenue to the electricity distributor during an outage created by vandalism, there will likely also be unplanned payroll expenses to get the repairs made as quickly as possible and the potential for unplanned utility contractor expenses. In addition, if the impairment to the substation is undetected, the risk of employees being severely injured increases markedly. When it comes to electric substation security, the old adage “an ounce of prevention is worth a pound of cure” is certain to apply.

Minimizing the risk of substation vandalism is only possible if a designed security system is deployed properly, sends triggered alarms to a qualified monitoring center and those alarm signals can be verified visually.

To gain an understanding of what makes an effective substation security system, a few items need to be considered:

What is video verification? In the most basic terms, video verification is the ability to verify the presence of a threat through the use of a video image in real-time or near real-time. Verified alarms are given a higher priority by emergency agencies when a crime-in-progress has been confirmed.

How can a video verification system thwart substation vandalism? The most important aspect of a well-designed video verification system is 24/7/365 monitoring. Deploying a video verification security system with live monitoring increases the potential to thwart a crime in progress exponentially. Dispatching responding authorities during a break-in event and capturing the evidence of the intruder that can be replayed and analyzed increases the chances of stopping a vandal dramatically.

Security Convergence

Deploying an effective security program requires more than just deployment of the hardware, software and monitoring. Key steps can be taken to ensure the likelihood of a successful security operation:

- Let the community you serve know that your company means business when it comes to keeping your system protected. Use your company's social network to promote security. Let everyone know that the utility company has deployed remote asset security systems. **Take credit for keeping infrastructure and employees safe**. Use a consistent message in employee and consumer newsletters, utility bills, and front-end IVR greetings.
- Make the message count. **Ask your customers to remain vigilant and aware**. Promote crime prevention and consider offering a reward for information that leads to arrests pertaining to any vandalism of utility assets.
- Meet with easement neighbors and let them know that you've deployed a video verification system.
- Reach out to local and county police and sheriff offices and inform them of your video verification system deployment. Schedule a meeting at the substation to show them the security system hardware. Walk the surrounding area outside of the substation. If there are clear hiding places or routes that a small vehicle may use to elude authorities, point them out. Demonstrating your investment in utility and community security will help create a more effective partnership with local law enforcement agencies.

System Type

There are primarily two different types of video verification systems: intrusion detection systems that send notifications if and when someone enters a monitored area and a more advanced system that offers the monitor the capability to take control of the camera(s) remotely with pan, tilt and zoom features.

Intrusion detection systems use a fixed camera that has a single focal point (not capable of pan, tilt, or zoom). Intrusion detection systems function well when securing an area with an existing fenced perimeter. The simplicity of these systems is elemental: if a person trespasses and walks past the intrusion detection camera and within the threshold of the motion sensor that is programmed to the camera, the camera will begin streaming a 10-second video clip to the monitoring center via a direct IP link. The video is reviewed and the monitoring and dispatch protocol are followed. The 10-second video clips are stored on a server, typically located at the office of the monitoring company.

Advanced video verification systems offer more features than the intrusion detection systems. These systems are typically connected via IP link and a live view can be obtained remotely from any Internet-connected device. In addition, the cameras of these systems can be controlled remotely, giving the monitor the capability of touring the monitored area with the camera. Advanced systems will also use a motion sensor, many times coupled with a thermal imaging camera. The monitor is alerted of an alarm event when the system detects motion and the prescribed thermal signature. Videos are stored on a ruggedized server at the site or at the monitor's office.

Considerations to make when choosing a system type

There are several considerations to take into account when choosing a video verification system including:

Infrastructure: What pathway does the video alarm signal take to the monitoring center: IP, cellular network, fiber optic, or another format? Are any of those pathways available at the locations that need protecting? Does the area needing video verified monitoring have an accessible supply of low voltage electricity? There are systems that will operate on NiCad batteries and systems that operate on low voltage electricity with an external back up battery in the event of a power loss.

Operational: When determining what type of video verification security system to deploy, several operational items need to be considered, including:

- **Will the camera (security system) be used for operational procedures in addition to security?** If yes, the need to be able to obtain an on demand live-view of the cameras from any Internet-connected device will be required of the system.
- **Can the system be programmed/calibrated remotely?** A system that can be programmed remotely will offer operational efficiency, especially for monitored assets that are longer distances from a home or the district office.
- **What mechanism can be used to arm or disarm the alarm notification?** Having the ability to arm and disarm the notifications on the alarm system will be necessary. Employees that are entering a monitored area will want to have the capability to disarm the system and re-arm it prior to leaving. Many advanced systems offer the ability to arm and disarm the system remotely using the software application that operates the system.
- **Does the system have a mechanism to save the digital record of captured video after it's sent to the monitoring center?** Having the ability to easily store, sort and obtain video evidence makes it easy to save electronic files and review them internally or externally with local law enforcement agencies.
- **Does the substation or asset site have a night-time light source?** If a system uses a thermal imaging camera or infrared illuminators, you may not require an artificial light source.

System Monitoring

Considering the assets the video verification system is intended to protect are remote, having the system monitored 24 hours a day is crucial to the value of deploying a system. Having a system that is not monitored 24 hours a day will only offer a digital video file review of the previous day's criminal activity. If the system in not internally monitored throughout the entire day, it is recommended that a qualified third party monitor is used during hours that internal staff will not be scheduled to monitor the video verification systems.

Video Verification Monitoring Protocol is most effective when it is simplified. The fewer subjective decisions a system monitor has to make, the more efficient the monitoring protocol becomes. An example of monitoring protocol:

1) Verify Video: Animal, Human, or Unknown
2) Respond: If Unknown or Human
3) Dispatch: Emergency Agency
4) Follow: Established Protocol Every Time

Using a qualified third party to monitor video verification systems is common. Utilizing a professional alarm monitoring center that is familiar with the electric utility industry can help to improve your operational performance with regard to security system monitoring and may alleviate having to staff your utility operations center 24 hours a day. Professional alarm monitoring centers that work with the electric utility industry can improve your operational performance with regard to security and remove the burden of 24-hour staffing from the utility. A qualified third party alarm monitoring center will have the capability to electronically receive the alarm signals and video feed of your video verification system. They are trained to follow a very specific protocol and dispatch your local emergency agency quickly and efficiently. In addition, the alarm monitoring company will be able to access your live view and record evidence after they've dispatched the emergency agency.

When choosing a third party alarm monitoring center, look for the following:

- **UL-inspected and Certified –** Alarm monitoring centers that are Underwriter Laboratories (UL) certified are inspected annually and audited by a UL-employed inspector. There are several criteria that a UL-certified monitoring center must adhere to including system redundancy, uninterruptable power supply limits, access control to their monitoring center, a minimum number of employees working in the alarm monitoring center simultaneously, as well as several other inspection qualifications.
- **CSAA Five Diamond Certified –** The Central Station Alarm Association (CSAA) is a trade organization of

alarm monitoring centers throughout North America. The CSAA not only publishes best practices for the alarm monitoring industry, they also offer certification of alarm monitoring operations that qualify alarm monitoring companies with the distinction that all employees that monitor and dispatch alarms have passed a rigorous battery of exams.

Conclusion

Securing expensive and critical substation and other remote assets utilizing video verification with security convergence provides utilities the ability to proactively protect employees and assets. A by-product of security convergence is the probability that expenses as they pertain to criminal activity can be minimized. Taking an integrated approach to asset security has been proven to be the most effective way to minimize damage and expenses by would be criminals – where a qualified, professional third party can be utilized to assist in ensuring your assets are protected.

Any security system that doesn't ultimately provide a high probability of crimes being prevented, and would-be criminals being caught, is not be considered a GOOD method or system. Knowing about a crime after it has occurred only addresses one aspect of security convergence.

A robust security convergence method will offer forensic evidence of a crime in progress – with a simple, and tested protocol that minimizes the risk of the crime in progress from being carried out.

Contact CRC

For more information about CRC's video verification solutions, email info@crc.coop or call 800-892-1578 and ask to speak with Mark Colton, business manager.