Application Data Sheet

Substation physical security

Benefits

- Reduces potential safety risks and damage from malicious activity, vandalism and theft with early alert of unauthorized substation access
- Deters malicious activity and serves as evidence for prosecuting perpetrators
- Logging of authorized personnel entering and exiting the facility
- Reduces truck rolls and enhances situational awareness, increasing operational efficiency and worker safety
- Flexibility in mounting locations for security devices – without worrying about availability of cables or incurring additional costs to run wires
- Delivers reliable and resilient communications foundation for NERC CIP-014-1 compliance

Tropos Technology Differentiators

- High capacity and low latency communications required for many physical security applications including real-time video
- Eliminates trenching costs and speeds deployment
- Granular control over application QoS ensuring priority for critical applications and accessibility at all times, even during outages or natural disasters
- Multi-layered enterprise-class security to help thwart potential cyber threats
- High reliability mesh technology minimizes effects of RF interference
- Resilient: automatically reroutes around failed nodes retaining operations; battery backup for continuous operation in the event of a power outage
- Supports legacy and IP networks for ease of integration into any substation
- IEEE 1613 certified for substation operation and proven reliable in extreme environments

Around-the-clock monitoring of physical security at transmission and distribution substations can be a key factor in minimizing damage from a wide range of threats that are becoming more commonplace. It is well documented that unauthorized access to utility substations can result in hundreds of thousands of dollars in financial losses as well as cause power outages. Unauthorized access may cause such damage as a result of theft of materials or equipment; damage to substation equipment; and can provide hackers with an opportunity to launch cyber-attacks from within substations.

Physical security used at substations encompasses a wide range of applications, all of which require a reliable high performance communications network to deliver centralized visibility and reporting. Utilities may select to deploy any combination of these applications, which include:

- Video surveillance – remote monitoring of video cameras positioned around the perimeter, at entry gates and/or sensitive locations within the substation. Combined with video analytics, video cameras can initiate recording and send an alert based upon changes in conditions such as detection of movement or heat, eliminating continuous recording of status quo conditions.

- Substation access control – identification, authentication and recording of authorized individuals accessing the facility can be centrally controlled and logged through use of physical access control methods such as biometrics or keypad entry. Alarms can be generated should

unauthorized users attempt to use these access methods enabling the utility to respond quickly to minimize potential problems. Hackers attempting to access substation computers and systems can also be thwarted.

– Perimeter sensors – fences around a substation can be configured with thermal/motion sensors that detect movement. This includes situations where someone may be attempting to climb, breach, or approach the fence. In addition, these sensors may trigger horns, lights or other physical deterrents to encourage unauthorized individuals to cease their activity and leave the facility.

– Gunshot detection, alert and location identification – when a substation is attacked by gunfire it can result in significant damage to equipment and risk the safety of workers on site. A gunshot detection system typically can identify the type of firearm as well as the exact location from which it was fired. If video cameras are configured as part of the gunshot detection system, they may offer a visual image of the individual that fired the gun which can accelerate in apprehending and convicting individuals involved in the illicit activity.

NERC CIP-014-1 compliance

NERC CIP-014-1 identifies a process for utility transmission stations and substations and their associated primary control centers, to assess and incorporate physical security risk management measures into critical locations that could comprise the backbone of the utility infrastructure. Its purpose is to identify and reduce the risk of critical power utility locations from physical attacks that could render them as inoperable or damaged, possibly resulting in additional problems including power instability, uncontrolled separation or cascading within an interconnection.

NERC has identified communications as one of the key building blocks essential for physical security. A communication system aggregates communication of security monitoring data, alerts, video and data information from multiple physical security devices and must provide high reliability and resiliency.

Wireless communication for substation physical security

As physical security is added to existing substations, oftentimes, additional communications is required in locations where wired communications is not available. The cost of adding wired communications in such instances is typically very costly or prohibitive without disrupting substation equipment and risking disturbing and interrupting power delivery. Wireless communications eliminates the need for expensive trenching and laying new cable and typically is far more cost effective and faster to deploy.

Tropos wireless mesh networks provide the high throughput, low latency and reliability required to support virtually any substation physical security application that can be supported by a wired network, including video cameras. Tropos mesh routers provide Ethernet and serial connections to attached physical security devices without native wireless interfaces, support popular utility automation protocols including DNP3 and IEC 61850, are specially hardened for substation operation (IEEE 1613) and provide the technical controls required to achieve NERC CIP v5 compliance.

Leveraging substation physical security networks for multiple applications

Another significant advantage of Tropos wireless broadband networks is that they can provide reliable communications for multiple substation applications in addition to physical security. For example, use of the network for substation automation, monitoring and control of IEDs located in the substation yard. Unscheduled maintenance can be reduced by use of the wireless network to monitor smart transformers or gas sensors mounted near conventional transformers.

Providing mobile workers at substations with wireless connectivity can substantially increase their productivity. It can provide them with field access to all the information from the operations center; the ability to file reports, access and update orders, order parts, etc. while at the substation, using their laptops and handhelds. Some substations are in remote locations that lack cell phone coverage putting workers at risk should a problem occur where they need assistance. By deploying voice over IP (VoIP) and a wireless network at the substation, worker safety is significantly increased.

In addition to performance, key features of Tropos wireless broadband mesh networks that make them well suited to support multiple substation applications include virtual LANs (VLANs) and quality of service (QoS). Each application can be supported on a separate VLAN that is configured with appropriate QoS settings. Using these capabilities, a utility can ensure that latency-sensitive applications get network access priority over other applications with less stringent latency requirements.

Substation physical security building blocks

The basic building blocks for substation physical security may include a range of systems such as video cameras, video analytics, sensors (thermal, motion), access control devices (biometrics, keypads), physical alert devices (audio, lights), computers, and their associated software and a communication network. Additional substation applications can be enabled securely using the same high reliability wireless communications network.

For the wireless network, the key elements include Tropos mesh routers and the Tropos Control wireless network management system.

For more information please contact:

ABB Wireless
555 Del Rey Avenue
Sunnyvale, CA 94085
Phone: +1 408.331.6800
E-Mail: tropos.sales@nam.abb.com

www.abb.com/tropos

Power and productivity
for a better world™

1KHA - 001 370 - SEN - 1000- 01.2015