21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2023 Grid of the Future Symposium

15 Years Continuous Journey Securing and Managing Edge Devices

A. HAMDON, J. ATKINS
SUBNET Solutions Inc.
Canada

SUMMARY

The journey of a mid-size utility in the US to secure their operational technology (OT) devices used to monitor and control their electric grids over the last two decades is a testament to the importance of cybersecurity in the energy sector. This paper will detail the various steps taken by the utility to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) regulations, starting with the 1200 Cyber Security (Urgent Action) published in 2003.

In 2008, the Federal Energy Regulatory Commission (FERC) approved updated NERC CIP regulations, which imposed mandatory critical infrastructure regulations for US Bulk Transmission Electric utilities. The utility promptly implemented its initial Substation Electronic Security Solution (SESS) in the same year to support compliance with these regulations. The SESS solution provided secure remote access to substation OT devices and supported automated collection of power system fault file data from the grid protection relays. Over time, the SESS solution was continuously enhanced to meet ever-evolving NERC CIP regulations. These enhancements included support for Operational Technology (OT) device password management, configuration management, baseline monitoring, as well as providing additional non-SCADA data from the large variety of OT grid monitoring and control devices.

These improvements allowed the utility to stay ahead of cybersecurity threats and ensure the safety and reliability of their electric grids. Most recently, the SESS solution was expanded beyond those mandated by NERC CIP to provide cybersecurity for the explosive growth of new OT devices that the utility will be deploying as part of its Advanced Grid Intelligence and Security (AGIS) program. This program is part of the utility's ambitious Grid Modernization initiative, which aims to increase the efficiency and reliability of the electric grid. The AGIS program will expand the device count to be four times larger than the current transmission system installation. Moreover, the utility plans to deploy the SESS solution to secure other corporate business units such as Supply Wind Generation collector substations and Gas Transmission critical infrastructure as well.

The utility's proactive approach to cybersecurity ensures that they can protect their infrastructure against new and emerging threats, while also complying with regulations and improving their operational efficiency. Most other critical infrastructure industries are in earlier stages of their OT cybersecurity efforts, and this paper will provide learning, best practices, and the various return on investments realized by all of the utility's efforts over the last 20 years. In conclusion, the journey of this mid-size utility in the US to secure their OT devices over the last two decades is a testament to the

Hamdon@subnet.com

importance of cybersecurity in the energy sector. The utility's proactive approach to cybersecurity ensured they could comply with regulations, protect their infrastructure against new and emerging threats, and improve their operational efficiency.

The paper details the utility's journey and is a valuable resource for other utilities and critical infrastructure providers looking to improve their cybersecurity posture and protect their infrastructure against cyber threats.

KEYWORDS

Device Management, NERC CIP, Compliance, Automation, Password Management, Event File Collection, Baseline Management, Remote Engineering Access, Cybersecurity, cyber security

1. INTRODUCTION

Electric Utilities have needed to secure their OT infrastructure and comply with internal and external regulations for many years. The evolution of compliance and the need for stronger cyber security practices has forced utilities to expand remote device management capabilities and apply cybersecurity best practices to an ever-growing list of OT devices. This paper focuses on a mid-sized power utility company, spanning several states, and their challenges with cybersecurity for their OT devices and maintaining grid reliability.

With the introduction of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) regulations, starting with the 1200 Cyber Security (Urgent Action) published in 2003, the utility began its journey to support compliance with these regulations. In 2008, the Federal Energy Regulatory Commission (FERC) approved updated NERC CIP regulations, which imposed mandatory critical infrastructure regulations for US electric utilities and defined the Bulk Electric System (BES). The standards protected the OT devices controlling BES facilities from various types of threats.

The utility set out to determine the scope of the critical cyber assets (now referred to as BES Cyber Assets) within their multi-state service territory. Substation cyber assets now may have Medium Impact, Low Impact and No Impact categorizations to determine the level of NERC CIP compliance needed for each device at each site.

Manual tracking of asset information for compliance purposes was very time intensive. Manual processes were also inherently inconsistent in the ability to track and manage change controls at the appropriate levels. Manual processes required compliance, engineering and field technical staff to physically travel to site to support the compliance program effort, in addition to their preventive maintenance and outage response activities. The same compliance and technical resources would then update numerous Microsoft Excel spreadsheets to support completion of regulatory agency evidential audit documents across three regional areas of company. In addition to substantial resource costs, the manual process did result in data variances within the regions, which made compliance reporting harder as the data needed to be normalized. Reporting for asset inventory/versioning control requirements is not easily supported. Manual processes were relied on for the utility's compliance but the process themselves were prone to human error, which led to increased compliance risk and time to execute.

The utility implemented its initial Substation Electronic Security Solution (SESS) to support compliance with these regulations in 2003. SESS facilitates remote engineering access to OT devices along with retrieval of event file information. Remotely access and managing the OT field devices was a manual process for the utility with engineers remotely logging into a device to view information or execute advanced device management functions, such as changing the password, firmware management or settings file/configurations changes. The device count was low and the manual process worked well and avoided the engineer having to drive to site and acquire the OT device information.

2. INITIAL PROJECT

The scope of the SESS device management project was initially limited to the BES devices identified by the utility. The list of devices on the BES was extensive, with approximately 4,000 OT devices from several different vendors needing management. These devices were located in the medium impact substation environments.

The utility worked hard to implement the initial SESS with a focus on managing the most critical of OT devices. The project started with the main goals of:

1. Implementing a remote engineering access solution. With the need to reduce or eliminate truck rolls to substations, a remote access solution was developed. Remote sessions saved the utility time and money by not having engineers drive to substations to acquire needed data. As an alternative to driving to site, an engineer could now remotely access the device's engineering port and view device information.

2. Event file collection of disturbance oscillography files and Sequence of Event Records files. OT protective devices capture valuable data at the very instant an event occurs on the power line. The utility wanted to consume these event files immediately to help in outage restoration efforts. In order to acquire the event files immediately, automation of the event file collection process was needed. Once the event file was retrieved, the file was written onto a shared drive for engineer's access and analysis.

The initial project addressed the utility's needs for a remote access and event file collection solution. Gone were the days of driving to site every time they needed a file from a device. The timesaving's of not having to drive to site was a welcomed benefit to many engineers.

The initial project had a limited scope of device support and was focused solely on the protective relays at medium impact BES substations. As a result, the limited scope of the initial project, IED management was still a heavily manual process. Users had to manually login into a device and manually change a password. Other devices the utility has in service that were not protective relays and not managed by the SESS. By managing the protective relay portion of the OT device infrastructure, the utility had confidence the relays would operate normally and provide for a reliable electric supply. For the remaining devices in the substation environment, there was no current plan to manage those devices.

3. CHANGING SESS PROGRAM FOR EVOLVING NERC CIP STANDARDS

Evolution of the NERC CIP standards required commensurate enhancements to the utility's SESS project to address the additional compliance elements added to the standards. To get ahead of the compliance curve, the utility embarked in an evolution of the SESS project by adding the following functionality:

1. Password Management – this functionality provides for greater security when a user is accessing any device. At times password security addressed the complication of keeping track of passwords with spreadsheets or lists. Common passwords were removed from being used and now each device has its own password, to the maximum complexity that the device supports. Passwords are encrypted in a SQL database to ensure security.

2. Baseline Management – this functionality was developed with a great deal of input from the utility since it provides CIP compliance monitoring and reporting functionality. Beyond compliance, Baseline Management provides the ability to validate that each device is correctly configured with the proper firmware and settings, which is key for reliable grid operations. With accurate baseline information, the OT grid devices ensures they act as configured and improves grid reliability by avoiding any abnormal operations caused by incorrectly configured equipment. Ensuring reliable grid operations is of paramount concern to the utility and the device baseline management was a manual, time consuming task. Baseline management addresses compliance to:

    a. NERC CIP-010-4 Configuration Change Management and Vulnerability Assessment.
    b. NERC CIP-007-2 R2 – Ports and Services
    c. NERC CIP-007-2 R3 – Security Patch Management

    The user can specify any number of "Software baseline profiles" which represent baseline configurations. The utility created Software baseline profiles for all device types and their variations within their system. Each profile can include Firmware, Operating System, Software and Patch entries. Software information collected needed to be verified by device and security experts before baselines were approved and configured in the SESS. With baselines in place, devices in the system were assigned to corresponding software baseline profiles. The SESS is configured to run specific jobs against devices on periodic basis. When device jobs are executed, the device information is read straight from the physical device and brought back to the SESS. The system automatically compares each device's information

retrieved from the physical device against information specified in the software baseline profile assigned to the device. If there are any deviations between baseline information retrieved from the device and baseline information set in the SESS, an email notification is issued so that appropriate action can be immediately taken.

Software baseline profiles support security patch management. All device changes are recorded and can be reported on. When applicable security software patches are updated on a baseline profile, it is easy to track if the patch has been deployed on an actual device. Devices without the patch can be marked as out of compliance.

Port baselines are also setup with significant collaboration between the software vendor and the utility. Port baseline profiles are similar to Software baseline profiles except instead of software information, port entries can be specified. Each entry represents communication endpoint on a physical device. The utility collected information on all ports on the network approved to be opened for device communications. If any ports are open that are not specified in the baseline device, the device will go out of compliance and email notifications will be sent to appropriate personnel.

3. The utility also enhanced their non-SCADA data collection and data historization. Many cyber assets have valuable data on the BES asset health of the utility's infrastructure; they wanted to provide this data to their data historian for historical trending and analysis. The utility is able to use the additional information and predict when and where maintenance activities are needed before equipment failure occurs. Predictive preventive maintenance has proven its value to many power utilities and this utility was now reaping the same rewards. Gone are the costly scheduled maintenance activities, where maintenance occurs on many pieces of equipment that do not requiring any current servicing based on their performance wear characteristics.

Managing the compliance process is a large part of the effort by the utility. By enhancing the SESS system, the utility was able to maintain current NERC CIP compliance process efforts and integrate additional compliance and operational characteristics for the same OT devices to improve compliance and grid reliability.

The utility identified 13,000 more OT devices in their Low Impact substations that would benefit from device management. The utility's Low Impact sites did not require the same level of device management as the Medium Impact sites but the utility's proactive mind-set for cyber security and workforce efficiency had the Low Impact OT devices come into scope for device management. The utility felt that the evolving NERC CIP standards would eventually comprise the Low Impact substation assets so the best approach is to include those assets to for device management within the SESS system.

With the large growth in devices to manage, more and more the manual aspects of device management were consuming large amounts of engineering time. The utility was constrained with hiring more resources to handle the device management for thousands of more devices. Automation of the SESS device management functions was the answer for how to manage so many devices with the workforce already in place. The utility worked closely with the vendor for automation of existing tasks.

4. GRID MODERNIZATION

Modernization of the distribution grid provides customers with a more reliable electric supply and helps the utility deliver its product to the customer with a more efficient power delivery infrastructure. The Advanced Grid Intelligence and Security (AGIS) is the utility's grid modernization initiative. Providing cybersecurity for the explosive growth of new OT devices that the utility will be deploying as part of its AGIS program is a challenging task. The AGIS program is part of the utility's ambitious

Grid Modernization initiative, which aims to increase the efficiency and reliability of the electric grid. The AGIS program will expand the device count to be four times larger than the current transmission system installations, to about 70,000 devices for the SESS system to manage.

Distribution devices for Grid Modernization are typically not present in the medium or low impact substation environments and are largely concentrated on pole-mounted infrastructure. The pole-mounted distribution devices are valuable additions to the utility's OT device infrastructure and as such, the utility determined the same level of device management is preferred for the pole-mounted devices as the medium and low impact substation IEDs received.

5. SYSTEM AVAILABILITY

The utility assessed the SESS system and found it to be critical to supporting their assets. They required SESS to be available all the time and as a result, a high availability architecture was created as shown in Figure 1. Four physical servers are running six virtual machines. Physical servers are in different geographical locations. Users login into the system via a multifactor authenticated RDP session. Having two Client Access Servers (CAS) allows for control of user distribution between two CAS servers resulting in enhanced performance and reliability. In case of one CAS server goes down, all the users will log into the secondary CAS to continue their work. Similarly, there are two Device Communication Servers (DCS) responsible for collecting information from OT devices and performing device management tasks. Workload is evenly distributed between two DCS servers resulting in high performance and system robustness. In case of one DCS server failing, the second one will pick up any workload automatically with system operations not disrupted. By separating the client access and the device communication servers in this way, the SESS system fulfills the Intermediate System requirements of NERC CIP-005.

In order to manage access security for the ~400 users that the utility integrates in the SESS system, corporate Active Directory for users and groups is part of the SESS security. This allows for seamless user management leveraging existing corporate Active Directory.

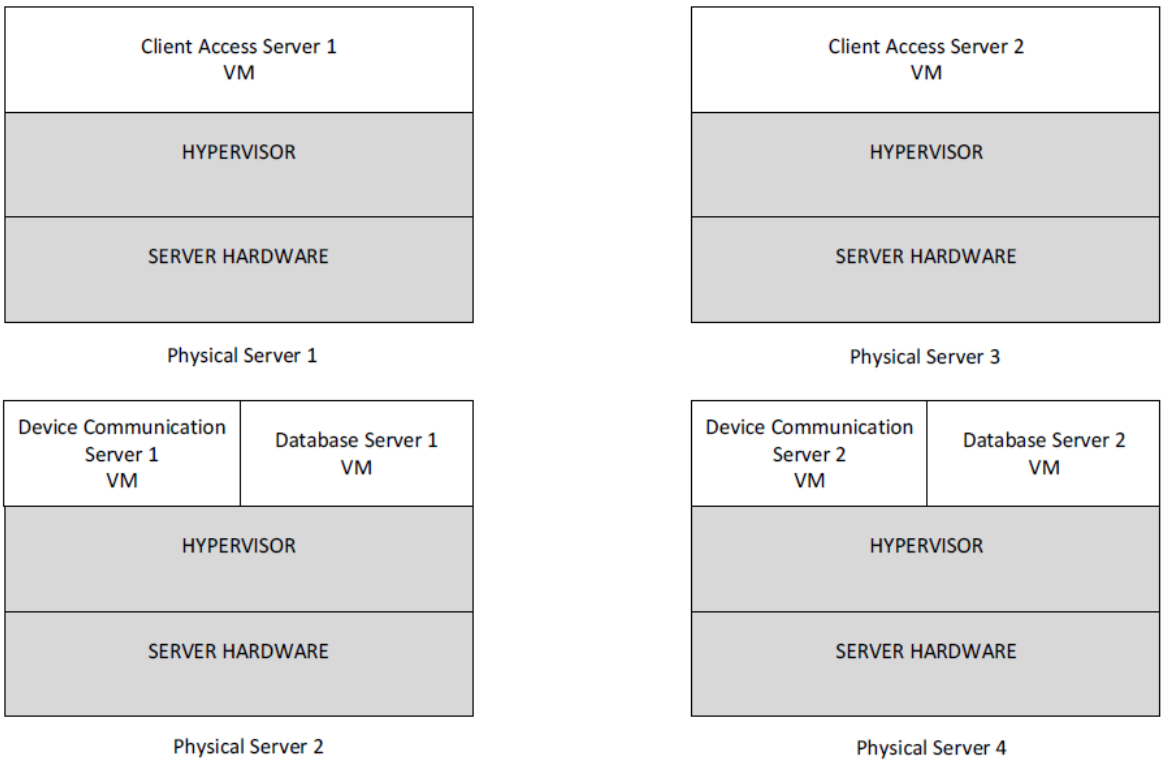

Figure 1 - High Availability Architecture

With a highly available architecture, the SESS system is available 99.9% of the time. By deploying SESS in a high availability scheme, the utility gained additional benefits.

1. System upgrades are not disrupting operations. SESS on DCS 1 can be disabled, then the server update can be carried out while the DCS 2 is running and serving users and performing system jobs. Once the upgrade is completed on DCS 1 the SESS will move to the secondary server and DCS 2 will be disabled to allow for DCS 2 update. This update process applies to all parts of the system DCS, CAS and Database servers.

2. Network maintenance/reconfiguration is another example when having redundant servers is invaluable. It allows for network maintenance/reconfiguration without any system downtime.

3. The utility has been upgrading SESS with latest vendor releases as many new features were developed to directly address the utility's needs. The upgrade process was streamlined and now takes only a few hours to execute. As the vendor's software has matured, the utility executes no regression tests after the upgrade. Only fixes and new features are tested by the utility.

6. VALUE TO THE UTILITY

NERC CIP value – By applying NERC CIP requirements to all devices configured within the SESS, regardless of CIP classification, the utility's grid infrastructure is future proof in case lower classification devices to be included under future NERC CIP evolving standards. Additionally, a standard approach across the grid infrastructure improves grid resilience

Baseline Value - Baseline functionality brings a lot of value to the utility:

1. Meeting CIP-010-4 R1, CIP-007-2 R2 and CIP-007-2 R3 requirements
2. System cybersecurity is strengthened. Unauthorized changes are detected immediately.
3. Email notifications about out of bounds deviations will alert users, even when they are not logged into the system. Previously an open port could go un-noticed but now that port would be quickly detected and a notification sent out to relevant parties to resolve the anomaly.
4. A well thought out system configuration is enforced. Consistent device and network configuration is encouraged.
5. Situational awareness of OT grid devices is highly improved. The utility has set up a landing page for SESS to show system compliance status on a graph, which list NERC CIP compliance status of all devices in the system.

Cost Savings Value – There are many areas of cost savings for the utility's SESS system:

1. Effective collection of CIP audit artifacts and consistent audit reports can avoid NERC CIP fines.
    a. Lowers staff anxiety levels
    b. Increases speed of obtaining CIP audit artifacts
    c. All the data in one place
    d. All the data in one consistent form
2. The utility's reputation is improved due to proficiency in producing CIP audit artifacts. As a result shareholder value is secured for the future.
3. SESS system's Remote Engineering Access (REA)
    a. Save engineer's time, users don't have to travel to site to perform their tasks
    b. Reduce vehicle maintenance with reduction or elimination of the need to drive to site
    c. Improve resource utilization, highly skilled personnel do not need to travel and can focus on task at hand
4. Reduce or eliminate overtime hours to manually acquire device information at all hours
    a. Improve workers work/life balance by reducing these OT hours

Additional value

1. SESS Password Management

    a. No need for personnel to perform CIP mandated periodic password changes, as these are now scheduled. Manual password changes required physical access a device hence driving out to site
2. SESS Microsoft Excel import/export configuration - The utility has been using native Microsoft Excel import/export functionality as main means to streamline the SESS configuration process. Time savings are substantial as most of the system configuration is done this way. The utility had significant input with the vendor on how the import/export process works as they heavily rely on it.
3. Work force efficiency/productivity
    a. Users can retrieve device/station information efficiently, no longer looking and searching for files. All documentation data can be stored in the SESS.
4. Elimination of human error. Reduce or eliminate rework.
5. Provide evidentiary support for forensic investigations

7. LESSONS LEARNED

There were many challenges and lessons learned during the project's execution. The following are a couple of those challenges and the solutions to overcome them:

1. Device Compatibility - Due to large numbers of device types within the SESS system, new automation device drivers had to be developed to interface with them. In order to implement missing drivers, the vendor worked closely with the utility to determine the driver's needs and identify the software development needed for each device driver. In a few instances, the utility sent the vendor sample devices for driver development, implementation and testing as the vendor did not have those devices in their lab.

2. IT infrastructure - IT infrastructure for the system is elaborate. Two sets of VMs hosted on multiple servers in different geographical locations requires careful setup in order for the system to have proper system security and performance. The vendor must work closely with the utility's IT department to ensure network security is set up correctly for the SESS. The SESS system has to be scalable as more assets are added daily. IT infrastructure has been proven robust and performant though a few changes had to be made collaboratively along the way to ensure the SESS is set up correctly. The vendor having a close relationship with the utility allows for quick and seamless communication between all involved.

8. SUMMARY and CONCLUSIONS

The journey of this mid-size US utility to secure their OT devices over the last two decades is a testament to the importance of cybersecurity in the energy sector. Having a program in place to support the initial compliance requirements started the process. Evolution of the program, as needed for compliance and efficiency, proved to be a successful combination of regulatory compliance along with workforce efficiency improvements. The utility's proactive approach to cybersecurity ensured they could comply with regulations, protect their infrastructure against new and emerging threats, and improve their operational efficiency. Close engagement and partnership with a competent vendor to supply technology and advance the capabilities of the SESS solution was key to project implementation and evolution over the years. The utility feels they are well positioned in the industry with a security platform able to handle increased monitoring, implementation of device management automation, and ability to apply future updates to accommodate constantly evolving regulatory compliance requirements. The utility has experienced far ranging cost savings from the elimination of manual tasks, reduction in travel to site for device management purposes, reduction in overtime costs and significant time saved that can be effectively utilized on other utility tasks.

9. RECOMMENDATIONS

The utility's other operations, such as gas distribution, can benefit from many of the same SESS program capabilities in device security and device management. Engaging the many other stakeholders in these other areas is needed to ensure understandings and clarity of the compliance requirements, the actual OT devices themselves that are being utilized and the data available from

those devices. Differences in industry can be overcome with enhancements in device driver technology. With a well engineered design, SESS project implementation in other areas of the utility is achievable.

BIBLIOGRAPHY

[1] US Reliability Standards - https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx
« United States Mandatory Standards Subject to Enforcement: (CIP standards)»

[2] CIP-010-4 - https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf
Pages 6 – 14

[3] PRC-005-5 - https://nerc.com/pa/stand/reliability%20standards/prc-005-5.pdf
(pages 1 – 7)