NERC CIP in the Real World on a Real Budget

(Strategies for NERC CIP compliance with Ethernet Technology)

Authors:

Chan Wong PhD., PMP, Engineer – 639 Loyola Ave, New Orleans, LA, (504)-495-3765, CWong@entergy.com

Eric Stranz, Business Development Manager – 7000 Siemens Road, Wendell, NC, (919)-279-5080, Eric.Stranz@Siemens.com

Stefan Nohe, Business Development Manager – 7000 Siemens Road, Wendell, NC, (919)-365-2006, Stefan.Nohe@Siemens.com

Abstract— Very real concerns of unauthorized use, cyber attacks, phishing etc have prompted the creation of NERC CIP rules for protection of facilities designated as critical assets. If hacked, these critical assets can have a significant effect on the bulk electric system (BES). With the use of merging units at the CT and VT connection we now have a digital system from the primary device to the control center. As Ethernet technology and implementation within the protection and control system is gaining more acceptance, security concerns are also increasing. In order to realize the cost savings of sampled values at the CT and VT cyber security must also be incorporated at that level. A cost effective system incorporates a comprehensive design strategy for network isolation, firewalls and device security. All these are needed for a complete interconnected system (from process to SCADA interface), that meets the guidelines of NERC CIP V5. The paper discusses implementation of these concepts using open architecture systems. Simple procedures are presented, allowing users to be confident that regulatory requirements are met without adding unnecessary complexity. Trends in security threats and requirements are summarized to give an idea of what we can expect in the future and how an appropriate design today will meet those future requirements without excessive hardware or setup.

Index Terms

IEC-61850, Process Bus, Cyber security, Substation, Protection, Control System, NERC CIP

I. Introduction

Increasing concerns of system wide outages due to unauthorized use, cyber attacks, phishing etc have prompted the creation of NERC CIP rules for protection of facilities designated as critical assets. It has been seen in the industry that very conservative use of technology has been implemented ignoring the improvements and operational advantages that new technology brings out of fear of non-compliance.

This Paper is intended to show that even the latest technology offers a high security against cyber attacks, utilizing Ethernet as communication media between circuit breaker and protection devices as well as on station level. The paper is mainly focused on the substation equipment and touches enterprise solutions or Electronic Access Control or Monitoring Systems (EAMCS) only.

II. About IEC 61850

Ethernet, a wide spread and field proven technology, has been used in a huge variety of applications. When Ethernet is used in conjunction with the IEC-61850 protocol suite it has become a solution that reduces engineering, reduces copper cabling and saves installation cost. The IEC-61850 standard opened the field of Ethernet applications and defined requirements and services for communication in Intelligent Electronic Devices (IED's). Three communications protocols are based on the IEC-61850 standard. One service for communications to supervisory or monitoring system is called Manufacturer Message Specification (MMS). The other two highly critical protocols are the Generic Object Oriented Substation Event (GOOSE), IED to IED communications defined in IEC 61850-8-1, and Sampled Values, process bus to IED communications defined in IEC 61850-9-2. MMS is an IP based protocol that uses ISO-OSI layer 3 communications where GOOSE and Sampled Values both use ISO-OSI Layer 2 communications. The communications standard defines all of the components within an electrical system including protection elements and monitoring points which are assigned to logical nodes and logical devices within the Substation Configuration Language (SCL) structure. These components have many pieces of information defined within them such as: Quality, Time stamp, value etc. IEC61850 does not use data point mapping as with other communications protocols and communicates the structure as is defined across the communications channel.

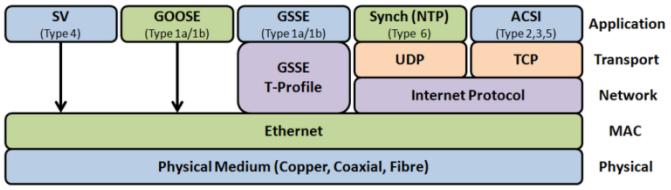
- **IEC-61850 MMS** –MMS was designed for reporting information and value changes to monitoring systems. Traditional communications protocols relied on periodic polling of the IED's to retrieve current values of data where as MMS will report data changes to the monitoring system without solicitation. These data points can all come with the time stamp from the IED it was collected from enabling the user of the data to build sequence of events alarm lists for quicker

diagnosis and troubleshooting. In addition, built into MMS is the ability to transfer Comtrade fault records stored within the IED's. A Simple IEC-61850 (SCD) file export minimizes configuration buildup effort of the monitoring system by containing the entire definition of all of the IED's defined within the substation.

- **IEC-61850 GOOSE** – GOOSE is designed to replace inter-connected copper cabling between IED's by implementing a high speed communications scheme for multicast events that occur within the IED. These event multicasts are subscribed to by client IED's on the same network. The multicast/subscription is mac-address based layer 2 communications. Prior to an event occurrence the server IED will periodically retransmit the status of the monitoring point with an increasing sequence number. When an event occurs, a multicast message is generated within milliseconds and repeated several times over the ensuing milliseconds before returning to its periodic transmission. Using sequence monitoring the client IED can report communications issues between devices which can help to solve problems well before any event required action.
- **IEC-61850 Sampled Values** – Sampled Values is the communications protocol used to transmit the CT and PT readings from a collection device (so called merging unit) to a protection IED. Many utilities are now installing the protection IED's inside the control house of the switchyard and installing long copper cable runs from the CT, PT and I/O connections in the breaker. A Sampled Values design would place a Merging Unit inside the breaker that connects PT's and CT's and I/O. This device would be connected over Ethernet Fiber underground to the control house and would multicast high speed measurement samples of the CT and PT measurements simultaneously with GOOSE multicast for I/O. IED's within the control house would subscribe to these messages and would take decisions on these readings as they relate to protection thresholds or logic. As with GOOSE, SV is also a layer 2 non-routable protocol based on the mac-address that is a multicast/subscriber design

The IEC 61850 protocol is a complete protocol suite, within the different layers of the Ethernet protocol communication. A simplified approach is to look at the OSI 7- layer and where the different IEC 61850 protocols are operating.

FIGURE 1 TYPICAL IEC 61850 PROTOCOL STACK



The MMS protocol suite is operating with TCP/IP and therefore falling within NERC CIP under routable protocols. The GOOSE and SMV protocol are classified as connectionless protocols and are operating below the IP level. The GOOSE and SMV protocol cannot be routed to different networks and therefore they are treated as non-routable protocols.

The difficulty for the utilities and the auditors is to document and ensure if an access point is utilizing routable capabilities and non routable capabilities.

III. NERC CIP

The North America Electric Reliability Corporation is leading the effort of specifying in the Critical Infrastructure Protection (CIP) series measures to protect critical assets within a substation. This paper will discuss certain requirements and how Ethernet technologies utilizing IEC 61850 can fulfill the requirement today.

The NERC CIP approach to cyber security is a layered approach, where an attack needs to overcome several layers of protection and security within the system. Going further a couple of abbreviations and nomenclature need to be clarified, in short and simplified language below.

- Electronic security perimeter (ESP) - All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet**.**
- Electronic access control or monitoring system (EAMCS) – System to authenticate and log access to cyber assets
- Electronic Access Point (EAP)– Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System
- Protected Cyber Assets (PCA) – One or more Cyber Assets connected using routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same electronic security perimeter. The impact rating of protected cyber assets is equal to the highest rated BES Cyber System in the same ESP.
  E.g. A stand alone substation HMI, if not needed for

control processing would be a PCA; however, if it was needed for control processing, it would be a BES Cyber Asset

- Cyber Asset:
  - Protection System
  - Substation automation
  - RTUs (SCADA Alarms)

A. Applicability

According to CIP -014-1 section 4.1 "Functional Entities" Stations or Sub's connected at less than 200kv do not fall under requirements for compliance by NERC CIP.

Stations between 200kv and 499kv fall under a voltage weighted calculation to determine their applicability. The number and weight of the incoming and outgoing transmission lines to the station are calculated in table CIP-014-1 - 4.1.1.2. Each 200kv to 299kv line is weighted at 700 and each 300kv to 499kv line is weighted at 1300. A combination of these connections to the station exceeding a weight value of 3000 causes the station to fall under the requirements of NERC CIP.

If the Transmission Facilities are operating at 500kv or higher or the interconnect is defined to be critical by the Reliability Coordinator, Planning Coordinator, or Transmission Planner the station, facility or interconnect must comply with the security requirements of NERC CIP regardless of line weight.

IV. Physical Security

Considerations for Medium Impact BES Cyber Systems with External Routable Connectivity are the main focus of this paper. Low Impact stations are not required by CIP standards to contain the same physical security requirements per CIP006-5 exemption 4.2.3.5. High Impact stations are not common as they usually would contain a Control Center within the station and have wide spread impact on other stations

A. Risk Assessment

An Initial Risk assessment must be completed to "identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection". After original assessment, if stations are found applicable, subsequent assessments must be performed every 30 months for stations existing and planned to be in service for the next 24 months. If not found applicable then every 60 months a new assessment is required.

B. Physical Security Plan (CIP-006 -5- Table R1)

In CIP-006-5 -Table R1 focuses on a documented plan that identifies, assesses and corrects deficiencies. This is called a Physical Security Plan. Each of the points in the table should be addressed as they apply to the Medium Impact BES Cyber Systems with External Routable Connectivity. The documented plan or plans must contain:.

a. Documentation of Operational and Procedural controls to restrict physical access

b. Physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access. A list of authorized individuals is required and accompanied by access logs. Physical access controls must use a two factor authentication for a defense in depth design. Examples include: Card Reader and keypad (something you have and something you know) or Card Reader and a guard monitored remote camera (something you have and something you are).

c. Monitor for unauthorized access through a physical access point into a PSP

d. Issue an alarm or alert within 15 minutes of PSP unauthorized access detection to identified BES Cyber Security defined personnel.

e. Monitor PACS for unauthorized physical access to a PACS.

f. Issue an alarm or alert within 15 minutes of PACS unauthorized access detection to identified BES Cyber Security defined personnel.

C. Visitor Control Program (CIP-006-5 - Table R2)

Table two requires that visitors or individuals not authorized for unescorted access be escorted by an authorized individual in a documented process that requires logging of entry, exit, contact responsible etc. In addition it requires these logs be retained for at least ninety days. These logs can be accomplished through a manual or automated system.

D. Physical Access Control System Maintenance and Testing Program (CIP-006-5 - Table R3)

This requirement mandates that all PSP access controls, systems and related devices be tested at least once every 24 months to ensure proper operation. This addresses FERC Order No. 706 Paragraph 581 directives to test more frequently than three years.

V. Different Applications

Modern protection system and use of distributed I/Os, e.g. process bus, promises capital and operational cost reduction. Ease of maintenance and restoration after catastrophic events are further arguments for distributed protection and control systems with Ethernet protocols.

The challenge is to define the electronic security perimeter (ESP) for the respective asset, in case the ESP is extended to the substation fence – the use of Ethernet within the substation is not restricted. NERC CIP V5 is allowing for the extension of the electronic security perimeter to the substation fence, the earlier known six wall principal from Version 3 has been changed to ease restriction.

The other case which will be discussed in this paper is a more common case; the physical security perimeter and electronic

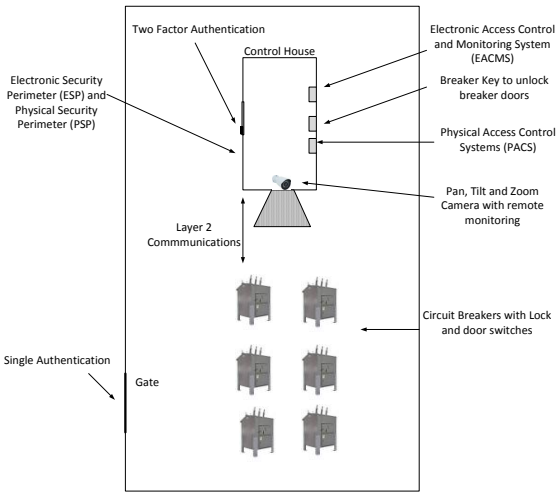
security perimeter are around the control house, e.g. normal key lock at the gate and additional access controls at the control house. In this case the distributed protection systems communications would breach the ESP and the remote I/O devices would need to be protected by another ESP including physical and network access control.
Several strategies to comply with these requirements are discussed in this paper. This more commonly used case in the industry needed more clarification, especially since the industry had no common opinion about it.
NERC provided an answer to this problem in the different FAQ documents, e.g. CIP-002-5.1: Communication and Networking Cyber Assets dated Oct. 2015 and CIP V5 FAQs_Consolidated_Oct_2015. Considering these responses by NERC the design considerations are dependent on the IP services, if any, that are enabled and running on the distributed I/Os.
Taking a deeper look into the use of process bus and Ethernet technology for remote I/Os within the second scenario is leading to a case by case decision and strongly depending on the applied best practice solutions on the remote I/O device.

A. ESP at the Control House, PSP at Fence

1) Physical Security requirements

In this scenario (See Figure 2) a single security control will be placed at the gated entry. This provides a locked access limiting the individuals allowed within the substation gate. Once inside the perimeter the individual will not be allowed to physically access any of the protective relaying, local HMI, substation automation or networking in the control house without additional two factor authentication per NERC guidelines (FERC Order No. 706, Paragraph 572)(See Figure 7). Once it is determined the personnel is permissible at the control house the individual will have access to devices and cabinets that reside within it. A card-locked cabinet within the control house should contain a key that unlocks all of the breaker doors in the yard. Each of the breakers is wired with a door switch that connects to a binary input of the merging unit or IED within the breaker. Upon opening any breaker door a signal is sent to the control center where visual confirmation is witnessed via the pan/tilt/zoom camera on the control house for access logging purposes. With this type of layering only selective personnel can access certain areas. Access logging and history is stored in the PACS System in the control house and indications and alerts are sent to the control center for access logging. Further access controls can be added to the PACS system box and Networking box to extend physical restrictions.

FIGURE 2: PHYSICAL DESIGN- ESP AT CONTROL HOUSE PSP AT FENCE



2) Electronic Security Perimeter

The electronic security perimeter would be the walls of the control house. For communication to devices/system outside the control house each interface is per default an Electronic Access Point. The requirement on the security is strongly depending on the utilized communication (routable / non-routable).

a) Communication between Control House and remote I/O non-routable

In this case, the communication from the remote I/O to the equipment residing in the ESP is limited to non routable protocols therefore another ESP definition around the breaker is not required. This also removes the requirement for additional network protection components for each breaker. []
Non-routable protocols are running usually on a layer 2 network, e.g. point to point communication or publisher/subscriber protocols which are real time. (e.g. GOOSE, SMV). (See Figure 3)
This understanding is also expressed in NERC "Communications Networking Lessons Learned" dated October 6, 2015.

b) Communication between Control House and remote I/O routable.

If routable services or communications are turned on for the remote I/O, e.g. configuration or diagnostic home page of the device, this would allow access to the station network from the breaker location. According to the NERC requirements, the device is a PCA and an ESP would need to be defined around the breaker component. As part of the ESP an EAP needs defined for the network connectivity to the remote I/O's within. To protect this connection firewalls, encryption etc. must be considered, increasing the cost to implement a networked solution. (See Figure 4)

FIGURE 3: NERC COMMUNICATIONS NETWORKING LESSONS LEARNED

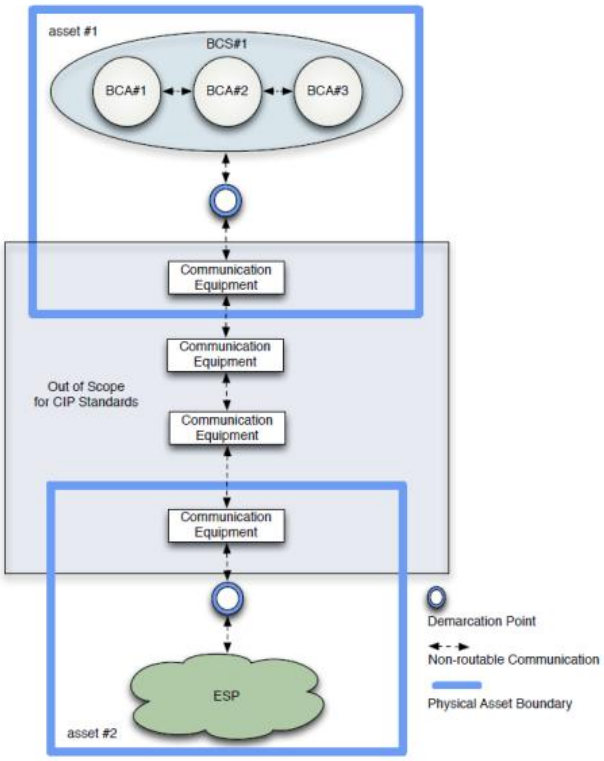
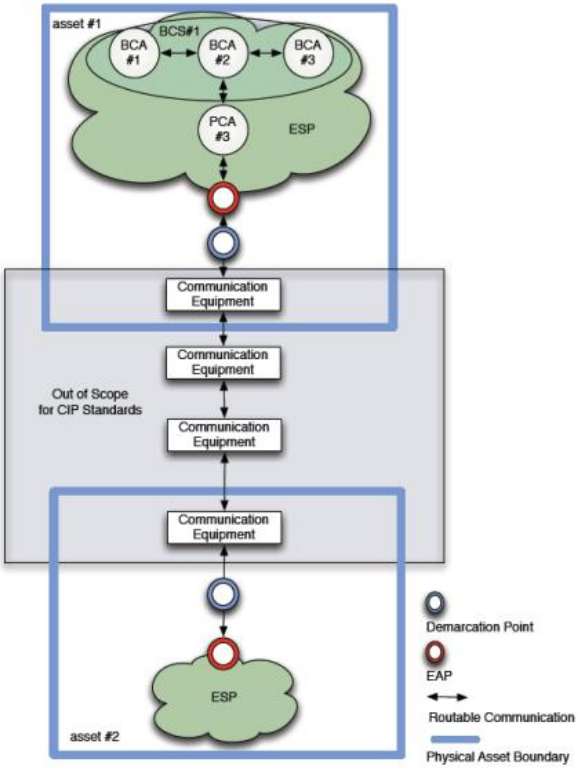


FIGURE 4: ROUTABLE COMMUNICATION



B. ESP and PSP at the Fence Perimeter

1) Physical Security requirements

In this scenario (See Figure 5) a two factor authentication must take place at the gated entry per NERC guidelines (FERC Order No. 706, Paragraph 572)(See Figure 6). This authenticates that the person entering the substation is permissible. Once inside the perimeter the individual will not be allowed to physically access any of the protective relaying, local HMI, substation automation, networking in the control house without additional authentication at the control house. Once it is determined the personnel is permissible at the control house the individual will have access to devices and cabinets that reside within it. A locked cabinet within the control house contains a key that unlocks all of the breakers in the yard. Each of the breakers is wired with a door switch that connects to a binary input of the protection relay or merging unit within the breaker. Upon opening the door a signal is sent to the control center where visual confirmation is witnessed via the pan/tilt/zoom camera on the control house for access logging purposes. With this type of layering only selective personnel can access certain areas. Access logging and history is stored in the PACS System in the control house and indications and alerts are sent to the control center for access logging. Further access controls can be added to the PACS system box and Networking box to extend physical restrictions.

2) Electronic Security Perimeter

The electronic security perimeter would be the Substation Fence. For communication to devices/system outside the control house but within the switchyard each interface is permissible to use routable communications as the entire station is within the Electronic Security Perimeter.

FIGURE 5: SECURITY PERIMETER IS SUBSTATION FENCE

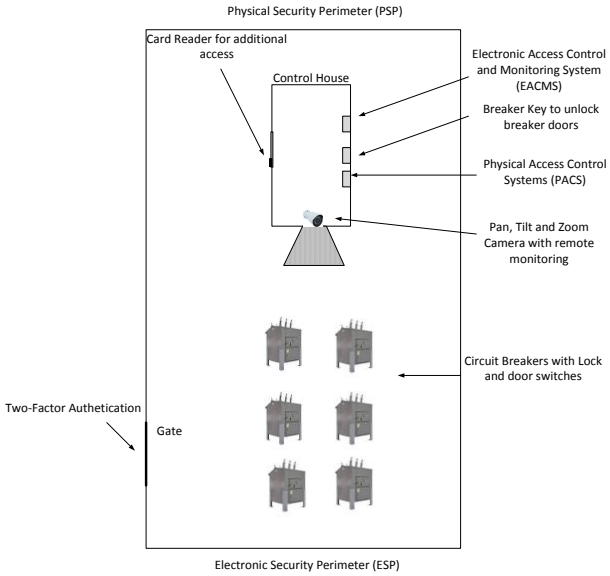
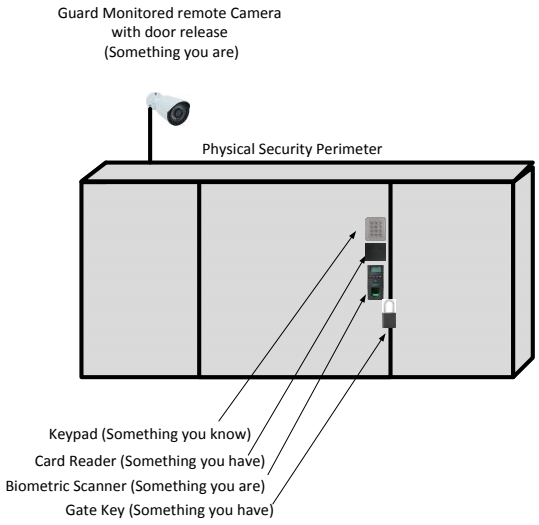


FIGURE 6: TWO FACTOR AUTHENTICATION



VI. ROUTABLE REMOTE CONNECTION – STATION BUS LEVEL

The access point for routable communication from outside the ESP into the ESP needs to fulfill the requirements of an EAP, independent if the communication source or device resides in the switchyard or outside the switchyard.

To achieve compliance the following requirements are needed:

- Communications needs to be encrypted. This can easily achieved by the use of network switches capable to encrypt the communication or the use of services like IPsec.
- The second requirement is limiting the traffic and applications while only allowing necessary traffic into the ESP. This can be achieved by commercially available firewalls and doesn't require the use of Data Diodes.
- The third requirement is to authenticate the person or device accessing the network. In the case of the remote devices and communication to remote devices, this seems to be an issue since even the latest generation of protection relays and merging units are not supporting any authentication mechanism to identify the device 100% secure. The authors want to point out that authentication can be achieved by supervision of the communication, which is layer 2 and layer 3 communication at the same time. An attacker would not only need to simulate the IP and MAC address of the device – he would also need to simulate GOOSE and SMV data, with the correct sequence number. Using sequence number tracking the subscribing device is continuously monitoring the communications. If a single packet is lost an alarm will be initiated. This alarm together with an Alarm that the communication was interrupted – can be used as an indication that an attacker wants to gain access to the station level. To limit the exposure a segregate network design is preferable.

VII. FIRMWARE, SOFTWARE UPDATES, PATCHING

Inside a typical substation design protective relays, HMI's and computers exist that may contain firmware, malware protection, antivirus protection etc. NERC requires that a process be in place that reviews system, firmware and software updates to the existing system install base. If it is determined there is a security vulnerability addressed in these updates it is required that the cyber asset be updated manually or through automated methods within 35 days from the announcement and detection of the vulnerability. It is not the authors intention to focus primarily on the kinds of systems offering these services for this paper as these systems would have been required regardless of technology used.

VIII. NETWORK DESIGN

Implementing IEC 61850 GOOSE and SV create very challenging requirements to Ethernet communication systems since failure in the communication system could result in damage to high-voltage switchgears and even cause power outages.

To enhance reliability of the communication, redundancy protocols are inevitable in power utility applications and should be a design consideration. Redundancy protocols such as RSTP, HSR and PRP provide system security even when a single failure occurs in the network. Each solution has benefits and drawbacks and should be studied to ensure the right fit for the application.

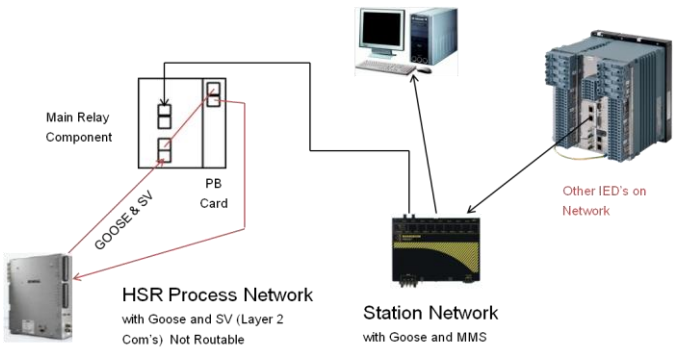
Additional consideration must be had with the IEC-61850 SV information that is multicast by the merging units as it transmits everywhere the network is connected to. This can be problematic as many computers and some IED vendors are not designed to filter this kind of data or if it is unwanted at such a high speed (417us). The result could be device Ethernet card lockup.

A. Network Architecture

Tying in with NERC CIP V5 it is important to isolate and prevent network intrusion. Since the merging unit is located outside of the control house and it is connected with an Ethernet cable this connection must be considered when designing the network for NERC CIP compliance.

Figure 7 is an example of a network isolated between Station and Process Bus, leaving only layer 2 communications on the Process Bus.

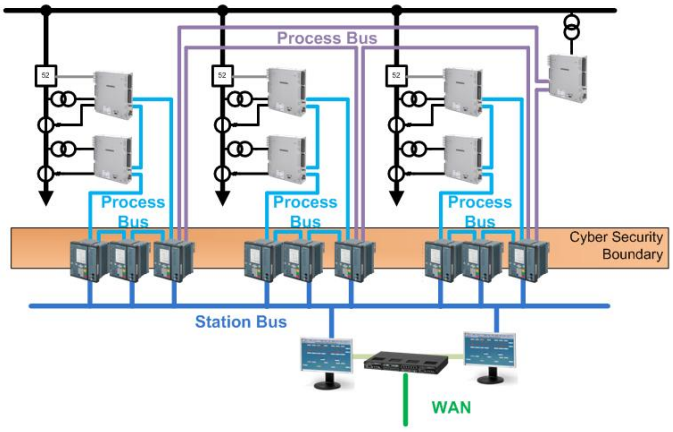
FIGURE 7: PROCESS BUS ARCHITECTURE



The network architecture has a significant impact on the NERC CIP requirements. Modern networks supporting different possibilities of redundancy and even the new released standard of Software defined networks are allowing for virtual and logical network separation.

The author wants to point out that a physical separation of process communication GOOSE/SMV on one network and GOOSE/MMS on another network such as depicted in Figure 7, is the simplest and most budget conscious architecture to achieve a NERC CIP compliant design.

FIGURE 8: NERC CIP COMPLIANT DESIGN



Such a design allows separating NERC CIP data from non-CIP data. In Version 5 of NERC CIP, data even not related to NERC CIP (e.g. PMU) would become NERC CIP data and the security guidelines needs to be followed – if this data is sharing a common network with CIP data, even if separated in virtual LANs

IX. BUDGET

The proposed security measures, network segregation and designs limiting the network to a non routable communication does not require any additional budget compared to a classic installation.

The slight increase in operational procedure, locks, key cards and camera are more than compensated by the promising savings of the process bus solution.

The proposed merging unit design with non routable communication between the breaker and the protection devices is offering an estimated installation cost savings of 30-40% for a twelve breaker installation compared to a conventional installation where the IED's are placed within the control house. In addition, further engineering cost savings are seen using IEC-61850 on a repetitive template design basis.

X. SUMMARY

In CIP V3 the ESP was defined as a 6 wall approach whereas V5 allows for much more flexibility to separate the PSP and ESP.

The intent of the paper was to show that even new technology can be utilized in compliance with NERC. This new technology promises operational and cost benefits that can be used without compromising security. Misinterpretation of the NERC CIP standards often lead to thinking that the older technologies are more secure even though NERC's primary goal is to improve operational reliability of the BES. Situational Awareness and Reliability are key benefits of utilizing the Ethernet technologies discussed in this paper.

It is an educational process within the industry to adapt and accept newer technology. The authors want to highlight the fact that the descriptions and diagrams used in this paper are partially taking out from the NERC standards. The paper serves as a guideline only, for approval and acceptance of a design consideration it is encouraged to discuss with your local NERC CIP compliance officer.

REFERENCES

[1] CIP006-5 Physical Security of BES Cyber Systems
[2] Lesson Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets
[3] CIP005-5 Electronic security perimeter
[4] NERC-CIP-002-5_1
[5] NERC-CIP-005-5
[6] NERC-CIP-007-5
[7] NERC-CIP-009-5
[8] NERC-CIP-010-5
[9] NERC-CIP-014-01
[10] FERC Order No. 706
[11] IEC-61850 8-1
[12] IEC-61850 9-2
[13] IEC-61850