Protecting the Power Grid

A look at NERC CIP-014 and Video Surveillance

PureTech SYSTEMS

PROTECTING The POWERT GRID
Protecting the Power Grid

– A look at NERC CIP-14 and Video Surveillance

The Department of Homeland Security said it well….

“Everything is dependent on electricity. EVERYTHING. Without electricity, we’re basically back in the 1850s.”

Most of us haven’t had to deal with not having electricity, internet, television, refrigeration or telephone so it’s often hard to imagine the chaos that might ensue if the power grid were to experience a major issue. Unfortunately, it is not a remote scenario, as the power grid has many vulnerabilities and threats. This paper explores protecting the power grid. It addresses the various aspects of NERC CIP014 and how intelligent video surveillance solutions can be deployed to address these vulnerabilities.

THREATS

When the security of the power grid is considered, the risk of terrorism typically rises as a major concern, with good justification. Should a terrorist desire, there are many ways to target the grid. One well known vulnerability is the fact that “less than 3 percent of all transformers in the U.S. are high-voltage, but 60% to 70% of the nation’s electricity passes through them.” An attack on one of these transformers would be significant, much less a coordinated attack on several. The problem is it’s difficult to predict any type of terrorist attack, but the positive side is that actions can be taken to reduce the likelihood and the resulting impact.

Another vulnerability is the threat of copper theft. The annual monetary loss on its own, nearly $1 Billion dollars in the US each year, is a strong case for action, but there are many other mitigating reasons related to this type of theft, such as

- potential loss of life of repair people,
- loss of power to customers and
- the risk introduced to facilities and operations that provide critical services, such as hospitals.

Figure – Critical Power Grid Assets
Unfortunately, the grid was never designed to withstand these types of attacks. However, today’s reality is that actions must be taken to correct these deficiencies.

When we look at the distribution architecture, points of vulnerability exist within each segment of the distribution chain. Typically, when we think about vulnerabilities, when look to the 57,000+ substations and power generating facilities, but there are many other targets including transmission poles, switch yards, maintenance sites and even control centers. The key is identifying those areas with the greatest risk and putting plans in place to remove those vulnerabilities.

REGULATION

In the United States, that’s the main objective of the NERC physical security standard. If terrorism, theft and property damage wasn’t enough to incentivize actions, then there is the mandate for compliance with CIP014. The current standard is in place and will likely grow over time. So, it’s best to determine not only how to meet the standard, but also understand how to address vulnerabilities throughout the infrastructure and ensure a growth path to address these items over time.

The NERC guidelines, are just that, guidelines of what should be addressed. There is still the question of how to actually meet the guidelines, taking into account effectiveness, operations and budget. There are several approaches to protect critical assets and meet NERC guidelines, and you should consider them in terms of their effectiveness and cost. After all, the end game here is protecting the power grid and ensuring that the lights will turn on when we all get home this evening. However, our particular expertise lies in the realm of surveillance, so we’ll focus on the importance of surveillance, specifically, intelligent surveillance, and how to use it to address, not only CIP014 compliance, but also
- Worker Safety
- Liability Protection
- Remote (and Automatic) Monitoring
- Deterrence (not just detection)
- And how to automate reaction to events

This paper explores the ways surveillance technology can be implemented to protect the power grid and meet NERC requirements. It is divided into five sections. Each section aligns with the five areas of concerns outlined in NERC CIP014

1. Detection of Attacks
2. Response to Attacks
3. Communication
4. Deterrence and Delay
5. Assessment of Attacks

**NERC #1 – DETECTION OF ATTACKS**

The key to robust detection is making the perimeter *smart*. One means to achieve that is through the use of video analytics. Video Analytics has several advantages

- It is reliable & affordable
- It can use existing equipment including cameras, lighting and recording devices
- It helps achieve both the detection and “verification” (Where other sensors may detect well, but may still require some type of visual confirmation)
- It’s intelligent and continues to be more intelligent.

When we at PureTech Systems talk video analytics, we refer to video analytics that have been enabled with “geospatial intelligence.” Geospatial means each video pixel has associated location data. As we will explore, that location data can be extremely beneficial for detection, situational awareness and reaction to an event.

The addition of “location information” to video isn’t that well known, but it has actually been around for quite some time. The alignment of pixels and physical location data, referred to as geo-referencing or geo-intelligence, provides information as to “where” each pixel resides in the terrain or map space. The result allows the software to understand an object’s *real size*, regardless of how many pixels it claims in the image.
As you can see in this diagram, although the dog actually encompasses more pixels (500), the associated location data tells the software that the dog is much closer to the camera, and in reality, is a much smaller physical target versus the man, who only encompasses 50 pixels due to his farther distance from the camera. This same location data also forms the basis to compute real velocity, real acceleration and aids in target classification.

So how does one go about “georefencing” a new or existing camera? It’s basically the creation of a mesh, done by telling the system, the actual “map location” that corresponds to a particular “video pixel.” So, in the following image showing a street view and corresponding map view of the same area, establishing this grid merely entails clicking on location 1 in the video, then clicking on the corresponding location on the map, then clicking on location 2 in the video, etc. By providing several key pixel/coordinate pairs, the system can interpolate the other points in the camera view. This process is only done once by the integrator at the time of installation.

Figure – Value of Geo-referencing
The result is a set of geospatial video analytics detection capabilities that is aligned with the types of vulnerabilities that occur along the power distribution architecture, and most other critical facilities. These include:

- Object Left Behind Detection
- Detection by Various Camera Types (Thermal, Visible, Wide Angle, Mobile, Fixed, PTZ)
- Target Classification – Human, Car, Truck, Boat
- Loitering
- Tailgating
- Software Based Video Stabilization
- Camera Auto Follow

Another benefit of video analytics is that its retrofittable into your current surveillance system. This type of intelligence can be added to an existing surveillance system through the use of a small edge device which can typically handle all the cameras at a substation. For a bigger facility, an add on server can be used to accommodate dozens of cameras. This software then works in conjunction with your existing NVR and cameras, coordinating control and sharing alarm information.
In cases where the system needs to be replaced or fully updated, a map-based video surveillance system can be put in place, providing added display functionality, as well as, collaborative capability with other sensors that you may have in your system now, or in the future.

From the perspective of “detecting attacks”, video has some unique attributes that make it an attractive option.

1) Its ability to accurately detect objects of interest, track those objects and understand various behaviors
2) Its ability to classify objects, such as Human, Car, Truck, and use that information for alarming and display
3) Its ability to incorporate location-based information, allowing determination of target location, real size, real speed
4) Adaptive background algorithms, which understand environmental conditions, such as rain, snow and lighting changes – and then ignoring these conditions when searching for objects of interest
5) Its applicability to all types of cameras and imaging devices
6) A high detection rate and low probability of alarms
7) Hands free auto tracking of targets through the use of a PTZ camera enabled with intelligent video algorithms

**NERC #2 - RESPONSE TO ATTACKS**

The second NERC guideline is having a means to “Respond to an Attack.” We don’t often think of our VMS as having the capability to “respond”, but in fact a system based on intelligent video surveillance can address this guideline. The key to a video surveillance system’s capability to actually “respond” lies in its ability to share data between sensors. We’ve discussed how the use of location-based video analytics provides insights such as target position, real-size and object movement, but there are other types of sensors within a typical surveillance system that are geospatial - meaning they can share and receive location data. When these sensors collaborate...
on target type and location, they can effectively react to various types of intrusions. To demonstrate this capability, let’s look at two different detect and respond scenarios.

The first scenario involves the use of a detection camera, enabled with video analytics.

**Figure – Scenario 1 – Video Detection**

The first scenario involves the use of a detection camera, enabled with video analytics. Once an intrusion occurs (point 1) the system can immediately detect the objects location (point 2) and issue a detection alarm including looping video, live camera view, and map location based on the detection by the fixed camera (Point 3). However, it also has the ability to share this data to other geospatially aware sensors, in this case a PTZ camera. Sharing the location data of the target allows the PTZ to swing to the exact location of the intruder and invoke a camera auto follow algorithm (points 4 & 5).
The same scenario is applicable to other types of security sensors which can provide the detection and target location information. These include sensors such as radar, access control, proximity sensor, fiber or intelligent fence. In this example, an intelligent fence provides the detection and position information (Points 1 & 2) and then passes this information to two PTZ cameras, which then slew to the target location, lock on to the target and begin to auto follow (point 3). It’s important to note that this capability is not dependent on camera type. Both visible and thermal PTZ cameras can be enabled to slew to cue and auto follow.

The use of location data has many applications, one example is referred to as “Scan to Target.” In the case where a detected target may be moving quickly, or the position data may contain a slight error, the system may steer a PTZ to the alarm location and there is no target present. Using the alarm position information, a scan to target algorithm can automatically scan the surrounding area with the PTZ camera in an attempt to acquire the target. If found, it can lock on and commence following.

NERC #3 - COMMUNICATION & NOTIFICATION

The key to the successful communication of an intrusion is the ability to provide a large amount of data in a method that is quickly understood. What happened, where did it happen and what’s happening now. A map-based surveillance system has the advantage of providing a wealth of alarm information in a single, easy to understand interface. In this case, the intruder is detected in the live video, but is also dynamically shown on the map with an icon indicating that it is a human. Breadcrumbs denote his track and direction of movement.
Additionally, an alarm window instantly provides a textual description of the event, an image capture of the detection, a looping video of the alarm, the live camera of the event and quick access to any PTZ cameras which have been assigned to follow the intruder. So, within a few seconds of the alarm, the operator has all the important alarm information automatically displayed.

If desired, this information can then be sent to assets in the field, providing them live information on their mobile devices at the point of intervention. Likewise, information obtained at the scene can be captured by the first responder and instantly shared at the central control station, and any other remote monitoring locations.

**NERC #4 - DETERRENCE AND DELAY**

Typically, when we think of deterrence and delay we don’t envision those actions being taken by the video surveillance system either. But in fact, intelligent video combined with audio and other devices, provides a very effective method for deterrence and delay. One of the primary means of deterrence using video surveillance is **Intelligent Audio Talk Down**. This is the capability to effectively follow an intruder with video an issue intelligent audio commands to deter their progress.

Much like the scenarios already described, Audio Talk down starts with a target detection, automatically steering a PTZ to the target location, locking onto the target and beginning camera auto follow, then utilizing an LRAD or other audio device, along with knowledge of the intruder’s actions to intelligent issue recorded commands to deter their actions.
In some cases, the audio device may be directional, being steered at the target using the same PTZ follow algorithm, in other cases, non-moveable speakers can provide the commands.

The key to successful audio talk down is the video intelligence, which allows accurate detection, tracking and selection of automated or live audio response. Knowing they have been detected and are actively being monitored is often enough to deter most intruders. However, high critically assets can further enhance the solution with loud hailers and dazzlers, which are designed to physically incapacitate the intruder with deafening alarm tones and/or blinding dazzler lights.

**NERC #5 - ASSESSMENT OF ATTACKS**

The final area of concern is the assessment of an event, in both real time, and post-mortem to aid in investigations, pursue prosecution and analyze potential improvements. Video comprises a very large matrix of data, updated 15 to 30 times a second. Video Analytics analyzes this video data - continuously converting it into meta data - which is then assigned to specific frames of video making it easily searchable and protected for purposes of evidence submittal. The associated video player includes the ability to add user annotations, save those annotations without corrupting the digital video signature, and then search the video based on those annotations.
Forensic search is another key capability that supports the ability to assess events. Most investigations need to understand where the intruder came from, or perhaps obtain different views of the intrusion to fully understand the details of the intrusion. A forensic search allows a user to select any camera, or just a portion of a camera’s view, and quickly search that video over a defined time period for specific types of activity. It also has the ability to ignore specific reasons, to speed up the search by avoiding regions of high motion. This results in a huge time savings and a higher accuracy search over the traditional method of fast forwarding through the recorded video. In the case of the PureActiv Forensic browser, video clips that meet the search criteria are quickly displayed as thumbnails, which can then be reviewed for relevance and then exported as evidence to support the incident.

Although a video management’s alarm function is often considered part of the “Detection” phase, it is also critical in assessing an event, including when the event occurred, the details of the event, related camera views and sensor data, as well as, the actions taken by operators. The above image details the wealth of data provided by the PureActiv VMS, including map-location of the event, still image, looping video and a full database record of alarm and user metadata.

SAFETY MONITORING

At this point, we addressed specific features and capabilities of today’s surveillance systems aligned with the five tenants of the NERC CIP014 guidelines. However, these same systems and capabilities can also be utilized for safety aspects of the power grid, including monitoring for employee safety and process compliance, documenting potential liability incidents with digitally signed video, as well as actively monitoring equipment for overheat, conditions, fire or smoke. One such use case
involves the use of thermal cameras to monitor and alarm for the overheating of a transformer due to loss of cooling oil. So, as you consider addressing the physical security of your utility assets, don’t forget to double dip and achieve advantages in terms of safety monitoring as well.

We’ve presented a great deal of information as to how you can go about protecting critical portions of the power grid through the use of intelligent video surveillance and complementary sensors. This table summarizes the solutions we discussed and how they align with the different sections of the NERC guidelines. You don’t need to implement all of these solutions at one time, but it’s worth taking the time to consider the best path that will get you the most coverage.

Figure – Video Surveillance Features to meet NERC CIP014
NEXT STEPS FROM PURETECH SYSTEMS

Case Study – Substation Physical Security: There are many solutions to help power utilities address physical security concerns identified as part of NERC CIP-014. One effective choice is the use of intelligent video, as outlined in this case study.

Substation Security Automation: The challenge power utilities worldwide are facing is finding an affordable solution, which can help detect, deter and facilitate an informed response to a substation security event. This article describes how technology can help detect, deter and facilitate an informed response to a substation security event.

8 Things to Consider When Designing a Camera Perimeter: There are many guidelines that have been released that provide information as to the type of security measures that should be considered when protecting these facilities. However, the details involved with making these measures a reality are often missing. This paper presents 8 things to consider when designing a camera-based security system, or when reviewing your existing one.

Tailgating Vulnerability at Substations: One vulnerability of substation access control is the fact that it can control opening a gate when an access card is presented, but it cannot control how many people or vehicles actually enter behind the authorized card holder. This article addresses this CIP vulnerability referred to as “tailgating” or “piggybacking.”

About PureTech Systems

PureTech Systems Inc. is a manufacturer of wide-area perimeter surveillance software solutions including internally developed outdoor video analytics, PTZ Auto Follow, multi-sensor integration and a map-based (real object size) command and control. It is offered to fortune 1000 firms, military, petro-chemical, water and electric utilities, seaports, airports and federal, state and local governments. With headquarters in Phoenix Arizona, PureTech Systems serves national and international markets. To find out more about PureTech Systems Inc. visit our website at www.puretechsystems.com, follow us on Twitter @PureTechSystems or sign up for our email list.