White Paper

Remote Monitoring and Control of Substations

Where do RMAC, NERC, FERC, and CIP5 Collide?

FAEWPCIP5©2015

Contents

Introduction

Bring up the subject of Information Technology, or IT, and most people at least understand the term. Mention Operational Technology (OT) and there is likely to be less knowledge of the subject or even a clear-cut definition of what it is. Simply put, OT is the hardware and software that is deployed to monitor and control physical devices in a control system network — whether these are smart meters or the electricity distribution system. OT is considered to be the cyber-physical layer interface where a click of the mouse can cause a pump to start, a valve to open, etc. When these systems started to be automated, the systems were proprietary and little (or no) regard was placed on cybersecurity. These early control systems were predominantly isolated with physical security being the normal method of ensuring the systems were protected.

There has been pressure brought by the IT departments in many utilities to use TCP/IP networking to connect these industrial control systems to the business or enterprise networks in order to accelerate the flow of information between the two networks and deliver what is being termed the "Converged Network." This is being driven primarily by the perceived need to share information regarding the control process (e.g. power usage, fluctuations, amount of oil or gas being pumped) with the business personnel. In the initial push for this "convergence," cybersecurity was not high enough on the agenda for the utilities or for the vendors designing and supplying the equipment.

However, events over the last few years have changed the assumptions on which newer industrial control networks have been built. Although the development of the "smart grid" has provided the drive for converging information and operational technologies, building out the "Industrial Internet of Things," it is now realized that some of the promised benefits, such as increased flexibility and efficiency, have a negative side. The "converged" network model (i.e., using IP) does not necessarily equate to networks being isolated and deployed in a secure manner and the old security models no longer apply. To secure and protect control and automation systems requires careful and measured action and developing a plan in-flight. The industry can and must learn from the experience of the IT departments, but the particular considerations of industrial control environments call for adaptation rather than duplication.

OT networks cannot be supported or treated like IT networks. IT systems are typically refreshed every 3-5 years, while OT systems have a life of 10-30 years. Critical systems running on unsupported, manufacturer-discontinued hardware is not unusual. Compounding this situation, OT engineers are often operating critical systems that need to be available the majority of the time — often expected to be 99.999% (5 nines), which equates to a downtime of only 5 minutes per year. IT engineers are used to patching Microsoft Windows systems every month, usually with a required reboot, making this target unobtainable. OT engineers therefore patch systems on a less frequent basis — only when absolutely necessary — resulting in not having the latest security patches applied to even the newer systems.

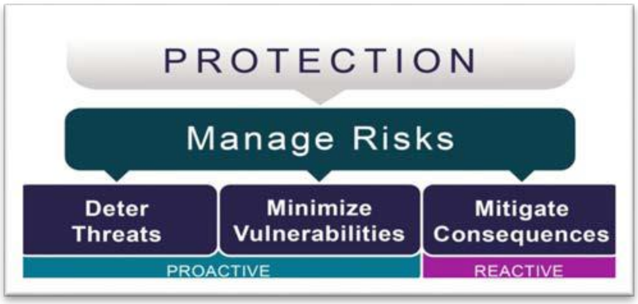
The interconnection of IT and OT systems has increased the attack surface of OT systems considerably. In addition, the lack of patching and inadequate cybersecurity awareness in the OT workforce makes these systems more vulnerable. The notion that adversaries cannot attack these systems has been shown to be false. Industrial control systems are complex and have unique challenges that are often unknown to IT personnel and IT security teams. Configuration and security testing of IT systems in an OT environment need to be handled differently than for an IT environment. Losing a database in an IT environment may lead to some data loss. In an OT operation, it might lead to having the whole process shut down with the consequential loss in revenue.

The development and deployment of new control systems over the last 10 years in particular has accelerated the blurring of IT and OT. However, the education of OT engineers in IT and security practices has not accelerated, nor has the education of IT engineers in the specifics of control networks. Both groups need to understand each other and work together to increase the security of our critical infrastructures.

Critical Infrastructure Protection (CIP)

To address the security concerns regarding the vulnerability of the OT networks in the utilities the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) have developed a series of Critical Infrastructure Protection (CIP) regulations. The regulations that address IT/OT networks are collectively referred to as CIP 5, although the regulations currently go all the way to CIP 11 and CIP 14 addresses physical security.

These regulations are designed to "protect from and deter potential threats to, utility facilities, substations, and control centers that if rendered inoperable or severely damaged could result in widespread instability, uncontrolled separation, or cascading failures within an interconnection."



Failure to comply with the CIP regulations will result in substantial fines being imposed on a utility by NERC, so how does a utility address CIP 5 compliance?

Establish an Integrated Security Program (ISP)

A central framework considering the security of all components is essential to optimize resource allocation and results. Documentation of devices, networks, procedures and processes will support both the development of the security program and its operation. Integrate security into business processes as well as operations, including procurement and decommissioning processes.

Manage the Integration of Information Technology into the ISP

In a recent SANS survey, 18% of companies still haven't started to deal with technological convergence or its security implications, and 36% are just beginning that process. With all signs indicating an increasing rate of IT-OT convergence for the foreseeable future, failing to plan for its management is a recipe for ballooning risk.

Increase Visibility into the OT Environments

The number of OT security breaches keeps rising and the length of time between incursions and their discovery isn't shrinking. Lack of visibility into control system devices and networks has always been one of the greatest barriers to securing them. Without an awareness of normal network communications and device activity, properly evaluating and improving asset security is not an achievable goal.

It is imperative to map all devices, physical interconnections, logical data channels and implemented protocols among devices. Armed with that picture of activity, it is vital to create a baseline to define normal control network activity and communication. With this information fully documented, it is then important to enable device logging and strict configuration and change management to keep records up to date and to automate log analysis to detect anomalous activity.

Protect the Weakest Points First

Many OT protocols are inherently vulnerable, making them very attractive targets for malicious actors. Despite this fact, these are often left unmonitored. This can effectively create a position of default trust to traffic from IT networks, a very dangerous state of affairs, CIP 5 requires that OT traffic and IT traffic is identified and they kept separate on the network.

Engage Trained Resources

OT security is not the same as IT security. Many tools and practices taken for granted in the business network will themselves cause disruptions in operations. Securing the converged environment requires expertise in both areas. Having the right people involved from the start is essential to reduce the risk of costly missteps.

The challenges of establishing and maintaining security of control and automation systems are numerous and the necessary tools and trained personnel in short supply. The goals are achievable, however, and the risks of not working towards them are high and rising. Companies that focus their resources on a considered, planned approach can lead the way in setting a new standard of reliability and resilience in the face of the changes besetting industry now and in the future.

Remote Monitoring and Control – RMAC

With more than 150,000 substations comprising the Bulk Electric System (BES) these, often remote, facilities are seen as one of the BES soft spots. The large number of targets that can be relatively easy to compromise can have a critical impact on the BES as a whole due the highly interconnected nature of the systems.

The substations are vulnerable not only to cyber-attacks but, as has been seen over the past few years, unauthorized access that has led to control house sabotage, coordinated transformer attacks and damage to transmission lines.

Therefore, remote monitoring and control of the substations is a very important way to protect the critical infrastructure, however it poses a series of challenges for both the OT and IT groups within a utility:

- Regulatory compliance
- Physical and cyber security
- Asset management
- Different network types
- Different network requirements
- Application visibility and control
- Operations management
- Sharing of management information
- Access to remote sites
- Manage equipment
- Remotely reset equipment
- Network resiliency
- Automatic rerouting
- Fault tolerance
- Network element backups
- Local ability to respond to events
- Routine maintenance
- Network performance

Addressing all these issues in a way that also achieves CIP 5 compliance is no easy task. FAE Telecom believes it can only be done effectively using a CIP-compatible network management environment. This is the only way to manage the OT/IT integration through increased visibility of the network and being able to identify and then protect the weakest points first.

Virtual interactive Network Environment (ViNE)

Gaining a true picture of the network must be the starting point for building the ISP. Until a utility knows exactly what is connected and what protocols are running (and yes, there are some surprises out there), it is impossible to protect what you do not know you have.

A Virtual interactive Network Environment (ViNE) creates a “virtual” computer-based picture of a network. A ViNE simulated network can be more extensive than can be created with any physical network environment.

The first step of a ViNE is “discovery,” where the ViNE automatically trawls the entire network and identifies every device connected and its configuration. This “virtual network” view is then stored and can be used as the base audit level for inventory for a NERC compliance audit. A ViNE is ideal for developing, testing and demonstrating applications for scalability, robustness, performance and effective policy implementations within an IT/OT integrated environment. It is possible to easily extend a physical environment without physically attaching additional hardware. A ViNE cost-effectively provides network designers, testers, implementers, and trainers a private, virtual network. This eliminates the overhead and headache associated with having to purchase, maintain and administer physical equipment – which could be physically and financially prohibitive for large-scale networks. A ViNE significantly increases the efficiency of designing, implementing and supporting large OT/IT integrated networks

ViNE combines real device hardware with emulated “virtual devices” to produce a larger, more complex configuration that is more flexible and more cost effective as a tool for network traffic simulation, device test, disaster planning and training. Multiple devices can be configured in such a way that when you have an effective ViNE of a large-scale network, network management applications cannot tell the difference between real device hardware versus the emulated device. Virtual devices serve much better as a test and training network in that anything that is modified on an emulated virtual device does not risk a network “crash” or seriously inhibit performance. .

A ViNE can serve as a robust proving ground for testing new devices without actually having that device in its physical form, allowing much more extensive testing of possible security solutions and new applications.

Management Software

The second step in the process is configuring the network management system that will allow a utility to address the series of challenges listed above. There are many management platforms on the market so this paper will approach it from a generic requirements perspective, examining what needs to be addressed and what a utility needs to look for when selecting a platform.

Regulatory Compliance

NERC CIP regulations require a utility to be able to:

- Provide secure authentication such as LDAP, Radius or RSA.
- Keep an audit trail of all actions on the network.
- Keep long-term historical data of all actions and incidents.
- Be able to effectively correlate alarms to circuits.
- Be able to have site isolation detection.

Asset Management

As was discussed in the ViNE section, a utility has to know what its assets are before they can be managed. Once the assets are identified the network management platform has to

- Control firmware
    - By reporting unsupported firmware versions.
    - Detecting unauthorized changes.
- Automate network element user account management.
- Provide external perimeter surveillance at the MAC layer.
- Support numerous devices using numerous protocols.

Operations Management

NERC CIP requires a utility to be both proactive and reactive so that it has to:

- Be able to detect a service degradation before a network outage occurs. This degradation could be caused by a network failure or a cyber-attack. Being able to see what is happening allows the utility a chance to prevent a failure.
- Detect a service-affecting outage and automatically activate an alternate route to restore the network
- Support all Performance Management information.
- Automatic alarming when threshold levels are surpassed.
- Predefine Quality of Service (QOS) criteria for circuit types.
- Detect bandwidth bottlenecks
- Monitor types of traffic (NetFlow, S/Flow)
- Offer operators a visual understanding of the network and circuit layouts
- Provide network grooming
- Have automated restoration procedures in place that will kick in to maintain connectivity and visibility in the unfortunate event a failure does occur.
- Meet the NERC requirements for Control Center fault tolerance by providing synchronized network management systems across the primary and backup control centers.
- Provide management fault tolerance so that any network management system failure does not prevent management of the network by passing control to the backup control center transparently.
- Allow CIP Network isolation from the internet and even operators to ensure protection from the outside world.
- Allow the sharing of critical information between interconnected utilities, whilst maintaining complete security.
- Offer extensive NERC CIP compatible reporting for compliance requirements

Application Visibility and Control

There are a multitude of devices in a substation supporting an even wider variety of network, environmental and control applications, so any management system has to:

- Support numerous environmental and control devices as well as network elements.
- Focus on reliable protocols for critical data – not just SNMP v1 or v2c.
- Support extensive alarm priorities to easily separate microwave, SONET, DCS, environmental, security, etc., to allow effective operator action.

- Understand the differences between fiber, copper, microwave and cellular networks.
- Recognize that geography may limit access types and speeds as have the ability to limit network management system traffic so as not to affect the primary purpose of the network such as SCADA circuits, protective relay communications, etc.
- Prioritize alarms based on criticality of the equipment for each site.
- Synchronize standing alarms, not just detect new alarms.
- Perform automatic correlation of AC power, generator running, fuel levels, battery levels
- Automatically detect anomalies such as fuel levels dropping when the generator is not running that may indicate either theft or a leak.

Equipment Management

Remote management, configuration and problem detection is crucial in maintaining the integrity of the network and in the majority of utility networks this complicated by the presence of legacy equipment. This aging equipment is in place to support critical applications and will not be replaced soon, requiring:

- Support of a range legacy equipment with the attendant legacy protocols.
- The support of any vendors equipment
- 24x7 connection with continuous health checks to ensure the equipment is not only on but functional.
- Dual access, when supported, to network elements so that there is no single point of failure for the monitoring and control functions.
- Use of DCC or overhead assists when IP is not available as many of the legacy products are pre-IP and do not support SNMP.
- The ability to issue controls to any type of device, not just flagging alarms.
- The support of automated procedures as much as possible as today’s networks are large and complicated - and getting even more so as they converge.
- The automatic backup of network element configurations.
- The retention of these backups, preferably multiple times.
- The reporting for those elements that are consistently problematic.

Physical and Cyber Security

As CIP is all about security then the following are critical capabilities

- Reporting of access (i.e. door open).

- Reporting of any unauthorized/detected MAC address.
- Prioritization of automated alarm based on time of day.
- The ability to automatically issue controls (i.e. sirens at the site)

Ability to Respond Locally

Identifying and responding to critical issues is crucial in effectively managing the incidents and as utility networks can be spread over many thousands of square miles of territory, the ability for local personnel on the ground to be able to respond in the most timely manner requires

- Access to the management system from anywhere, with secure web access for lightweight devices such as smart phones or tablets
- VPN access to permit remote access to devices

Conclusion

The CIP regulations are newly issued and they have evolved over years of increased emphasis on protecting critical infrastructure, taking much from the Department of Defense's experiences and working groups. One thing is for sure, the regulations will continue to be developed and the scope expanded beyond the current 69Kv and above substations.

Effectively meeting the regulations is more than just checking a box, it requires a careful consideration of how to implement an appropriate level of protection. The key to passing a NERC/FERC audit is having a management hardware/software platform in place that addresses significantly more than just monitoring. It also requires cooperative effort, learning and understanding by both the OT and IT networking groups with in a utility.

No utility can ensure 100% protection. What is critical to the Integrated Security Program though is having a plan that:

- Defines how threats will be deterred.
- Mitigates vulnerabilities.
- Minimizes consequences.

The ISP must use a measured, programmatic approach, with the most effective response to meeting CIP requirements involving many different areas of a utilities operation.

1 Liberty Lane East # 13
Hampton, N.H. 03842
www.faetelecom.com
855.GO-FAETEL (855.463.2383)