# Application vs Security: The cyber-security requirements in a modern substation automation system

Sagar Dayabhai (Pr.Eng)
System Control Manager, CONCO Energy Solutions (PTY) Ltd, A subsidiary of Consolidated Power Projects

*Abstract*

**Smart grid enabling technologies which exist in modern substation automation systems require the use of switched Ethernet and TCP/IP based protocols to exploit the available network capacity and data transfer rates needed for the use of IEC 61850 and other SCADA applications.**

**This paper discusses a best engineering practiced approach of developing the cyber-security requirements for a modern substation automation system with IEC 61850 encompassing an advanced communications network. This paper presents several challenges facing utilities with implementing cyber-security and the potential threats and vulnerabilities which exist in the context of a substation automation system.**

**The use of intrusion detection and prevention systems, control system protocol inspection using deep packet inspection mechanisms, logging, forensic analysis and regulatory compliance capabilities is discussed. Anomaly detection and event forensics is explained through a case study performed on a typical substation automation network.**

**This paper further outlines the training requirements and presents an overview of the cyber-security standards applicable in a modern substation system.**

**Keywords: IEC, SCADA, IP, HMI**

## I. INTRODUCTION

Several benefits can be derived from substation automation applications including the intelligence to identify and deal with abnormalities, predict events and adjust the grid accordingly; demand side management; efficiency; improved plant availability and reliability amongst many other key metrics. Consequently, to engage and implement these technologies, the need for a reliable communications network infrastructure capable of supporting these systems and services is required.

In many cases, the implementation of these communication networks is not optimized to achieve the security requirements of the system and applications. Moreover, in cases where the cyber-security requirements are considered, the resulting networks are more complex than necessary or required. Modern cyber-security solutions encompass features that far-exceed familiar access control lists that exist in a firewall. The security posture in a substation is constantly changing and is affected by evolving threats, product vulnerabilities, rapidly changing technologies in security appliances, business processes, and people.
Utilities face several security challenges when evaluating their risk appetite and developing their cyber-security strategy.

Some of the security concerns and design requirements that need to be addressed include common governance procedures, secure remote engineering access, cyber-security training, managing threats and cyber-attacks in a SCADA system, security controls, common standards and security policies, compliance reporting and current and emerging cyber-security technologies.

Moreover, a deeper understanding of the threat vectors and vulnerabilities that affect utilities in the context of their application requirements is needed to develop the cyber-security requirements and design.

## II. APPLICATION REQUIREMENTS

In the power system, the focus has been exclusively on implementing equipment that can keep the system reliable. However, recently, the substation automation and control system that supports the monitoring and control of the power system has come to be extremely critical to the reliability of the power system [9]. To ensure this reliability, the substation automation system is designed with the following typical application requirements:

- Fault tolerant network design.
- Low latency network and high speed reliable communications system required.
- Real-time data access of mission critical data for power system operations.
- Secure remote access to data is needed due to the large number of stakeholders involved in the availability / reliability of the power system value chain.

Business and operational processes communicate across OT and IT networks increasingly using standard IT systems, standardized IP based protocols and public communication infrastructure [7]. Consequently, the substation automation infrastructure is considerably more vulnerable to cyber-attacks then a conventional isolated legacy

system with non-routable protocols. Security by obscurity has traditionally been the primary approach to addressing cyber-security in these systems [9].

It is a common misunderstanding for utilities to address cyber-security by specifying the technology and the security capabilities of the products and systems in order achieve a secure substation automation system or to counter the equivalent security risk. Deploying firewalls, secure hardened servers and anti-virus software is not sufficient to ensure security compliance. Furthermore, it is often assumed that the substation automation system is protected using robust and technologically advanced security appliances following processes and policies presented in the IT domain. Figure 1 presents a comparison of the security requirements of a substation automation system and an IT based system [10].

| | Energy Control Systems | Office IT |
|---|---|---|
| Anti-virus / mobile code | Uncommon / hard to deploy | Common / widely used |
| Component Lifetime | Up to 20 years | 3-5 years |
| Outsourcing | Rarely used | Common |
| Application of patches | Use case specific | Regular / scheduled |
| Real time requirement | Critical due to safety | Delays accepted |
| Security testing / audit | Rarely (operational networks) | Scheduled and mandated |
| Physical Security | Very much varying | High |
| Security Awareness | Increasing | High |
| Confidentiality (Data) | Low – Medium | High |
| Integrity (Data) | High | Medium |
| Availability / Reliability | 24 x 365 x ... | Medium, delays accepted |
| Non-Repudiation | High | Medium |

Figure 1: IT/OT domain security requirements [10].

Addressing cyber-security for critical assets in the substation automation space requires the employment of a holistic Defence-in-Depth approach. The concept of Defence-in-Depth is discussed later in this paper.

## III. SECURITY CHALLENGES

Several utilities face security challenges amongst other financial and commercial issues which prevent them from meeting the application requirements of substation automation. This includes:

- The increasing amount of data now available from a substation IED and the multitude of stakeholders that require access to this data increase the attack surface and the complexity of the network.
- Geographically vast sites require remote access and visibility for real-time data transfer of operational and non-operational data which have high infrastructure costs for communications and security.
- Lack of visibility and control of existing ageing infrastructure.
- Cyber threats on existing OT networks.
- Vulnerabilities on existing OT networks which include:
    - Human errors.
    - Training, skills and inadequate procedures and policies.
    - No anomaly detection.
    - Insecure communications.
    - No disaster recovery / response plan in place.
    - No Monitoring and logging.
    - Lack of knowledge in SCADA protocols.
    - Lack of compatible forensic tools for field devices.

## IV. CYBER-ATTACKS

Utilities are faced with several potential threats and vulnerabilities which can lead to cyber-attacks and are often not understood. These potential threats can occur when there are changes in technology; socio-economic and political conditions is experienced; during domestic and international terrorism activities; espionage, malicious and recreational hackers attempting to attack the utility; disgruntled / ex-employees seeking revenge; during attempt of fraud and/or a consequence of infrastructure deterioration.

Many risks exist which can compromise the state of the power system and a utility should consider addressing and applying risk mitigation plans to prevent vulnerabilities being exploited from threats. Some of these security concerns and risks on the substation automation system are identified below.

- Illegal gathering of control and protection settings information that could be used in a subsequent attack [3].
- Protection settings altered with the intent to degrade the reliability of the device and the power system protection system [3].
- Attempts to shut down the substation / power-system [3].
- Equipment inaccessible to users and possibly services are non-functional through a denial of service attack.
- SCADA system illegally accessed and damaged and/or functions illegally altered.
- Metering data is illegally accessed and altered.
- Planting of malicious code that triggers a delayed or coordinated attack. These are one of the most complicated types of attacks to manage and can be the most damaging.
- Shut down the regional control centre and/or national control centre controlled by the SCADA system either immediately or in a controller manner depending on the inter-

connection of the substation network, telecommunications network and the control centre SCADA system.

There are various vulnerabilities which exist in a substation automation system which can be exploited to penetrate the system and compromise the electrical power system by applying the security risks identified above. This can cause considerable loss or complete destruction of primary plant equipment in the substation and create a disturbance in the power system resulting in interruption of energy supply to consumers. Attacks gaining control of protection IEDs and SCADA systems can perform unauthorized switching operations which in the incorrect sequence could cause a large power system failure and / or blackout.

Attacks are often performed by targeting specific vulnerable systems and services including operating systems, protocols and communication networks in the substation automation system.

The expanded use of open protocols for purposes of tele-control and SCADA and use of TCP/IP based networks in the substation have increased the attack surface despite the benefits derived from its inception.

The availability of a high-speed TCP/IP based communications network and the inter-connection of WAN/LAN networks in the operational domain has made remote access to protection, automation and control equipment possible. This has allowed utilities to increase key performance indexes by rapidly identifying, diagnosing and repairing faults. However, incorrect security management of this network can result in the SCADA system being used as a backdoor into the corporate IT system to obtain company and personal identity information. This vulnerability is further exacerbated if utilities employ the use of unmanaged insecure public communications system in the substation for purposes of metering, remote access etc.

Conventionally, embedded systems focused on specific industry domain / use case applications. In a modern substation automation system, the increase in amount of software components and standard operating systems have propelled the exposure of malware and viruses in this environment.

Amongst performing their core protection function, IEDs are also used for voltage regulation, automatically switching high-voltage plant equipment during fault localization and system restoration and encompass high frequency measurement of phasor quantities used for intelligent decision making processes designed to improve the reliability and stability of the power-system. Furthermore, these devices report warning signals and critical alarms to control centres and local HMI systems for situational awareness and alarm management. Illegal access, control and alteration of data reported from these devices can present disruptive and catastrophic events on the power-system. It is now necessary not only to consider the security appliances used to protect the substation automation system but extend the scope of the security system to detect anomalies and present information to the utility in a manner which can detect and prevent such an attack.

Moreover, engineers are required to engineer the protection systems in the substation with fail safe scenarios which include synchronization, redundancy and software based interlocking for safe operating sequences to serve as an additional layer of protection security for the power system. This supports the Defence-In-Depth strategy and serves as an additional layer of security.

***Attack timeline***

The number of cyberattacks has increased in the past few years. There have been quite a few attacks in recent years targeted in the energy sector [11]. Figure 2 portrays a timeline of recent cyber-attacks.

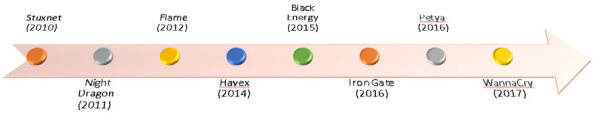


Figure 2: Attack timeline on Industrial Control Systems.

- WannyCry Ransomware (2017) which targeted computers running the Windows operating system by encrypting data and demanding ransom payments in the Bitcoin currency. The attack affected 200, 000 computer systems across 150 countries.
- Petya ransomware targeted at windows based operating systems encrypts hard-drives file system table and prevents windows from booting and demands ransom payments in the Bitcoin currency. It has targeted numerous industrial plants throughout the world including nuclear power plant in Ukraine.
- Iron gate (2016) is malware designed to work on Industrial Control systems employed a man in the middle attack to capture normal traffic on HMIs to replay it to mask anomaly detectors.
- Black Energy malware (2015) is an advanced persistent threat which specifically

targets HMI software and performs keylogging, audio recording and capturing of screenshots and is modular capable of moving through network files onto removable storage media. This malware was used as an attack against the Ukrainian power companies as announced by the industrial control systems cyber emergency response team.

- Havex targeted the energy sector in 2014 by scanning several commonly-used control system protocol ports and interrogating information available from servers.
- Flame (2012) is a malware designed to attack the windows operating system. It is responsible for propagating over a LAN, records screenshots, keyboard activity and network traffic and sends this information to several command control servers scattered around the world.
- Night Dragon (Trojan) (2011) was directed at finding project details and financial information about oil and gas field exploration and bids. Attackers started by compromising public facing Web Servers through SQL injection and move to internal computers using passwords gathered from local hacking tools.
- Stuxnet (2010) targets SCADA and PLC systems and was responsible for causing substantial damage to Iran's Nuclear program.

## V. TYPES OF ATTACKS

It is important to understand that power utilities are not exempt from the generic attacks that every other corporate or industrial company faces. These attacks aim at infecting as many computers as possible and can impact any person regardless of their employer [11]. A description of some of the general common attacks that are used on substation automation systems are described below.

### *Replay Attack*

This type of attack in which data is intercepted and maliciously repeated or delayed. In the context of a substation automation system, this attack is used for capturing of SCADA commands which can be replayed at a later stage.

### *Man in the middle attack*

Attackers place themselves between a user and/or device by establishing an independent connection. The attacker breaks the connection of the user / device under attack and impersonates the connection and re-establishes the connection of the user/device through the attacker.

### *Brute force attack*

This attack is a trial and error method targeting encryption and/or passwords with the intent of decoding passwords/ encrypted messages through exhaustive efforts.

### *Dictionary Attack*

A type of attack which attempts to break passwords or defeating a cipher by trying a list of pre-defined words in a dictionary.

### *Eavesdropping*

Eavesdropping occurs through many forms. The most common and core of eavesdropping is to silently listen to valid communications and learn about the system.

### *Denial of Service (DoS)*

The DoS attack floods a network with an abundance of requests so that the network becomes saturated and cannot respond to legitimate traffic. In Distributed DoS attacks, multiple computers are used to generate large amounts of traffic targeted at a network. A Distributed DoS employs a botnet to send simultaneous requests to the target system. This can slow down the target system to the point where it becomes impossible to work on. Martian IP packets commonly arise and can be seen on a network during a DoS attack.

Vulnerabilities in a product / IED can be triggered by an attacker that can take a product out of service. This is not a flood of data but still considered denial of service.

### *Advanced Persistent Threats (APT)*

APT is a complex attack targeted on a network over a long period. APT processes use malware and intelligent data gathering techniques to exploit vulnerabilities in a system. APT attacks are executed by coordinated human intervention rather than autonomous code and through a continuous monitoring and interaction process to complete their specific attack objectives.

### *Platform Vulnerabilities*

In any complex protection and automation system in a substation, there are bound to be bugs and security vulnerabilities found in IEDs. Security vulnerabilities in IEDs and applications are regularly identified by OEMs and are fixed through a software/firmware/patch upgrade of the device/software to prevent attackers from using

them to compromise systems/services in the substation.

***Zero-day exploits***

A zero-day attack is directed at a vulnerability of a software application that is unknown to the vendor / OEM and exploited by attackers.

***Watering Hole attacks***

This attack targets a specific group of users by infecting websites that members of the group are known to visit. The intent is to infect the targeted user's computer and gain access to the network at the user's place of employment. These attacks focus on legitimate and popular websites and exploit the sites vulnerabilities and inject malicious code that redirects the user to a separate site where the malware is hosted. This compromised website is now ready to infect the user with the inject malware upon access.

## VI. SCADA THREATS AND VULNERABILITIES

Infrastructure attacks on SCADA systems are taking place daily all around the world. In 2014, the energy sector reported the most reported incidents [15] as shown in Figure 3.

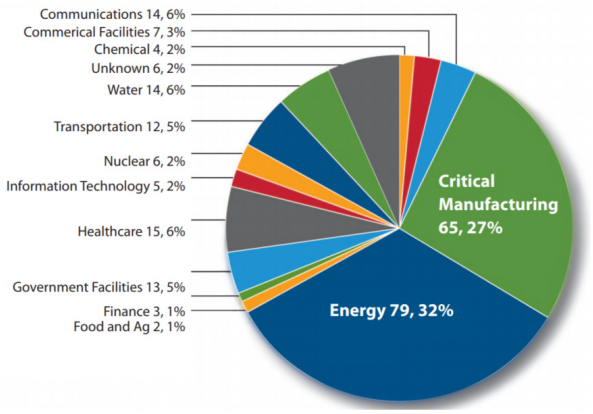


Figure 3: Industrial Control Systems Incident reports [15].

A challenge facing most utilities as discussed above is the large number of legacy systems and protocols that exist in the substation and the security vulnerabilities associated with such devices. Given the life-cycle of the protection and automation equipment in a substation, it will be a few years before substation automation devices using IEC 61850 are in widespread use employing the security defined in IEC 62351 (discussed later in this paper).

Protection and Automation devices are rarely replaced and usually undergo refurbishment after 15-20 years of its life-span. Any security vulnerabilities associated with legacy systems and protocols cannot be addressed through patches as their functionality is defined in established standards that take years to change [13]. Furthermore, they often use proprietary operating systems that have not been subjected to security hardening. Their software cannot be updated or patched frequently due to access limitations or concerns over downtime.

A summary of the type of threats and vulnerabilities that can be exploited by an attacker is described below. The likelihood of the attack being successful increases if the attacker has already gained access to the devices in the substation either locally or remotely.

- Legacy software lacks sufficient user authentication and data authenticity verification mechanisms allowing unauthorized access and exploitation of IEDs connected to the public communications infrastructure [15].
- Access to IEDs in the substation with default or simple passwords and baselines configurations allow attackers to access and compromise the substation.
- Legacy IEDs and protocols lack the ability to encrypt communication. Attackers use man in the middle and reply attacks to exploit weaknesses. Control / data packets unencrypted and visible through a network sniffer can leave the system and services vulnerable to attacks. The security of TC57 related protocols developed by the IEC is addressed in IEC 62351 discussed later in this paper.
- Making use of configuration mistakes in security [2].
- Infecting laptops while outside the substation automation network, later infecting internal system's when they're connected to the network for data collection, software/firmware updates etc. [2].
- Invalid data with no input validation as legitimate traffic allow attackers to execute arbitrary commands based on the application layer protocol. e.g. reset commands. The security weaknesses make it possible to send malicious commands to IEDs to crash and to disrupt the power system by sending control operations on controllable primary plant.
- SQL injection via exploitation of unprotected web-servers and applications which exist on HMI and SCADA systems [15].
- Network/port scanning and probing [15].

- Exploitation of zero-day vulnerabilities in substation IEDs and associated software applications [15].
- Allowing anonymous SCADA protocol connections to the system permitting unauthorized devices on the network [6].
- Generating large protocol messages which cause buffer overflows. This occurs when messages with a bigger value is received in an IED. Devices which do not validate the size of receiving messages in its logic often result in device malfunction. This platform vulnerability is exploited to compromise the IEDs in the substation [6].
- Analogous to buffer overflows, a similar vulnerability exists in platforms on certain protocols with no input validation containing illegal APDU, frame lengths and malform packets.

The SCADA network in a substation makes use of specific and often proprietary protocols depending on the function the IED is serving. Many of these protocols have limitations and security vulnerabilities as discussed above which make them susceptible to attacks. As an example, the Modbus protocol is widely adopted today in the substation and DER environment providing a client / server communication model. The protocol provides no security against unauthorized commands or interception of data. An attacker with the IP address of the device and with access to the network can use a Modbus Client simulator to create an assortment of attacks [15]. These attacks include:

- Running a reconnaissance attempt using a scanner to determine what function codes are supported in the Modbus Server.
- Issue write requests to Coils which could result in undesired control operations.
- Intercept existing Modbus connection with a man in the middle attack to interpret the response/request messages.
- Run a Brute ID Scan and send a read identification command and analyse responses from the server that will contain vendor, model, version etc. to discover devices on the network.

Another example is using the open protocol standard DNP3 with a DNP3 simulator and protocol analyser. Unlike Modbus, when analysing DNP3 messages, it is not necessary for the attacker to have seen the request message to decipher the response message. Common attacks include:

- Capturing and analysing DNP3 messages over the network or over a radio link if the radio frequency is known. The messages provide the attacker with information about the no. of RTU's, network topology, device functionality, I/O and RTU addresses etc.
- An attacker can install a DNP3 network simulator between the master and outstation that can read and fabricate DNP3 messages and/or network traffic between the master station and outstations. The easiest manner to perform this attack is through a radio network as physical access to the network is not required, only line of site or proximity to the nearest base-station and a single remote-station radio with the correct frequency is needed [2].
- DNP3 link layer attacks and performing data modification to DNP3 frames and disrupting the protocol implementation and behaviour of DNP3 devices. Several substation gateway vendors have had this vulnerability identified in their products at some point during the product's life-span [2].

Traditional firewalls using ACL do not encompass the granularity to inspect packets at the application layer to address these attacks in the substation. This issue is further aggravated with new substation automation systems adopting TCP/IP based protocols including IEC 61850 MMS.

Moreover, these firewalls are unable to distinguish the difference between a firmware update between taking place on an IED, a settings change or a read-configuration. Thus, blocking certain network related firmware upgrades or restricted commands with appropriate firewall rules results in the blocking of all SCADA traffic in the substation. As this traffic is deemed mission-critical, most engineers opt to allow all data to pass through the firewall [13]. The solution to address these attacks is to employ deep pack inspection firewalls designed to understand SCADA protocols at the application layer. However, few utilities have adopted this approach of mitigation of SCADA attacks at the application layer.

In 2014, Dell Computer Corporation reported an increase in SCADA attacks almost twice compared with the statistics in 2013. World-wide SCADA attacks increased from 91, 676 in January 2016 to 675, 186 in January 2014 [7]. In many cases, SCADA attacks often go unreported. Consequently, some utilities may not even be aware that a threat exists until they are targeted. Vulnerabilities can be present in current and emerging IEDs in substations and can be present for years before they are revealed. Figure 4 presents the most vulnerable components as reported by Kaspersky Labs [12]. The leading components all belong in the substation automation environment.

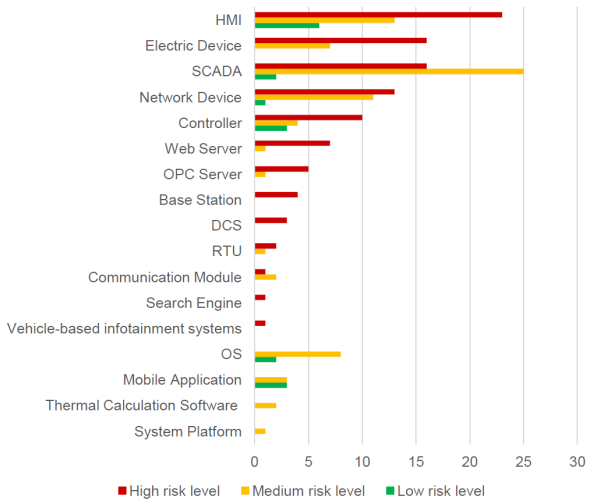


Figure 4: Vulnerabilities per component [12].

The top most widespread types of vulnerabilities are presented in Figure 5.

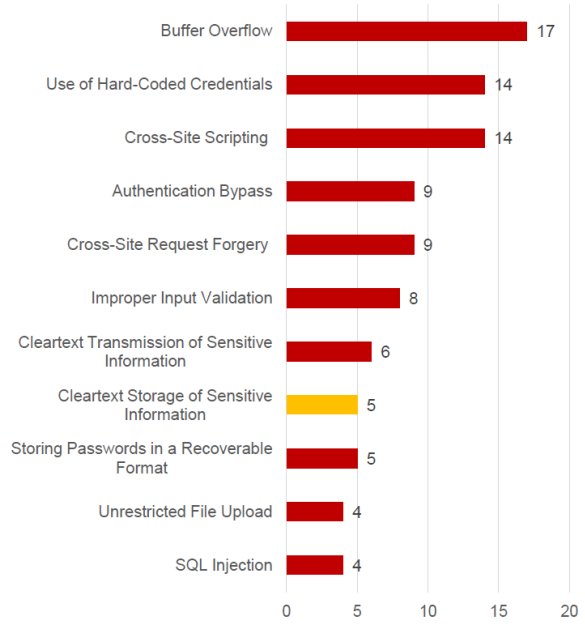


Figure 5: Types of Vulnerabilities [12].

## VII. SECURITY VS APPLICATION

The overall target is to reduce the system's attack surface as much as possible. To achieve this, it is important to perform an audit of the existing environment. This audit should include a data validation process encompassing an inventory of all cyber-assets (legacy and current), hardware/software versions, communication links, user access and privileges, access points and architecture of physical and logical connections of the system.

This exercise will allow the utility to have a transparent view of the system to perform a security risk assessment based on the potential threats and the vulnerabilities which exist. These results together with the criticality of the system and business impact attacks can be used to develop the cyber-security strategy. The financial investment required and the cost/benefit can then be assessed based on the overall risk appetite.

The design of the security system is often not optimized to achieve the requirements of the applications. The resulting design is often far more complex and the financial investment does not motivate the inception of the overall security system implementation. Utilities are then discouraged to embrace cyber-security as result of the cost implications. The following sections cover some of the best engineering practiced security designs which need to be employed when developing the security posture of the substation automation system. Some of these security controls can be achieved in a cost-effective approach allowing utilities to prioritize and adopt accordingly.

### *Policies and Procedures*

It is important for utilities to promote understanding of regulations / standards using top to bottom approach starting from the executive team. Employees need to be reminded and trained on the security policies and their expected behaviour and role in the organization in the context of cyber-security [2].

Utilities are required to establish the following processes for security management:

- Establish system back up and disaster recovery plans [4].
- Establish configuration management process [4].
- Establish defence in depth layered approach for security management.
- Conduct penetration testing and vulnerability analysis of access points to substation automation network to evaluate the protection on these connections. The network is as secure as its weakest point.

### *Strong Access Control and Authentication*

Vulnerable physical and electronic access to substation networks is a strong enabler for several cyber-attacks. The following are some of the recommended controls for use in the security design:

- Recommend employees to use open-source password software/generators to eliminate

the use of weak passwords. Enforce a complex-password policy to mitigate dictionary and brute force attacks.
- For remote access to sites of strategic and critical importance to the reliability of the power system, use multi-factor authentication from two authentication vectors to prevent identity / credentials theft.
- Employ role based access control with varying level of rights using a defence in depth strategy.
- Default passwords should not be used in substation IEDs to eliminate backdoors.
- Always use account lockout / delaying mechanisms on substation IEDs for brute force mitigation.
- Always enable Inactivity/session Timeouts on Substation HMI systems and all web-based applications to prevent authorized and privileged connections from remaining open with no activity. This will ensure that a substation operator's last logged in credentials are logged-off automatically.
- Modern IEDs support Centralized Authentication (RADIUS / LDAP) and password management using role based access control which facilitate a defence in depth security strategy [4].
- Password management policy should include periodic change of passwords.
- Protect passwords via encryption.
- Enforce the concept of least privilege on all systems. Avoid the use of unnecessary privileges including authorization to deploy applications, change whitelisting regimes, disable security policies and/or modify application permissions.
- Enable password-protected console or virtual terminal access.

***Monitoring and Logging***

Monitoring and logging is a function of nearly every modern IED and a requirement for substation automation security. However, the true potential of monitoring and logging is rarely harnessed by utilities.

- Security logs provide the means of detecting intrusion attempts and unauthorized activity. Many attacks are intended to be silent and gather information (e.g. Espionage) and can last for a long period and can precede a malicious event. User audit logs recording and reporting instances of valid and invalid user authentication and session terminations.
- Use warning banners and usage policies to discourage electronic intrusions and enable electronic monitoring and trespass prosecution. This customizable facility is available on modern IEDs in a substation.
- Ensure that all control operations are logged on the Substation HMI and Gateway and provide for individual accountability through protected action logs per user. Ideally, the alarm/operator logs should not be deleted or should only be deleted by a user with an escalated privilege level of authority.
- Log alarms and security logs in the substation. Management of alarms is a critical component of monitoring and logging and should be processed and classified per the models defined in ANSI/ISA 18.2-2009 and IEC 62682 [16].
- Security logs should be regularly scanned to detect anomalies / abnormal behaviour / APT's.
- Syslog is a standard, software packages can analyse security data and generate reports / security metrics. It is available on most networking, SCADA products and operating systems, but often never used or disabled. Syslog is a protocol used for sending events to a data collection server or Security Information and Event Management (SIEM) server.
- Using a SIEM can help correlate related alerts in one place. This centralized repository can be used as a tool to cross-reference threat intelligence information to generate action plans, identify anomalies and facilitate revelation of unnoticed attacks.
- Using a SIEM, establish an incident monitoring process with intrusion detection that includes monitoring and alerting network administrators of malicious network activity.
- In the case of renewable energy plants and small DER systems, an operator will not be constantly monitoring alarms and events at the HMI or SCADA system. Consequently, it is critical to have a facility which provides rapid notification of alarms and disturbances on the power system. Notification using SMTP and SMS can be employed to facilitate this. Ensure that watchdogs and alarm contacts are configured to actuate for access, password and setting change events and report using these notification systems.

***Security Controls***

The security risk assessment can be used to plan the Defence in Depth strategy as the risk assessment covers all inter-connections, dependencies and considers all cyber-assets and access points. This strategy is critical to provide effective layers of monitoring and protection of the substation automation system.

The intent is to reduce the opportunities for an attacker to take advantage of traversing laterally through the network and have a large complement of systems available to fulfil the objectives of the attack. This also increases the difficulty of reconnaissance activities. Several security controls can be implemented to supplement the Defence in Depth Strategy by providing a layer of boundary protection at the substation. These controls include:

- Implementing VLANs as a security mechanism is a common practise. However, using default and native VLANs which are not correctly configured on Trunk ports can allow network connectivity to other VLAN segments.
- Ensure that all networking equipment has the Dynamic Trunking Protocol associated with VLANs is disabled all ports are configured as static access ports.
- Refrain from using VLAN 1 for in-band management traffic. Separate management traffic from user data / protocol traffic.
- All logical / physical ports that are unused should be disabled.
- Prevent unauthorised access to substations and control centres using access control and physical security and surveillance measures.
- Disconnect direct connections to SCADA / Substation automation networks. Utilization of DMZs for the secure transfer of data to business networks is the secure approach [4].
- Ensure that secure remote access is provisioned with multi-factor authentication and VPN access is limited to jump servers which access the substation automation system.
- Deny by default stateful Firewall protection should be in place guarding each point of entry [4].
- Employ Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). These solutions monitor and create alarms for any traffic outside of normal operations. Simple rules can be created for alerting, management, logging, blacklist and whitelist alerts. IPS acts by further blocking traffic that does not meet the defined rules and needs to be strategically positioned in-line with firewalls [18].
- Deep packet inspection of SCADA traffic in the substation automation system can significantly improve the security and reliability of the system [13]. Next generation Firewalls which can perform deep packet inspection at the application layer and can understand the specific SCADA protocols addresses several SCADA threats discussed earlier. Worm / malware designers work to stay under the radar by hiding their network traffic inside protocols that are already common to the network they are attacking.
- Secure wireless transmission over the air should be employed to prevent eavesdropping. e.g. capturing of DNP3 messages over the air. This includes RF communications for area radio networks or using Bluetooth for recloser access.

***Patch Management***

Evaluate the patch and security management capabilities of the supplier and their products. When performing such patch / security upgrades, ensure the authenticity and integrity of security patches.

Application whitelisting is an alternative approach of reducing the attack surface of a substation automation system. It establishes a known baseline to prevent unauthorized executables from running and eliminates anti-virus patch requirements and assists in malware protection. It can reduce the complexities of managing patches, addresses the lack of security patch support from vendors and can be used to prevent distributed DoS attacks. This process applies stable configurations on an embedded system that does not need to change over time.

## VIII. CASE STUDY: ANOMALY DETECTION AND FORENSIC ANALYSIS

Historically, many automation and control systems in a substation have been islanded in separate networks and not connected to the public communications network or a larger WAN/LAN network. However, the security through segregation approach does not fully guarantee and protect the system against cyber-attacks [11]. Networks are often rarely completely isolated and in some cases, configuration updates are periodically done, log files transferred, remote access provided for support from the supplier / OEM, system interaction and files transferred through a USB or temporary modem etc.

An additional source of concern is that many countries have started to embrace deregulatory energy market for smaller independent power producers (IPP). In many cases, these IPPs operate autonomous DER systems feeding energy into the grid but do not have full IT/OT support at these facilities. These DER systems typically deploy new technology which can contain unknown vulnerabilities. These systems are expected to operate over 10-20 years of the plant's life-span. Even though these sites make up a small portion of the grid, they need to be carefully monitored. Small outages or changes on the DER systems can have a domino effect for the whole power grid.

A case study was performed on a typical DER system to determine the level of security which exists in a network and to be able to ascertain if a system is sufficiently secured.

A behavioural analytical system with Anomaly Detection was used to perform forensic event analysis on a typical DER system that would in some cases be connected to a public communications network for purposes of external monitoring and control.

These monitoring tools have a library of known vulnerabilities in the substation automation environment and have a self-learning baseline profile that is used for determining the detection characteristics. e.g. Illegal APDUs and frame lengths. Alerts are provided on a packet that exceeds the maximum size [6].

Additional vulnerabilities can be added and the detection characteristics can be used to apply a whitelisting regime on the network based on the results of the forensic event analysis.

Prior to implementing the anomaly detection system, no issues or security concerns existed based on the information available to the operator and all sub-systems were performing their functions as expected.

The results of the forensic analysis include the following [18]:

- Duplicate MAC Addresses found on the network based on a masquerading issue on the firewall.
- Inconsistent unidirectional response messages were picked up on a Modbus connection signifying a configuration related issue.
- GOOSE traffic observed at various segments of the network signifying a potential leakage of GOOSE traffic.
- Visibility of public routable subnets found in network using HTTP/HTTPS/SSL/ICMP.
- Alerts / Vulnerabilities detected based on existing SNORT rules and CVEs.
- Constant ICMP attempts with no replies
- Broadcast traffic found

In addition to the above alerts, additional information on the traffic traversing through the system is also available. This includes:

- An estimate of the amount of SCADA traffic capacity per site (SCADA Protocols traffic)
- An estimate of the amount of non-SCADA traffic capacity per site (IT data, non-SCADA protocols)
- Changes in network and traffic volumes / speeds / rates.
- Vulnerability assessment to determine the level of compliance and produce a report that outlines the structure of the system.
- Protocol Distribution indicating the statistics for each type of protocol in the system that is being monitored during the period as shown in the Figure 6 below.

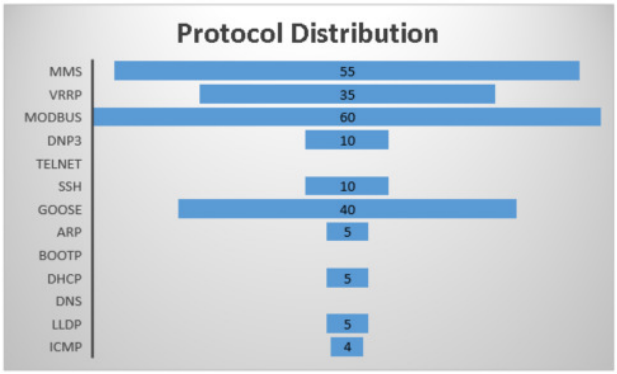


Figure 6: Protocol Distribution of devices.

The importance for utilities to perform such forensic analysis on large networks cannot be further emphasized and stressed. It is vital for utilities to explore this avenue to gain a better understanding of their networks and determine if their security designs are providing the required level of protection needed for their critical substation automation systems.

## IX. TRAINING

Training is a fundamental component of any robust cybersecurity strategy. Hands-on training featuring Red Team/ Blue Team exercise within an actual substation automation environment using a Training Management System is necessary for employees to face real world cyber-attacks in their operational environments.

Security training management systems monitor and log the performance of each employee based on the scenarios they have been trained in and the objectives they are required to achieve. Cyber-attacks are injected into the network which emulates real-world attacks and various scenarios exist based on the type of attack for employees to detect, respond/diagnose and prevent the cyber-attacks.

Despite having all the necessary tools, dealing with cyber-attacks is a complex task requiring a level of forensic analysis needed. Cyber forensics training will empower employees with the necessary skills to perform forensic analysis on a system. This includes:

- Experience with working on domain controllers.
- Understanding how to work with windows event logs.
- How to perform and manage firmware / patch updates and ensure the integrity of patches.
- Practice working with Windows and SQL server logging.
- Understanding how to work with windows event and security logs.
- Understanding how to work with IIS Server / Web server logs.
- Understand how to view and interpret firewall logs.
- Understand how to use authentication logs (failed / successful logins) during brute force attacks.
- Understanding how to interpret Audit logs / Event logs.
- Practice working through handling of cyber-investigations including:
    - What has happened (Victims/ Actors/ Disaster).
    - Possible suspects.
    - Detect and analyse the reason / cause of the incident.
    - Preventative measures / Remedial action plan / Mitigate the attack.

## X. CYBER-SECURITY STANDARDS

Several international standards cover technical and organizational aspects of cyber-security. Various standards exist to describe technical security requirements of an organization, policies and procedures, technologies and solutions. Most relevant cyber-security standards and regulatory frameworks include:

- IEC 62351 Parts 1-13 Data Communications and Security
- IEEE 1686 Intelligent Electronic Devices Cyber security capabilities.
- IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security.
- IEC 62443 Parts 1-4 Security for industrial automation and control systems.
- NERC Critical Infrastructure Protection Parts 001-014

The IEC 62351 standard describes the end to end security of the communication protocols defined by the IEC TC 57. This end to end security is either at the transport or application layer and refers to mutual authentication, integrity and confidentiality of data (Parts 3 – 6). The figure below describes the inter-relationship between the TC57 protocols and IEC 62351 [9].

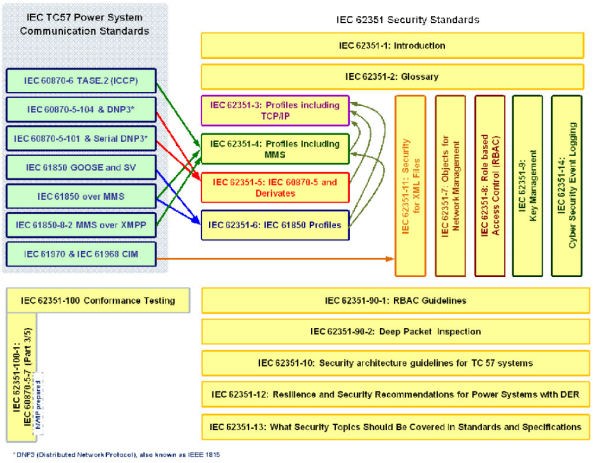


Figure 7: Inter-relationship between IEC TC57 and IEC 62351 standards [9].

The ISO/IEC 270xx standards provide the guidelines for implementing, improving and maintaining information security management in an organization. These standards are not described in detail as it presents an energy-system wide guideline for information security management which is beyond the scope of this paper.

IEEE 1686 defines the features that need to exist in an Intelligent Electronic Device (IED) to accommodate CIP programs. The standard covers IEC access, configuration, firmware revision and data retrieval from an IED, encryption of communications to the IED [8].

IEEE 1402 identifies and discusses security related to human intrusion in a substation. Various methods and techniques that are being used to mitigate both physical and electronic intrusions are also presented. The standard has a large focus on physical security and discusses the criteria for substation security, security methods and its effectiveness, intrusions and a substation security plan.

NERC has developed Critical Infrastructure Protection (CIP) security guidelines for the electricity sector which outlines the minimum requirements needed to ensure the security of electronic exchange of information needed to support the reliability of the power-system. The CIP standards Parts 001-014 provide a cyber-security framework which includes electrical, physical security, personnel security, training and awareness, configuration management and vulnerability assessments.

NERC CIP is formally controlled and enforced in the US and Canada. Organizations who are involved risk significant fines and penalties for lack of compliance.

There exists a variety of standards and guidelines applicable in substation automation and power system security. Even though there is no single comprehensive standard covering all dominions of the power-system, the abovementioned collective literature is now gaining increasing acceptance the world-over and is believed to include those that are most relevant to the energy sector [8].

IEC 62443 is a cyber-security standard for industrial automation. The standard covers products and systems as well as organizational, operational and process-related security aspects [8]. Certain parts of the standard are developed for the purposes of security certification programs.

## XI. CONCLUSION

Security by obscurity has traditionally been the primary approach to addressing cyber-security in substations. The expanded use of open protocols for purposes of tele-control and SCADA and use of TCP/IP based networks in the substation have increased the vulnerabilities and threats facing utilities on the power system. This paper discusses the threats and vulnerabilities in the context of substation automation.

Intrusion detection and prevent systems, advanced threat prevention techniques, deep packet inspection of SCADA protocols, monitoring and logging, forensic analysis and regulatory compliance capabilities is discussed in detail. A case study using an anomaly detection system to perform forensic analysis has been presented with the outcomes and benefits of the study explained. Lastly, the paper outlines the requirements for training and provides a brief overview of the cyber-security standards applicable to utilities in the energy sector.

Cyber-security is an evolving process and constant work and training is needed to maintain and keep up with the security policies / procedures and security infrastructure. No system can be considered 100% secure and risks should always be reviewed and managed. Consequently, to maintain the security of a substation automation system, constant monitoring is needed in the overall environment.

## XII. REFERENCES


[1] EWICS TC7, “Electrical Power Systems Cyber Security Case Study”, 5086 v1.1, January 2016.

[2] Check Point, “Protecting Industrial Control Systems and SCADA Networks”, Check Point Software Technologies Ltd, July 2015.

[3] Mirzoev T. Z., “Automation Security”, The department of Electronics and Computer Technology, College of Technology, Indiana State University, January 2007.

[4] US Department of Energy, “21 steps to Improve Cyber Security of SCADA Networks”, retrieved from https://energy.gov/oe/downloads/21-steps-improve-cyber-security-scada-networks, November 2017.

[5] Bartman T., Carson K., “Securing Critical Information Systems”, Schweitzer Engineering Laboratories, April 2015.

[6] Anderson D., Kipp N., “Implementing Firewalls for Modern Substation Cybersecurity”, Schweitzer Engineering Laboratories, February 2010.

[7] Dell Inc, “ Dell Security Annual Threat Report”, Dell Computer Coproration, July 2015.

[8] Buchi F., Fries S., Kroeselberg., “Cyber Security Standards and Regulations in Energy Automation Systems”, Siemens AG – Energy Management, Germany,

[9] Cleveland F., “IEC62351 Security Standards for the Power System Information Infrastructure”, IEC TC57 WG 15 Security Standards version 14, June 2012.

[10] IEC, IEC 62351 Parts 1 – 13, International Electrotechnical Commission, Available from https://webstore.iec.ch/publication/6912, November 2017.

[11] Wueest C., “Targeted Attacks Against the Energy Sector”, version 1.0, Symantec Corporation, January 2014.

[12] Andreeva O., Gordeychik S., Gritsai G., Kochetova O., Potseluevskaya E., Sidorov S., Timorin A., “Industrial Control Systems Vulnerabiltiies Statistics”, Kaspersky Lab, July 2016.

[13] Byres E., “Understanding Deep Packet Inspection for SCADA Security”, Version 1.0, Tofino Security, December 2012.

[14] Eldar L., “ICS\SCADA Networks Cyber attacks forensics workshop”, Cyberbit, September 2016.

[15] NCCIC, “Incident Response / Vulnerability Coordination in 2014”, ICS-CERT Monitor, US Department of Homeland Security, September 2014-February 2015.

[16] ISA, “ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries”, Industrial Standards Automation (ISA), 2009.

[17] NERC, “Reliability standards for the Bulk Electric Systems of North America, CIP 007- 3 – Systems Security Management”, North American Electric Reliability Corporation (NERC), January 2013.

[18] Cohen-Sason D., Himelblau H., CONCO Energy Solutions – SCADA Shield Report, Cyberbit R & D, Israel, October 2017.


## BIOGRAPHIES

Sagar Dayabhai is currently pursuing his PhD at the University of Witwatersrand (Wits), South Africa in the field of Smart Grids. He received his BSc Eng. (Electrical) degree from Wits in 2009 and his MSc Eng. (Electrical) degree in 2014. He is a registered professional engineer with the Engineering Council of South Africa (ECSA). Sagar was one of the IEC Young Professionals elected for South Africa in 2016 and is currently a member of IEC TC57 WG10 and WG15. After working at Eskom in the field of Telecommunications and SCADA, he moved to Consolidated Power Projects (CONCO) as a Senior SCADA / Automation Engineer. Sagar now holds the position as the System Control Manager at CONCO Energy Solutions