Envisioning a Cyber Network Security framework for Smart Grid Utilities in compliance with the critical Infrastructure Protection (CIP) version 5 standards.

Critical Infrastructure Protection: Modeling Utility Network Security

MINT Capstone Project

By Syed Shayan Perwaiz

Project Advisor :
Mr. Faisal Sheikh
SCADA Security & Network Analyst at EPCOR

Contents

Table of Figures

1 Identification and Inventory Management

In the case of SCADA system, the advancement has happened quiet recently. For the past few decades it was considered as an isolated environment and security was well achieved by its obscurity and segregation from corporate networks. By late 90s, it became evident that the infrastructure needs more automated approach through the introduction of programmable controllers (PLCs) and other devices that can be mastered from a master control system. Presently the devices have become more flexible and intelligent to make decision on encoded thresholds (minimizing human interaction and errors) and reporting it to Remote Terminal Unit (RTU) or Master Terminal Unit (MTU).

This generation of SCADA systems is known as 'Internet of things' with system controls exceeding the geographical boundaries. Threats have proportionally increased with distributed control system operations by remote access and external routes, making these industrial systems more of a Cyber Asset. We cannot build a system immune to these threat as new threats are out every day but the only way to mitigate is to recognize those threats and vulnerabilities in our system and put appropriate measures in place. The approach should always be to minimize the risk, impact and frequency of breaches.

1.1 PURPOSE:

The footprints of securing an organization lead to its foundation, which is to identify and categorize the functional entities of a system. This includes all the critical assets and associated critical assets in the system. An identification mechanism is required to define the cyber system entities, such that an impact based relationship can be created between these assets. Thus identification is the first step of understanding your systems infrastructure, components, and processes; which then follows with the means of preventing it against adverse impact, loss, compromise, misuse and disoperation or instability.

The attackers can be very effective in taking advantage of any undetermined item in the systems. The traditional security has led us to create very secure zones like DMZ where we place all the new and unparalleled security devices to secure our data and services but this focused approach has also created other loopholes for attackers to indirectly gain access and exploit these services. These can be the newly added system, a guest device, or an authorized device connecting from remote location.

1.2 IMPLEMENTATION PLAN

This identification is accomplished through the execution of the methodology to inventory, evaluate, classify, document and review Cyber Assets and associated defined attributes. The use of unidentified term can create variances in the document. When comparing the entities in the Critical system, it is considered that all entities whether they exist at the facility or physically collocated at other location if connected to the system (external route connectivity) should be considered in the security domain. Once they qualify these entities can be checked for security and threat level they fall under.

The Approach:

The better approach to evaluate the system is to start from the top where you can explore the system boundaries. It can start with identifying the SCADA system type that falls into three categories:

- Industrial process - Includes power generation and distribution, fabrication etc.
- Infrastructure process - Power grids, water treatment, Oil & gas, civil defense etc.
- Facility Based - Building, airport, ships etc.

Once the system type is determined the next step is to understand the geo location of the system. Usually the today's SCADA systems have well distributed operation expanding to countries or even continents. This is beneficial in tracking the legitimate network flows and other unrecognized flows. The systems can have multiple facilities (functional sub system) under one umbrella therefore we will recognize each one of them as separate entity. System components should be placed in the inventory it can be done through automated tools as well as using different documentation method. Once we are able to scrutinize all the element of the system then it can be evaluated based on the impact analysis.

Hence the classified information need more of an executive view to make management decision, a logically well explained diagram can help in this scenario where asset and impact based relationship can be displayed. This process can be more interactive and decisions can be made by management to include or exclude entities before applying policies to identified assets.

1.3 SYSTEM COMPONENT IDENTIFICATION & CHARACTERIZATION

You know the boundaries of your systems; it is the time to parse through the system entities. Results might differ with your approach but it’s better to categorize them on their generic attributes such that when it’s time to delegate responsibilities we easily align them to individual role to monitor or analyze them. Once entities are categorized you can sub categorize them on their functional attributes. The approach should be to develop a structure that has the ability to adopt new equipment and service for the next few years, providing a leverage to vision a growing system. The following elements are just a guideline for categorizing the system inventory:

- Physical Cyber Assets
- Telemetry system

- System Components
- Services & Process
- Software Inventory
- Threats
- Human Resource
- Impact level

1.3.1 Physical Entities

This category might give you a more generic view of assets but anything we consider should fall under cyber network and equipment involved in its operation. Considering control systems, we are bound to involve all the field units and sensors as well as network assets in detail. The figure below gives you a better view of Control systems.

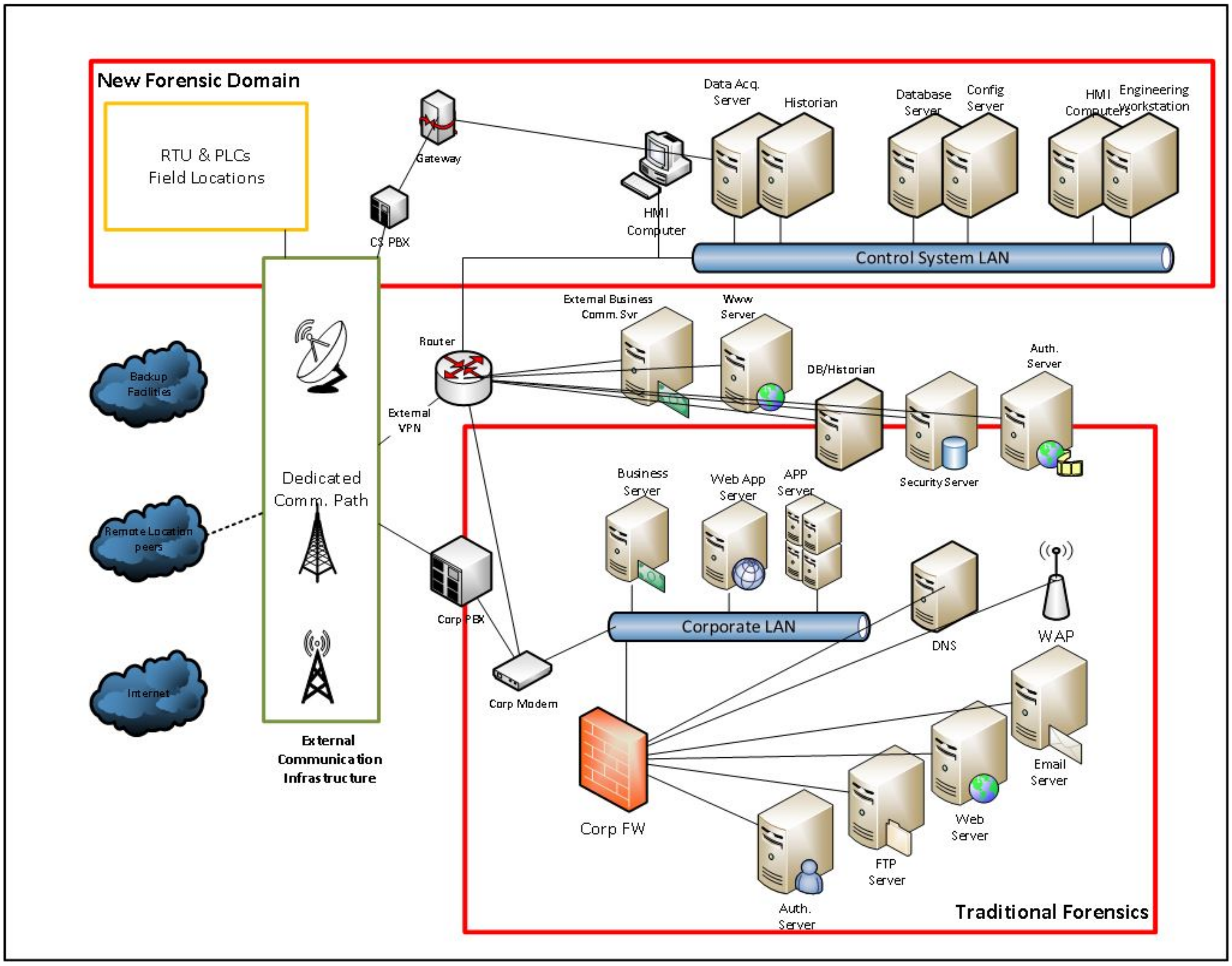


Figure 1 – Control System Physical Architecture

- *Field Instruments*

In early day these instruments were manually controlled like water pumps, valves etc. but with time, things have evolved and now they can be controlled remotely through command this is achieved by placing an actuator on top of the system to execute the instructions. These devices mean more of passive devices as they do not perform any logical operations. The communication is usually unidirectional; For example, in the case of actuator the purpose is to listen and perform the operation whereas sensor will only be sending data to preceding controllers (PLCs/RTUs).

The impact can be high but usually these are not compromised directly unless the controller is being infected. Inventorying these devices does require additional tools to scan passive devices. It is important to document the position and location of every sensor in the system, since these can be found in great number in any control system. A separate drawing is maintained for their representation in every industry.

- *RTUs/PLCs*

RTUs were once seen as a relay agent to forward instructions, but today's RTUs are far more powerful with its ability to Master the field instrument independently by monitoring all real time data and logs. This increases risks as they can perform operation if disconnected from the controller they can operate and take decisions based on encoded values and thresholds. The impact can be high if compromised.

- *Network Communication Devices*

Equipment under this category usually works on TCP/IP protocols. These are considered as the backbone of any cyber system communication routing. These include router, switches, firewall, intrusion detection and prevention equipment (IDS/IPS), wireless access points, hub, bridges etc.

In the field where latency required less than 1m/s for the protection devices to communicate with the RTU's, special networking gears been used which support real-time protocols such as DNP3, GOOSE, OMNICOMM, MODBUS etc.

While creating inventory for these devices it is mandatory that we know purpose of each device at its position and capabilities .For example, a firewall can work as Stateful firewall, application firewall, proxy agent etc. Router helps you in further identifying the logically separated groups and department. Inventorying these devices include the following attributes, Hostname , Equipment model, Serial number, type, location, allowed subnets and hardware redundancy.

The criticality and impact of these devices vary by the position in the system, as these can be seen in different perspective for example a front end firewall protecting the network from WAN intrusions, whereas a switch present a Local Area Network in any facility.

- *Workstations*

Workstations are sometimes neglected in the case of control systems, but putting them into inventory and identifying their access is critical. These are usually considered as weak link to break into any origination as administrator are more focus on securing servers. We can see some recent example of '*Stuxnet'* where it was penetrated into the facility through a USB connected to the host resulting in exploiting the system.

While inventorying the host it is mandatory to explain the purpose whether it is a user assigned host, an engineering workstation or will be used with a guest account, so privileges can be defined with it. The attributes includes location, hostname, user, connectivity and port accessibility (i.e. USB and other portable accessories).

- *Servers*

Identifying the server location is an important task; usually a breach one server can expose the logical network of whole server block. The inventory of server requires their role and service to be defined properly as they might be working in cluster or in a group. Server can be further segmented logically on their purpose. For example, print server and Data acquisition server need to be further segregated.

1.3.2 Telemetry System

Their use has readily increased for the past decade, as information relaying has increased in distributed systems. Initially the systems were connected through leased line but the cost of infrastructure was considered quiet high. Today's radio devices support better cellular communication with diagnostic capabilities. These telemetry system used industry specific communication protocols to relay messages e.g. MODBUS ASCII, MODBUS RTU, Enron MODBUS and MODBUS/TCP, DNP3, GOOSE, IEEE-61850. Inventorying the telemetry device include the radio access point, signalling band, protocol and encoding used. These systems are considered as associated critical assets as when disrupted can create instability in the system.

1.3.3 System Entities

These include the logical aspect of the cyber systems, some key characteristics are mentioned below.

- *IP Address and Subnets*

IP addresses identifies the digital grouping of devices, these can be segmented to break the impact in case of breach or based on essential, authorization and functional entities. Every subnet needs to be well documented and explained. Critical assets must have static IP binding to their hardware address these should be defined in the inventory management systems as well as on each device. IP address conflict should be alerted by the inventory system.

- *MAC Addresses*

Maintaining the hardware address in the inventory provides better visibility in the case of new asset or any asset replacement in the system.

- *Hostname*

It helps in keeping track of assets. Hostname should be well structured such that it can indicate the location, type, and identification number for the asset.

- *Operating System & Firmware*

Inventorying the operating system and firmware on the devices will keep system integrity intact against the known vulnerabilities, thus can be patched using security update and service packs. It is also necessary to explain that the update status of each system should be maintained in the inventory as the system joining the network after some time can be rectified as vulnerable system and effective measure can be taken against them.

1.3.4 Services/Process Identification

Identifying services and processes in the system requires in-depth understanding and prolong monitoring of network traffic, applications and system screening. We can classify them into local and industrial services. Apart from that we also need to recognize the process and procedures followed in credential management, authorization etc.

- *Local Services*

These include basic system service like email, web, remote desktop, file and printer sharing feature etc.

- *Critical / Industrial process*

These are industrial processes running data acquisition or passing instruction to the devices. These service needs to be monitored and analyzed as only the standard messages should pass through and any irregularity should be logged.

- *Ports in use*

All host port should be blocked for any incoming session from firewall; only administrative port should be left open. These can be identified by running port scanning software and other tools like metasploit. Attributes should include port number, service and application allowed on that port.

- *Privileges*

Privileges are the rules that govern every organization and allows administrator to give additional right and resources to selective users. All documentation should be maintained in this regards, the attributes in involves the users, purpose, domain and allowing authority.

- *Credentials*

Details for all the active user credential should be maintained along with their authorization, privileges. The user access should be maintain by date; this means if any user has left, joined or has changed his responsibilities within the organization should be reflected in its credential status.

1.3.5 Software & Application

All authorized software history should be maintained along with the user group that is allowed to use it. Inventorying the software base is critical to track the legitimate activity on the network. The attributes should include name, version, platform supported on, user group access, type, and purpose in the system.

1.3.6 Threats

Threats can be difficult to trace if you are not looking in the right area. Instead of following the threat payload we need to identify the pattern every attack carries. I.e. target individual, deliver payload, upload file, run process, survive reboot, create outbound connection (CnC), internal recommence, spread in environment and wait for instructions. If we follow the pattern, we can easily find few traits in this process that can be used in our purpose. Here we will just identify the basis threat that any SCADA system will under.

- *Deliberate/Malicious Insider*

In these attacks an insider can be involved to bring the malware in the organization by the easiest mean this is a USB; as it happened in the case of 'Stuxnet'.

- *Accidental Insider*

An accidental insider can be an executive that has carried his asset outside the organization where it was exploited by an attacker. Once the system rejoins the local network the attacker get easy access to the network assets.

- *External threat*

The outside attack can be bots, DDoS or any service exploitation through the public network etc. We can also take note of the incoming connections from geo location where our company is not involved in any business.

1.4 Asset Impact Analysis

1.4.1 High Impact

The Cyber Assets criticality is defined as when they are found damaged, unavailable or misused the particular will have its impact with 10 minutes of operation, which can further result in disruption of operation in the whole system. Though these assets are always placed in redundancy but when considering them for impact analysis the redundancy is always neglected. These assets require highest level of security and privilege user access.

1.4.2 Medium Impact

All associated cyber assets that are directly involved in the operation of Critical Cyber systems. If rendered unavailable, degraded, or misused will impact in the degradation of Critical Cyber System but can be covered by the introducing the redundancy and fault tolerance in the system.

1.4.3 Low Impact

All other asset that does not fall in the High and Medium impact categorize, but still consider as the part of Cyber systems and can be misused in the system.

1.5 COMMON TOOLS FOR DATA COLLECTION

1.5.1 Automated asset tool

Today we have tools available in the industry that can discover asset attached to your local or remote network, irrespective of Operating system and agent installation. These tools have the ability to rectify systems, applications, database, OS and service running on the hosts. You can also gain reports from systems that are not connected to the network installing the software agent on it. These kind of software not only have the capability to detect but also analyze the gathered data; hence providing the administrator the better visibility of system behaviour and abnormalities in most circumstances.

Examples of such software's are Lansweeper, Spicework, and Openaudit etc.

1.5.2 DHCP

DHCP can serve as a tool in large industries where IP addresses are assigned dynamically to the assists, thus it can record the leases along with the client information and active time.

1.5.3 Network level Authentication

Network level authentication such as 802.1x allow administrator detect the connected host, as well as the details about the owner of the device.

1.5.4 Flow Monitoring/Traffic Analyzers

These tool help you collect flow statistics from all network ports and when used in conjunction with traffic analyzers provide you detailed graphical view of your network flows based on data, destination, session lengths etc.

1.5.5 Audits & Tests

Audit and penetration tests help in identifying the missing loopholes as well as forensic audit on network payload can help you identify current potential malware in your facility.

1.6 METRICS FOR INVENTORY MANAGEMENT

Once the tools are working and inventory is well maintained, it is the time to check the effectiveness of our asset management system. The result can be obtained by implementing the following procedures.

- The time your system takes to log a new device and generate alert to the system.
- How easily it can detect a system that has not been patched for some time and generate alert to admin.
- Are you able to detect a large amount of irregular data flow across the organization?
- Are you able detect new service on you network
- Are you able to identify the geo-locations your company network is connected?

2 Management Controls & Personal Trainings

Security control and personal training identifies management support for accountability and responsibility awareness in every environment. The security control policies provide a framework to every organization to build a safe and minimal risk structure against the identified assets of the organization. The personal trainings help individuals to understand company values and importance of security policies. The trainings are always valued as awareness and knowledge against the threats can only help you protecting the organization's integrity.

2.1 SECURITY MANAGEMENT CONTROLS

The widely used frameworks sometimes prove inappropriate for SCADA system, though IT systems are frequently considered the integral part of process system. We need to customize and tailor the policies and standards before applying it to industrial control system.

The example could be of an antivirus that should be installed on every system in the organization but few industrial machines are customized and restrict the installation of software. There the policy should be to utilized vendors solutions for hardware based antivirus to protect those system entities.

The Approach

The principle of setting up Security control start with identification, since we have achieved the identification and inventory of the asset in the earlier section we will continue with the categorization in respect to the security controls. Once we have highlighted the functional categorizes of the control system it is better to setup the baseline for the policies.

In previous section we relied on top to bottom approach but here it is better to start in the reverse order therefore we will focus on the low impact assets. This will help us in setting up the ground rules or the basic principles of the organization. Once achieved; we will then move towards the medium impact assets here the baseline rules will be low impact assets rules. Similarly when review the critical high impact assets the baseline will be the medium impact rules as illustrated in the diagram.

Since the policies can be very vast topic and approach to cover all risk require us to go through the Human resource and other departmental policies and regulations as well, therefore while discussing the policy we will only consider the electronic attacks.

2.2 FRAMEWORK CORE

The core provides us visibility about the risks, threats and its impact on business continuity and integrity. The core compromises of four element: Functions, categories, subcategories and informative references.

- **Functions**
  This helps us split procedure into different categories and stages of risk assessment and prevention. It is very necessary to define the categories in detail as the categories will set up stakes, roles and responsibilities for management and executives.

- **Categories**
  The categories define different types of procedure depending on their outcomes and risk they possess to organization. For example, asset management, asset control, detection process.

- **Sub-categories (optional)**
  These can be needed if different outcome is expected or there is some exception to procedures.

- **References**
  An important part of any every documentation that serves as an evidence that which standards and protocols were followed while developing this policy. This can vary with respect to the region, industry etc.

2.2.1 Core Functional Life Cycle:

- **Identify**
  We consider foundational aspect of business, future goals, integral value, assets, business strategy, management structure and risk attached to it.

- **Protect**
  This can include procedure and practices that will discourage an attacker's move towards infiltrating the organization. It can start by putting up physical security, red zone, limited and authorized access and strong passwords etc.

- **Detect**
  Detect refers to an ongoing procedure and policies. This should include logging, monitoring of network flows, operating system and application vulnerability check, regular audits, ad hoc audits and etc.

- **Respond**
  These are usually applied either a threat or vulnerability is detected or an incident has happened. The policies can vary depending on the incident from shrinking the impact to reporting criteria of an incident.

- **Recover**
  The activities and procedures required to cover the damages and restoring system capabilities and business integrity. This also includes taking measures to retain the customer and stakeholder confidence in the business.

2.3 CATEGORIZING THE SECURITY CONTROLS

- **Asset Management (Identify) –** This include properly inventoried of hardware, software, services and dataflow mapping. Cyber-security staff responsibilities and workflow should also be included in it.
- **Governance (Identify) –** This include organization informational flow and security. Internal roles and external information communication with legal and regulatory partners.
- **Risk Assessment (Identify) –** This includes all threat and vulnerabilities to be identifies and documented. These should include both external and internal threats, risks to prioritize and impact analysis.
- **Risk Management (Identify) -** This include the strategy and analysis to what extent the organization is tolerant to business integrity risks and critical infrastructure risk.
- **Access Control (Protect) –** Access control includes credentials, authorization, web access, data accessibility etc. The policies should always start from implicit deny and focusing allowing specific permission to individual depending on their roles and responsibilities. Network integrity can be maintained by segregating the network into integral parts.
- **Awareness & Training (Protect) –** The policy includes continuous education of users and awareness about the policies and procedures of organization, as well as their roles and responsibilities towards it. This not only includes implication of policies upon them but also the users and executives should be trained to protect, detect and report system risks and vulnerabilities to management.
- **Data Security (Protect) –** The data protection mechanism and location procedure should be mentioned. Data categorization is mandatory, also creating policies for its encryption and on-wire data protection. Data access authorizations and disposal methods and criteria should be well explained in the policies.
- **Protective technology (Protect) –** This includes policies against the removable media, and controlled access to SCADA and process systems and uses of limited services and across network.
- **Anomalies and Events (Detect) –** This includes policies for analyzing events and logs of cyber networks and SCADA systems to understand targeted attacks and threats. The policies can also involve routine audits, thresholds checks, and unauthorized applications present on network.
- **Security continuous monitoring (Detect) –** This involves continuous monitoring of assets through physical means and access logging. This includes policies to enforce permanent staff to monitor surveillance videos and logging access at all times. Procedures to run vulnerability scans, software vulnerability described by vendor and other external resources. Procedures to get information from

external service providers. Every anomaly detect should be documented so as to create future procedure and strategies. A continuous improvement is required in detection mechanism.

- **Mitigation (Respond) –** This includes policies and procedures needed to contain and eradicate impact in the case of an event. The roles and responsibilities should be defined in various aspects covering physical, system, network or process control exploit.
- **Response planning (Respond) –** Basic practices to be taken by every individual or person in case of any system comprises.
- **Impact analysis (Respond) –** System notifications are investigated, along with forensic investigation of impacted system. Exploited assets isolation from the system.
- **Recovery & Planning (Recover) –** Recovery included procedure for future from current experiences and putting up more proactive strategy to cover the leaks.
- **Business Integrity (Recover) –** These include procedure and policies to recover business integrity after impact and retain client, internal stake holder confidence on the system.

2.4 Implementation Tier And Profiling

The Tiers gives an understanding to management of the organization's cyber risk and methods to safeguard against it. The tiers are divided into four part , executives has to decide which level of risk management system they want to implement on their organization depending from awareness to highly advanced technical systems.

- **Tier 1** – Only risk and threat to business is analyzed but no further actions are planned on it.
- **Tier 2** – The strategy to mitigate in planned and procedures are developed but have not been implemented or approved across the organization. This can be due to the organization structure and multiple demographic locations.
- **Tier 3** – The policy and procedure is formally approved all across the organization. These are continuously provisioned and updated by the responsible authority.
- **Tier 4** – This is an adoptive tier, where the originations start creating policies from their previous policy enforcement experiences. This is achieved by using awareness programs and activities across organization such that individuals are encourage to identifying loopholes to the management.

Framework profiling is another aspect that describes an organizational alignment of current cyber risks and goals to targeted ones. This needs to be calculated such that the gaps can be filled with appropriate action, gauging technical resource and assets, funding and even changing the tasks prioritization.

2.5 CREATING AWARENESS & PERSONAL TRAINING

A decade ago, technology was a lot more different as it is today. The operating systems were considered the easiest prey from attackers view, and rightly so worms and viruses can very easily be transferred or penetrated to the systems due to lack administrative capabilities in the OS. But let's take a look at modern operating system like Windows 7; things have improved a lot it can take attacker days, months or even years to penetrate into the system. With features like firewall, memory randomization, minimum automated services and automated patching have made them more secure than ever. So where do we lack now? why we still get compromised because we have not invested on human operating system for the past few decades. 'Human Operating system' a new term, yes it is because human also store, process and transfer information. A simple demonstration of this will be how much organization's resources are spent on electronics and technical assets like firewalls, Antivirus, authentications, licensing etc. Though these are the quickest way to fix things but the weakest link is still human, that will take time as well as resources to secure.

Now before we start securing our people, we have to understand in detail what vulnerabilities they possess as machines can be programed and can give you the same outcome again and again which human cannot. We are creatures of habit as well, this can be seen in our work, and either it is technical or social anything. The behaviour of human is persistent what was centuries ago e.g. our risk of losing life in ocean is still be sharks but risk of losing life through a cyber-attack on electric/nuclear facility is still far from our thought.

2.6 SECURITY AWARENESS METRIC MODEL

Awareness has never worked in the past, as the organizations are more focused to retain the compliance but putting up annual PowerPoint security presentation. Also you have to admit that someone will always fall prey to these attacks like phishing or external media, even in one the high secure organisation the results indicate above 5 percent of negligence. The important aspect is the understanding of where your organization stands today.

- **Non-Existent**
  These organizations are very few in number who have not implemented any awareness techniques in the organization or the organizations that still have focus only on technical assets.

- **Compliance Focused**
  Most of the organizations are under this category, these organization do events and presentation annually, or sending email security email ones in while just to display their auditors about their compliance.

- **Promoting Awareness**
  A step forward and taking people as important security asset, organization that not just stop at maintaining compliance but also encourage user to participate through more interactive program and engage random individuals to come up and share their thoughts. Engage user to change password and limit web access etc. This involves scheduled seminars, newsletter posters in the organization.

- **Long-term Sustainment**
  Long term sustainment means developing a culture in an organization where everyone feels that security is their responsibility. It should not be considered as a burden neither by management nor users. The management introduces security for individuals not only in the organization but at home for their families and kids. This is becoming a more successful approach as the concept of BYOD (Bring your own devices) and work from home is becoming more in common. Planning on provide more visual content as well easily accessibility to training, includes video quizzes

- **Setting Metrics – Learning from Experience**
  Setting metrics, very few organizations have achieved it where they have started calculating the impact of security awareness and employee response. These can be achieved by using various phishing tools and calculating the percentage of user that still fall into it. Thus planning and prioritizing the upcoming event and training on it.

2.7 THREE KEY ELEMENTS OF TRAINING

2.7.1 Who

The training suite should never be the one size fit all in the organization. The customization is required because every employee does not have the same set of responsibility nor has the same access level. Attacks have also been targeted towards the individual it can be CEO or a regular sales or IT person; though the motive can be different for every attacker. Our trainings should also be customized for different staff type, this can vary from one business to another, some basic are described below.

- **Senior Management**
  They are first step of awareness in any organization, so other can follow their footprint. They are also the high value target and usually they always have one foot outside the organization in meetings, seminars, business events etc. because of the nature of job you are not always with them to protect their assets so they should be well trained to safeguard information at any given condition. Training like external media usage and remote access comes quite handy in these cases.

- **IT Staff**
  IT staff are usually the most privileged users in the organization, thus not be neglected though they have high technical skills remains more vulnerable than any other users. The basic training IT staff

should get is the information sharing , for example while working usually the code or configuration is shared on internet to get the solution which also open gates for the attacker.

- **Contractors / Guest**
  Contractors and guest are usually there for few hours, days or months but awareness towards the policy of the organization is mandatory. This should be scheduled seminar rather a brief description on couple of pages. This can include basic policy for external media, unauthorized use, the place you can go, access to internal network, internet web restrictions etc.

- **Non-technical staff**
  Non-technical staff some time does want the access to network just for their leisure purposes, such as access video and other social networking webs. These can have a few problems and it is difficult to directly impose something. Their development about security needs more grooming and thus need initial training and session on awareness.

- **Perimeter Security staff**
  These include security staff that secure the perimeter, should know about the unauthorized entry or activity they see near red zone etc. Trainings in case of breech or containing effect.

- **Process controller Engineers –** The systems are certainly different from the other organization system therefor require special training of staff to understand SCADA risks and potential threats.

- **Help Desk**
  They are generally inquired from outside for internal staff information and availability. The staff should be rained to detect suspicious attitude of the client, as well as method for authenticating users which calls from outside and want to know some general information about organization, but help them to use the information in their advantage.

2.7.2 What

"What" brings too many questions, what should be the content of the training? What are the priority security concerns to organization? The few guidelines are mentioned below.

- Do not put a lot of trainings in anyone plate, that is difficult to digest.
- What is the priority should come first to the employees.
- What are the goals you will achieve from the training?

The first step before discriminating them on their roles and responsibilities is to make them realize why they are a threat? Why they can be targeted? What is their importance to organization? (Once you start respecting your employee's integrity they will respect the organizations integrity as part of their own). Then comes the fundamental contents of training what you should be electing depending on the priorities. These are explained below.

2.7.2.1 Basic Security Awareness

- **Username and Passwords**
  Discourage the use of same password for multiple account especially between your professional, financial and personal accounts as increases the risk of getting compromised. Password managers can be used to manage passwords. The password length and complexity process needs to be explained to users. Users should also know about malwares that can silently work on user device and log key strokes.
- **Email Phishing**
  Emails are one of the powerful weapons of attacker as all formal communication governs by email today and hacker can take face of trusted entities. User should be trained to identify the email patterns and other characteristics like verifying the source domain name, URL verification, attachments etc. Also users should know whom to report in the case of suspicious email and before sharing their personal information with unknown user.
- **Browsing Awareness**
  This is the primary way for users to get information. Users should be informed about attacker techniques like malware hiding under different tools and software resulting in compromised browser also updating the browser plugin can save you from vulnerabilities. For example, checking the unknown website's rating before visiting it.
- **Social networking Awareness**
  Sometimes seems how easy to share your thoughts and information and getting to known the same about others. User should be made aware what information put them to risk and how attackers use those information to gain their trust.
- **Data Security**
  How to handle sensitive information, always transfer or save information that are trusted and authorized by your organization. User should be aware of value of sensitive data and the ways to store it based on criticality. This can include methods of encryption and file sharing access.
- **Wireless connectivity**
  Train users to prefer connectivity of on secure Wi-Fi network, this include pre-shared authentication and wireless standards like WPA and WPA2.
- **Remote Access**
  User should be trained to on how to connect remotely and they should not auto save the credentials for connecting. Similarly the user should only connect from devices authorized by the organization. The uses of those devices are strictly forbidden by any other person or family member.
- **Help Desk Awareness**
  Helps desk employees should consider it as a nerve center of organization and any information they have is very critical for organization. Tannings and session should be arranged on how an attacker can benefit from their helping attitude and gain access to potential information.

2.7.2.2 SCADA Awareness

- **Network Access**
  Users should be made aware of how an internet accessible system can be used by applying few queries locating mapped ERIPP and SHODAN and how a malware can travel vertically in the system as well as on routable paths too.
- **Interconnects**
  Awareness about application that interconnect our system can be exploited to gain access of plant and other systems. The training can also include remote connection either through dial-up to ICS or other cyber systems.
- **System Management**
  Training people how important it is to cover exploits; vulnerability in software discovered yesterday if not patch on time can be exploited in minimal time. Same goes with out of date antivirus, IDS/IDP signatures**.**
- **Governance**
  It is sometimes the policies that let management escape elements from cyber threat and are then exploited by the hacker. Management and executive should be trained how to develop a procedure to identify the critical element and their categorization.
- **Social Engineering**
  People need to be trained about the selective information they should provide to outside third party vendors, as well as vendors should be bound by agreement to keep the information confidential.
- **Cyber Actors**
  Awareness on who hacker and what they can achieve from exploiting the SCADA system. These should be well categorized like national threats, political threats, kiddy scripts, and internal threats.

2.7.3 How

How represent the part of delivering the information to users. No matter how strong your content is, if you do not have the right tools and techniques to deliver it will never work for you. Same is the issue in cyber security trainings; nobody wants to become a student once they join the industry. Their priority becomes different; the only way to work with them is to align their goal with yours.

For example, if you try to teach them why secure password restricted web access is important at office premises they will try to discard your information as these does not matter in what they are here to achieve. But if the subject is defined as how necessary is for them to secure their multiple account and privacy information before being compromised financially or for extortion. How unsafe are their family member at home when they access a phishing website. The information you will provide will remain the same in both context but their way of looking and accepting it will be quite different.

The few basic guidelines used by industry professional are mentioned below:

- Never force your staff to get trained, rather engage them in the program.

- The communication should always be bi-directional, bringing up experiences from your life and theirs will keep the interest realizing them the extent of vulnerability.
- Security is same in every aspect be it either professional or personal life.
- Do not let them think that they have to change the behaviour, when entering office premises as the work ethics have changed a lot with the concept of BYOD(Bring your own Devices) and work from home. Making them understand the importance of patching and regular security updates.
- People are busy .Scheduling sometime make life difficult for staff to participate, but if you use other method so they can learn at their own time is very flexible and achievable. We will discuss the tools in the later section.
- Acknowledgments and appreciating staff always motivates the passive users to participate. Discovery of new vulnerability by a user should be acknowledged. Similarly, user mistakes should kept down so they don't get discourage.

This section also needs a discussion on tool and interactive application for knowledge and trainings.

- **Seminars**
  These will give an interaction platform with the employees. The information shared on these platforms should be the first hand experiences and activities that will make the security training course interesting for them.
- **Video/Webcasts**
  Video and webcast provides users the flexibility to gain knowledge at their own time and place. This also gives trainer the leverage to use the same video with different audio language in different regions. A minute video each day can be very effective and less time consuming to convey your message and realizing them each day how important the security is for organisation.
- **Quiz, Bookmarking**
  Quiz provides user an experience of how secure they are, as well as provide you with stats about the organization security. Bookmark a rather old concept but can also help user in resuming the training later if they have other important tasks to do.
- **Newsletter**
  A step towards awareness on day to day new threat, risks and breaches around the world.
- **Screensavers & Posters**
  These are good important to guide users in their routine task. A poster near equipment disposer will always realize user than they have taken proper measure to destroy the information on that equipment.
- **Dashboards**
  A very important operational tool to explain user the current threats organization is facing. For example, a phishing email from a fake airline company show up in your organization, similarly other virus and malware.

2.8 Continuous Learning Program

Training content should be should be reviewed every six months or at least annually. A year can bring lots of changes in attacks, compliance and technology variations. The users should be updated with new trends and technology. A framework for measuring the impact of awareness program will help develop future training and loopholes that are still needed to be covered. Come up with a plan for each year based on last year experiences and identify each topic you want to focus for each quarter. This should be well aligned where you want to see your organization in next 5 year. Bring up a chat and share it with users and management so they can find themselves in it and their achievement. Remember security is not your job it is a collective effort.

3 Industrial network architecture

The high level architecture of today's industries looks much the same when this one way delivery system was developed. Communication system supported the development of control systems providing extensive control and monitoring capabilities as well as precise transmissions.

For example, in power utilities the concept of teleportation has enhanced the scope and visibility in detecting power outages at customer premises, thus does not require relying on customer feedback.

3.1 INDUSTRIAL NETWORK STANDARDS

The network should be based upon well-known communication standards. The equipment to be considered should comply with industry open standards such that multivendor environment is appreciated as to reduce the network cost in future. The equipment and technology should be modular to step up for future network demands. NIST standards can also be used comply with basic communication standards.

3.1.1 Internet Protocol (IP):

Almost every communication in the SCADA has been progressed to IP, irrespective of physical and logical connections. In the past where serial connectivity was used, it has now been relayed over IP networks with emerging support from application as well.

3.1.2 Legacy Protocol and Multiprotocol Label Switching:

In our system we still need the legacy protocols that are unsupported on IP infrastructure and other encapsulation mechanism. There we need a multiprotocol suite that can carry our real-time data over IP as every other communications. MPLS is also widely used for closed service groups of application and endpoint apps. The other feature involves fast recovery, security robustness and QoS capability for delivery of real time service for endpoints.

Examples can be seen in the case of RTU or real time data delivery where organizations prefer to migrate on IP but remain consistent with system integration.

3.1.3 Network Performance:

SCADA systems are considered critical for network performance, this implies to end-to-end delay for network traffic carried over common network infrastructure.

For example, applications like CCTV, SCADA have their individual and diversified requirement for delay, priority and data rate on link.

3.1.4 Network Reliability:

Operation and service reliability is no way a degradation factor for any SCADA system. The reliability of SCADA system is so critical in comparison to business networks (99.96% annual uptime) against 99.99999%. This can also be interpreted as 210 minutes to 5 minute of downtime annually. This can be achieved by 'n-level' redundancy starting from nodes to links.

For example, the devices are specially designed by vendors like CISCO such that there is no moving object (like fans) and can sustain extreme temperature and other environment factors.

3.1.5 Network Security:

Operation security holds a paramount importance and many time consider as a national critical asset. The security should be well designed as to cover all aspect from hardware to software. The design should allow isolation of services from corporate environment and restricted access.

3.1.6 Scalability:

The network scalability involves minimal physical changes for the deployment or extension of new and old application services. The key feature involves capacity management and visibility after next 5 to 7 years. As laying these infrastructures require a lot more cost then enterprise infrastructure.

3.1.7 Efficient Routing and Aggregation

The use of IP gives us the leverage for increasing the efficiency and optimal route path selection for every application between core and endpoints. It needs to be consider for optimal fast rerouting, complete network awareness at core and minimizings convergence time in case of failure.

3.1.8 Secure and Unified Network Management:

The expected explosive growth in the volume of data collected in the Smart Grid for use by a large number of applications requires implementation of data management systems that are secure, that provide low delays when the data is accessed, and that provide data privacy based on utility security policies.

To provide a unified end to-end network management solution for network provisioning and configuration, troubleshooting and alarm correlation, maintenance workforce dispatch and management, capacity management, and network security, it is advisable for utilities to deploy operations support systems (OSSs) that will work with the element management systems from multiple vendors. Where possible, these OSSs should ideally also integrate with the utility’s grid operations and management, asset management, and financial systems.

An industrial network shares many similarities to enterprise networks; such as in wireless and wired networks. There are several dissimilarities as well; utilities are required to pass real-time data on the network. This prioritizes the data availability in place of integrity and confidentiality. The protocols also require changing their behaviour to UDP.

Though enterprise and industrial systems are both based on IP and secure is a major concern for both of them, but we keep both SCADA and corporate network completely isolated from each other.

3.2 NETWORK ARCHITECTURE BY FUNCTIONS

3.2.1 COMMON TOPOLOGIES:

The utility system utilizes a variety of topologies to gain maximum advantage and efficiency in the network. The industrial networks are usually distributed in nature varying due to protocols and link layer (underlay) characteristics. The use case of different topologies is explained below.

- Ring topologies are efficient in the case of high availability and fault tolerance, where multiple rings can be created for high availability within the substation layer 2 networks.
- Bus networks are high regarded in synchronous communications where have limited bandwidth and communication is mostly best effort. For example, the coordinated communication can be between pump, indicator, and fire alarm as each has a synchronized time for passing the signals.
- A point to multipoint topology or in other words a star network can be used to communicate between different sensors while simultaneously reporting it to historian and HMI.
- Figure needed-
- Mesh and wireless mesh are technologies used in WAN circuit as well as Field Area networks (FANs). We will be discussing these networks in detail later in this chapter.
- A multi or dual homed network provide a point of sharing information between two completely isolated networks, these usually happed at servers in internal DMZ where data could be accessed or moved from more to less secure networks.

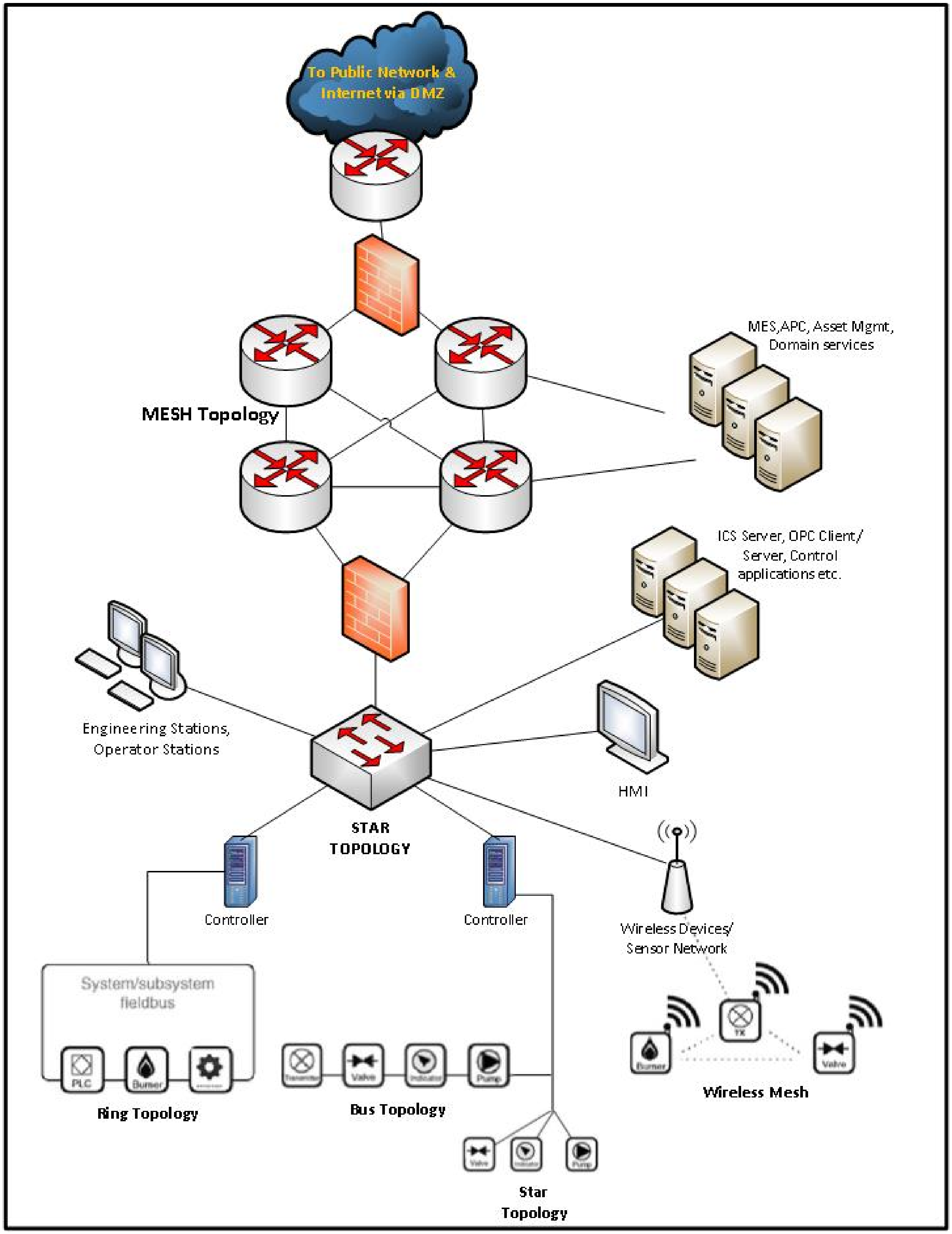

To Public Network & Internet via DMZ
MES,APC, Asset Mgmt, Domain services
MESH Topology
ICS Server, OPC Client/ Server, Control applications etc.
Engineering Stations, Operator Stations
HMI
STAR TOPOLOGY
Controller
Controller
Wireless Devices/ Sensor Network
System/subsystem fieldbus
PLC
Burner
Ring Topology
Transmitter
Valve
Indicator
Pump
Bus Topology
Valve
Indicator
Pump
Star Topology
TX
Burner
Valve
Wireless Mesh

Figure 2 – Common Topology Layout

3.2.2 Core Edge Architecture

We consider an application centric approach for developing communication architecture of any utility. A network of this set of attribute is required to be built for the applications deployed in modern utilities. We consider wide area network as a part of core, where Field Area Network is being used by the endpoints to relay their information over the WAN.

As of now, IP is the protocol used for this purpose and all application & legacy applications are supported by MPLS framework. MPLS is an underlay for new applications with minimum or no changes required in the physical network. A utility core resides in the head office or service area of data and control centers. All other elements like substations are connected with core through the wired medium like optical fibre. The other distributed services can use wireless access and other radio stations to communicate with the core. The figure illustrates a bit about architecture of high level design.

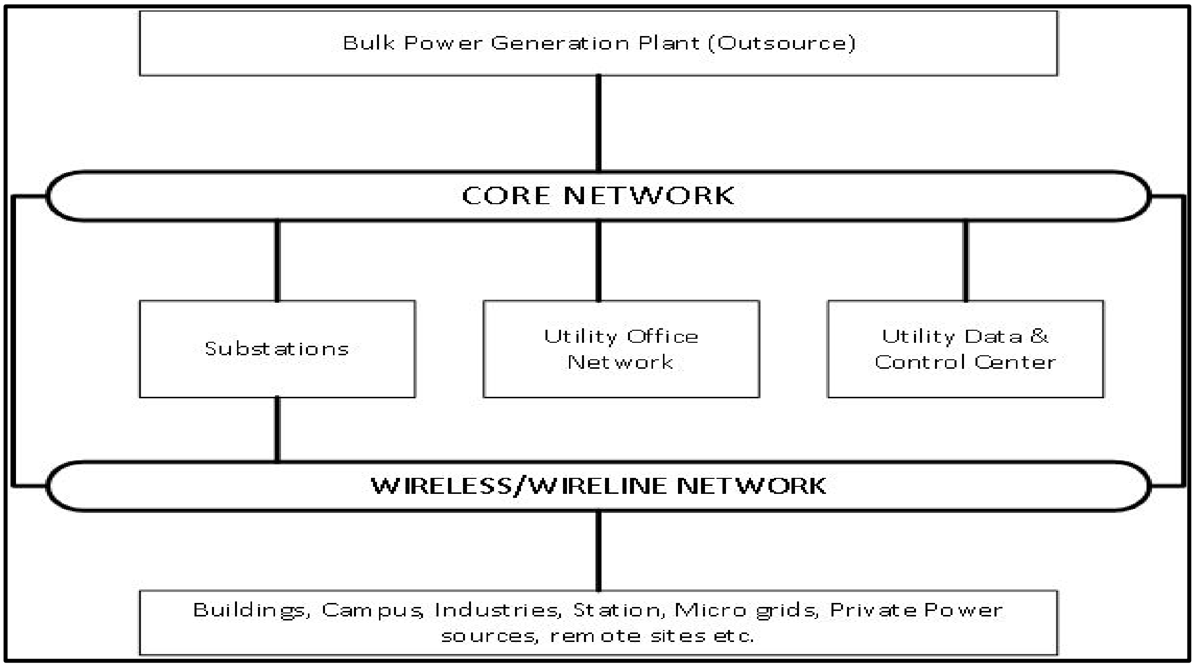

Bulk Power Generation Plant (Outsource)
CORE NETWORK
Substations
Utility Office Network
Utility Data & Control Center
WIRELESS/WIRELINE NETWORK
Buildings, Campus, Industries, Station, Micro grids, Private Power sources, remote sites etc.

Figure 3 – Core Edge Arcitecture

3.2.3 Wide Area Network (WAN)

The wide area network involves the following step of deployment.

- When installing new equipment, use the recommended equipment with to location and circumstances. Before installing the new equipment always installs the firmware recommend by the company.
- Recheck the IP schemes before bring the equipment into production environment, as a mistake can bring routing loops and other disruption to utility WAN network.
- Interior gateway protocol such as OSPF or ISIS can be used across the WAN architecture to WAN routers, whereas cluster routers can run BGP on the edges as well.

- When setting the route preference always consider the media between the sites as. As WAN architecture can have different links from wireless to optical fiber. The traditional technologies and protocol should also be considered.
- Layer 2 QoS should be configured on the links to keeps the real-time traffic at priority.
- When implementing MPLS over the network WAN router will be the Provider Edge (PE) routers whereas interior router should be configured as Provider (P) routers. The cluster router are to be considered as Customer Edge (CE routers). Features like traffic engineering and fast rerouting should be used to make use of the protocol suite and increased reliability.
- A firewall or unified threat management should be applied in line between WAN routers and cluster routers if the services are not integrated in the routers.
- Any router or other network equipment deployed at a substation location should be "utility-grade" network equipment that comply with the IEEE 1613 [1613-09] and IEC 61850 [61850-01-10]. Further, these network elements at the DCC as well as at substations should provide for dual power supplies, switching fabric, interface cards, and other component redundancy as appropriate. Hitless product upgrade may also be considered, particularly for the network elements at the DCC and many substations. These network element functions should be included in the network design in every phase as well as in the final phase design. Their inclusion in the design inputs will affect not only the network costs but also the reliability design. (Communication Networks for Smart Grids - Making Smart Grid Real, 2014)

3.2.3.1 Network Traffic Flow

- The data between endpoint will flow through the cluster router at that location. The cluster router will communicate with each other on separate link that exist only between them, not through the connected WAN routers.
- In the case of collocated cluster routers and WAN routers that traffic between the endpoint will pass through Local Area Network connecting Cluster and WAN routers.
- The Cluster router can also perform the role of router aggregation if multiple location exist in the vicinity. Therefore IP scheme should be used accordingly.
- With special cases like AMI or DA the network traffic will be aggregated and pass through the Data concentrators.
- The cluster routers not connected to aggregated cluster router can connect to WAN routers over respective Field area networks.
- The Field area networks should be treated as point-to-point links when connected to WAN, the technologies can be wired or wireless medium. The other circumstance can exist but should be considered unique in their case.
  - VPRN services can be used for Point-to-point connections, as in the case of AMI data concentrator.
  - For wireless connection a network service provider based LTE service can be used to make connection to the WAN routers collocated at service provider location.
- Configure L1 and L2 MPLS services between the endpoint pairs for legacy connections that must be maintained based on utility requirements for continuing such connectivity beyond the planning

horizon. Legacy should be replaced as soon as possible if the cost effective and reliability is no longer a factor.

- The target network provides an end-to-end IP connection between the endpoints traversing through multiple point-to-point connections. Thus, the connections between the PMU, IED, and CCTV camera at substation A with, respectively, the WASA&C, SCADA master control, and security management servers in the DCC go through the substation LANs, the CR at the substation, connecting WR, zero or more WRs and IRs, the WR at DCC, and the CR at DCC. The connection between the wind farm DG and the IED over the utility-owned LTE network goes through the end and the EPC elements including the PDN-GW. (Communication Networks for Smart Grids - Making Smart Grid Real, 2014)
- The use of VPRN in MPLS is great advantage apart from legacy connection, as separate IP network can be deployed on top of it to connect multiple endpoints. In term of security closed user group can be created by using the technology.
- Network service provider MPLS VPRN solution can be used to extend the communication and bringing redundancy over the utility owned infrastructure.

3.2.4 Field Area Network (FAN)

Utilities in today's network extend their visibility to monitor every device on the networks well as are able to access and control them. They can range from station power management, generation to distribution switches and have user meters. For this purpose they need a network that is flexible, scalable and providing the security. Utilities consider these networks a field network commonly called 'Field Area network'. These networks accumulate a variety of topologies and mediums to communicate on legacy infrastructure and new technologies.

3.2.4.1 Solution Components

- 802.16e/Wimax
- LTE
- Light Radio
- Copper and Fibre
- Communication over Power line

3.2.4.2 Architecture Capabilities

- High Availability
- Network Security
- Stand-based integration
- Legacy equipment support
- Ease of operation & Visibility
- Unified communication over FAN
- Application based

3.2.4.3 Components of communication networks

- ***DA gateway***
  This can be a standalone device connected through the serial interface or through the Ethernet providing network service Field device; the communication can be wireless medium using various wireless technologies.

- ***Field Area router (FAR)***
  It is used aggregation device collection network traffic from RTUs and field based PLCs connected in mesh topology. All services provided by field edge router are IP based.

- ***Substation Automation Router (SAR)***
  The substation router aggregates IP traffic from multiple substations providing rich set of IP services

- ***Head end Router (HER)***
  Communication with Control center applications and aggregated traffic from different substations and different IP networks.

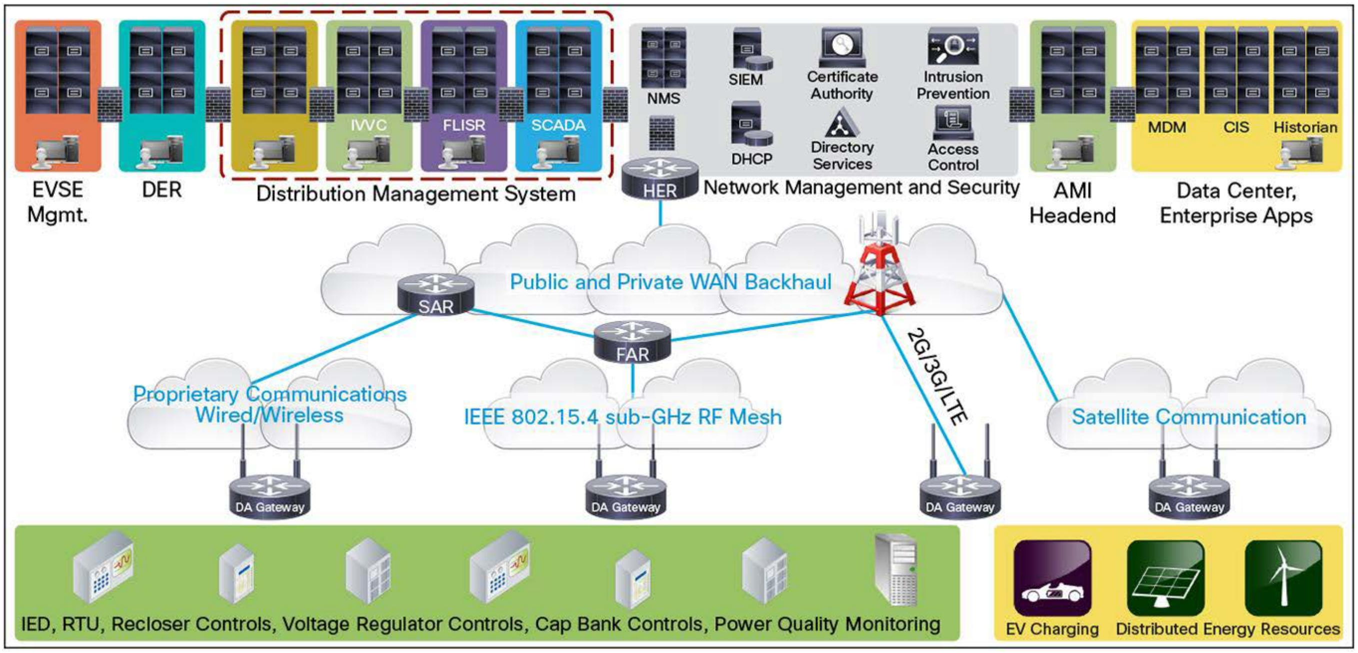

EVSE Mgmt.
DER
IVVC
FLISR
SCADA
Distribution Management System
NMS
SIEM
Certificate Authority
Intrusion Prevention
DHCP
Directory Services
Access Control
HER
Network Management and Security
AMI Headend
MDM
CIS
Historian
Data Center, Enterprise Apps
Public and Private WAN Backhaul
SAR
FAR
2G/3G/LTE
Proprietary Communications Wired/Wireless
IEEE 802.15.4 sub-GHz RF Mesh
Satellite Communication
DA Gateway
DA Gateway
DA Gateway
DA Gateway
IED, RTU, Recloser Controls, Voltage Regulator Controls, Cap Bank Controls, Power Quality Monitoring
EV Charging
Distributed Energy Resources

Figure 4 – Field Area Networks (Communication Networks for Smart Grids - Making Smart Grid Real, 2014)

3.3 Network Segmentation

The term 'segmentation' means allowing access but with controlled and granular level of communication on the network. Network segment brings the concept of cyber security and limiting resource access by building design that brings security within itself. A traditional segmentation occurs at layer 3 by breaking the broadcast domain or virtualizing the larger broadcast into smaller by added tags to it.

In today's world how segmentation applies to industrial networks. It starts in the same layered manner down from physical layer where we introduce 'Air gap'. It is important to understand the concept of segregation, which means complete isolation. For example in the case of VLANs it is considered as network segmentation because they are virtually separate but the hardware resource is still shared. VLANs can be segregated at layer 3 where router separates the broadcast domain. Another point of explaining network segmentation for utility is the separation of endpoints across distinct network.

We will be going through the zones later in our discussion, while designing network segmentation should be supported where possible with the zone. Few examples are given below;

- Public network (Internet)
- Operation network
- Process network
- Control network
- Plant network

3.3.1 Communication Flow Control

- **Absolute** – Complete isolation, both flows are completely denied.
- **Conditional** – Exceptional traffic is allowed, by filtering and policy control.
- **Bidirectional** – Communication is enforced in both directions.
- **Unidirectional** – Traffic allowed in only one direction.

3.3.2 Layered Segmentation

- **Physical layer** – Preventing data transfer in the event of change or disruption of physical medium between separate networks. Attacks such as 'Sneaker Nets' can bypass the physical medium as well as restricted access on network to user sometimes provoke them to use thumb drives to carry data over other medium.
- **Data link layer** – VLAN is deployed at layer 2 to separate broadcast domain and later 3 devices (layer 3) are placed in the network for providing controlled communication between them. The improper implementation of VLANs can create vulnerabilities like VLAN hopping etc.
- **Layer 3 segmentation** – Several devices exist at network layer such as router and firewall. These utilize protocols such as IP and perform many operations from access control list, encapsulation and multilayer protocol support. The addressing need to be well defined and structured to create proper flow and security structure across organization. A well-defined Access control list at this layer all reduces the risk surface to application which minimizes target attacks to session hijacking attacks.

- **Upper layer segmentation -** All network traffic that is carried over IP is considered in upper layer, these include contents, session and applications. Application aware IPS could be used for content filtering and anomaly filtration; in-line and offline IDS can be used to monitor traffic anomalies various ways such as based on application, protocols, session or flow.

3.3.3 The principle of least route

The principle is to allow each individual the least access path such that it can only fulfil its function. It is important to know the concept of 'purpose built networks' that is any unused or unidentified path should be blocked by access control lists or by null route to destination.

We can also introduce the concept of source routing where specific nodes from the group has better route availability than others.

3.3.4 Wireless Networks

Wireless network are considered as unsafe and insecure as compared to wired networks because of its physical containment, as it can be accessed by any physical receiver of same type. It is possible to block transmission by using jammers or signal absorbing equipment like 'Faraday Containment' but the cost is still very high for implementation.

The new protocols have evolved industrial communication system like one wireless and wireless HART using HART common protocol on 802.15 radio or ISA 100.11 on wireless IEEE a/b/g/n/ac; transporting utility protocols like ANP3, goose messages and 61850.

Long range wireless network are also used communicate with devices and utilized for remote areas that lack telecommunication infrastructure and for reliability purpose as secondary links.

3.3.5 Remote Access

Remote access is one necessary evil requirement of any industrial communication today. The reason can vary from 24x7 supports for SCADA systems as third party assistance to remote access to engineering system that are distant and requires time to access physically. Following are the security controls that is to imply when introducing the remote access in utility.

- Dual authentication
- Single path availability for remote access
- Allow least privilege to user as compare to regular privileges.
- Define role and time based access
- Remote access device in DMZ.
- No split tunnelling
- Encapsulation and encryption
- Providing jump station a landing point for remote connection
- Strong credentials
- Non scripted connections
- Logging and monitoring

3.4 PROTOCOLS

Industrial protocols are most about real-time communication, initially designed to work on very low bandwidth on serial connection (from 9.6kbps to 83.4kbps) but with time have transformed to work with IP/TCP based communication network. The most widely used protocol is UDP to relay real-time data.

The industrial protocols were segregated into two types; one connecting the process end device (sensor) and basic control devices as well as some supervisory device where the other protocols were focused on communication between higher supervisory systems and system to system communication.

3.4.1 Field Bus protocols

3.4.1.1 DNP3

Distributed Network Protocol is a set of communication protocol for process automation systems. Unlike other field bus protocols its purpose to provide a communication between SCADA master station to remote terminal unit, endpoints and intelligent electronic devices. Initially the protocol was designed to be very reliable in terms of their predecessor as Modbus but was potentially design for security.

Much work has been done on this protocol introducing service authentication, encryption on serial and VPN connections.DNP3 works on layer 2 providing multiplexing, defragmentation, error checking link control prioritization. Major feature includes characteristics from upper layer and applications.

3.4.1.2 IEC 61850

A protocol especially designed for power grids substation automation. The structure of this protocol is very new rather mapped on some other protocols like MMS (Manufacturing Message Specification), Goose messages, Simple measured values (SMV) etc. The protocols have good reputation for latency with response time less than 4 milliseconds for protective relay and work on TCP.

3.4.2 Backend protocol

3.4.2.1 OPC

It is a major backend protocol providing integration at higher level between systems and subsystems, whereas fieldbus protocol was designed to carry low level data from PLCs & RTUs. The idea was to provide a platform through protocol independent of vendor protocol underneath. This was extracted from Microsoft where integration capability is provided to different vendor by building a protocol that can communicate with their software and hardware.

The OP follows a client server model where the client initiates a process which triggers the application on remote server that will execute the code in it using remote procedure call. Once the process is completed on the server the processed data will be sent back to the client.

Since the protocol requires it to be merged with the ICS framework, creates a lot of security concern; some major issues are mentioned below

- Legacy authentication - The protocol is designed to support legacy application and devices on network. Some of these support unauthenticated services such as on earlier NT systems resulting in vulnerability waiting to be exploited.
- RPC vulnerability - The protocol itself uses RPC for communication there inherits all vulnerabilities from RPC. This could result in remote code processing and other bot attacks.
- Unnecessary ports and services - The vast spectrum of this protocol allows it to support non IP protocols such as NetBIOS, hence firewalls and devices needs to be tuned to make these services available.
- OPC server integrity - A fake server can be created and make communicated with the other devices on the network creating disruption of services.

3.4.2.2 Intercontrol Center communication protocol

The protocol is also known as IEC60870 or ICCP protocol designed especially for energy sector organization for bidirectional communication on WAN links between control center, substations, remote stations and other utility facilities.

The ICCP utilizes the client server model where server has all the data &functions and clients requests from the server. Communication between them is also on TCP, most often these protocol and application are provided on the gateway hardware specially designed for these hardware. It is primarily a unidirectional protocol but the function can be switched between control center and a substations therefor in most cases bidirectional communication is used. The security concern are present in ICCP protocol, we will discuss the major concern down below.

- Lack of authentication & encryption - the protocol does not have its own mechanism for authentication or encryption rather replies on the layers beneath to facilitate with the services
- Trust relationship - The explicitly defined relationships could end up exchanging table with the rogue devices
- Accessibility - The protocol is used on WAN therefore the threat vector is quiet high because of its convergence with the internet. At any point of misconfiguration the result can be a breach or an attack such as DoS

4 Threats & Vulnerabilities

Industrial control systems are built to cater large scale operation of continuous manufacturing, production and facilitation. Modern industrial systems are gaining access and control. Each day the new system in energy is gaining access to the internet of things, where new contributors are joining hands with traditional system. In the case power grid or smart energy more private energy contributors are connecting each day providing energy through hydro plants, solar panels or wind turbines. The power becoming decentralized and infrastructure is a part of service delivery. The control system network can have a high impact in the case of a successive network penetration. In this chapter we will discuss more about types of attacks, threat vector and few of their examples as well.

4.1 INCIDENT CHARACTERIZATION

- **Modification in system, OS or application configuration**
  These modifications include any changes made to the system that suppress its behaviour or activity in case of alarm or operational task.

- **Modification on RTUs and PLCs**
  A malfunction of PLCs or RTU can happen though the devices are hardcoded but behaviour can be manipulated in decision making.

- **Misinformation in operations**
  The impact can happen in the form of wrong reports sent to operator for decision making. This can be used to sabotage the utility or hide a malicious code itself.

- **Safety and control manipulation**
  Modification is made to safety and control systems in this case when a threshold for activity is achieved, the safety procedure are unable to perform operation thus can result in disastrous consequences.

- **Malware**
  Malware can infect system and can be used by attacker as RAT (Remote Access Tool) to access utility and more command can be implemented to destroy or gain access of the system.

- **Information Leakages**
  Information can be financial or facility designs or chemical compositions that can have impact on company and as well on countries too. Example can be design tasks from nuclear facility.

- **Information Variation**

A slight variation in information can have significant impact in large utilities financially and with reputation.

4.1.1 Difference between Safety & Security Systems

Safety system does have their significant in the system but cannot comply the role of industrial network security. SANDIA National laboratories performed a simulation to justify their point simply creating a man-in-the-middle attack, which can change the values between valves similarly a modest attack on industrial control system front processor in bulk electric facility can prove to be a major loss.

VIKING (Virtual Infrastructure and Control System Management) is currently investigating threats on automatic generation control. System within the electric power network responsibilities for adjusting the power output of multiple power generator with respect to the demands. It is an automated process maintaining the inputs and output threshold maintained, researchers manipulated the input data resulting in loops and disturbance in the whole system.

Thus, it is important to understand that safety & network security are completely isolated domain in cyber security. A safety system can be altered through a communication network.

4.2 ATTACK VECTORS

4.2.1 - Access Control System

- These include access cards, closed circuit television (CCTV), Building Management System (BMS) and vendor portal.
- The attacks include RFID spoofing, exploiting the BMS patching or using unauthorized IDs.
- The result can be an unapproved access, loss of surveillance or additional access to ICS system.

4.2.2 - Analyzer/Management System

- Remote system for maintenance or utility network. They can also be vendors system working remotely.
- Improper implementation of OPC (Common protocol) or remote VPN access breaches due to maintenance or an unpatched application.
- Production loss or facility wide infection, control loss etc.

4.2.3 Application Server

- Remote interactive session, plant networks, business integration systems and software vendor portals.
- Vendor software, unpatched apps, OPC insecure implementation, database injections and hijacking the interactive sessions.
- Results can be credential or information loss, unauthorized user access, or plant operation suspension.

4.2.4 Asset Management System

- These include database involved in plant operation and maintain user and inventor. Also in this new era they are managing the mobile device information their logs and reports.
- Reason can include unpatched application, malware installation on mobile devices which exploit the vulnerabilities of database, remote communication session etc.
- Loss in business, financial or production data. A possible alteration of data in database. Unauthorized access etc.

4.2.5 Controller (PLC)

- Attacks vectors can an engineering workstation, operator Human machine interface, unapproved devices, USB or external medium, controller network.
- The reason can be traditional attack like replay attacks, DoS buffer overflow, a protocol vulnerability, insecure communication, exploiting functional capability of protocols or any network asset
- Loss can be in the form of manipulation of data or utility operation shutdown or suspension.

4.2.6 Historian

- Business network integrated with the utility, ERP system communication with data server, Remote access, data base communication.
- Reason can be unpatched application, malware on invalidated vendor firmware, excessive access through firewall, or insecure unencrypted communication, unauthenticated communication.
- The loss can be the manipulated batch or process records, credential theft, generation of unreliable reports for business and ICS systems.

4.2.7 Directory Services

- This includes file sharing, LDAP or any other authentications, printing spooler, remote access, back or replication, vendor support service etc.
- Attacks can include DNS spoofing, NTP replication, firewall exploitation by vulnerability detection, unpatched application, unencrypted communication, unauthenticated devices.
- Losses can include communication impact through DNS, authentication disruption through LDAP, NTP and credential hacking. Malware distribution and unauthorized access are another two thing that can expand quickly.

4.2.8 Engineering Workstations

- Engineering application and tools, client applications, external media etc.
- Reasons can be unpatched application, expose trusted connections, ICs applications, vendors firmware and malwares.

- Result can be utility sabotage, work delay, manipulation in graphical results, alarms and other critical systems.

4.2.9 Perimeter protection (Firewall/IPS)

- Perimeter include trust boundaries and connection business and control units, updating of rule, policies, user accounts, untested, unverified patches and management controls, credential reapplication across network.
- The impact can be gaining of unauthorized access across network, bypassing zone restriction, credential theft, multiple security point comprised by exploit one endpoint etc.

4.2.10 SCADA servers

- Non-SCADA client applications, Application integration communication channels, Data historian, Engineering Workstation, Control network, Software vendor support portal
- Reason can be unpatched application, malware on invalidated vendor firmware, excessive access through firewall, or insecure unencrypted communication, unauthenticated communication.
- Plant upset / shutdown, Delay plant start-up, Mechanical damage / sabotage, unapproved operation of operator graphics, untimely process actions, manipulation in ICS database, critical status, alarms, and operation disruption of ICs devices.

4.2.11 Telecommunications systems

- Device facing internet or visibility or access through public platform.
- Expose of public and private keys or connections. An unrecognized public connection inside the organization, fake or unapproved access points, non-regulated network boundaries. Remote access from vulnerable device or unapproved mobile devices or unpatched hardware firmware.
- The other attacks vectors are safety systems, BMS (Building Management Systems), operator HMI, ICS operators, plant operators, uninterrupted power system, patch management etc.

4.3 COMMON ATTACK METHODOLOGIES

The major reason for any attack is the insecure communication protocol and delicate authentication and communication stack on devices. Once the malware is in the system, tools such as ‘metasploit’ and ‘meterpreter shell’ are used to gain remote control of that infected host, other tools like key logger or injectors can be used to cater data and manipulate industrial controls.

The other methods include resonance to gain information about the system and use the basic knowledge for exploiting. Once access a persistence scheme is used to spread the control over the SCADA and corporate infrastructure or assets. Sometimes these can be used to launch a secondary attack on other connected systems.

The attack can be a compromise which means making a piece of code (malware) or equip capable of performing. An attack can be a statement to target for performing certain action. Similarly system can be exploited by functionality or by vulnerability. For example issuing a 'shutdown' command cannot be considered a weakness in functionality but an application path or authentication loophole give user privilege to inject shutdown code (Malware) that will be considered vulnerability. Several attacks have been identified until now; we will discuss some them in detail here.

4.3.1 Man-in-the-Middle

The attack is carried by snooping the network traffic between the two communicating traffic, thus the attacker connects to both devices pretends to be an original communicator and relay the communication between them. This can happen more easily in industrial processes as not all equipment communication is encrypted or any authentication mechanisms used.

4.3.2 Denial of Service

DoS attacks are famous creating open session and making service unavailable by consuming system resources. This way illegitimate request makes suffer the legitimate requests thus sometime making service unavailable or crashing the application server. Industrial systems the impact can be of significant value as the control process that operates on real time data which not only requires availability but in timely manner. Thus it can bring system offline as safety equipment will trigger or complete system shutdown can happen.

In the case of power grid if an HMI loses service availability or control over a single RTU due to inconsistency or DoS. Attacks like this can lead to 'Loss of View' a critical condition to put the operation halted.

4.3.3 Reply Attacks

The information in this type of attack is sniffer reported and then the network packets are either used maliciously or with some alteration. The ICS traffic is captured from the field, and then these packets can be used to command the field devices or to send erroneous report to master station which can push them to take inappropriate decisions. In other cases if the authentication messages are logged in symmetric encryption. These can be authenticating unapproved devices on the network.

The goal of sabotaging the plant can so easily be implemented just by resending the same messages or altering it with few bits of code. As explained by Ralph Lager at 2011 Approved System Cyber Security conference by injecting 16 bit of code in front of existing logic resulting in an endless loop preventing the remaining logic.

4.3.4 Compromising the HMI

Compromising the HMI can be sometimes much simpler than Man-in-the-Middle or Replay attack. Controlling the device through the HMI console interface can be exploited by compromising the host attached. Once the host is compromised, software like Metasploit is used to find vulnerabilities where Meterpreter can be used to install a VNC code for remote Access. This gives the complete view of the system to hacker.

4.3.5 Blended Attacks

Most attacks are now very sophisticated adapting to environment changing states by following blended threat model. Another aspect is the attack vector that is covered in blended attacks carrying multiple types of malware increase the attack severity. The first in its kind that was discovered was Stuxnet but other version has also be seen like Sky wipe (Flame) which involves complex algorithm and designs.

4.4 Examples of Cyber Attacks

We are now seeing more attack on ICS today as the myth of control being completely safe by isolation no longer acceptable. The first documented cyber-attack was of Stuxnet on ICS in 2010. Since then a new chain of attacks has been reported. The high profile target were more energy and power companies where the investments and loses are far greater and critical. Stuxnet was just the beginning of the sabotage attack followed by Shamoon, Flame and Dragon Fly.

4.4.1 STUXNET

A poster-child for malware industry, a well-equipped malware is capable to infect ICS and was in operation since early 2007. It removed any doubts about the security of our industrial systems by the use of sophisticated threat actor commonly known as advanced persistent threat.

Stuxnet was equipped with multiple zero day attacks covering multiple generation of windows platform from Windows 2000 to windows 7 and windows server 2008. The target was not only server but Siemens devices like SIMTAC, WinCC and PC7 along with S& PLC device and communication protocol like PROFIBUS. These devices were operational in enrichment of uranium through centrifuge.

The main capabilities of Stuxnet are mentioned below:

- Capable to infect windows based systems through zero-day attacks, and used built-in tool such as rootkit and using captured certificates from network.
- Capable to bypass anomaly and host packet inspection by using trusted process and inject its DLLs to them.
- Perform changes in DLLs of trusted processes apart from inserting the new DLLs.
- Always scans the connected and operating system capabilities, the scans for the antivirus and other security application installed on the other host.
- Uses multiple ways to spread itself on the network by integrating itself to removable media, files, processes, network payload etc.
- Targets specifically Siemens SIMITAC WinCC, once detect on the network tries to inject SQL database to make its authorized to access the connected PLCs undetected.
- Uses infected PLCs to watch for specific behaviors by monitoring PROFIBUS.
- It has the capability to sabotage the centrifuge system by changing the frequency of motor speed.
- It is capable to demolish itself after execution on system, lay dormant, rebuilt itself, update with other peers on the network,
- It includes a variety of stop execution dates to disable the malware from propagation and operation at predetermined future times.

(Knapp & Langill, December 22, 2014)

4.4.2 Shamoon/Distrack

Shamoon also know Distrack have great capabilities to gather information from the system as well as system damaging capabilities. The intelligent footstep of this malware were to exploit the system, create a connection through RAT, exfiltrate the information and the moved through the network to other systems but covering the foot on previous system by changing the file information or even changing the master boot records.

The components of Shamoon are mentioned below.

- Dropper – The tool is used for network wide propagation and infecting the systems initially to perform future commands
- Wiper – The payload is used to make modification and destruction to file system.
- Reporter – a component designed to communicate stolen data and infection information back to the attacker.

The malware was detected at Saudi Aramco where 30000 systems were infected in the oil and gas companies.

(The Shamoon Attacks, 2012)

4.4.3 Flame/Skywiper

It is also a kind of adoptive persistent threat that spread across the system. the tool capable to gain access and send information over the secure links to over 80 domain server changing consistently to different geo locations.

More than a dozen modules were found in this malware to carry the attack.

- “Flame” –Auto Run infection routine handler (Sky wiper is often referred to as Flame because of this package)
- “Gadget” – A tool for updating the base malware software, this tool updates new module payload and evolve the design of malware.
- “Weasel” and “Jimmy” – A tool hard disk and file parsing.
- “Telemetry” and “Gator” – handle C2 routines
- “Suicide” – self-termination
- “Frog” – A payload to crack and snip password
- “Viper” – the tool is used to take screen capture of the system.
- “Munch” – A network sniffing tool.

4.4.4 Dragon Fly / Energetic Bear

The attackers have been in operation using the tool from 2011, in June 2014 it was discovered and Symantec issued a whitepaper on it. The malware has compromised strategic system like energy and power sector for spying and could have cause mass damage lately. The major function are the remote access tool (RAT) named Backdoor.oldrea & Tojan.Karagany

Initially the target was aviation but after its success they expanded it to US and European energy sector in 2013. Countries affected by this malware were US, France, Spain, Poland and turkey.

- The first phase includes phishing emails.
- In the second phase water holing is used in websites used by energy sector organization, these website redirect them to another page for malware installation.
- The third phase was torjaning the industry equipment software.

The attack to spread the malware across a huge system gain information and then modules will be added later to sabotage the system. No sabotage modules were discovered when this malware was detected. (Targeted Attacks Against the Energy Sector)

4.5 MODERN ATTACK TRENDS

The threats have changed with the time moving up in the protocol stack from layer 2 and layer 3 to (application, session and data presentation. Even the most recent trends display a non-platform approach, where attacks have shifted from Operating System (like Microsoft, Marcos) vulnerabilities client applications. As browsers became more strong and purposeful with add-ons and plugins like adobe reader, flash player and app installation made them more prone to attacks.

The applications have gained a wider ground in industrial control systems especially power systems. The malware itself is evolving with its mutated logic it has the ability to take decision by analyzing the environment such in the case of Stuxnet with robust logic and able to demolish itself after execution.

The industrial application provides communication between supervising system to field unit like PLCs and RTU. The application is seen as vulnerable because they carry all the control information across the utility and most system are utilizing the protocol level security as devices have very less capacity to run application and security app on it. Industrial application layer is not exploited many times the behaviour is change within the control information or a miscommunication is created between the supervisory control and devices connected to it.

Digital bond in 2012 displayed a new form of industrial attack name 'Basecamp' where IP protocol stack is used to manipulate the control of Roxwell Automation logic. In this case Roxwell was just a tool and exploitation was created in underlying protocol with IP. Later in 2013 Adam Crain of Automatic displayed some vulnerabilities from IP protocol. This time the protocol was DNP3 as discussed in earlier chapter the protocol is widely used between outstation and master stations.

5 IMPLEMENTING SECURITY & ACCESS CONTROL

5.1 SECURITY ZONES AND CONDUITS

The term 'Security Zones' and 'Conduits' look rather similar but server for different purposes. A security zone is a layer of abstraction between two different group of devices based on their control, functionality, or purpose in the utility. The can be based on geo-location, reliability of information, trust level or simply access control. In the case of layered security we can see zones nested into each other to further distinguish the traffic or asset type. Conduits on the other hand are an opening in the zone such that assets in the zone communication to assets in other zones in limited and controlled manner.

An example can be a trusted and an untrusted zone on firewall where conduit allows the communication between them. This can be a unidirectional communication from Trust to Untrust zone.

5.1.1 ZONE IDENTIFICATON

Zones are a brad term of identification in the utility. Defining a zone in a utility can be considered as categorization at different level. This is quite different how we describe our network in the enterprises. The zones can be architectural, control, functional, data and organizational flow based. Every zone criteria has its own significance to cover and separate group of assets at different security level.

The granularity of defining the zone can put them in overlapping state. For example a zone defined on the basis of physical Sub-Control system can be overlapped by the zones designed on protocols. It is not a demerit of any security system; rather it indicates a strong grouping policy and zoning criteria behind each asset. This enables these assets to categorize at multiple levels by different individual creating a layered security model and controlled access mechanism over end-to-end network.

5.1.1.1 Network Connectivity

The important concept in industrial security is functional groups which can be based on safety, control, peer-to-peer communication protocols, remote accessibility encryption type and authentication and availability. Here we will discuss few security criteria on which zoning should be done in any utility.

It is defined by network segmentation often by unidirectional link by hard marking the boundary by putting a single link out of the group of system. However this should be consider for wireless as well because the boundaries some time not clear and are neglected in those cases. Thus physical boundary is the major section but logical boundaries are also present in our network. This can include layer 3 device like router and firewall also at layer VLANs cannot be neglected and many possibilities exist such as VLAN hooping or ARP spoofing.

5.1.1.2 Control loops

The control loop represents an automated process, which few devices will perform their operation in acyclic manner providing the derived result. The loop also defines the process is isolated and confined to few devices.

5.1.1.3 Supervisory Control

The supervisory control monitors, manage and keep all the event data organized from the control loops, since these are all server that are used to managed the utility processes lies in a same functional group. The devices can include HM, engineering workstations and other supervisory stations.

5.1.1.4 Plant process Control

Plant process control lies above the supervisory control engine provides visibility through historians and other management applications. These functional element can be consider a backbone process control system. The protocols used by these devices is mainly backend protocol.

5.1.1.5 Data storage control

The data storage control can be middle ground for information between business process and industrial process. The devices used in this functional group is storage area network. Gathering data from business and industrial control systems and generating desired statistical analysis for executives.

5.1.1.6 Remote accessibility

The networks are designed to connect with remote devices or to provide out of band management to system. The methods used for communication are external to the communication systems like dialup connection or satellite links. The elements of this group lies beyond trusted and untrusted networks. The method of connectivity is different as they use various encryptions and authentications. There can multiple groups in the remote access as these can be from devices, individual and other third party members. Therefore each can be group separately on their authentication, encryption, accessibility and means of connection.

5.1.1.7 System criticality

The assets no matter what part of group they needs a second review based on their criticality and their risk assessments. These standards are set for every industry by different organizations. All assets should lie in this group and be segregated based on their impact on system. This will decide the level of security to make the operation reliable.

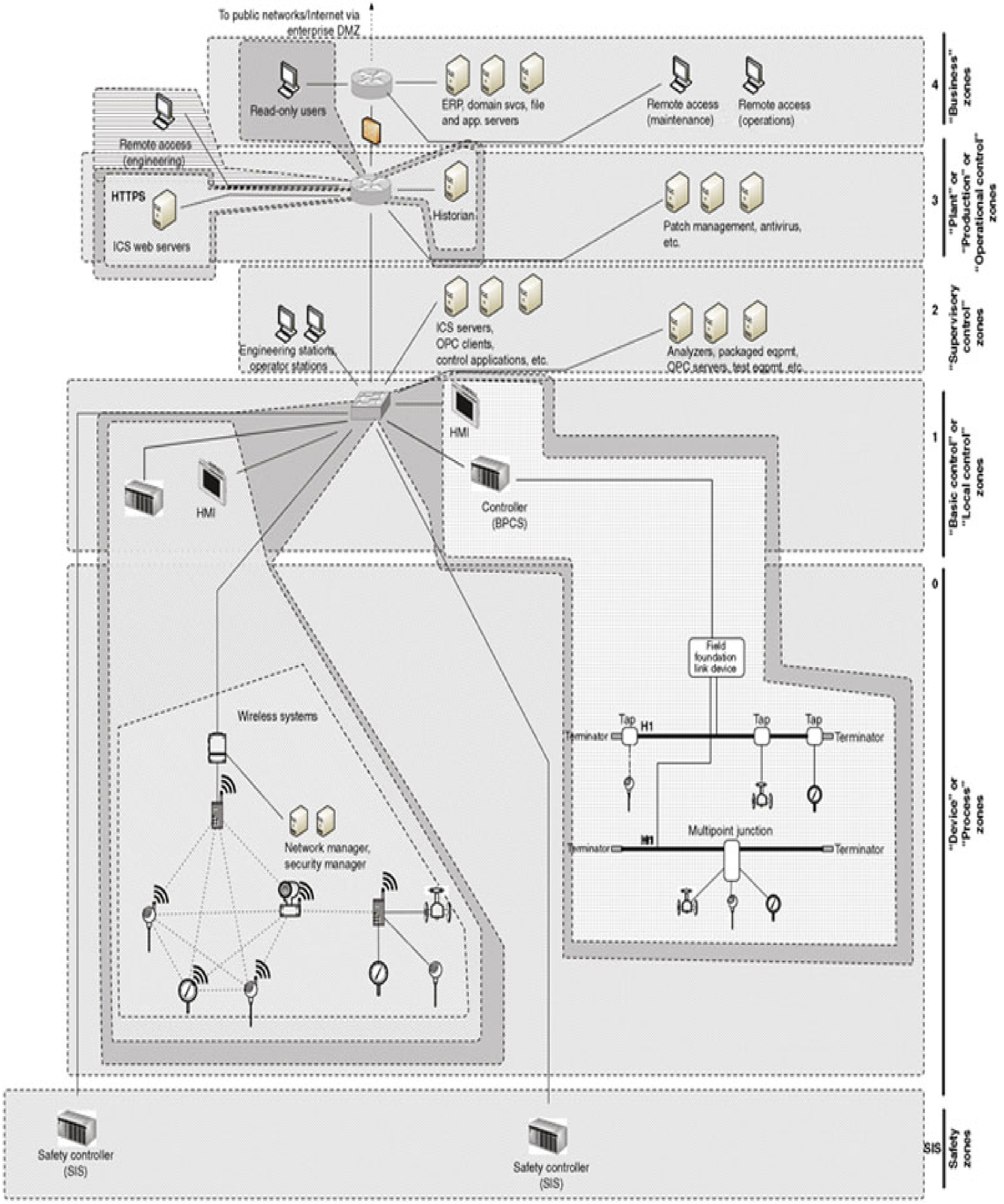

To public networks/Internet via enterprise DMZ
Read-only users
ERP, domain svcs, file and app. servers
Remote access (maintenance)
Remote access (operations)
Remote access (engineering)
HTTPS
ICS web servers
Historian
Patch management, antivirus, etc.
Engineering stations, operator stations
ICS servers, OPC clients, control applications, etc.
Analyzers, packaged eqpmt, OPC servers, test eqpmt, etc.
HMI
HMI
Controller (BPCS)
Field foundation link device
Wireless systems
Network manager, security manager
Tap
H1
Tap
Tap
Terminator
Terminator
Multipoint junction
H1
Terminator
Terminator
Safety controller (SIS)
Safety controller (SIS)
SIS
4
"Business" zones
3
"Plant" or "Production" or "Operational control" zones
2
"Supervisory control" zones
1
"Basic control" or "Local control" zones
0
"Device" or "Process" zones
Safety zones

Figure 5 – Zone Functional Diagram (Knapp & Langill, December 22, 2014)

(Knapp & Langill, December 22, 2014)

5.1.2 IDENTIFYING SUB-ZONES

Subzones holds a strong point in any security infrastructure, pertaining that it is upon the functional criteria that assets within the zones are safe from each other. The assets in the zone can be further segmented based on their vulnerability level and trust level. For example, a vendor laptop in a zone could bring vulnerability in the network therefore its access should be limited to certain devices it need to connect to in the zone. The can be implemented by transparent firewalls, VLAN ACLs or by creating private VLANs etc.

The other example could be of BYOD(Bring your own device) in the network, where the device might possess the same functional level but needs to separate on the basis of vulnerabilities therefore sub security zone is mandatory to isolate the device as soon as it attaches itself to the system.

5.1.3 IDENTIFYING THE CONDUITS

Conduits can be considered as a type of zone that holds only communication infrastructure and protocol used between the communications of zones. This means all electronic devices, communication medium (channels), encryption protocols, utility control protocols and conduit hold several characteristic that secures communication between zones.

- Security policies
- Asset Zone mapping
- Asset and zone vulnerability and risk assessment
- Approved and rogue device on network
- Conduits on network

5.1.4 ZONE SEGMENTATION

We have discussed the topic of network segmentation in our earlier chapters. Zones have physical assets in their inventory and any asset that is not included in the list in the inventory should not be allowed to make communication with their zone devices. In order to make them communicate use a semi trusted zone know as DMZ.

It can be possible that the zones cannot be separated at network layer as both devices might be running in a flat layer 2 network therefore we need segmentation solution layer2 such as VLANS. Devices can also be configured so they have restricted access on the network. An example confining a different subnet mask on the host, changing the gateway etc. For higher layers a next generation firewall can be used on conduits to prevent communication at application layer. The best practice should include;

- Follow and inventory every connection going into and out of the zone.
- Zone separation should start in layered manner. Physical layer should be examined first up till application.
- Critical conduits should be dealt with multiple controlled accesses.
    - Physical layer separation through diode or unidirectional gateway.

- Switching and protocol control
- Through next generation firewall controlled application access.

- Policy enforcement for link monitoring and link usage, so that irregularities can be easily identified.

5.2 IMPLEMENTING NETWORK SECURITY CONTROL

The network security control is am implementation of conduits to secure the incoming and outgoing zone traffic while keeping authenticated traffic network. We will discuss in detail how we can categorize our network devices as well as their placement in establishing secure conduit. We need to declare the perimeter for each zone through standards and their criticality. The following level of security is defined in NERC CIP standards that declare minimum requirements so as to make industrial control network safe at each level.

1- Critical Systems

The priority of the assets is highest, therefore required practice is to introduce unidirectional parameter at physical layer, with firewall, IDS and IPS at layer3. Further enhancement are application firewall, app monitoring. Placement of IPS and firewall should be inline and IDS is to out of band. Host can use their own protect mechanism to protect themselves individually.

2- Medium Impact System

These systems need to be secured with Firewall or IPS or IDS. Recommendation is the deployment of all three devices mentioned below.

3- Low Impact System

These device are general system and does not possess much threat to environment; therefore a firewall with built-in IPS is fairly enough for these systems.

Note: It is the Firewall and IPS that has been recommended at every stage of the security by standards because this forms a better inspection mechanism. Where Firewall does 'Shallow Packet Inspection' reading through the initial layer and allowing policed traffic and IPS providing a deep packet inspection on the filtered packet. Thus it saves computation on IPS as the traffic is already filtered through the firewall.

Note: Another aspect when implementing IDS or IPS are their placement. IPS is always placed in line but the process can be very resource intensive while inspecting traffic. It is recommended to select the specific traffic type and protocol so that no jitter or packet drop is observed over the network. It is important to understand the type of traffic that pass through the conduit. An IPS can also drop legitimate traffic in case of any anomaly suspicion but these drop can create sever impact on ICS analysis, reporting and decision making. However ion the case of traffic between corporate and industrial control network, IPS implementation is recommended where packet drop will stop anomalies or malware propagation to the other system. These packet drops are not critical rather mandatory to be dropped. The IDS deployed out of band will help detect anomalies and traffic patterns on with an alert can be sent to administration who can further clarify on situation before putting the appropriate action against them.

The industrial Control system uses different protocol set like DNP3, IEC61850, and Modbus etc. The equipment we need should be able to understand these protocol and its anomalies. Mostly vendors like Cisco, Juniper, HP, Checkpoint does not have a large variety of hardware to support these protocols. Hence we look for different vendors like Silent Defense, silent force, secure crossing etc. To perform deep packet inspection and other functions on network. Many vendors have developed their separate database for industrial signature package for IDS and IPS.

5.3 NETWORK SECURITY IMPLEMENTATION

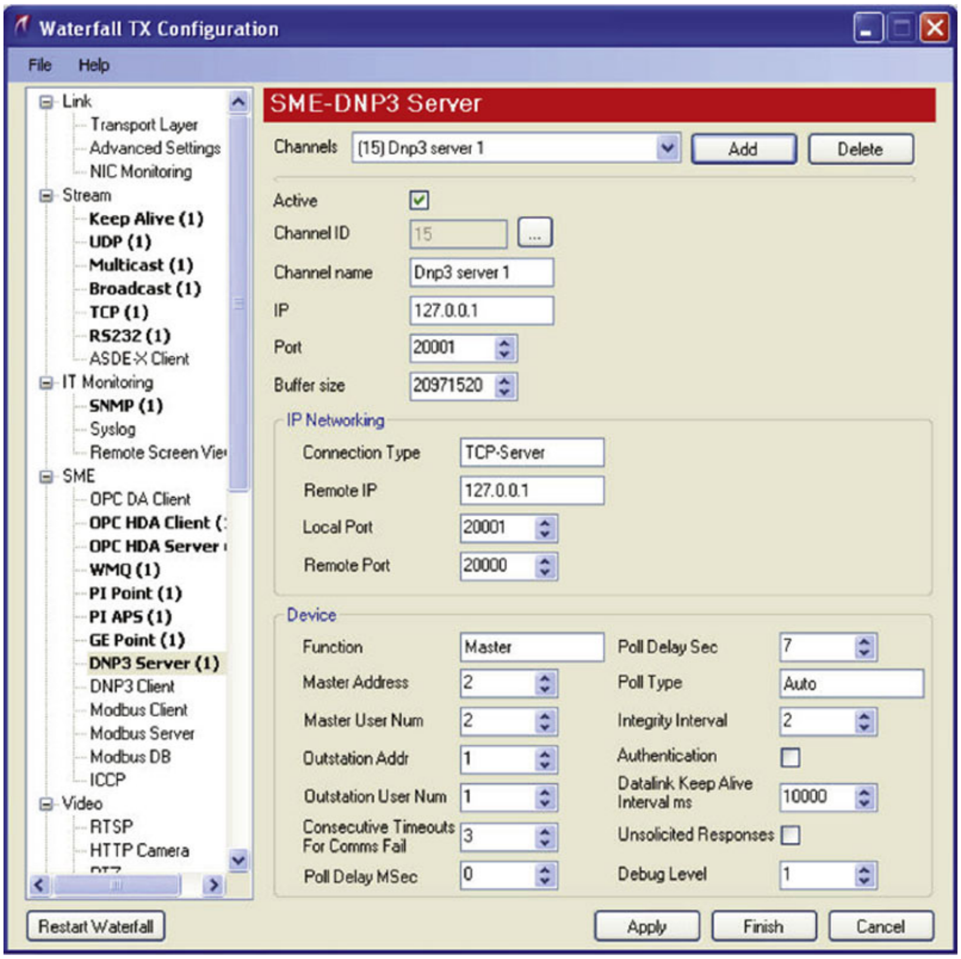
The security guideline considered in this section will serve as baseline for implementation however a detail policy enforcement is required with respect to utility need and concerns. We have already created zone and conduits therefore implementation will be easier for us.

5.3.1 Data Diode

A unidirectional gateway also called data diode is used as part of network security to limit the communication to one direction, this physically limits the communication. The diode has the adoptability to change the communication at any instance making it a bidirectional communication and changing its characteristics when finished communication.

Many applications used TCP based protocol that requires bidirectional communication in order to synchronize and perform. Considering these sorts of scenarios a dynamic or more realistic solution was required therefore vendors introduced software based implementation of physical diode. Where the receiver fakes the behaviour for the transmitter such that application can be made to communicate on unidirectional link. This not only allows control over physical communication but also provide a granular control over application communication.

The example show the waterfall communication system that implements DNP3 as protocol for unidirectional communication.



SME-DNP3 Server

Channels: (15) Dnp3 server 1

Active ☑

Channel ID: 15

Channel name: Dnp3 server 1

IP: 127.0.0.1

Port: 20001

Buffer size: 20971520

IP Networking

Connection Type: TCP-Server

Remote IP: 127.0.0.1

Local Port: 20001

Remote Port: 20000

Device

Function: Master

Master Address: 2

Master User Num: 2

Outstation Addr: 1

Outstation User Num: 1

Consecutive Timeouts For Comms Fail: 3

Poll Delay MSec: 0

Poll Delay Sec: 7

Poll Type: Auto

Integrity Interval: 2

Authentication ☐

Datalink Keep Alive Interval ms: 10000

Unsolicited Responses ☐

Debug Level: 1

Figure 6 – DNP3 Unidirectional Configuration

5.3.2 Firewall Implementation

Firewall implementation is based on rules; the rules follow a specific priority sequence either from 'Low to High' number or from 'top to bottom’. All firewall have implicit deny at the end denying every traffic from lower security zone to higher security zone. This brings us to allowing specific traffic across network. The firewall allows user to create multiple zones setting their priority of communication and network interface that belongs to the zones.

There can be multiple functions applied at a time to the matching flow on firewall. This can be the 'Allow/Permit', 'Deny' and 'Reject'. It is important to discuss deny and reject here as both has the same purpose but differs in their functionality. When reject is used the Firewall drops the packet but send the message back to the originating host. The information can turn lethal in understanding the firewall type or rules by attacker. Where 'Deny' is more secure as it drops packet no further action is taken on it, sending no information back to originating host.

Groups can also be used to identify assets on firewall making management becomes easy and no object is missed or over authorized. Maintaining controls for every individual object can be hassle and create configuration issues in large organizations.

Configuration guides.

- The first policy should always be implicit deny bidirectional; the default exist only from lower secure zone to higher secure zone.
- Allowing the communication between specific servers and client systems should be granular, this means specific IPs, ports, services and time based policies should be used. Putting a comment with the rule help in documentation and clarifies information about the author.
- If allowing a range of IP addresses it's better to create group with the name and description.
- The network traffic between SCADA and Data control systems is always based on IP protocol, there any other protocol should be dropped.
- All traffic communication between data control system & SCADA to the enterprise network should transit through DMZ.
- Only allowed legitimate IP address of the zone should leave the zone, place a rule on top to always match the source address before sending the traffic out of zone.(Tools can also be used to check IP spoofing within the zone).
- NO control devices should access the internet. The system should be isolated from the internet.
- The management traffic of firewall should pass through the separate channel, encrypted links can be used and any authentication for firewall interface should be a two-factor authentication. A limited IP access should be allowed on management interface.

5.3.3 DEEP INPECTTION & PREVENTION IMPLEMENTATION

The devices used to detect network traffic anomalies either in active mode or in passive mode (out-of-band) are placed in the network behind the firewalls. IDS and IPS both the same set of signature but varies in their action on anomalies. IDS can generate an alert, log the packet or ignore the threat, whereas IPS is able to drop the packet or reject the session by sending TCP RST or drop the packet with logging.

Every policy defined on the device will dictate the type and nature of anomaly to be checked in the packet. The goal is not just to stop the malicious code but to understand the network traffic behaviour and change in network traffic trends. In the case of any zero day attack the network behaviour change can help in diagnose the malicious activity.

The example of this behaviour could be large data transfer, or an encrypted session from RAT (Remote Access Tool) to command and control will display the new trend in network thus generating an alert.

Custom Signature - Most of the signatures developed are based on standards created by the Snort, therefore most vendors follow the same rule and signature standard. Creating a custom signature will stop irregular messaging between devices. For example, a PLC receives a command from vague host existing in the same zone or domain, but if a custom signature exist on those commands for messaging and only allowed a particular host for it, then the attack can be stopped as IPS will check the message and drop the packet as this signature is allowed from particular host.

SIGNATURE SELECTON

The signature today exist in hundreds of thousands, if all signature are loaded the packet inspection process will not only be latency intensive but can result in packet drops or even crashing the device. The functional zoning will help us select the right set of rules and signatures on the devices. The guideline to perform is as follows;

- Begin with more robust signature sets, with many active rules.
- Delete signature of non-used protocol in zone and place a broader rule to deny all traffic in the zone.
- All signatures to be loaded for the protocol that exist in the zone.
- All signature should be selected with right action on it and signature should be updated regularly.(*Note*: Do not allow device to directly update itself from internet rather use an update server as transit point for the signature updates)
- Local certificate should be installed on IDS or IPS so they can decrypt the message and check for anomalies, any non-decrypted message should be dropped and logged as well.
- Log all traffic from remote users so that any irregularities can be checked if reported later.

ANAMOLY BASED DETECTION

We have only implemented signature based rules for preventing and diagnosing attacks. Though there are other ways to effectively evaluate network security and traffic patterns. The anomaly based detection works on network in a broader perspective. The device works in passive mode; IDS accumulated statistical data from the network and based on the data sets a normal behaviour of the network. In industrial systems it is easy to expect a constant behaviour from the network and devices as they are bound to perform repetitive operation. Any reported change in thresholds of outbound or inbound traffic, session counts, and bandwidth spikes, number of connections or new source address can easily be checked. The anomaly detection threshold are automatically set by the IDS but can be made to work with SIEM to model across the network.

THE SOPHIA PROJECT

The Sophia project was initialed by the military organization for network finger printing. It is done through device that captured all the network flow for certain period of time and establishes a predefined sequence of events in the case of every network flow. One this template is completed this sophisticated fingerprint is placed to monitor and match every traffic flow on the network. Sometime this flow is represented as whitelisting any exception in flow will reciprocate in the form of an alert. If the flow is legitimate the event will be added to network fingerprint else action is taken against it. This technology was displayed in Dec, 2012 lately made available for public sector organization by NexDefense.

PRTOCOL BASED DETECTION

The protocol anomaly detection requires in-depth knowledge about the protocol and proprietary work done by vendor on those protocols. Many vendors include proprietary features or protocol design creating a new protocol. Thus applying any detection mechanism can generate unsuccessful detections creating it completely meaningless. The need for implementing this anomaly is to detect the zero day attack based on protocol manipulation.

5.3.4 Industrial security Appliances

- ***ICS UTM -*** It is a hybrid application that provide a combination of feature including policing, packet inspection, antivirus, remote access capabilities. The solution can be consider as a layer defense mechanism.
- ***Content filtering Application firewall -*** The policies are capable to filter traffic based on the packet content, the only problem that can happen is when packets fragmented and the content judgement is difficult on it.
- ***Content decoder & capturing -*** These are used to check application session and contents being transferred in the session. The can be very intelligent in the zones where critical information is stored as they designed to stop data and information theft from the system either by insider or outsider. DMZ is the most preferred zone for these devices.
- ***Network whitelisting -*** Network whitelisting requires network fingerprints so that only good traffic patterns are allowed to pass all unknown traffic patterns are either block or an alert is generated to the administrator. The Sophia project from NexDefense is one of its examples.

5.4 IMPLEMENTING HOST SECURITY & ACCESS CONTROL

Network can be considered one aspect of industrial control security, through malware propagation is primarily spread though network. In most cases it can initiate through network but apart from workstation and server there are several devices that is that is attached to network like HMIs, PLC, RTUs, supervisory control systems etc. This poses several interface like USB, serial or a wireless interface that can open vulnerabilities.

Many of the devices have hardened code on it but much need to be done on devices that does allow you to update and make changes to the firmware. Several control mechanism can be deployed on these devices. We will discuss in detail the improvising that should be done on the host for system reliable operation and protection. These include;

- Application Control and execution protection through whitelisting
- Inbuilt firewall and malware protection
- High availability through authentication and encryption.

Before discussing technologies in detail we have to analyze the device and their capabilities to run the host security tools.

- **HMI -** Run host firewall, host intrusion detection system, antivirus, application whitelisting and block all other service and ports. Application of these technologies can vary depending on operating system version, as modern operating system have inbuilt capability to detect and prevent most known attack vectors.
- **PLC / RTUs/MTUs -** Since not much application can be installed on these systems therefore firewall and deep packet inspection can be installed, where security can be tightened externally through other network devices.
- **IED -** Not much can be done on device itself, external security vector will have the charge to secure them.

Note: The external security vectors are a great debate in vendors today, as different companies are coming up with their own external solutions to protect these devices. Such in the case of Siemens where they introduced new processor to new PLC with built-in feature like firewall and IDS. Whereas other vendors like caterpillar, Honeywell, Schneider electric etc. are coming up with next generation external security systems.

5.4.1 Host Firewall

Host firewalls are similar to network firewalls except their functionality is limited to a single host on which it is deployed. The firewalls are capable to maintain and check the session state fully. The guideline can be the same as the network firewalls. The importance of host firewall becomes more significant when the policies and restriction re applied on outbound traffic as well. Though a study is required to understand the host application in the case of any malware transferred on the system like Dyagon Fly in the past can be confined to only an individual system rather infiltration through the zone. Further an event or log collector can be synchronized with these firewall so as to check any alerts generate by the system. The firewall should be configured with respect to each individual host.

5.4.2 Host Packet Inspection

Host inspection is also similar in function as the network IDS and IPS but the boundaries are confined to a single host. These can very significant inspect the signature related to that particular host as network IPS are usually overloaded with signatures to check therefor more granular approach is placed on network IDS and IPS. Some traffic can skip through it therefore Host IDS and IPS provide a second layer of obstruction. Also custom signatures can be installed to check if any data theft is occurring form the host or not; a check-point for zero-day attacks.

5.4.3 Antivirus

The antivirus is needed to check the local system files for any malware, Trojan or unreported application. The antivirus should be regularly updated with need signature files.

5.4.4 App whitelisting

Application whitelisting is a new trend adopted by the industrial security teams for zero-day attacks. This requires in-depth knowledge of application and their communication mechanism and approach to the organization assets. The term 'whitelisting' itself is not a complicated mechanism rather simple listing of application available within the utility, system or an asset. Host application whitelisting is allowing a list of application that is only required to be executed on the host and everything needs to be blocked and reported. In the case of any malware penetration on the system will block execution on the system.

It is very important to understand AWL can be a part of solution put can never be consider as a complete solution against local execution of code it can protect against app, but does it secure against script, macros or any code that has been attached with whitelisted application and misuse of whitelisted applications.

This is rather a new concept with few drawback therefore not much have been deployed in industrial application but multiple industry vendors and security companies are working to provide an integrated significant solution for vendor devices. The companies include MacAfee, Windriver (VxWorks RTOS), SIEM form Nitrsecurity and trustifier Kernal Security etc.

5.4.5 Patch Management

Patches are an everyday routine task in every industry and organization. The patches can vary from an upgrade to new feature or fixing a bug or vulnerability in the system. The approach to stop vulnerability is not a proactive approach but rather a reactive approach. Little can be done in changing the approach but patches can protect from future exploitation of known vulnerabilities. Patch management is big task as need adequate time for system and resources on the network. Further no application should be allowed to patch directly from the internet. In the past it has been reported about vendor website being hacked and redirecting update request to vague webpage result in download of a malware. The patch management server should be created it is better to create multiple server with respect to the functional zones.

5.4.6 System Availability & Patch Management

The industrial systems have always been designed to provide a very high availability rate above six-sigma standards. In the case of patch management most changes at system level and need to power cycle the device thus this can create a delay or disruption in operation. Through backups are always available but it's always considered as downtime when invoking the redundant hardware. Hence patch needs to be planned before application. The patch can be categorized as

- Critical - a vulnerability that can be exploited without the user action.
- Important -A vulnerability that can impact by information theft and leakages.
- Medium - Exploit that can be mitigated also by configuration and changes to system.
- Low - Although a vulnerability but very difficult to exploit in current system.

On these impact level patch management aggressiveness can set to monthly, weekly or hourly notice (mostly within 48 hours.)

5.4.7 Pre-deployment testing

Not all patches are meant for every organization and devices. The device can have multiple firmware depending on the asset usage also it is possible that the device support multiple feature but the patch that has been released for a particular is not used by your organization or being block. This can result in wastage of time and resources. There can be other reason like not all patch have the perfect lines of code, the patch itself can carry some vulnerabilities also sometimes when introduce a new firmware patch not much pre-testing has been done on real environment. In that case some vulnerabilities always exist. The best practice is not apply the latest patch or firmware. Unless recommended by vendor cover a very critical vulnerability. The patches in the era of virtualization if applicable should be tested and verified on virtual machine first and once sure about the desired result and vulnerability protection by using penetration tools against it can be applied in the organization. The other significant method is to apply the match not on the core system rather from less important device if available in the system. For example a PLC or RTU that need to be updated should not tried and test in the main facility but good to check on remote small utility where the impact can be controlled easily. Some redundant hardware require synchronized firmware therefor it should kept in consideration in pre-deployment testing.

5.4.8 Process Automation

The process of automation is required to further strengthen the security as human processes have always been susceptible to mistakes and inconsistency. The human vigilance is always important in the case of monitoring and decision making as center external vector have to included that cannot be always defined in machine. Automated device configuration and patch updating is the two new path that industry in focus for less configuration leakages and a standard based deployment can be made across the utility. In the case of updation many vendor use different method for updation such as script, complete installation or an executable, the other way to look around is the group of device based on their criticality, reliability and other functional aspects. Backups before updation of devices are another vector that requires consistency, especially with hundreds of devices. Process automation allows visibility of the utility during the updation or deployment period, and has the ability to take decision if any disruption or irregularity is observed during the course of action. The process automation should be a combination of multiple systems including disaster recovery, automation firewall, user right management, time synchronization, patch management and etc.

5.5 AUTHENTICATION MECHANISM

The authentication is the identification of user credential from the system. This user authentication can exist on multiple levels depending on the asset or system criticality and risk assessment. The levels vary from minimal authentication to detailed multifactor authentication. The authentication mechanism is divided into four levels.

- ***Level – 1***
  At this level no user proofing is needed a successful authentication can be a simple token request on a secure authentication protocol. Though plaintext passwords are forwarded a rather simple encryption should be used. This level of authentication can be compromised by using eavesdrop or sniffing to protocol conversation on the network and then applying dictionary or brute force attack.
- ***Level – 2***
  This is a single factor authentication that requires user identity information to verify in the database. A wide range of technologies are available for this authentication. Replay attacks and other simple attacks can be controlled from it.
- ***Level – 3***
  Level -3 authentications includes multifactor authentication which involves user credentials as well as one time password from cryptographic protocol. This password can be of three types ‘soft’ crypto toke, ‘hard’ crypto-token, and one-time password. This can stop multiple attacks such as eavesdropper, Man-in-the-middle, replay, online guessing and verifier impersonation.
- ***Level – 4***
  A highest level of secure authentication. The security as same as level-3 except hard cryptographic key are used and these key should on a physical object that is to be in possession of user. These keys are well explained in FIPS 140-2 level modules.

6 Behavioural Anomalies & Threat Detection

In the previous chapters we have designed and implemented network security and tracking each aspect of it. We will accumulate lots of data from the network events. To use this data effectively we need procedure and methods to identify the exception and threats mentioned in those events; so further action can be taken against it.

6.1 EXCEPTION HANDLING

Exception can occur at any time either in a new configuration, modification in the environment, time based access etc. It is important that whenever these exception are made the administrator should be notified, such that administrator can analyze the need of it and approve, else decline those change. Most of the time intruders try to add more access to their profile to gain control of network.

Another part of this exception could be the changes happening in the organization structure. For example an employee promoted to a new role in the organization or temporary access to system; both these cases requires modification in the system. Therefore an automatic system should be placed that can understand the utility access and generate alert.

Few examples are as under;

- An authentic user connecting from a rogue IP or device. This can be detect by any log analyzer
- Application or protocol operating in unauthorized zone. This can be detected through IDS
- Industrial control functions originating from unauthorized device
- An unexpected shift hour user activity, detected by authentication server.

6.2 BEHAVIOURAL ANOMALY DETECTION

Irregularities can be observed in several ways to aspect from configuration and access control. In this section we will discuss several automated tool that will help in real time environment to analyze the events and log but human vigilance and analysis is always important to make decision on it. Tools are there to help and compute the data to meaningful correlated manner. A baseline is always the critical part to detect any irregularities as the event data sets what's normal in the network. The process can take month or even year to set a strong baseline.

6.2.1.1 Setting Baseline metrics

Establishing a baseline provides a comparison of expected behaviours and current behaviours. It is important to discuss the difference between baseline and trend analysis. A baseline is always a constant value derived from a simple or complex algorithm whereas a trend analysis is a difference in the past and future results.

The simplest method to setup to stop a baseline is to collect all data in a given time frame and find the average of it. In ICS the baseline is set on several statically analysis and tolerance mechanism; it also includes the peak and off-peak time, their average and sometimes related with correlated events as well. We will discuss the baselines for different entities;

- ***Network traffic***
- Can be measured by number of new IPs, destination or source address, sockets, bandwidth utilization or session duration, timing etc.
- These can be measured by collecting different flow like net flows, flows etc. from routers and firewall. Also probes can be set in IDS to provide relevant information.
- Multiple system NBAD, and SIEM and log management server can be used.

- ***User Activity***
- These can be record of user session, login/logoff attempts and logging user routine tasks.
- These can be maintained through various application logs, through active directory service and session managers etc.
- These can be recorded in SIEM and log management servers.

- ***Process/Control behaviour***
- This can involve new codes, number new operation and configuration changes applied.
- The logs should be captured through data historians, application monitors and by external controls.
- This can be managed by SIEM and data historian.

- ***Event/Incident activity***
- Gather events, alarms or any log generated before disruption of services.
- The logs are usually gathered from Firewall, IDS, IPS content filter etc.
- These are usually reported to application monitors and other industrial appliances.

6.2.2 Anomaly Detection Tools

- **NBAD systems**

The system are based to focus more on network anomalies by going through unusual trends and events. Set the parameter based on network characteristics and generate if any level threat existence reflected in the behaviour of the real-time network. Many vendors have come out with their integrated solution that can not only prevent regular attack but can detect mac spoofing, spoofing, IPFanout and connection rate detection. The example of these vendor can Arbor network NSI, Juniper STRM, IBM QRadar, Exinda, Pathsolutions, Riverbed Technology (Cascade), HP network Immunity Manager, Symantec Advanced threat protection, Sourcefire 3D, etc.

- **SIEM**

SIEM can be deployed on different platform as an application, software or managed service. It stands for Security information and event management. The product hold multiple capabilities beginning with the gathering data from the network, workstations, database and other equipment providing a consistent data for event logged across the utility. It they formulates a correlation between the events from different assets creating a base line for the behaviour. Once the base line is set any changes to against those fingerprint is reported as an alert. The enhanced featured also providing humans to analyze and make decision by providing by detail graph and statistical analysis of the system. The system can help in the case of an event of exploitation, it can then be determined through these system for forensic investigation proving a detail activity of malware in a timeframe. There are several products available in the market that fulfils the requirements such as Alienvault Unified Security Management, Assuria Log Manager, GFI event Manager, vSIEM Telemate, Open Source Security Management, HP ArcSight, EIQ Network SecureVue.

6.3 BEHAVIOURAL WHITELISTING

Behaviour whitelisting is different from anomaly detection as they usually follow a trend of malware control mechanism. Behavioural whitelisting follows users and assets and identifies the irregularity between them. For example finding the rogue user in the network and automatically tightening the security against it until administratively allowed in the system. There can be three kind of irregularities,

6.3.1 User whitelisting

User whitelisting is a process of analyzing all the user account, their privileges, action, and their activities. In the case of any attack or hijacking of user credentials every user activity can traced and any misused account trails can be followed and alerted back to user and administrator. At certain level where hidden account or back door are used by the attacker can generate exemption report. Also any creation of new account will add the account to bad list unless placed administratively into whitelist. In the past, WinCC account was used by Stuxnet to carry out its operation in the facility.

6.3.2 Asset whitelisting

Asset whitelisting is keeping an inventory for every zone by list every asset in it. This prevents from rogue device connectivity to the network, by generation an alert for presence of a new device in the zone. This can easily happen, even mistakenly or by insider threat. Multiple methods can be included to prevent these action; for example disabling dynamic address learning in network or by introducing layer security such as 802.1x or disable unused port on the network. In the case of wireless network hidden SSIDs or dual authentication can be used on the network.

6.3.3 Application whitelisting

Application binding can be done with the functional zones, so that only specific can have the right to perform mentioned operation in the zone. This will distinguish any unapproved code or function within the zone. This can be achieved by parsing through the application code and understanding protocol behaviour on the network and generating its finger print over the network. This can be a communication method, or request for particular function for the asset etc. Few examples of application whitelisting is as under;

- Functions are only allowed to pass the read-only command.
- Master devices are allowed to use the protocol collect data from assets in the network.
- Few mentioned codes are allowed to run from the application
- application can only communicate on authenticated and encrypted session

- Use of non-registered certificate by application

6.3.4 Smart lists

The smart list is a step forward towards the containment of negative alerts. The process was first adopted by European SCADA authorities. Lately it has been adopted by many industrial vendors. The basic purpose of smart list is further scrutinizing of an alert and justifying its alert level before it is forwarded to administrator. This happens mostly in the case of Application whitelisting when a protocol or application is detected to perform operation apart from its regular operation in this case the whitelisting will compare with whitelists in the other zones and compare the event conditions only a unique or offensive event. If the behaviour matches in any other whitelist then further procedure are used to validate the authority who executed the code and it purpose. If every is acceptable in those condition the alert is changed to information but still sent to administrator.

The impact can check these action in blacklist as well and if found can directly take remediation and prevention mechanism against it. At present SIEM does not support these feature but can be future element with some artificial intelligence and visibility to take decision proactively.

6.4 THREAT DETECTION AND IMPACT ANALYSIS.

Threats are sometimes very sophisticated they do not display themselves at once. They take time sometime weeks or months to propagate in the network. These threats are very well designed such that they set thresholds for attack just under the major alarm thresholds. These patterns are commonly misused by all devices because the behaviour is still under the expected range. The threat use this to make their way by exploiting both Information and operation technology.

This was observed in the case of Stuxnet, which managed to make its way to pass through all the barriers by using complicated algorithm and taking advantage of lack of correlation between IT & OT systems.

These attacks cannot be detected by any devices in real time system, although an event and log management system is needed to relate every individual attack and can detect a greater pattern of a single threat. The algorithm and devices are needed that can read the events in greater context by accessing event report form every individual asset in the system and find relative analysis on them. It is not just IT systems that are in the utility we also have an operational technology systems which includes SCADA, ICS and other services. A correlation need to be achieved between them so any incident reported in one system can find its track to the other system. In the past this has been a major vulnerability exploited by the attackers.

7 Security Monitoring & Logging

The word 'Monitoring' defines a lot of elements in the system, but required more description in its scope. In a system there are several data points and infrastructure components that generate logs, alerts, message information which can overwhelm the database and automated system resources to analyze it. Therefore to make system behave correctly and timely, monitoring process needs to be defined and structured such that real-time data can be utilized to provide priority results.

There have been several approaches to accumulate and manage data, how simplest one is to segregate the monitoring process with functional zone, thus confined monitoring to limited set of assets is provided. It can be combined with operation technology so to form a collective log management system for the zone; making it easier for the system to correlate events.

The monitoring on the basis of load testing is another way to determine how many devices can be grouped together in a zone. This include sample load tracking by taking normal & peak frequency of events report.

The operational technology like PLCs, RTUs, and IEDs does not generate alert but do generate lots of information for historians to keep track therefor these information can collected through the Historian, where concise amount of information can be filtered for monitoring and retention.

7.1 MONITORING ELEMENTS

7.1.1 Security Events

The security events are generated by the security devices; it can be a network or host application like firewall, IDS/IPS, content filters and etc. When an alert is generated the event can be either positive or negative (False positive). The numbers of these generated events are very important as an increase in significant amount of 'False positive' events can hide threat. An important point to mention here is when you create granular polices on the device, it does support your routine operations but does generate a lot of 'False positive' alert making real threat difficult to be distinguish among them.

In order to retain event data only, real alerts should be captured and false positive events should be filtered out. This is very useful in Forensic investigation to catch the threat patterns and existence across the system. The best practice is to manually generate legal traffic in the system and create policies such that no alert generate for them.

7.1.2 Assets

Almost all the assets with operating system installed on it generate internal log for their activity, system failure, system information, modification in system or configuration, new application installation etc. The health of this system can easily be monitored and maintained through this log. The asset logs are helpful in the event of any misuse of authentication services or changes in the file system. These log should be integrated with industrial software for integrity such as 'tripwire' and 'ncircle'.

7.1.3 Configuration

Configuration monitoring can easily be done through the monitoring of configuration file on the asset. The configuration monitoring has multiple parameters to look after as described below.

- Identification of basic configuration either through template or provided guideline.
- The change control authority.
- Configuration change impact on the system.
- Identify, check and alert if any other changes are occurring in the system at same time.
- It is important the check the administrator role, responsibility and timing of change window with other systems. The configuration change window and information can also be attached for authorization.

7.1.4 Applications

Application monitoring is need to check the health of the application and it access to the users. The logs generated by the application can include user authentication, accounting of user. In case of patch update or new installation in the system the application behaviour can monitored across the network.

7.1.5 Network

Network does not mean security other behavioural characteristics and information can be collected. Such as logging of all network flows, session duration, amount of data transferred, bandwidth usage and link utilization can be monitored. The data gathered can be used for creating network finger print, future up gradation in the network, and application behavioural understanding. This also includes maintaining QoS across the network, as industrial traffic is all about real-time data. SNMP trigger and authentication can be sent to logging services.

7.1.6 User Identities & Anomalies

User is a generalized term, it can be human account or asset that need authentication to communication directly to each other. In this case an HMI that gather data from all the station and field equipment need individual authentication login with these assets. There are several systems that can be used for maintaining and managing user credential and providing authentication services with accounting and authorization such as NETIQ from Sun, Active Directory & LDAP from Microsoft and IBM Trivoli identity.

7.1.7 Additional Context

User identification is away to collect data about activities within the system. There can be other ways in which data can be gathered some of them are mentioned below.

- **Directory Service -** Provide information for users asset, role, services and privileges in the utility
- **Identity services -** Provides correlation between accounts, privileges and usage of right in the utility.
- **Vulnerability Scanner -** it generates result by scanning system assets, files and other service and report in any unique variable are found on network that requires administrative attention.

- **Penetration testing tools -** Penetration test simulates an attack vector and logs that will be generated in that scenario; the penetration test highlight the weakness of the system and provides further security enhancement opportunities in the system.

7.2 SECURITY MONITORING METHODS:

7.2.1 Log Collection:

Log collection is the simplest process to collect all report and activity information from the device. It can be sent in the form of a file after some time interval or every log is sent individually by the device to log collection, which then manages it in own pattern. On configurationally aspect, an IP address needs to be defined for sending the logs to the server. Software agents can be used to authenticate and retrieve the logs from the device.

7.2.2 Direct Monitoring

Direct monitoring uses network probes to catch the network traffic, this can be done though IDS and IPS inspection, application monitor, sniffers and etc.

7.2.3 Indirect Monitoring

The inferred monitoring is collection logs indirectly through other devices. In this case the device in middle collects the logs from the devices underneath hierarchy or even checks their status if no logs can be collected from them. The middle devices take responsibility to provide activity and health status to the log monitoring system.

Inferred monitoring is used in the case of encrypted message where these device decrypts the message and then inspects it before sending the messages to log server, the other way is to leave encrypted intact and generate alert for unencrypted traffic.

7.3 INFORMATION MANAGEMENT

Information management is the next step of arranging of raw data and doing analysis on logs with situational awareness. The syslog and SIEM are capable to perform many functions without user interventions and perform data event correlation. These information management tools provide a detailed graphical view of all collected data. The queries can be sent as well to get specific analyzed information for business or industrial purposes.

7.3.1 Queries:

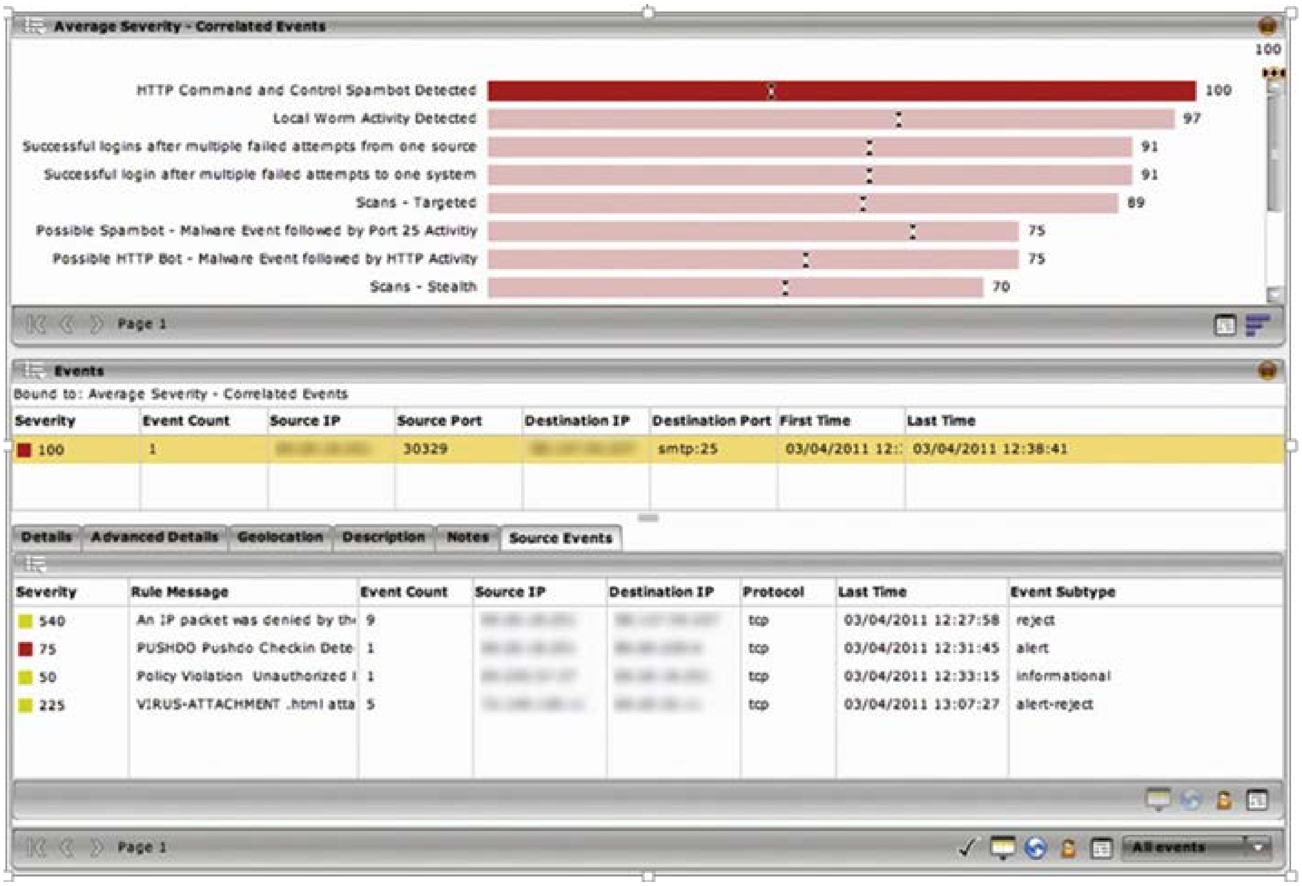
Queries are used to attain certain reports from data management systems. These queries can be plaintext or SQL query. Some example of queries can be:

- Most bandwidth consuming workstations
- Most frequently reported events

- o Most extensively used application on network
- o Most critical event reported in a certain time

The management system should be able to analyze your data and provide security and business decisions. The results can be different formats such as text, graphical charts, values, interactive report as well. For example administrative activities for NERC compliance.

The next query shows incidents.


Average Severity - Correlated Events
100
HTTP Command and Control Spambot Detected 100
Local Worm Activity Detected 97
Successful logins after multiple failed attempts from one source 91
Successful login after multiple failed attempts to one system 91
Scans - Targeted 89
Possible Spambot - Malware Event followed by Port 25 Activitiy 75
Possible HTTP Bot - Malware Event followed by HTTP Activity 75
Scans - Stealth 70
Page 1
Events
Details
Advanced Details
Geolocation
Description
Notes
Source Events
Page 1
All events

Bound to: Average Severity - Correlated Events

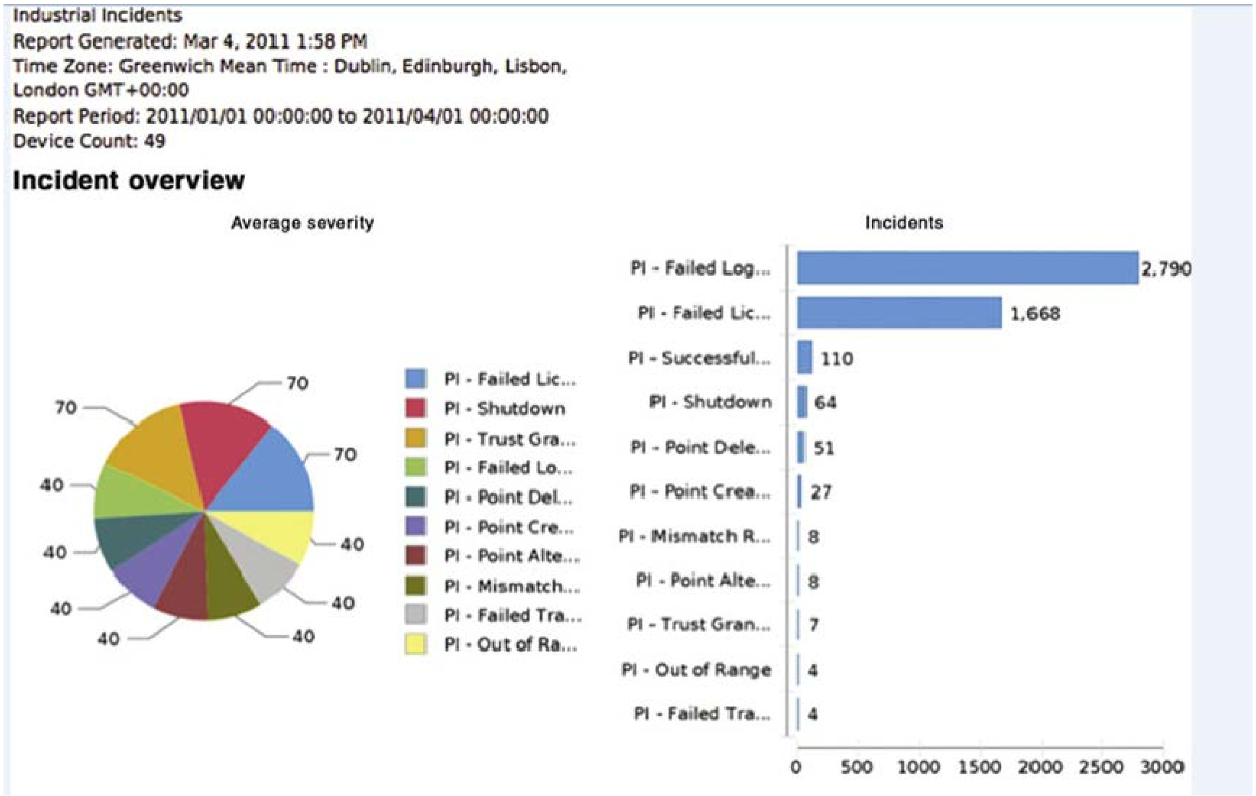
Severity	Event Count	Source IP	Source Port	Destination IP	Destination Port	First Time	Last Time
🟥 100	1	[redacted]	30329	[redacted]	smtp:25	03/04/2011 12::	03/04/2011 12:38:41

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
🟨 540	An IP packet was denied by th	9	[redacted]	[redacted]	tcp	03/04/2011 12:27:58	reject
🟥 75	PUSHDO Pushdo Checkin Dete	1	[redacted]	[redacted]	tcp	03/04/2011 12:31:45	alert
🟨 50	Policy Violation Unauthorized I	1	[redacted]	[redacted]	tcp	03/04/2011 12:33:15	informational
🟨 225	VIRUS-ATTACHMENT .html atta	5	[redacted]	[redacted]	tcp	03/04/2011 13:07:27	alert-reject

Figure 7 – Sample Network Querries

7.3.2 Reports

Reports provide a formatted content for logs and events. The reports can be very detailed or brief but has the capacity to present any data. SIEM example of Historian authentication failure is displayed in the following snapshot.



Industrial Incidents
Report Generated: Mar 4, 2011 1:58 PM
Time Zone: Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London GMT+00:00
Report Period: 2011/01/01 00:00:00 to 2011/04/01 00:00:00
Device Count: 49

Incident overview

Figure 8 – Sample Report

7.3.3 Alert

Alert displays a reactive approach through logs and application of system. We will discuss few method of alert notification by SIEM systems.

- Physical indications such as light on devices etc.
- Notification sent to particular administrator or group depending on severity
- Involving particular vendor support contact, and collecting all the details for technical support persons.
- Taking backups and executing script to contain impact.

The SIEM can also suggest decisions when alert are generated for administrative assistance.

7.3.4 Incident Investigation

The log management tools are helpful in understanding and providing in-depth detail about the incident. This includes a time based sample of incident reporting and changes occurred in the utility. The quick detail for incident like assets, IPs username can easily be tracked. The system is also useful in providing reports about the impact domain of incident.

In the case of an incident, automated response behaviour of SIEM can be seen by the following examples,

- In the case of alert, asset network interface can turn down or the device can shut down.

- Running a network script to contain the impact of threat.
- Disabling of user account if found utilized on a rogue device.

7.4 Log Storage & Retention

7.4.1 - Nonrepudiation

Nonrepudiation represents the data integrity as in the case of any incident raw data of event may be required to prove the incident notes to auditors. There are several ways to retain the integrity by pulling checks such as checksum, protection storage and etc. The use of digital signature put a hash algorithm on top of data and calculates the value. In any circumstance if the data changes the calculated hash value with also differ from previous one. Facilities like SAN can be used to provide data security by authentication and encryption.

7.4.2 Data Storage

A study shows that hour duration of time in midsize organization can generate 170 GB of log data, this number can be completely avoidable in industrial networks if proper mechanism is used to install rules in the network. Every industry standard provides different duration for data retention. NERC represents 90 days to 3 years of duration, depending on log data and events. Few points to consider here is the storage mechanism.

- This can be stored on tape on regular basis.
- Log file size and compression method to store logs.
- Period of retention for every file and its disposal method after the retention period is over.

7.4.3 Data availability

Data availability defines how much data is available for analysis at current moment. This data is also called live data as it can be required to provide trend analysis at any moment.

We will consider the NERC standard where list of all net flows is required up till three years. A query on flows generated from outside the zone to inside is executed the SIEM will 3 take years of data to process this query it might not be possible at that moment to have all the data therefor to make the result available multiple process can be run to read from archive as well as from current data. Once the processes are completed then their results can be combined to provide a single report. Considering the industrial security need the available data can be managed in smaller zones for efficient retrieval. The important thing to consider for data availability is:

- Meeting the compliance retention time.
- Average number of event collected at a sample time.
- Response time availability after the incident has occurred.
- Analysis reporting criteria, how detailed and extensive information is required.

8 Acronym

BMS	Building Management System
CCTV	Closed Circuit Television
CE	Customer Edge
CIP	Critical Infrastructure protection
CR	Cluster Router
DCC	Data and Control Center
DLL	Dynamic Link Libraries
DMZ	Demilitarize zone
DNP3	Distributed Network Protocol 3
FAN	Field Area Network
GOOSE	Generic Object Oriented Substation Event
ICCP	Intercontrol Center Communication Protocol
ICS	Industrial Control Systems
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IP	Internet Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Interior Router
ISIS	Intermediate System to Intermediate System
ISP	Internet Service Provider
I.T	Information Technology
LER	Label Edge Router
LSP	Label Switched Path
LTE	Long-Term Evolution
MiM	Man-In-Middle
MMS	Manufacturing Message Specification
MODBUS	Modicon Communication Bus
MPLS	Multiprotocol Label Switching
MTU	Master Terminal Unit
NBAD	Network Based Anomaly Detection
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSP	Network Service Provide
OSPF	Open Shortest Path First
OSS	Operating Support Systems

OT	Operation technology
PE	Provider Edge
PHY	Physical (layer)
PLC	Power line communication
PPP	Point-to-Point Protocol
PROFIBUS	Process Field Bus
QoS	Quality of service
RF	Radio frequency
RSVP	Resource Reservation Protocol
RTT	Round-Trip Time
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Control Language
SIEM	Security Information and Event Manager
TE	Traffic engineering
UTM	Unified Threat Manager
VLAN	Virtual LAN
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
WAN	Wide Area Network
WR	WAN router

9 References

- Deshpande, K. C. (n.d.). *Communication Networks for Smart Grids - Making Smart Grid Real.* Springer.

- Knapp, E. D., & Langill, J. T. (December 22, 2014). *Industrial Network Security, 2nd Edition.* Syngress.

- Response, S. S. (2012). *The Shamoon Attacks*. Retrieved from http://www.symantec.com/connect/blogs/shamoon-attacks.

- Symantec, C. W. (n.d.). *Targeted Attacks Against the Energy Sector .* Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf.

- NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

- CPNI. GOOD PRACTICE GUIDE PROCESS CONTROL AND SCADA SECURITY. Retrieved from https://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf?epslanguage=en-gb

- SANS, Security Awareness program Guidance, Retrieved from
  - http://www.securingthehuman.org/resources
- Symantec. Emerging Threat: Dragonfly / Energetic Bear – APT Group. Retrieved from
  - http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

- OPEN IEC61850, Retrieved from
  - http://en.wikipedia.org/wiki/IEC_61850
  - http://www.openmuc.org/index.php?id=24
- SANS Institute. A Practical Application of SIEM Automating Threat Identification, Retrieved from
  - http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781
  - http://www-03.ibm.com/software/products/en/qradar-siem/
- Security for Process Automation with SIMATIC PCS 7. Retrieved from
  - http://www.industry.siemens.com/topics/global/en/industrial-security/products/pages/process-automation.aspx
- Symantec. Patch Management Best Exercises. Retrieved from
  - http://www.symantec.com/business/support/index?page=content&id=HOWTO3124
- Tofino Security. Making Patching Work for SCADA and ICS Security. Retrieved from
  - https://www.tofinosecurity.com/blog/making-patching-work-scada-and-ics-security

- John Dirkman, P.E.. *Best Practices for Creating Your Smart Grid Network Model*. Schneider Electric.

- Metin Ozturk and Philip Aubin. *SCADA Security: Challenges and Solutions*. Schneider Electric.

- Schneider Electric. (March 2012 / White paper). *SCADA Systems: Telemetry & Remote SCADA Solutions*.

- NIST. (April 2006 / Information security). *Electronic Authentication Guideline*.Retrieved from
  - http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

- NERC (CIP-002-5). Cyber Security — BES Cyber System Categorization.
  - http://www.nerc.com/files/CIP-002-5.pdf
- NERC (CIP-003-5). Cyber Security — Security Management Controls.
  - http://www.nerc.com/files/CIP-003-5.pdf
- NERC (CIP-004-5). Cyber Security — Personnel & Training.
  - http://www.nerc.com/files/CIP-004-5.pdf
- NERC (CIP-005-5). Cyber Security — Electronic Security Perimeter.
  - http://www.nerc.com/files/CIP-005-5.pdf
- NERC (CIP-006-5). Cyber Security — Physical Security of BES Cyber Systems.
  - http://www.nerc.com/files/CIP-006-5.pdf
- NERC (CIP-007-5). Cyber Security — Systems Security Management.
  - http://www.nerc.com/files/CIP-007-5.pdf
- NERC (CIP-008-5). Cyber Security — Incident Reporting and Response Planning.
  - http://www.nerc.com/files/CIP-008-5.pdf
- NERC (CIP-009-5). Cyber Security — Recovery Plans for BES Cyber Systems.
  - http://www.nerc.com/files/CIP-009-5.pdf