Honeywell

Preparing Utility Substations for the Physical Security Requirements of NERC-CIP-014

At 1 a.m. on April 16, 2013, PG&E Corp.'s Metcalf transmission substation in California's Santa Clara County was attacked by snipers. According to reports, someone slipped into an underground vault and cut telephone cables. Within a half hour, the snipers opened fire—taking down 17 transformers that funnel power to Silicon Valley—and escaped before police arrived on the scene. Jon Wellinghoff, chairman of the Federal Energy Regulatory Commission (FERC) at the time, called it "the most significant incident of domestic terrorism involving the grid that has ever occurred." Whether or not the now widely publicized Metcalf incident can be called an act of terrorism, it brought to light several key shortcomings in industry security standards. The numbers below expose only the surface of the substation's alarming vulnerabilities:

Minutes snipers opened fire	19
Number of transformers surgically hit	17
Minutes until first response	51
Cost, in millions of dollars, of damage	15
Days to bring the substation back online	27
Attackers caught	***0***

The incident gave power companies, industry observers, government officials and the general public a glimpse into the type of damage that could be inflicted on the nation's power grid if similar attacks were carried out again elsewhere.

In the wake of the attack, the FERC issued an order for the non-profit North American Reliability Corp. to develop security standards for Bulk Transmission Owners and Operations. This white paper will provide an overview of the regulations expected to face substation managers in the next two years, how those regulations will impact the makeup of substation security, and the types of technology investments utilities should consider when designing security solutions to comply.

Section 1: New Threats, New Rules

Security is a constantly evolving industry with threats rising from unknown sources every day. In a regulated world, companies must prepare for both threats they can anticipate as well as for threats not yet uncovered. The term "attack" can be used to describe an increasing number of incidents that challenge the security of a utility company. Theft of materials for scrap sales, cyber-attacks on company data and destructive events aimed at damaging or interrupting power service all are at the forefront of the industry's security discussion.

Substations have the enormous responsibility of keeping power flows balanced by transforming voltage to safe, appropriate levels for electrical use and routing it to the correct location. At the same time, their unique settings often cause major concern for attacks; usually they're unmanned and in remote, open locations, making them ideal targets. Furthermore, many aren't equipped to relay signals in the event of a security incident. For example, when a substation's telephone lines are cut without a proper security system in place – a massive security breach – no one it is alerted, and therefore no one can respond. In the case of Metcalf, action was taken only after someone happened to hear gunshots, which was too late to change the outcome. These crucial shortcomings combined with the sheer quantity of electrical substations – there are 55,000 large substations scattered around the U.S., 400 of which are deemed "critical" – expose hefty security challenges the government is seeking to address.

Before December 2014, only one set of physical security requirements, CIP-006 Version 3, was in effect. After **April 1, 2016,** however, three physical security standards are expected to be required across North and Central America:

- CIP-014-1 addresses immediate risk to critical substations and control centers, as defined by FERC
- CIP-003-6 requires operational and procedural controls for Low Impact Bulk Electric System (BES); and
- CIP-006-6 requires operational and procedural controls for Medium and High Impact BES Cyber Systems, including additional protection of communications cabling.

The details and precise implications of these new security standards are yet to be fully deciphered. For example, operational controls can mean anything from door locks to card readers and video surveillance, and procedural control could be something as simple as a guard with a sign-in book. Whether FERC will further define these specifications or leave them to the discretion of the individual entity is still uncertain. Regardless, compliance will be strictly enforced starting in 2016, and the new standards are expected to significantly impact all substations in the form of physical access controls, perimeter intrusion detection, monitoring alarms, incident response, logging, and testing and visitor programs.

It's very much worth noting that regulations typically take years to go into effect. The fact that regulators are attempting to fast-track the new standards in a mere matter of months speaks to how urgently utilities need to reform in order to avoid another Metcalf-like incident. Stronger still is the motivation to stop individuals from causing injury or death to anyone, including themselves.

This paper will focus on the imminent CIP-014 physical security standards for critical substations and ways to comply with them to prevent losses, not to mention reputational damage. In essence, CIP-014 can be summarized as the requirement to deter, detect, delay, assess, communicate and respond to physical security threats, which will be explored further in the following sections.

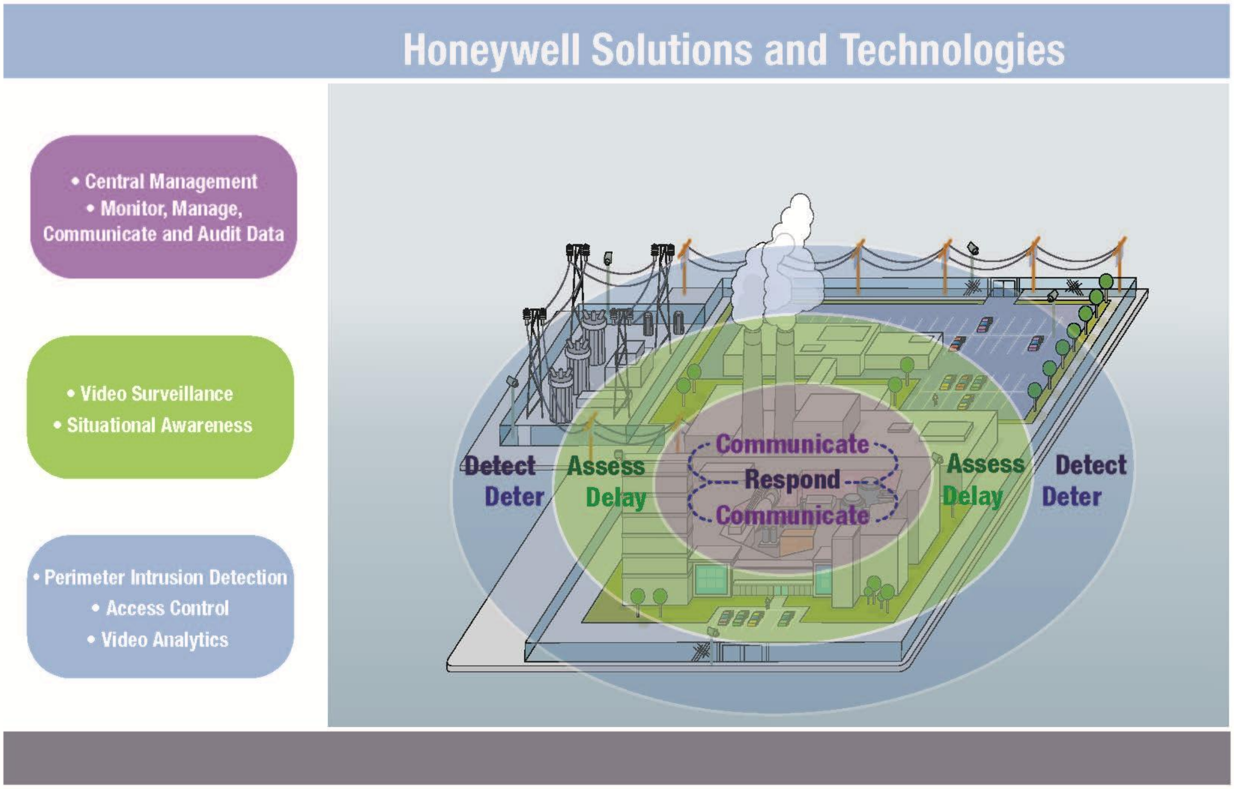
Section 2: A Solution to Mitigate Potential Threats

The utility industry is one of the most regulated in the world, and that was before CIP-014. Penalties for CIP-014 could range from $10,000 to $1,000,000 *per day* of violation, and in order to comply with the new standards, facilities will need to adopt more tightly integrated systems. Designing a sustainable "early warning" system that can reduce risk and maintain compliance involves mastering a three-pronged approach:

1. Perimeter intrusion detection
2. Video management
3. Access control

Maximizing the effectiveness of these three technology categories requires an integrated approach in which operators themselves can access, control and manage each prong through a single user interface. This can be achieved with a central management system.

The below table provides a general overview of what will be outlined in the next few sections: how, specifically, this three-prong approach operating via a central management system is designed to meet the requirements of CIP-014 to deter, detect, delay, assess, communicate and respond to threats.



Honeywell Solutions and Technologies

- Central Management
- Monitor, Manage, Communicate and Audit Data

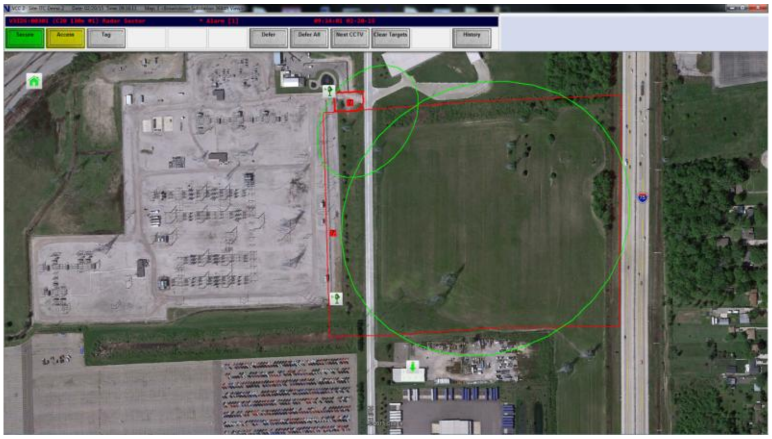
- Video Surveillance
- Situational Awareness

- Perimeter Intrusion Detection
- Access Control
- Video Analytics

Section 3: Perimeter Intrusion Detection in CIP Compliance

At a basic level, defending the perimeter means installing a layer of security outlining property borders. In the past, facilities equated perimeter security with chainlink fences and padlocks. Today, by stark contrast, advanced sensors should be considered “bare bones” to a perimeter defense system. The modern perimeter should not only keep unauthorized persons off the property but they should also notify the appropriate authorities well in advance of a detected threat; up to two minutes before an approaching intruder is ideal, for allowing enough time to receive, process, and respond appropriately to the alarm.

Most challenges to deploying perimeter protection stem from geographic conditions. Expansive perimeter boundaries, water boundaries and difficult terrain limit the type and increase the cost of perimeter protection solutions. To tackle these challenges, perimeter solutions must be ruggedized to withstand the harsh and unstable environments in which many substations are located, including desert, forests and mountains. When regulations require utilities to create hardened perimeters and detection beyond the perimeter – which is often the case for NERC and CIP – highly defined buffer zones of 30 yards beyond the perimeter specified in the regulations is recommended.



Beyond defining and ruggedizing the perimeter zones, it’s important to invest in flexible radar technology, which has advanced well beyond the traditional ground-based solutions. Whereas older sensor technology often causes high rates of false alarm and can’t be scaled for evolving deployment, newer solutions provide built-in flexibility and enhanced nuisance alarm filtering and analytics. Fewer false alarms can save significant money and resources in the long-run, and ultimately increase system reliability and peace-of-mind. Coupled with video analytics, today’s radar technology can alert an operator of an *approaching* threat up to two minutes in advance, which is light-years when it comes to detecting and preventing an emergency (and complying with CIP-014). Another feature to look for is open communication architecture over a wide variety of media, such as wire, fiber, Ethernet and wireless. This will ensure a sustainable system that can be adapted with ever-changing regulations and communications platforms, avoiding costly re-installments.

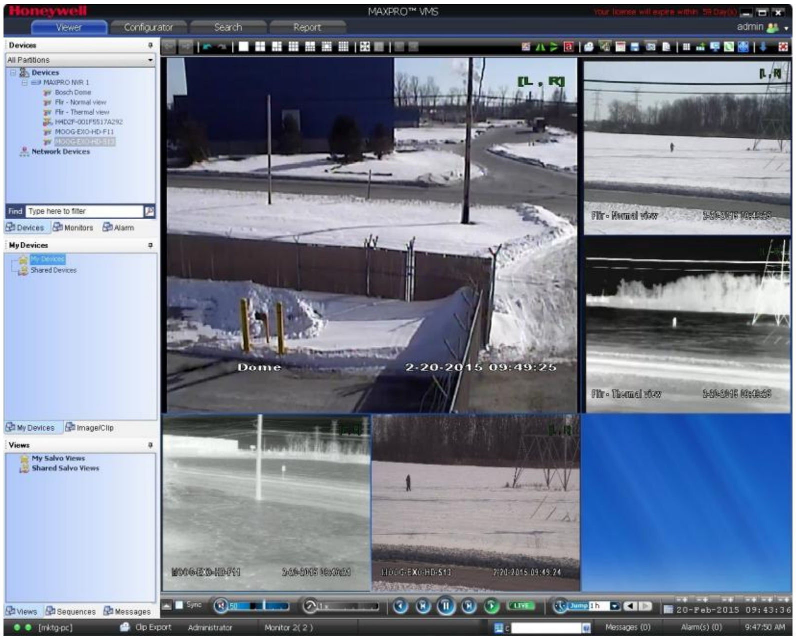
The most successful security solution assimilates perimeter with video management and access through a central management system, which will be a repeated theme throughout this paper. The perimeter solution itself should combine visitor management, access control, video management and intrusion into one platform. All of these parts should integrate to enable the operator at the central station to make quick, informed assessments of alarm conditions for the most accurate and efficient response possible.

Section 4: Video Surveillance in CIP Compliance

Video is another key component to any security system, and can offer so much more than individual configurations for viewing and recording. While the quality of the camera should be taken into consideration – a sharp image can illustrate crucial evidence – today's video solutions are all about the analytics. Embedded IP video analytics can provide valuable intel, allowing an operator to locate necessary views and navigate within any site, as well as verify events to reduce false alarms. Video should work seamlessly with the motion detection systems to capture images and send them to the central station screens for assessment. There, the operator can confirm a threat, make a judgment, and – in cooperation with physical security systems – select the appropriate next course of action right then and there, arming or locking areas as needed. Today's smart video capabilities not only provide live detailed insight, but they deliver the proof necessary for alarm verifications and third party evaluations. Honeywell's integrated alarm management allows Video Only operators to view, virtually go back in time, and respond appropriately to any video alarm in the system, naturally adhering to strict assess-and-respond regulations.

For enterprise installations, there will likely be more sites and connections than any one security professional can manage at a given time. Honeywell offers a unique solution in enterprise format. The management server maintains connections and health assessments of all the connected recorders, and the recorders, placed locally at the site, can continue to operate with or without connection to the central management server. They contain not only the power to record video and manage alarms, but also house in-unit analytics. This provides critical sites with ultimate autonomy in case of communications failure. Through the management server, these sites now can be arranged in any viewing configuration the operator should choose. Pre-determined salvos and sequences can appear as the operator logs in, and moving from site to site is as simple as a point and click.

Regardless the facility size, it's important for recording devices to be robust and self-redundant with duplicate power, hard drive and network connections. They should be managed as any other critical asset in the network and provide sites with enough power to record via incident-only or real time frame rates. That doesn't mean, however, that the devices need to be fancy or expensive. Even the highest level cameras with built-in analytics can't make a site immune; in fact, overly sophisticated firmware may just prove more difficult to manage and program, not to mention pose a greater risk if damaged. Honeywell allows *any* connected video source to be routed to the analytics engine for inspection, which streamlines the process from the work station and lowers the total cost of ownership. It also allows customers to avoid unnecessary investment in higher priced cameras and concentrate their spending on the actual security functions.



Section 5: Access Control in CIP Compliance

Electronic physical security has adapted along with the evolution of CIP regulations. Beyond securing a physical structure, utilities are tasked with advancing security into and outside of their buildings. The primary goal of an access control system is to manage which specific individuals can enter specific areas during pre-determined times and days. The management of access control requires operators to monitor for unauthorized access to a site.

Any utility will have assets secured at the corporate level, the NERC/FERC level and perhaps even the nuclear level. Each of these branches of utility operations will have separate requirements on how Access Control is managed. It is important for utilities to partner with a security manufacturer like Honeywell to deploy a flexible and dynamic system that can operate within these very discrete conditions and regulations.

Flexibility in the configuration of an access control system will allow utilities to adapt to the ever-changing regulations of the industry. As new vulnerabilities are uncovered, systems will have to upgrade their capability to match the standards of security. Honeywell promotes this requirement by offering systems that are scalable, flexible and ever-advancing.

CIP standards are evolving to require more than just a single alarm from an input to create a response. The integration of multiple systems gives utilities the best defense against malicious attacks and regulatory fines. In addition to being able to integrate with intrusion detection, video management, visitor management, mass notification and other security subsystems, the ideal solution should also integrate with HR systems such as SAP; this is critical for applications such as terminations processing to ensure employees who leave the company immediately have their access privileges revoked. Additionally, physical security must integrate into other IT, OT or electronic systems through the use of a SIEM or other aggregation software. The data available from edge locations is now being collected together for system trends and conditions for verified incidents. For safeguarding purposes, backup sites and edge-level logging systems should be established to recover data where data centers fail.

In fact, the management of data is as valuable as the security of facilities. The number one source of regulatory fines comes from inadequate reporting capabilities under audit. Honeywell has developed simple and effective tools to manage the secure import and export of data necessary to maintain a successful access control system.

With regulations in mind, access control is a combination of managing human activity and electronic alarms. Effective access control systems should be able to alert operators of an unauthorized access event within seconds, and log a person's initial entry and exit. Additionally, access control should be integrated with visitor management technology that ensures visitors are continuously escorted if they are not approved to be unescorted. Finally, these systems are required to be maintained and tested every 24 months. Honeywell offers professional services and system optimizations to meet this requirement.

Specific features of Honeywell's solution that were designed to meet NERC CIP requirements include:

- Direct integration into a regulated access authorization database
    - Data transfer utilities and authenticated interfaces allow for the direct import of regulated database information to Honeywell access control systems.
    - Completed Work-Flow engines can integrate to Honeywell systems for authenticated changes through approvals.
    - Certification management tools can work to remove regulated access from a record whenever a card holder is outside of their training requirement.

- Compliance reporting tools
    - Advanced auditing capabilities provide utilities ultimate system history reports through a current/previous database value report
    - Customizable reports that can be easily generated and shared allow for easy collection of data to mitigate the risk of fines.

- Multi-credential access authentication
    - Allow authorized personnel to authenticate at an entrance using multiple pieces of information
        - Something they have – a card or FOB
        - Something they know – a pin number
        - Something they are – biometric scanning

- The ability to electronically register remote visitors
  - Electronic records of registered visitors ensure that every person at a regulated site is accounted for and properly escorted.
  - In emergency scenarios, all employees and non-employees can be accounted for quickly and effectively.

- Remote capabilities that allow clients to access the system through terminal servers, as well as multiple authentication
  - Data security and authentication can be preserved and managed centrally.
  - Every aspect of an employee's digital identity can be migrated to their current physical location.

- Field hardware (panels) that use one firmware, remove users/passwords and support open port management
  - In accordance with CIP regulations, firmware is logged and reported in the Central Database for Utilities to maintain the latest released and available versions in all of their field hardware.
  - Strong password enforcement and non-accessible panel operating systems at the edge upholds strict Cyber Security regulations.

Specifically, Honeywell's advancements in access control respond to the current CIP regulations while allowing customers to prepare for future regulations as well. The open nature of the configuration admits for future technology assimilation. The use of advanced perimeter security, including video analytics, thermal cameras, seismic and fence detection systems, and even ground based radar systems have been deployed. When biometrics and two or three factor identification is required, Honeywell is working with these deployments to deliver security built to support the regulations.

Section 6: Central Management Solutions

As mentioned throughout this paper, perimeter, video and access control systems can be effective, but not to the full extent that CIP-014 is expected to achieve as standalone solutions.

Arguably the most-critical element of designing an effective solution to comply with the CIP-014 requirements is the seamless integration via the central management system, bringing each security subsystem (perimeter, video, access, intrusion sensors, etc.) into a single platform. The central solution, monitored at a company's Corporate Command Center for 24/7 support, provide visitor, data and document management and have robust reporting capabilities to ensure compliance with federal regulations. Increased security threats to enterprise infrastructure, heightened customer awareness of security offerings, and technology advancements in outdoor and wireless sensors, as well as integration methods, have boosted growth in this sector.

An ideal solution should provide flexibility to integrate with third-party systems. While it can be efficient and effective to design a solution using technology from a single provider, the reality is that many substations use equipment provided by different manufacturers. As such, an open central management system is highly critical to designing a solution that can meet the requirements of CIP-014. A Honeywell central management system, for example, can be used as an access control and reporting product only, or as an integration platform to which solutions can be easily added. This allows substations to leverage existing hardware as the system grows, and the common user interface helps minimize IT and training expenses.

At a minimum, such a system should be able to integrate perimeter protection, video management systems, surveillance cameras and access control panels. The newest versions of Honeywell's central management systems all enable substations to constantly add integration features, such as compatibility with additional perimeter products, and enhancements to accept multiple wireless/biometric readers.

Now that the integrated three-prong security approach has been discussed, below is a chart outlining the overall strategy to meeting each of CIP-014's requirements, in addition to how Honeywell is equipped in providing a scalable and sustainable solution for compliance now and in the future.

Edge Security Role in Meeting CIP-014 Req. 5.1

CIP-014 Req. 5	Compliance Strategy	Honeywell Solution
Deter	Visual and audible warnings from strategically mounted devices deter many threats before they occur. Combining smarter perimeter structures with advanced detection devices will not only deter attacks at the sight of security, but actively warn assailants that their activity is recognized.	Perimeters with visible fence detection, ground based radar, video surveillance with active video analytics and intrusion detection all integrated into audible warning systems and operator consoles.
Detect	The goal of a strategically deployed sensor system on a perimeter should be to provide notification of potential breaches at the actual perimeter lines. At a basic level, this can be achieved, for example, using fence-mounted or individual infrared sensors at the perimeter/border. Advanced sensor systems, such as radar, can notify operators of a potential breach as quickly as two minutes in advance of a perpetrator *approaching* the border, providing more room for response and action duty.	Multi-layered sensor deployment for early warning detection and location, analytics alarms and/or radar for perimeter approach, perimeter alarms for reach and breach, confirmation analytics alarms within the perimeter and direct alarms from physical barriers upon breach. Rule based logic combines video, radar and sensor technologies integrated into one system.
Delay	The most obvious way a perimeter solution can delay an impending attack is its physical presence (i.e. intruders need to physically get themselves past the fence). The longest delay, however, won't truly prevent anything unless the aforementioned sensors can communicate with a central management system to alert operators.	Visible detection devices and audible alarms to delay approach, integration with sensors on physical barrier structures such as fences, gates, walls and doors with multi-credential access. Advanced sensor systems, such as radar, for early detection allow operators to deploy forces to physically delay intruder.
Assess	When integrated into a central management system, perimeter sensors are coupled with video and shown on a map-based display, which offers situational awareness for quick assessment.	Advanced situational awareness allows one alarm to populate across multiple systems and allow for unified management and response. Video surveillance, access control and alarm view and verification can be driven and automated at one operator station. Map based user interfaces display geospatial information for "assessment at a glance."
Communicate	Move accurate data and alerts to the correct personnel and/or workstations. Confirm response and actions through effective alarm response procedures.	Integration to standard notification paths via e-mail and intercom can increase efficacy. Add this to the integration of all system alarms into a central management system for an automated global alarm

		monitor that can be viewed at multiple locations simultaneously.
Respond	Use all data to determine the correct course of action and dispatch the appropriate response. Confirm locations, threat presence and type of response with the elements of video surveillance and sensed alarms.	Global alarm ID and integration between systems allows for a unified alarm monitor with pre-programmed response codes and instructions. This reduces "in-the-moment" mistakes and allows for system wide confirmation of alarm response.

Section 7: Beyond the Central Solution: Additional Management Services

In addition to physical security regulations, the management of personnel and system data also carry the weight of risking heavy penalties, as touched upon in Section 5. Incorrect or incomplete data can predicate a fine through the audit process, just as an actual security breach. Services such as Honeywell Security Management Solutions provide deeper resolution to these compliance requirements. The ability to automatically populate data from other sources in several industry standard formats reduces data re-entry and the chance of human error. Audit logs in the software go beyond the requirement to not only show a record of activity but also the prior value that was modified or deleted. The ability to push that data through direct integration or through common report exports allows for the ultimate level of communications compliance. The correct data will always be exactly where the user needs it.

While the data regarding personnel and systems operation must be accurate, it is also important to keep those management systems up to the current release level. When integrated systems are sourced from separate vendors, the collection and maintenance of all regulated data can become time consuming and confusing. Always look for the latest versions and release notes under software service agreements, as well as the ability to streamline hardware and software upgrades.

Taking a step back from data management, one of the largest challenges for utilities is developing and designing a security plan, especially with the new onset of rigorous standards. Awareness of the types of technologies and solutions that are available does not necessarily mean that utilities know how to assess their sites and pull together an integrated, comprehensive solution. Many security providers such as Honeywell offer professional services to help facilities understand their vulnerabilities, and then work with them to develop a security plan that is regulation compliant, mitigates risks and is within budget.

In order for a security solution deployment to be successful, every element, including selection of technology, logistics planning, implementation and life cycle planning, must be thoughtfully considered and managed. Honeywell partners with integrators and technology providers to guide the process from beginning to end.

In addition, robust training and education of the solution installation, operation, administration and maintenance is of course crucial. State-of-the-art training, both standard and customizable, ensures both integrators and end-users have the knowledge they need to deliver and sustain an effective security solution.

For more information on Honeywell's Professional service offering please visit:

Honeywell Professional Services: http://www.honeywellsystems.com/support/professional-services/index.html

Honeywell Training Solutions: http://www.honeywellsystems.com/support/access-video-training/index.html

Key Honeywell Solution Features for CIP Compliance

In summary, the rollout of CIP-014 will cause immense security implications for utilities substations throughout the U.S. If adequately prepared, utilities professionals can maximize the effectiveness of their security systems in time to avoid harsh penalties and ultimately insure against breaches like Metcalf. Here is a recap of some key Honeywell features that can help facilities achieve compliance now and in the future:

1. **Perimeter Intrusion Detection:** Honeywell's rugged perimeter detection can withstand harsh environments, and radar solutions offer deployment flexibility and enhanced filtering for accuracy. This technology can provide up to two minutes of advanced notification of an approaching threat, giving extra time for response.

2. **Video Surveillance:** Operators can view, record and respond to any video alarm in the system (available in accessible enterprise format), which can also be used to adhere to strict assess and respond regulations. Honeywell's video surveillance can be integrated with smart embedded video analytics to reduce false alarms, as well as with physical systems to take action such as lock or arm.

3. **Access Control:** Honeywell's access control system provides sustained connection between human activity and electronic management, and is flexible enough to integrate with intrusion detection, video management, visitor management, internal communications, and HR systems. It can adapt to ever-evolving industry regulations and upgrades.

    a. **Data Management:** Compliance is only achieved when properly documented, and Honeywell offers simple and effective tools to securely import and export important facility data. Honeywell Security Management Solutions helps reduce the chance of human error with software-embedded audit logs tracking activity and keeping records of that activity.

4. **Central Management Solution**: Finally, a central management system brings it all together into a single platform that works smoothly to ensure high-level compliance. Honeywell's solution is able to integrate with third-party systems, allowing substations to leverage existing hardware and infrastructure to minimize training and expenses, but also allow for future changes and add-ons.

    a. **On-going Services:** Beyond the Central Management Solution itself, Honeywell offers professional services and system optimizations to meet bi-annual maintenance and testing requirements. Honeywell has designed specific features to meet NERC CIP requirements outlined on page 8, and can offer consultation on facilities' vulnerabilities to determine a custom security plan.

Combining world-class products, 24/7 services, and consultation from top-trained security professionals, these integrated approaches are able to meet and go beyond each of CIP-014's requirements to deter, detect, delay, assess, communicate, and respond to security threats, as outlined in Section 6.

Conclusion

Moving beyond individual tactics, the keywords in Requirement 5 of CIP-014 are "collectively" and "evolving." The subsystems outlined above can fill gaps in a substations' security, but are more effective in satisfying the requirements of regulations such as CIP-014 when tightly integrated. Rather than go through an OEM third party and have to juggle and connect multiple functions, vendors and control systems, manufacturers such as Honeywell offer one robust solution. Perimeter, video and access and control management systems should work seamlessly together to meet government compliance that already exists as well as the onslaught of new standards from CIP-014. Honeywell's layered security offerings integrated with a central management solution provide an end-to-end security solution that's scalable and designed to meet the tailored requirements for each unique substation.