Securing IEDs against Cyber Threats in Critical Substation Automation and Industrial Control Systems

Pubudu Eroshan Weerathunga, Anca Cioraca

1. Introduction

The operational technologies that support critical infrastructure industries, such as manufacturing, transportation, and energy, depend heavily on information systems for their monitoring and control. Industrial control system (ICS) is a general term that is used to represent systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations, such as programmable logic controllers (PLC). Substation Automation System (SAS) controls the power system via instrumentation and control devices.

In a cyber war scenario, energy and financial sectors are considered most critical to the National security. According to Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), attacks on energy sector have increased over the years [1]. Since Power grid and industrial systems are facing growing number of cyber threats, cyber security attacks on the critical infrastructure can't be considered theoretical anymore. We need to consolidate cyber security counter measures and policies in the power grid, and comply with requirements of cybersecurity standards.

Since NERC CIP v6 is enforceable, utilities are required to meet security regulatory compliance requirements. IEEE 1686 defines features and functions to be provided in IEDs by vendors to accommodate NERC CIP programs. And ISA-99/IEC-62443 standard series defines procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). Vendors have implemented a broad range of cyber security features in their IEDs to facilitate these requirements. It is important to understand these cyber security features and implement them correctly to comply with utility security policy. Successful cyber security of IEDs is a combined effect of technology, procedures, policies, training, monitoring and diligent enforcement.

This paper first investigates cyber threats against IEDs and cyber attacks such as the one on Ukraine power grid. It then discusses cyber security industry initiatives and standards related to IACS and SAS security. This paper discusses SCADA network architecture and the importance of zone architecture with conduits in IACS. Lastly, this paper presents examples of IED integration with third party security systems; such as Remote Authentication Dial-In User Service (RADIUS) server, Security Information and Event Management (SIEM) server, Key Distribution Center (KDC), password management system, firewalls, Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).

2. Threats

The electric power grid enables and supports other critical infrastructure sectors, including the oil and natural gas, water, transportation, telecommunications, and financial sectors. With the development of smart cities, smart cars and smart home, our dependence on electricity continues to grow exponentially. Considering the geographical area that the electric grid covers, the grid has a large attack surface that is vulnerable to many threats at different points. The US grid consists of 55,000+ Transmission substations and 450,000 miles of high Voltage transmission lines. Because of this large distance between substations, scaling and separation in control has become the biggest security concern for utilities. Some facilities are in rural areas, in open fields, without any security. Threats to critical infrastructure range from natural disasters, extreme weather conditions, physical attacks and cyber security attacks. Considering all threats and where these attacks might occur, consequences can vary drastically. Not all components of the grid are considered equally critical. NERC CIP V6 "BES categorization" specifies impact ratings and selection criteria of Bulk Energy Systems (BES) depends on their criticality and geographical location in the substation [2]. Transmission and Generation infrastructure are considered higher critical than local distribution infrastructure. In transmission and generation substations, control centers that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP) hold a high impact rating.

Utilities are faced against both physical attacks and cyber attacks. Most common physical attack in rural substations is copper theft. Stuxnet was the first sophisticated cyber attack reported on critical infrastructure. Stuxnet is a malicious computer worm, first identified in 2010, that targets the Iran's nuclear program. In April 16, 2013, a physical attack occurred at Pacific Gas and Electric's (PG&E's) Metcalf transmission substation. Two fiber-optic lines running underground near the substation were cut, and more than 100 rifle shots were fired at the substation's transformers. Then in both 2015 and 2016 December, Ukraine electric grid experienced power outages caused by remote cyber intrusions.

3. Lesson Learned from the Ukraine Attack

On December 23, 2015, Ukraine electric experienced power outages caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers and lasted for several hours [3]. Within the Ukrainian electrical system, these cyber attacks were directed at the regional distribution level. Also attackers generated thousands of calls to the energy company's call center to overload the system and hence to deny access to customers reporting outages.

The Attackers might have started this attack first with spear phishing and then gained access to the business networks of the Ukraine oblenergos. Also, investigators have found BlackEnergy 3 at each of the impacted oblenergos. BlackEnergy 3 is a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks and download custom spams/plugins. BlackEnergy 3 malware was known to have been used to deliver KillDisk. Through spear phishing, attackers got the credentials of the business network. They used virtual private networks (VPNs) to enter the ICS network. And they used existing remote access tools within the environment to issue commands directly from a remote SACDA HMI. Also, they

have changed the firmware in the Serial-to-Ethernet converter devices, that converts IEC-60870-5 101 to 104 communication protocol. And attackers used a modified version of KillDisk to erase the master boot record of impacted organization systems as well as the targeted logs. Outage were directly caused by SCADA hijacking. Technologies such as BlackEnergy 3 and KillDisk, were used only to enable the attack. Firmware change on Serial-to-Ethernet converter, schedule disconnects for UPS systems and deny service on Call center were used to delay the restoration efforts.

The important question is "Can this kind of attack happen in North America?". After the Ukraine attack, NERC issued level 2 NERC alert and request NERC entities to provide details of defense against such attack. NERC utilities had to provide details of their incident response plan, secure remote access, Malware detection, Two-factor authentication, VPN accessibility, network segregation and backup voice communications methods.

Tactics used in the attack on the Ukraine grid include spear phishing, malware, credential harvesting, lateral movement and remote control. Utilities can fight against spear phishing by growing user awareness through training, spam filtering and blocking access to uncategorized internet sites. IT department can evaluate user awareness by sending monthly test phishing emails. To fight against malware, utilities must assign least privileges to accounts and services by default, use host based Virus scanner, use sandboxes and IDS/IPS systems. Credential Harvesting can be eliminated by strong password policies, using password managers, limiting administrator rights and using Privileged Identity Management (PIM) system. Lateral movement of the attack can be prevented by network segmentation with firewalls and enforcing two-factor authentication between trust zones. Unauthorized remote controlling can be prevented using two-factor authentication, jump hosts and device certificates. By applying patches and keeping systems up to date, administrators could limit the amounts of vulnerabilities attackers can exploit.

With the development of new device searching tools such as SHODAN, anybody can search the open vulnerabilities in any system or device that is connected to the internet. Therefor, we should investigate our own utility presence in SHODAN using search queries, and reduce our presence in such queries. It is important to reduce the attack surface, so we should keep only minimum number of access points and implement necessary monitoring on them. But this could be challenging in interconnected systems, therefor we can leverage techniques such as application whitelisting, firewalls and compartmentalization. And with proper personal cyber security training, we could reduce sphere phishing attacks.

4. Industry Initiatives

Industries and government are working more closely together to strengthen planning procedures and response protocols in an event of real cyber security attack on critical infrastructure. NERC conducts industry wide GridSecCon conference and GridEx grid security exercise to bring together cybersecurity and physical security experts to share emerging security trends, policy advancements, and lessons learned related to the electricity sub-sector.

Cybersecurity Capability Maturity Model (C2M2) focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology(IT) and operational technology(OT) assets. Electricity Subsector C2M2 (ES-C2M2) is the energy sector-specific versions that comprises a maturity model, an evaluation tool, and DOE facilitated self-evaluations. ES-C2M2 is developed to help measure and improve the industry's cyber readiness. This model helps utilities to evaluate, prioritize, and improve cybersecurity capabilities and prioritize their investments to enhance cybersecurity. Oil and Natural Gas Subsector C2M2 (ONG-C2M2) specifically tailored for the oil and natural gas segments of the energy sector.

The Cyber Risk Information Sharing Program (CRISP) facilitates the timely sharing of cyber threat information and situational awareness tools among participating utilities. The Electricity Information Sharing and Analysis Center (E-ISAC) serves as the primary security communications channel for the electricity sector and enhances the industry's situational awareness to cyber and physical threats. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by sharing control systems-related security incidents and mitigation measures. ICS-CERT offers the Cyber Security Evaluation Tool (CSET), a self-assessment software tool for asset owners to conduct their cybersecurity assessments.

5. Cyber security standards

There are numerous cyber security standards that act as Guidelines and frameworks standards, regulatory standards and normative standards, each category having a scope and purpose. NIST "Framework for Improving Critical Infrastructure Cybersecurity" consists of standards, guidelines, and practices to promote the protection of critical infrastructure [4]. The NIST ICS framework provides a comprehensive set of recommendations for securing ICS. NISTIR 7628, Guidelines to Smart Grid Cyber Security explains Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements [5]. NIST SP 800-57 gives recommendation for Key Management [6]. NIST SP 800-82 provides a guide to Industrial Control Systems (ICS) Security [7]. NIST SP 800-53 provides security and privacy controls for Federal Information Systems and Organizations [8].

Regulatory standards are imposing compliance to the rules and requirements they set. One of the most renowned regulatory standards in North America is NERC CIP v6 [2]. NERC v6 covers BES cyber system categorization (002), security management controls (003), personnel and training (004), Electronic Security Perimeter (005), physical security of BES Cyber systems (006), Systems Security Management (007), incident reporting and response planning (008), recovery plans (009), configuration change management and vulnerability assessments (010), information protection (011) and physical security (014). IEEE 1686-2013 standard defines functions and features to be provided in IEDs to accommodate critical infrastructure protection (CIP) programs [9]. The standard addresses security regarding the electronic access control, audit trail, supervisory monitoring and control, configuration software, firmware quality assurance, port access and data retrieval from an IED. This document provides a baseline of security requirements and features to be provided in electric utility IEDs. IEEE 1686

has a broader area of influence than NERC CIP, as it is an international standard with strong influence everywhere outside North America.

Normative standards are those concerned with finding technical solutions to the requirements specified in the foundational regulatory standards. A very important set of standards for the P&C field is the IEC 62351 series, "Power Systems Management and Associated Information Exchange - Data and Communications Security". The scope of the work of WG15 is to develop a standard that assures security of protocols specified within TC57 and their derivatives. IEC 62351 standard series covers Data and Communication Security - Security for profiles including TCP/IP (part 3), Security for profiles including MMS (part 4), Security for IEC 60870-5 and derivatives (part 5), Security for IEC 61850 profiles (part 6), Security through Network and System Management (part 7), Role-Based Access Control (RBAC) for Power System Management (part 8), Key Management (part 9), Security Architecture (part 10) and Security for XML Files (part 11).

ISA/IEC 62443 (originally referred to as ISA99 standards) is a series of standards that define procedures for implementing a comprehensive set of cybersecurity measures for industrial automation and control systems (IACS). These documents were originally referred to as ISA99 standards, as they were created by the International Society for Automation (ISA). Later, they were renumbered to be the 62443 series. It describes several categories of security technologies and provides preliminary recommendations and guidance for using those security technologies. As shown in Figure 1, the elements of IEC 62443 are arranged into four groups based on their primary focus and intended audience [10]. The general group includes elements that introduce concepts and models, and glossary of terms used through out the series. Policies and procedures group focusses on policies and procedures associated with cyber security management system and patch management. 62443-2-4 standard specifies requirement for suppliers of IACS. System group addresses requirements at the system level including various security technologies, security risk assessment and security system design. 62443-3-1 provides an evaluation and assessment of many current types of cyber security technologies, mitigation methods and tools. The standard describes Role based authorization, password/token authentication, firewalls and Intrusion Detection Systems (IDS) security technologies. Component group includes elements that provide information about detail requirements associated with the development of IACS products.

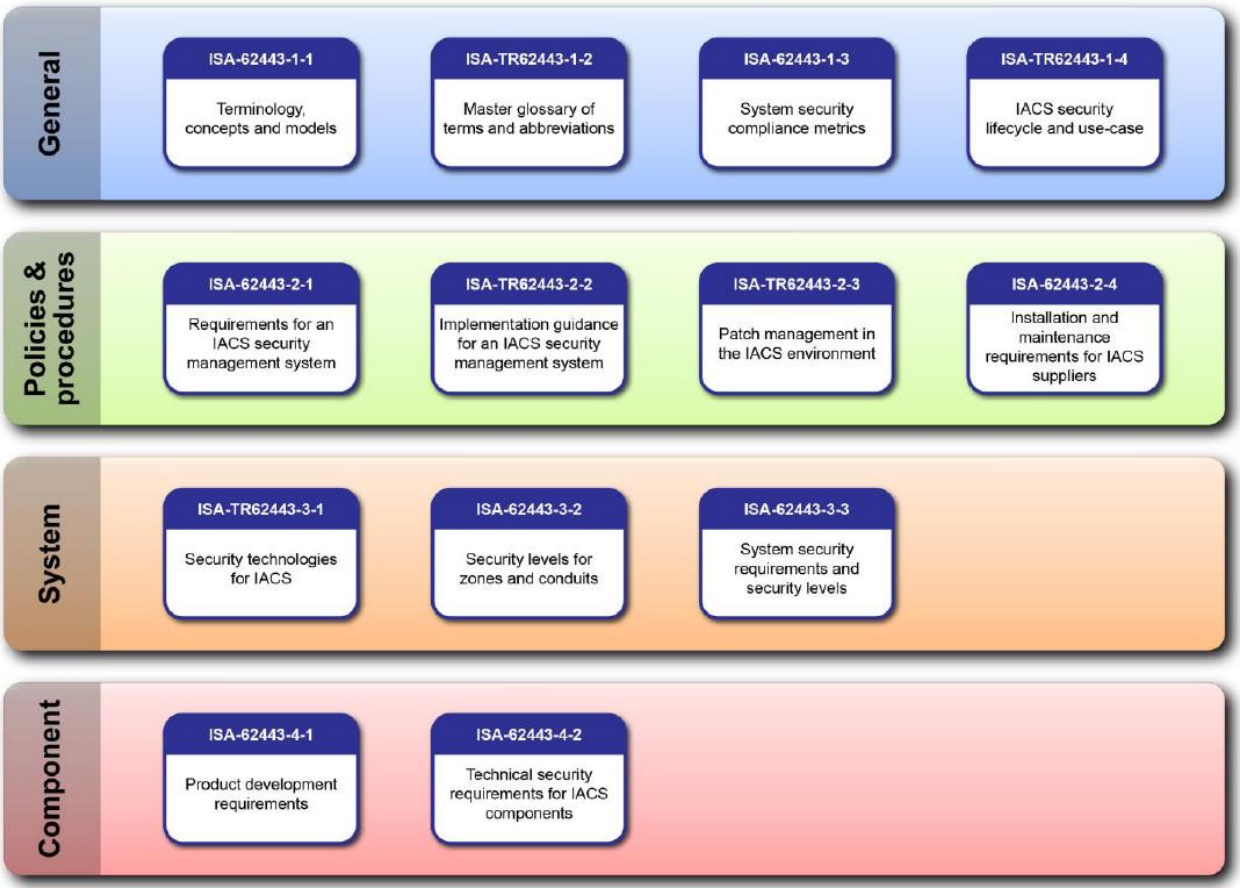

Figure 1: ISA -62443 work products [10]

6. IACS Architecture

Considering the broad range of threats that Industrial Automation and Control Systems (IACS) are exposed to, there are no simple ways to secure everything. Every IACS presents different risks and vulnerabilities. A better solution is 'Defense in Depth', that protects the control system by multiple layers of defense that are distributed throughout the control network. To implement 'Defense in Depth' model, Utilities must have a clear understanding of how all the technology fits together and where all the interconnectivity resides.

Dividing IACS system into zones can assist industries in creating clear boundaries in order to effectively apply multiple layers of defense. It is a core requirement of the in the ISA/ IEC 62443 standards for Security for IACS. ISA 62443-3-3 provides ways to segment IACS system into zones and conduits [10]. The utility can establish its zones by grouping them based upon the results of the high-level cybersecurity risk assessment or other criteria, such as criticality of the assets, operational function, physical or logical location, required access. Conduit is the path for the flow of data between two zones, and it controls access to zones. Conduits resist Denial of Service (DoS) attacks or the transfer of malware, and protect the integrity and confidentiality of network traffic.

The intention of this grouping is to identify assets which share common security requirements in order to manage security risks and to achieve a desired target security level for each zone. Target Security Level (SL-T) is the desired level of security of the zone. SL-T is determined by performing a risk assessment. And Achieved Security Level is the actual level of the particular zone. Equipment in the zone have a Security Level Capability (SL-C). As the part of the system design process, the designers would select controls and components with necessary SL-Cs to meet the SL-T requirement. Also, introducing controls on a conduit mitigate the difference between a zone's security level capability. Upgrading conduit controls is often more cost-effective than having to upgrade every device or computer in a zone. There are several options for implementing security technologies on a conduit. Industrial firewalls and virtual private networks are the most popular ones. Industrial firewalls control and monitor traffic to and from a zone.

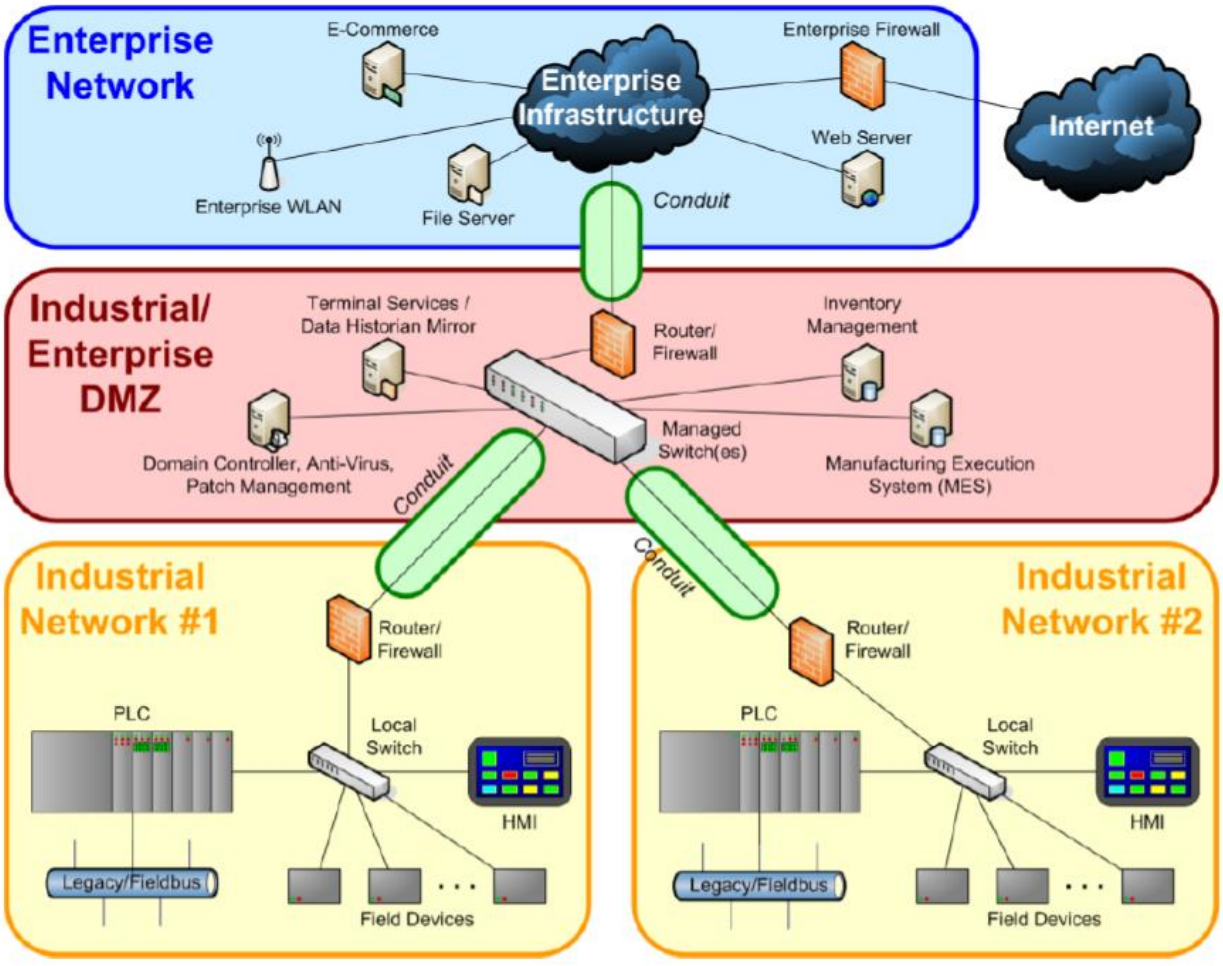

Figure 2: High level Manufacturing example showing zones and conduits [10]

The Figure 2 shows a high-level representation of a manufacturing plant broken down into zones connected by conduits. It has four zones shown: Enterprise network,

Industrial/Enterprise DMZ (Demilitarized Zones), and two Industrial networks. The Enterprise Network Zone includes connectivity to the Internet, remote offsite facilities, Email servers, Domain Name System (DNS) servers, and IT business systems. A wide variety of risks exist in this zone because of the external system connectivity. A demilitarized zone (DMZ) is a network that acts as an intermediary for underlying zones and devices, so that they avoid exposure to untrusted networks. DMZ lies between Enterprise Network and Industrial Network. The DMZ adds an additional layer of security to the Industrial network, since an external attacker only has direct access to equipment within the DMZ.

7. Substation Automation System

Supervisory Control and Data Acquisition (SCADA) is the main functional element of Substation Automation System (SAS). SCADA is used to collect asset monitoring data, and equipment status information, combined with the ability to issue control commands to circuit breaker. SCADA can also provide automation, such as automatic control logics, switching sequences and interlocking. Substation collect metering data, equipment status information, and send these to the Substation Control Room, and can assert control commands received from the Control room as well. In a substation bay level, both protection & control operations and SCADA control operations occurs. Protection operations such as circuit breaker trip commands and circuit breaker reclose commands requires to be highly reliable and have high operating speeds. SCADA operations necessary for normal operations, such as retrieving data, monitoring data, managing the data and data flows, and controlling equipment needed for routine operations and maintenance. Protection & control owns relays, SCADA owns Remote Terminal Units (RTUs). Figure 3 shows bay level substation architecture where Substation Bay controllers, protection relays and Phasor Measurement Units (PMUs) in the Relay Room collect data from the switch gear in the substation. Process bus is used to exchange sampled values, equipment status, and equipment controls between primary system equipment (the process level) and bay level devices (such as protective relays). And then these collected data are sent to Substation control room over the station bus.

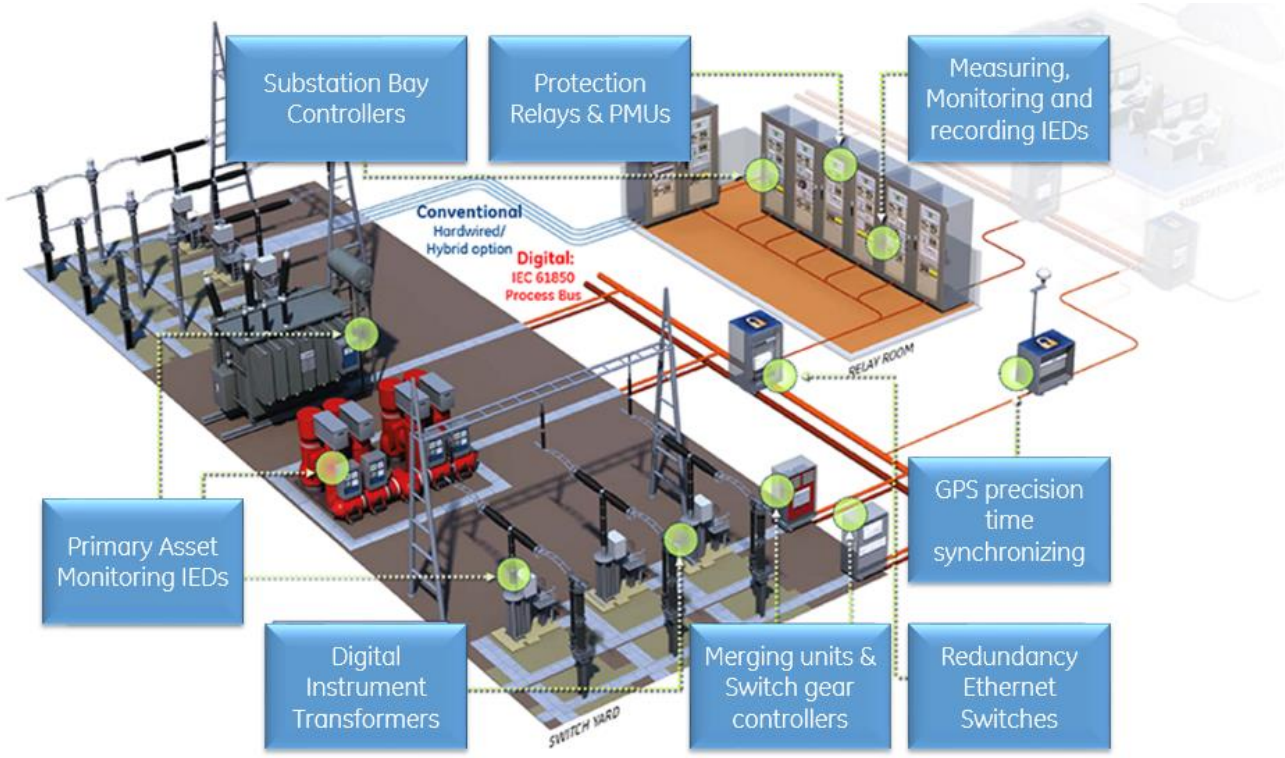

Figure 3: Substation Automation Bay Level

Figure 4 shows how a substation control room is connected to the relay room to monitor and control substation data. All the substation data is sent to the Energy Management System (EMS) or Distribution Management System (DMS), which ensures cost efficient and reliable operations of the power system. SCADA systems are based on communications, and over the time hundreds of different SCADA protocols were developed to enable this sharing of data between devices. In North America, the most common protocol in use is DNP. IEC 61850 standard models standard ways to represent data, and standard ways to make data available.

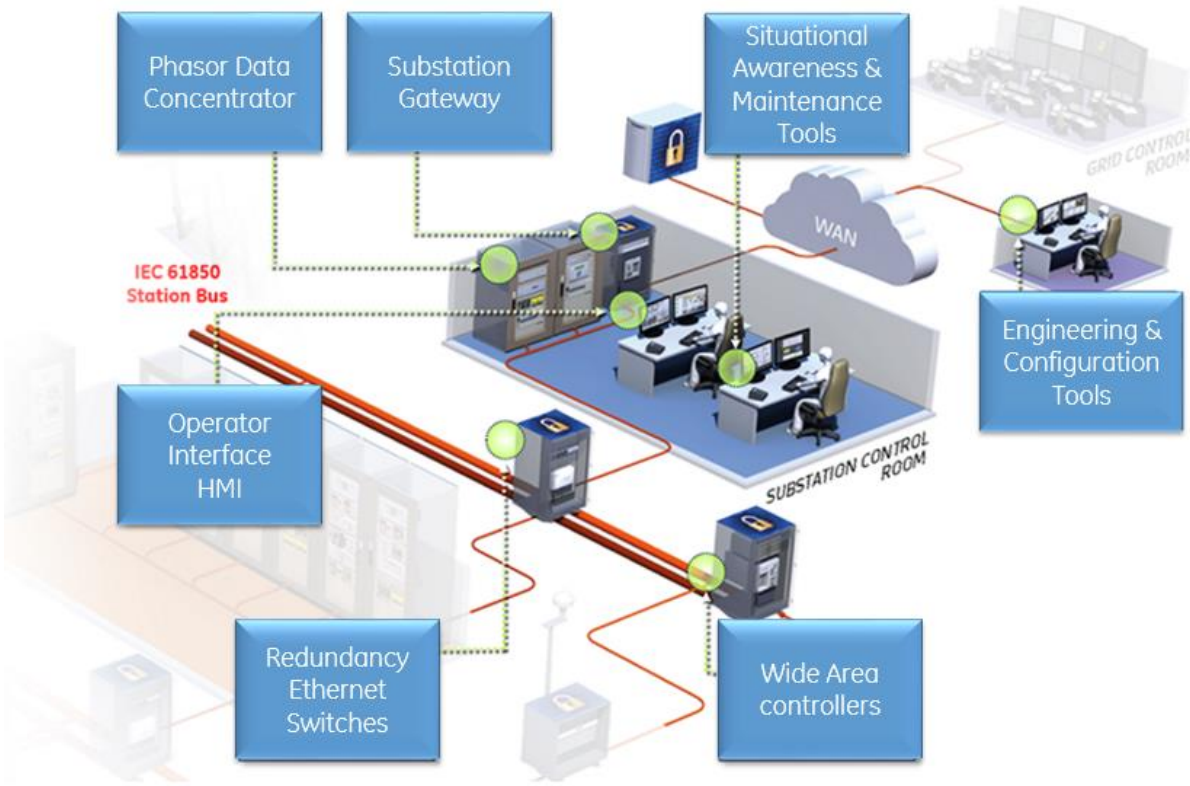

Figure 4: Substation Automation Station Level

8. Integration IEDs with security systems

When deciding security solutions against current threats facing energy sector, utilities must keep in mind that no industry can eliminate risk completely. Therefore, Defense-in-depth approach is applied by layering security elements to successfully protect the infrastructure by multiple layers of defense that are distributed throughout the control network. Utilities and industries can use different security systems with IED security features to achieve Defense-in-depth security. IED vendors provided many security features in their IEDs to facilitate secure integration. This section presents how to integrate IEDs with third party security systems to achieve holistic security.

8.1. User Authentication and Authorization

Identification and authentication are required for all users of IEDs in the critical infrastructure. Most of the IEDs enforce local authentication at login. These local accounts should be created in the IED and their default passwords should be changed. If the IED supports role based access, these accounts have to be assigned to specific roles. Local authentication is hard to manage since each IED has to be reconfigured when accounts or

passwords are changed. Central authentication makes account and password management easier.

IEC 62351-8 specification defines Role-Based Access Control (RBAC) for enterprise-wide use in power systems. This standard describes criteria for defining roles, role assignments and role-to-right mapping with respect to power systems. It also provides a mandatory list of role-to-right mappings that utilities can use in their IED configurations.

As CIP-004-6 Personnel and Training R4.3, mandates that utilities should verify accuracy of all user accounts, user account groups, or user role categories, and associated privileges once every 15 calendar months. The privilege review is to ensure that every user is assigned with least privilege access, and utilities can enforce this by practicing role based access control. First they should determine specific roles on the system (operator, engineer, observer, administrator, etc.), and then group access privileges to the roles and assign users to those roles. Role-based access permissions eliminate the need to perform the privilege review on individual user accounts. CIP-004-6 R5.2 requires that in the case of reassignments or transfers, the individual's authorized electronic access is revoked. This step may include deletion or deactivation of accounts used by the individual. Microsoft Active directory can be used for user account management.

CIP-007-6 Systems Security Management R5.1 requires utilities to have a method to enforce authentication of interactive user access. Requirement Part 5.1 ensures that IED authenticates users that can delete/modify configuration. Interactive user access does not include read-only information access such as front panel displays or web-based reports. Then CIP-007-6 R5.2 requires to identify and inventory all known enabled default or other generic account types. Default accounts provided by a vendor should be removed or disabled prior to production use of the IED. If this is not possible, the passwords provided by vendors must be changed from those default accounts.

CIP-005-5 Electronic Security Perimeter(s) R2.1 requires utilities to have an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. The Intermediate System serves as a proxy for the remote user. R2.3 requires multi-factor authentication for all Interactive Remote Access sessions. The use of multi-factor authentication provides an added layer of security, rather than only passwords.

8.1.1. RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol that enables IEDs to securely communicate with a central server to authenticate users and authorize their access to the requested IEDs. RADIUS allows utilities to maintain user accounts in a central database that all IEDs can share, and It provides centralized authentication, authorization and accounting for users. In a large network with many users, RADIUS allows a single server to perform all authentications. Hence, it poses a point of failure. Therefore, best practice is to have primary and secondary RADIUS servers to increase system reliability. RADIUS messages are sent as User Datagram Protocol (UDP) messages. Normally, UDP port

1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages.

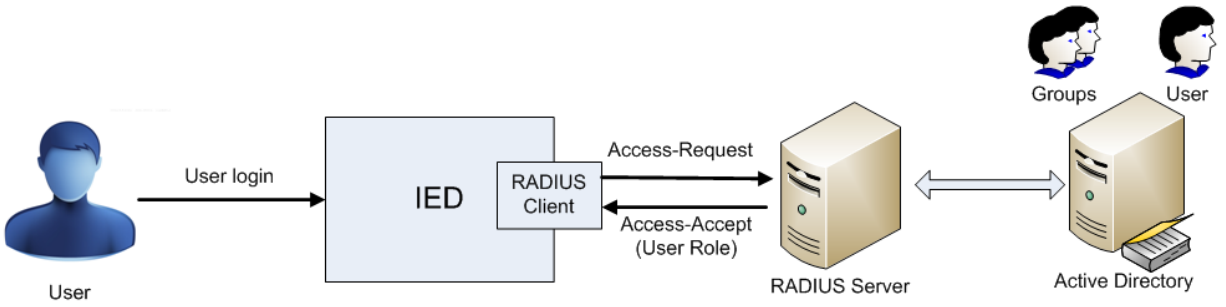

Figure 5: RADIUS user login

Figure 5 shows how a user gets access to an IED and gets authenticated and authorized by RADIUS server. User simply logs in to the IED, then IED RADIUS client sends Access-Request to the RAIDUS server. If the username is found and the password provided is correct, the RADIUS server returns an Access-Accept response. This message informs the RADIUS client in the IED that the connection attempt is authenticated and authorized. For additional security, RADIUS is also flexible enough to allow for other forms of authentication, such as those implemented using EAP. Mostly used RADIUS methods are RADIUS-CHAP and RADIUS-PAP, and secure EAP methods such as EAP-TLS, EAP-TTLS and EAP-PEAP. Sometimes utilities have to decide on the RADIUS method they are going to use depending on the support of the RADIUS server that they are using.

8.1.2. TACACS+

Terminal Access Controller Access Control System (TACACS) is a client/server protocol that operates in a similar manner to RADIUS. Most current level of TACACS is TACACS+. TACACS+ provides centralized validation of users attempting to gain access to IEDs. It provides separate and modular authentication, authorization, and accounting facilities. TACACS+ has been widely implemented by Cisco. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation

8.1.3. LDAP

The Lightweight Directory Access Protocol (LDAP) is an application protocol that provides mechanism to connect, search and modify directory. LDAP directory service is based on client/server model. There are few differences between LDAP and RADIUS. LDAP does not directly support user accounting as RADIUS. Also, LDAP by itself cannot support multi factor authentication. To retrieve information from the directory database, an LDAP directory is queried by a LDAP client. LDAP is the main access protocol used by Microsoft's Active Directory. LDAP does not require any security. However, by using Transport Layer Security (TLS), LDAP can encrypt user sessions between the client and server.

8.2. Logging

Substation network administrators requires increased visibility into network infrastructure to identify potential failures in critical devices and applications. When we investigate a device or service failure, it is important to seek the root cause of the problem. Security Information and Event Management (SIEM) devices aggregates data from various logs and provides real-time analysis of security alerts. SIEM system centrally aggregates all the event logs (security logs and general event logs). Security events, such as log ins and log outs, user lockouts due to multiple login failures, configuration/setting changes, firmware upgrades, server access failures are examples of activities that should be monitored and made available to SIEM for analysis. If an anomaly is located, operators are alerted based on the severity of the intrusion. The logs of both real-time and historical logs are stored for a retention period defined in the security policy.

Some IEDs support both local logging and remote logging features. Local logs are saved in the IED, can be archived using different methods. Syslog protocol is used to transport these IED events to remote logs. Syslog is a great way to consolidate logs from multiple IEDs into a single location. A syslog client would reside on each IED, while the Syslog server will be embedded into the SEM system. IEDs can be configured to send syslog messages to report all the events and errors to a remote syslog receiver. Syslog implements a client-server application structure where the server listens over UDP on the port 514 for protocol requests from clients. The syslog message provided by the IED includes the facility code and the severity level. Syslog servers should be able to generate alerts, notifications, and alarms in response to anomaly in messages.

Based on CIP-007-6 Systems Security Management R4.1, utilities should Log events at the BES Cyber System level or at the Cyber Asset level (IED level) for identification of, and after-the-fact investigations of, Cyber Security Incidents (successful login attempts, failed access attempts and failed login attempts and detected malicious code). CIP-007-6 R4.2 requires to generate alerts for security events. Alerts can be configured in the form of an email, text message and alarming. And as per R4.3 requirement, retain applicable event logs for at least the last 90 consecutive calendar days.

CIP-008-5 Incident Reporting R1.1 requires utilities to identify, classify, and respond to Cyber Security Incidents. In R1.2 requires utilities to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (E-ISAC) within one hour after determining that a Cyber Security Incident is reportable. R2.3 requires utilities to retain records related to Reportable Cyber Security Incidents.

8.3. Privilege Identity Management

Privilege account holders like administrators, and security engineers, have a lot of privileges assigned, such as changing settings, configurations and accounts in the substation networks. Privileged accounts are frequently targeted by attackers and malicious insiders to

change firmware/ configuration on IEDs and gain control of the SCADA infrastructure. Hence, privilege account passwords have to be changed and stored in secure vaults. Privileged Identity Management (PIM) is an area of Identity Management that focuses solely on privileged accounts. PIM covers special needs of privileged accounts, including their provisioning and life cycle management, authentication, authorization, password management, auditing, and access controls. CIP-007-6 Systems Security Management R5.6 requires utilities to enforce password changes or an obligation to change the password at least once every 15 calendar months.

8.4. IED Redundancy

Redundancy in the network protects against failures caused by network components failures. IEDs, such as protective relays, with two network interfaces support redundancy by sending the same traffic simultaneously through both interfaces. This type of redundancy is also known as parallel redundancy and it offers zero-time recovery, essentially not interrupting the traffic at all. The two parallel redundancy protocols are Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) [11].

Both PRP and HSR provide redundancy at the Ethernet layer of the TCP/IP stack. Redundancy and zero-time recovery are beneficial for protocols, such as GOOSE, which requires real time delivery. Link Redundancy Entity (LRE) module responsible for duplicating outgoing packets and sending them over the two redundant networks, as well as for dropping one of the duplicates at the receiving device. LRE are called DANPs (Doubly Attached Node) in PRP or DANHs (Doubly Attached Node) in HSR. If one path fails, the destination will still receive one of the two duplicated packets.

PRP may be used with any topology, such as tree or ring, but it requires two independent networks and switches for connecting devices. With HSR the network size is reduced to half compared to PRP. A disadvantage of HSR however is that it cannot be mixed with regular devices on the same ring. Regular devices may still be used in HSR rings if they are attached through a device called “red box”, which is essentially a converter from a singly attached network to a doubly attached network. PRP networks make more sense if the size of the network is not a concern. If the size is a concern, HSR works better.

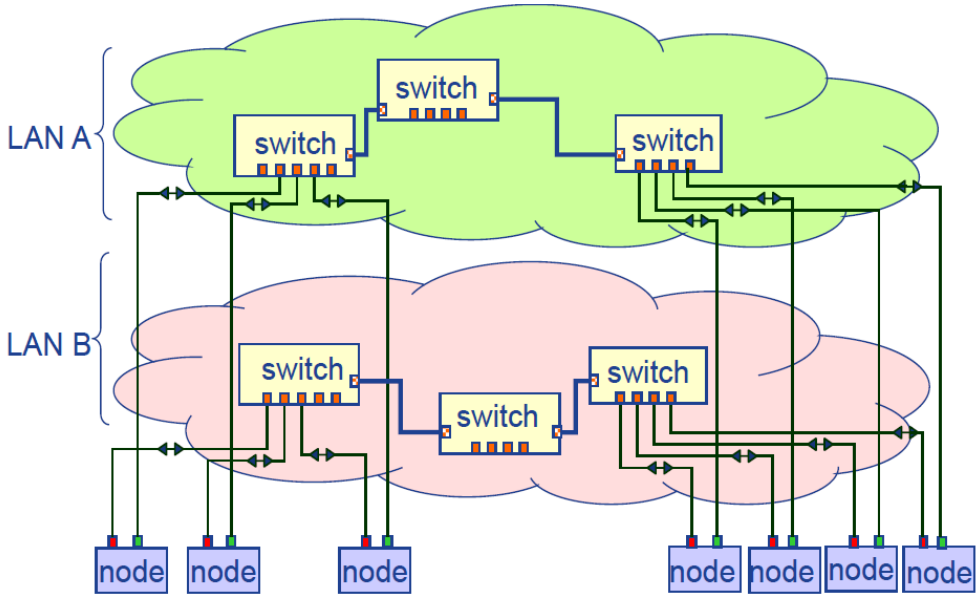

Figure 6: Example of PRP network [11]

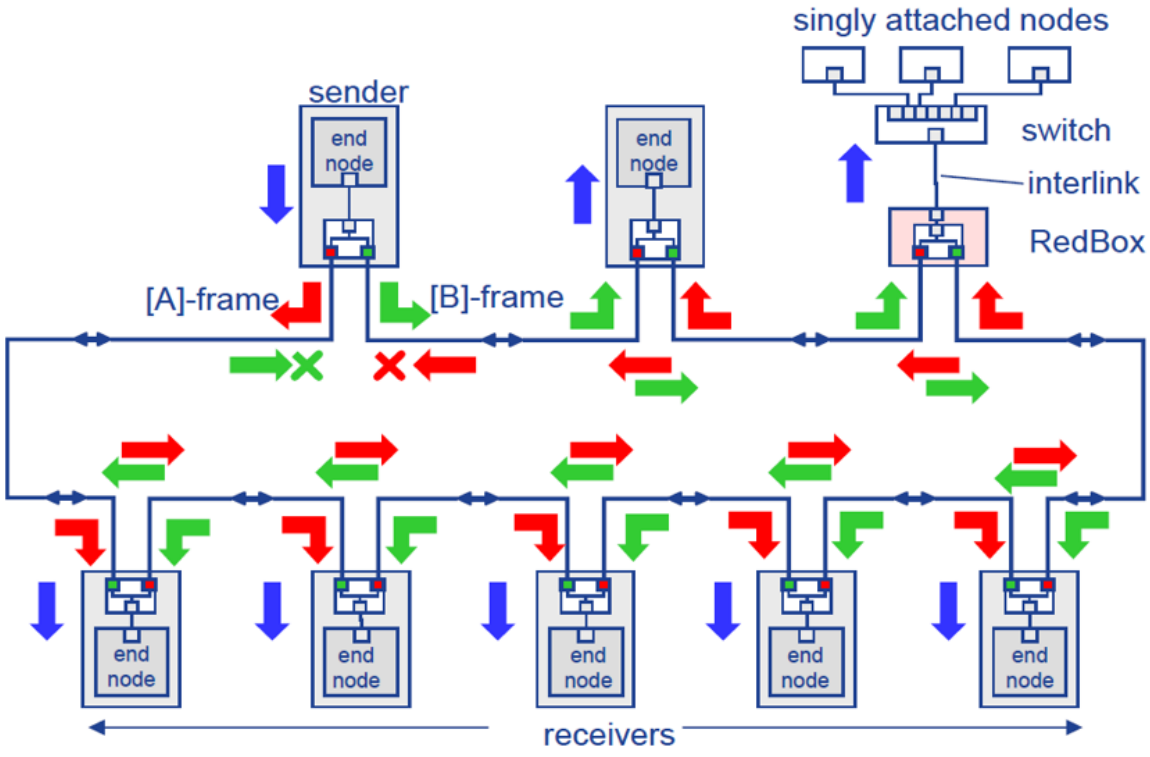

Figure 7: Example of HSR network [11]

8.5. Security Keys and Key Management

IEC/TS 62351-3 standard covers security of protocols IEC 60870-6 (TASE.2 / ICCP), IEC 60870-5-104, IEEE 1815 (DNP 3) over TCP/IP and IEC 61850 over TCP/IP, and specifies the use of TLS as security mechanism. IEC/TS 62351-5 describes security of both serial and networked profiles used by: IEC 60870-5, 101,102,103,104 and DNP 3 (IEEE 1815). IEC/TS 62351-5 proposes challenge-reply mechanism using an MAC (unilateral, two-pass authentication), and ensures interoperability between stations and backward tolerance with non-secure devices. IEC/TS 62351-9 standard specifies how to generate, distribute, revoke and handle digital certificates, cryptographic keys. It also covers handling of asymmetric keys (private keys and X.509 certificates), as well as symmetric keys (pre-shared keys and session keys).

With development of secure DNP3 protocol and secure R-GOOSE, IEDs needed to be configured with pre-shared keys or configured to manage keys to provide the required secure SCADA communication. Then Utilities have to decide how to distribute these keys among IEDs. For symmetric keys, easiest way is to use pre-shared keys in the IEDs. More secure way is using a Key Distribution Center(KDC) to share a key with each of all the other parties involved in the communication. For asymmetric keys, we have to use a Public Key Infrastructure (PKI) to create, manage and distribute keys.

In secure R-GOOSE, key management is based upon Group Domain of Interpretation (RFC 6407 – GDOI) [12]. GDOI provides the capability of a Key Distribution Centre (KDC) to provide symmetric keys securely via either clients requesting the keys or the KDC pushing keys to the appropriate subscribers.

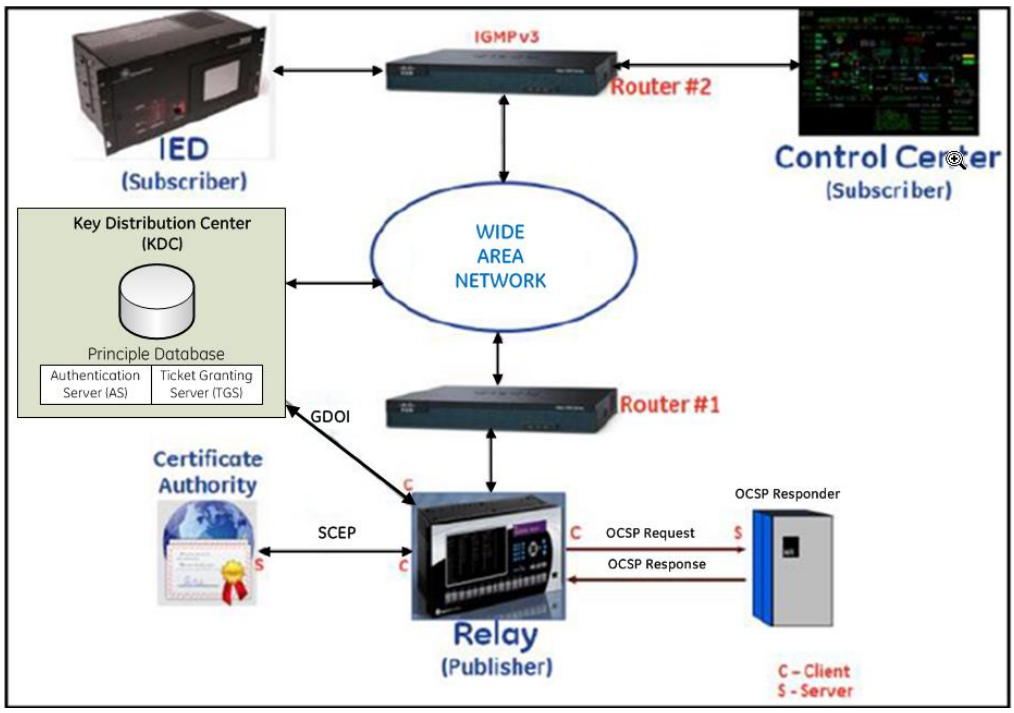

Figure 8: R-GOOSE Security Architecture (simplified) [12]

A simplified version of secure R-GOOSE architecture is shown in Figure 8. To provide secure R-GOOSE, first the IED has to get a certificate for itself. The device uses the Simple Certificate Enrollment Protocol (SCEP) protocol for communication with the Registration and/or Certification Authority (RA/CA) and downloading the X.509 certificate. Once the certificate is obtained, Publisher/subscriber initiates the second step, which is connection establishment with KDC server using GDOI protocol, as described in IEC 62351-9. Device sends the certificate it obtained to KDC and requesting KDC's certificate. Online Certificate Status Protocol (OCSP) is used to verify the revocation status of these certificates.

Only if the certificate verification succeeds, the KDC sends a Security Association (SA) including information on security algorithms for encryption, and integrity check. Devices (publisher/subscriber) send acknowledgement if they support the security algorithms mentioned in SA. Upon acceptance from devices, the KDC sends the symmetric keys to devices. These keys are used for signing and, optionally encrypting the R-GOOSE.

8.6. Monitor and control Traffic

According to CIP-007-6 Systems Security Management R3.1, utilities should deploy method(s) to deter, detect, or prevent malicious code. There are different options available such as antivirus solutions, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions to achieve this. And CIP-007-6 R3.2 requires utilities to mitigate threats from detected malicious code. Antivirus products may automatically remove or quarantine malicious codes. And white-listing can mitigate the threat as it will not allow the code to execute.

CIP-005-5 Electronic Security Perimeter R1.1 requires to place all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). The ESP defines a zone of protection around the BES Cyber System. It implies segmenting of BES Cyber Systems by requiring controlled Electronic Access Points between the different trust zones. And CIP-005-5 R1.2 requires all External Routable Connectivity through an identified Electronic Access Point (EAP). CIP-005-5 R1.3 requires to enforce inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. The EAP should control both inbound and outbound traffic, and this is the first level of defense against zero-day vulnerability based attacks. CIP-005-5 R1.5 requires utilities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems or other forms of deep packet inspection techniques.

8.6.1. Firewalls

firewall is a device that monitors and controls the incoming and outgoing network traffic based on security rules and policies. Firewalls may operate simply by filtering out unauthorized data packets based on their addresses, port/services or it may use complex packet inspection to determine legitimate communication. Firewalls are categorized as Network firewalls and Host-based firewalls. Network firewalls are positioned between

networks and they filtered traffic between two or more networks. Typically firewalls provide the first level defense against external threats. They are normally positioned in the outer layer of the network, in the boundary of Electronic Security Perimeter (ESP) as defined in NER-CIPv6. Host-based firewalls provide a layer of software on one host that controls network traffic in/out to that machine. There are some IEDs, such as substation gateways, that are equipped with host based firewalls.

8.6.2. IDS

An intrusion detection system (IDS) is a device or software application that monitors networks or systems with aim of detecting and reporting malicious activities or policy violations. Network based IDS is known as Network Intrusion Detection System (NIDS), and device based IDS is known as Host based Intrusion Detection System (HIDS). A software that monitors important operating system files is an example of a HIDS, while a device that analyzes incoming network traffic is an example of a NIDS. NIDS preforms analysis on the passing traffic and alerts of anomalies are reported to administrators. NIDS could be used with a firewall, to detect if someone is trying to break into the firewall. HIDS takes a snapshot of existing system files and compares it with the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator. IEDs could use HIDS to detect unauthorized configuration/setting or firmware changes.

An Intrusion Prevention Systems (IPS) is the same as an IDS with the added ability to prevent the attack, by taking actions on the detection of an intrusion attempt. IPS can take preventive actions, such as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address. IPS may also be applied to HIDS, in that anti-malware software can prevent file infection.

9. Conclusion

Grid security is a top priority for the electric power industry. We should take actions to prevent attacks, such as the cyber intrusion attack on the Ukraine Power Grid. Planning for and preventing potential attacks are critical to the national security. Considering the broad range of threats that IACS and SAS are exposed, protecting the power grid and IACS is very complex task. Therefore, we should practice 'Defense in Depth' methods, that protect the IACS or SAS by multiple layers of defense. Successful cyber security of a system is a combined effect of technology, procedures, policies, users, monitoring, standard compliance and diligent enforcement. To secure IEDs, their security features should be enabled and configured properly. IACS and SAS can achieve required IED cyber security by proper integration of third party security systems with IEDs.

10. Reference

[1] Industrial Control Systems Cyber Emergency Response Team – ICS-CERT Monitor Newsletters, [Online]. Available: https://ics-cert.us-cert.gov/monitors

[2] North American Electric Reliability Corporation – Critical Infrastructure Protection, NERC-CIP v6, [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[3] R. M. Lee, M. J Assante, T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid", 2016 [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[4] NIST, "Framework for Improving Critical Infrastructure Cyber Security ", version 1.0, February 12, 2014

[5] NISTIR 7628, "Guidelines to Smart Grid Cyber Security", September 2014

[6] NIST SP 800-57, Recommendation for Key Management, Part 1

[7] NIST Special Publication 800-82, Revision 2, "Guide to Industrial Control Systems (ICS) Security"

[8] NIST Special Publication SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations"

[9] IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE 1686-2013

[10] Security for industrial automation and control systems Part: System security requirements and security levels, ANSI/ISA-62443, part-3-3, 2013.

[11] A. Cioraca, I. Voloh, M. Adamiak "What Protection Engineers Need to Know About Networking", in Proceedings of the 68th Annual Conference for Protective Relay Engineers, Texas A&M university, Texas, 2015.

[12] M. Kanabar, A. Cioraca, A. Johnson, "Wide Area Protection & Control using High- Speed and Secured Routable GOOSE Mechanism", in Proceedings of the 69th Annual Conference for Protective Relay Engineers, Texas A&M university, Texas, 2016.

Biographies

Eroshan Weerathunga, is a product cyber security lead for Substation Automation System products at GE Grid Solution. Eroshan has worked on several Substation Automation product implementations and he has over 5 years hands on experience in software architecture and cyber security design. He received his B.Sc in Electronics and Telecommunication Engineering from University of Moratuwa, Sri Lanka in 2009. And his M.E.Sc in Electrical and Computer Engineering from Western University, Canada in 2012.

Anca Cioraca, is a Cyber Security Principal Engineer for Grid Automation products at GE Grid Solutions. Anca has thirty years hands on experience in system / software architecture,

specialized in communications, networking and cyber security. Anca has a Master of Engineering degree in Electronics and Telecommunications from Bucharest Polytechnic University, Romania. In 1991 Anca moved to Canada and for the following twenty years she focused on software architecture and cybersecurity for network devices, such as routers, firewalls and security servers, while working for Motorola, Enterasys, Siemens and WatchGuard. In 2012 Anca joined GE Grid Solutions. Anca is a member of IEEE Communications Society and the IEC TC57 working group WG15, where she actively contributes to the definition of security requirements for the TC 57 series of protocols.