Operational Technology Intrusion Detection Application for Power Grid Security Operations Centres

MSc Research Project
Cybersecurity

Keith Cooney
Student ID: 18201270

School of Computing
National College of Ireland

Supervisor: Dr Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Keith Cooney		
Student ID:	18201270		
Programme:	MSc in Cybersecurity	**Year:**	2021
Module:	Research Project		
Supervisor:	Dr Imran Khan		
Submission Due Date:	20th September 2021		
Project Title:	Operational Technology Intrusion Detection Application for Power Grid Security Operation Centre		
Word Count:	**6054**	**Page Count**	**25**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Keith Cooney

Date: 20th September 2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Operational Technology Intrusion Detection Application for PowerGrid Security Operation Centre

Keith Cooney
Student ID: 18201270

Abstract

The Electrical Power Grid provides our modern society with electricity. It is a complex, distributed, cyber-physical machine that supports not just our activity in the home but also what we do in our work such as factories, offices, healthcare facilities, banking, and communications. Critical National Infrastructure is a fundamental service, and its presence and reliability are often taking for granted until it fails. When we experience its absence, its effects on our lives are immediate and, if absent for a prolonged period, catastrophic. The modern power grid is much more data orientated due to its adoption of Internet Protocol (IP) which presents a greater attack surface for Threats to exploit. The power system incorporates industrial technologies such real time control & protection and energy management systems. These are known as Operational Technology (OT) which are somewhat distinct, but related to, Information Technology (IT). Data produced by these OT systems have not been utilised by IT security systems such as Security Incident Event Management systems (SIEM) to aid IT Security Operations Centres to analyse and respond to threats that occur on the OT estate. Modern SOC's monitor IT assets whose critical equipment is hosted in premises and datacentres. However, a different type of SOC is required for monitoring OT power system assets (e.g., substations, transformers, high voltage switching devices, sensors, generators etc.). This OT/IT SOC must take information from IT system but also OT systems to provide improved situational awareness.

1 Introduction

This paper focuses on cybersecurity for critical national infrastructure, specifically electrical Transmission and Distribution (T&D) networks. Most jurisdictions have some form of electricity grid supplying power to domestic and commercial customers. Modern society has come to rely upon electricity production, transmission, and distribution to support our way of life and power the computer infrastructure of the information age which we live. The High Voltage (HV) power network comprises power lines, power cables and HV substations that contain switching devices (e.g., HV circuit breakers) and transformers that can step-up or step-down voltage between different voltage levels (*Figure 1*). The HV substation is an important node in the electricity network as it interconnects different power system assets and integrates the critical control and protection systems to enable the system operators to control and monitor the power grid (NERC, 2013). Modern HV substations contain sophisticated automation systems including provision of local and remote control from a Network Control Centre (Kumar, 2010). A power grid may have 100's or 1000's of HV substations all of which are monitored and controlled by the Control Centre Supervisory Control and Data Acquisition (SCADA) system.

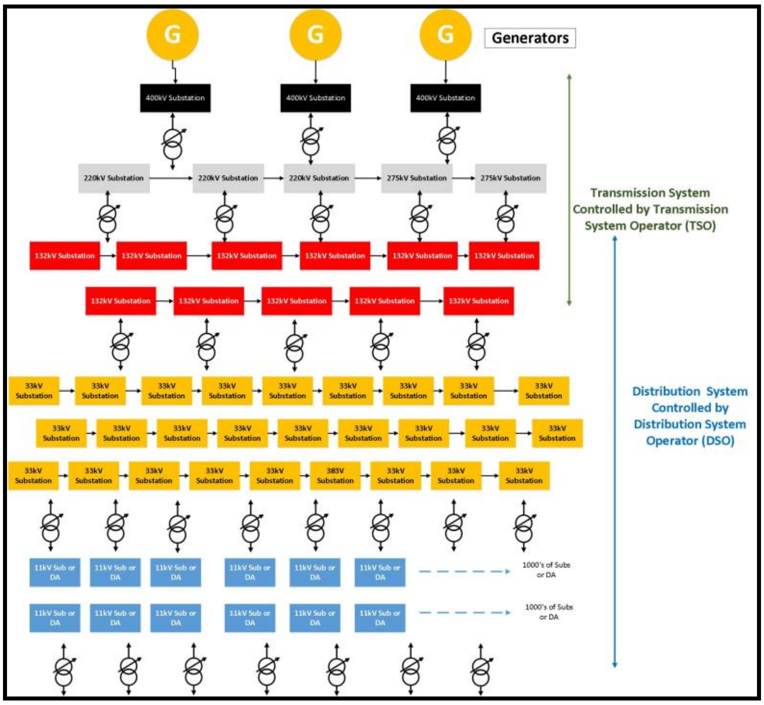
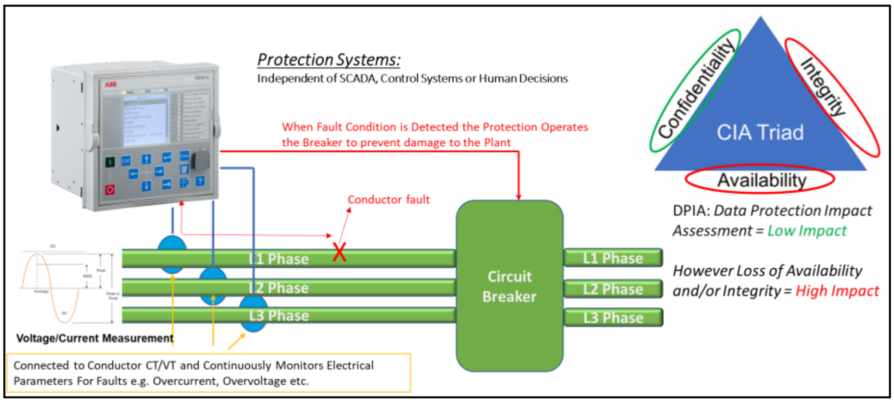


Figure 1: Electrical Transmission & Distribution System.

Grid OT Systems: Digital Substation Automation Systems

Each HV substation deploys a control, monitoring and protection system. The primary purpose of the protection system is to monitor the currents, voltages and electrical impedances in the power systems cable/overhead line phases, transformers, and switchgear. In the event of monitored electrical parameters going outside of acceptable bands the protection systems are programmed to take immediate action (within milliseconds) to avert a dangerous fault condition by directly operating the HV circuit breaker(s) (Chen, 2011). The HV circuit breaker is designed to 'break load' of the energised plant it protects e.g., HV power cable or HV/MV transformer. The substation protection system is the most critical safety systems, and its high availability and guaranteed data accuracy/integrity is vital to ensure dangerous high voltage incidents do not arise that may result in damage to plant, injury or death to staff or members of the public.


Protection Systems:
Independent of SCADA, Control Systems or Human Decisions

When Fault Condition is Detected the Protection Operates the Breaker to prevent damage to the Plant

Connected to Conductor CT/VT and Continuously Monitors Electrical Parameters For Faults e.g. Overcurrent, Overvoltage etc.

DPIA: *Data Protection Impact Assessment = Low Impact*

However Loss of Availability and/or Integrity = High Impact

Figure 2: Protection Device Continuous Monitoring of Plant.

The substations control system is not as time critical as the protection system and its purpose is to monitor the substation for changes in plant condition such as analogue changes (e.g., to kV, Amps, MW, MVar), fault conditions (Protection has Tripped, SF6 Gas Pressure is Low etc.), acquire real-time state of devices (e.g., CB in Closed Position, CB in Open Position, Transformer at Tap 12 etc.). This real-time data is logged locally by the SAS system and transmitted to the centralised power network SCADA (Ma *et al.*, 2010).

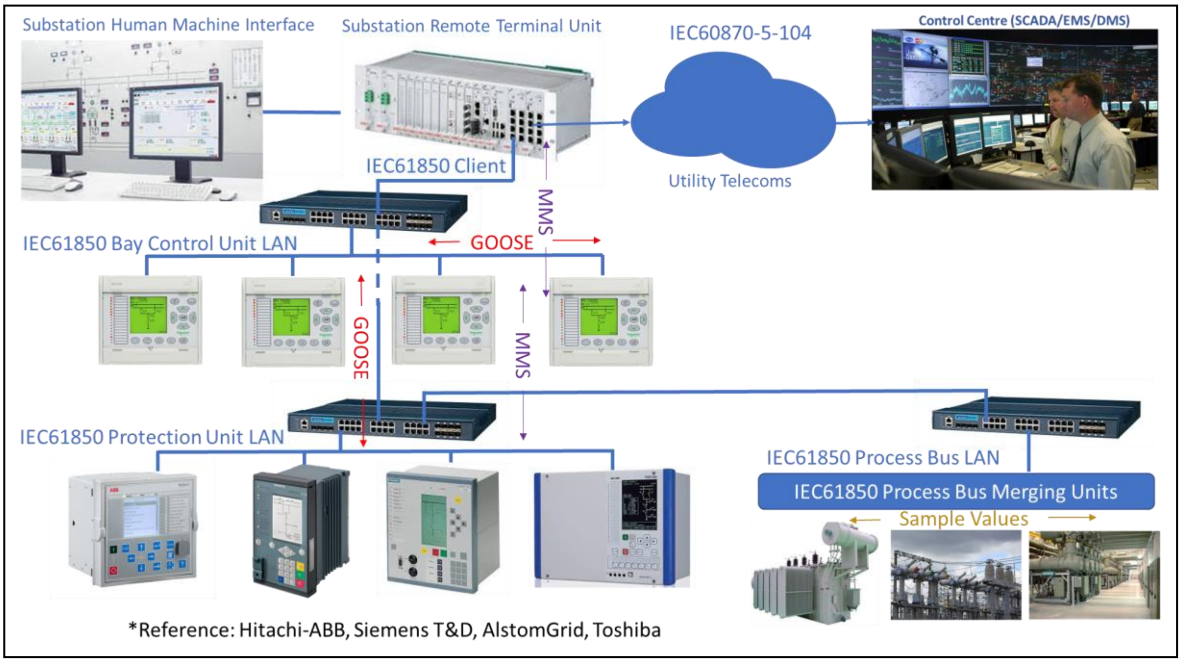

Substation Human Machine Interface
Substation Remote Terminal Unit
IEC60870-5-104
Control Centre (SCADA/EMS/DMS)
Utility Telecoms
IEC61850 Client
MMS
IEC61850 Bay Control Unit LAN
GOOSE
GOOSE
MMS
IEC61850 Protection Unit LAN
IEC61850 Process Bus LAN
IEC61850 Process Bus Merging Units
Sample Values
*Reference: Hitachi-ABB, Siemens T&D, AlstomGrid, Toshiba

Figure 3: Digital Substation Automation System with Control Centre SCADA.

Digital substations designed in accordance with IEC61850 standard (Cooney and Lynch, 2012) are the most modern SAS used by power utilities. IEC61850 provides high speed peer to peer communication services that can be used for time critical protection functionality (Madonsela, Davidson and Mulangu, 2018) - *refer to Figure 3*. Using GOOSE messaging over the substation OT LANs, protection devices can communicate mission critical signals to each other (e.g., Trip signals, CB Position Indication) reliably without risk of packet loss. The substation's data is carried over high-speed LANs and not physically 'hardwired' between devices. IEC61850 incorporates a high-speed process bus providing highly accurate, digitized, time stamped samples of plant analogue signals from the instrument transformers (Hughes, 2015). IEC61850 has revolutionised the power grid substation by adopting a completely data orientated approach and this standard is a key enabler of the 'Smart Grid' (Smart Grid Coordination Group, 2014).

While the substation utilises the IEC61850 standard to integrate the intelligent electronic devices into a high-speed IP network, the communication of the substation with the network control centre SCADA typically uses other telecontrol protocols. The most common in Europe is the IEC60870-5-104 (Matoušek, 2017). IEC60870-5-104 is an IP protocol (IANA, 2010) so it can traverse Wide Area Networks (WAN).

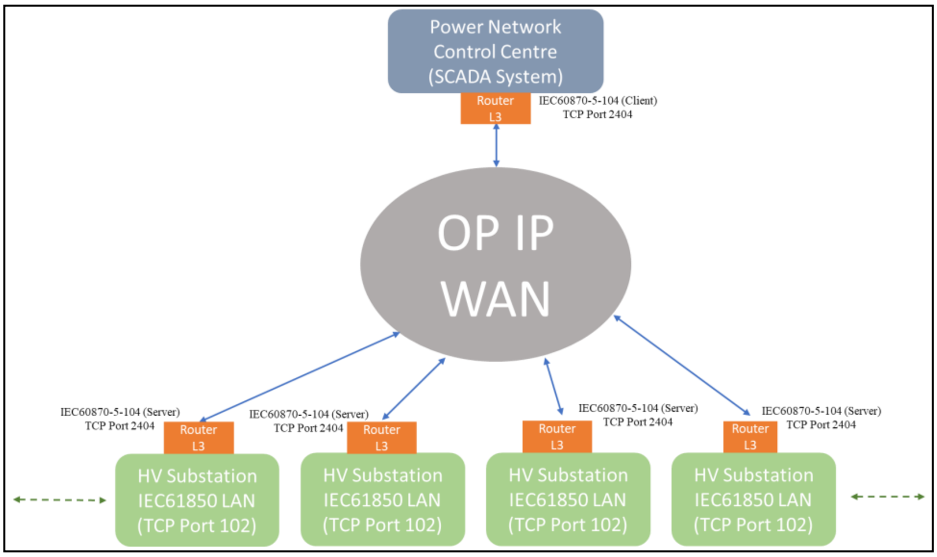


Figure 4: Operational Technology IP Network – Power Grid

While these protocols have transformed the communications infrastructure of power grid automation systems cybersecurity was not factored into to the design. These protocols are insecure and lack assurances with respect to confidentiality and integrity (Kerkers, 2017). Cryptography, integrity checking, and non-repudiation are not characteristics of the protocols. They can be easily read, manipulated, and fabricated by threats with access to the network.

Grid OT Systems: Supervisory Control & Data Acquisition (SCADA)

The power grid OT systems comprised 100's or 1000's of HV substations and independent medium voltage (MV) devices to protect, monitor and control the network. These distributed automation systems produce OT data that is usually concentrated in a centralised SCADA application. The power grid SCADA is in the Control Centre(s) – often there are several control centres e.g., the Transmission Control Centre that operates the HV transmission system and the Distribution Control Centre that operates the HV/MV distribution system (Knapp and Samani, 2013).

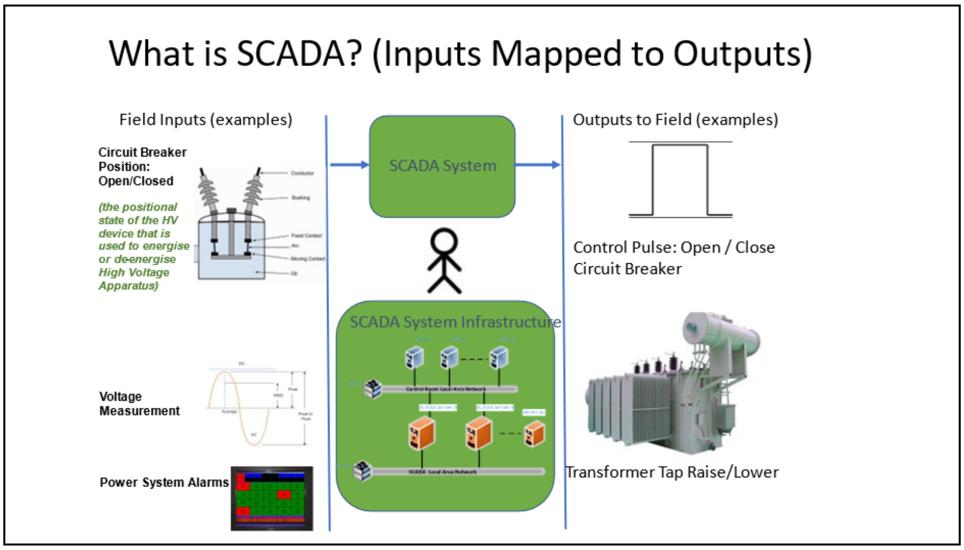

What is SCADA? (Inputs Mapped to Outputs)
Field Inputs (examples)
Circuit Breaker Position: Open/Closed
(the positional state of the HV device that is used to energise or de-energise High Voltage Apparatus)
Conductor
Bushing
Fixed Contact
Arc
Moving Contact
Oil
Voltage Measurement
DC
Peak
RMS
Average
Peak to Peak
AC
Power System Alarms
SCADA System
SCADA System Infrastructure
Outputs to Field (examples)
Control Pulse: Open / Close Circuit Breaker
Transformer Tap Raise/Lower

Figure 4: Power Grid SCADA – Human in Feedback Control Loop

SCADA can control the entire grid in real-time by remotely operating circuit breakers and transformers and disconnect or deenergise connected customers. Therefore, power grid SCADA is a *high impact* system with respect to cyber risk (NERC, 2009). A failure or unauthorised action by SCADA or its users can have adverse effects on society.

OT cybersecurity is a relatively new field evolving over the last 10 years due to increasing threat landscape (Lunden, 2021). Traditionally OT systems were physically isolated from other networks, the so called 'Airgap', but within the modern power system, the traditional airgap no longer exists (ISA, 2021). Power systems need to exchange data with enterprise zones and possibly over insecure networks like the internet, but the cybersecurity controls that are common in enterprise IT zones, may be absent or ineffective in OT zones. In response to this deficiency, the European Union issued the Networks and Information Systems Directive 2018) to member states mandating Operators of Essential Services (DCCAE, 2019) such as power utilities, meet and maintain a minimum cybersecurity maturity via NIST cybersecurity framework (Institute of Standards, 2014). Much work is ongoing worldwide to increase the cybersecurity of the critical infrastructure on which society depends. Other notable challenges facing those responsible for securing OT estates include the lack of understanding between the respective fields i.e., IT professionals and OT professionals (Ernst & Young, 2018).

This project seeks to enhance existing tried and tested cybersecurity controls to accommodate OT systems. Specifically, Intrusion Detection Systems (IDS), Security Operations Centres (SOC) and Security Information Event Management systems (SIEM) are powerful tools to defend an organisations enterprise zone. However, these tools have not been extended much to the OT zone. This project will investigate methods to utilise the data produced in the OT zone and correlate it for improved continuous security monitoring

Research Question:

What enhancements can be made to traditional enterprise zone continuous security monitoring systems to accommodate the surveillance of the Power Grid OT estate?

2 Related Work

OT and IT systems are related by their use of similar communications technology but there are important differences between domains. The table below compares OT and IT domains (Conklin, 2016).

Table 1: Characteristic Differences between the IT and OT Domains

Information Technology	Operational Technology
Cyber System (*Effects on the real world are indirect*)	Cyber-Physical System (*Directly effects the real world*)
Relatively Short Lifecycle (*Hardware / Software lifecycle 10 years*)	Relatively Long Lifecycle (*hardware/software may last 15, 20 or even 20+ years*)

Changes to IT occur regularly (*IT networks are very dynamic*)	Changes to OT occur rarely (*Once commissioned OT tends to be left alone)*
Data availability not Time Sensitive (*Latency of data update is not critical*)	Data Availability is Time Sensitive (*Latency of data update is critical to mission*)
Safety is not directly dependant on IT (*IT system not used for emergency action*)	Safety may be dependent on OT function (*OT system must take action to avoid incident)*

These differences influence the level of security deployed. For example, the table below summarises the acceptable security controls that may be considered for each domain based on operating constraints. While this is not the case in every instance, it is generally indicative of how IT and OT system approach security. OT Cybersecurity standards such as IEC62443 have been developed with these characteristic differences in mind (IEC, 2009).

Table 2: Differences in Deployment of Cybersecurity Controls

Information Technology	Operational Technology
Patching of system software and operating systems occurs regularly. *(Availability not primary concern. Update malfunction rectified with rollback but accepting disruption)*	Patching of software, firmware and operating system occurs rarely. *(Constrained by Availability Requirements / upgrades require rigorous test as safety is priority / high cost)*
Data Confidentiality is Primary Concern *(Cryptography for data at rest/in transit are critical security controls)*	Data Availability is Primary Concern *(Data may not be sensitive. If exposed losses may not be incurred. Cryptography may not be deployed due to complexity and impact to availability)*
IT not strictly Segregated from other networks (e.g., internet). User access to external data sources is necessary.	OT is usually strictly Segregated from networks of higher risk. Data exchanged between security zones is carefully controlled
Threat & Vulnerability Management tools are deployed to quickly remediate vulnerabilities. *(IT systems, properly managed, have low vulnerabilities)*	Threat and Vulnerability Management tools may be deployed but vulnerabilities not quickly remediated due to availability constraints. *(OT systems tend to have many vulnerabilities.)*
Antivirus technologies heavily deployed to detect and block threats. Signatures are updated daily.	Antivirus rarely deployed on critical OT systems due to risk of performance degradation and updates causing malfunction.
Application Control commonly deployed on Enterprise IT.	Application Control may be applied to OT once thoroughly tested to ensure blocking of critical process does not occur.
Electronic Perimeter of IT network will usually implement Intrusion Prevention where threats are automatically blocked by security appliance.	Electronic Perimeter of OT network may implement Intrusion Detection Only. Blocking of critical OT traffic not recommended.

Attacks against Operational Technology Systems may be characteristically different when compared to attacks against IT systems. In IT systems the attack is usually against Confidentiality as the attackers seek to exfiltrate sensitive data from the organisation. This may be used for financial gain e.g., extortion, fraud, ransom. In OT systems the physical process may be the target of the attack (Langner and Schneier, 2013). The objective may be to disrupt the process control from performing its critical function. Usually, an attack on an OT system is an attack on its Availability and Integrity.

The electricity industry has been targeted by state sponsored Advanced Persistent Threats (APT). Two notable attacks on Ukrainian Utility in 2015 (Robert M. Lee, Michael J. Assante and Tim Conway, 2016) and 2016 (Slowik, 2019) have been studied. In the first attack, the APT used spear-phishing to socially engineer utility employees into infecting the utility corporate IT system. Once establishing a foothold, they searched the IT system for credentials to give them access to the OT zone via existing remote access VPNs. Once gaining control of SCADA they manually controlled the circuit breakers disconnecting power to 250,000 people. The follow up attack used a different technique where malware (Assante, Lee and Conway, 2017) was deployed onto the SCADA servers which simulated the protocols used by power utilities to control and monitor the substations (i.e., IEC60870-5-104, IEC61850 & OPC).

The International Electrotechnical Commission (IEC) protocols, that the 'Industroyer32/Crashoverride' malware manipulated against the Ukrainian Utility have no cybersecurity protection. Recent working groups within IEC have produced the cybersecurity standard IEC62351 (Schlegel, Obermeier and Schneider, 2017) that is intended to 'harden' the existing IEC protocols (i.e., IEC60870-5-104, IEC61850 etc.). IEC62351 introduces security already present in the IT domain such as Public Key Infrastructure (PKI), Transport Layer Security (TLS) and Role Based Access Control (RBAC). For the Ukraine example of *Crashoverride*, use of IEC62351 may have prevented the manipulation of the protocols as PKI provides assurances with respect to data integrity, replay attacks and confidentiality. Field units would have rejected the spurious command packets due to certificate-based authentication. Use of IEC62351 would provide additional layers of security in line with the widely accepted 'Defence in Depth' approach.

The Purdue model (Williams, 1994) is often applied to secure OT systems. Purdue has been adapted to suit the integration of OT and IT layers and a more straightforward description can be found in (HSE-UK, 2017) and (Checkpoint Software, 2020).

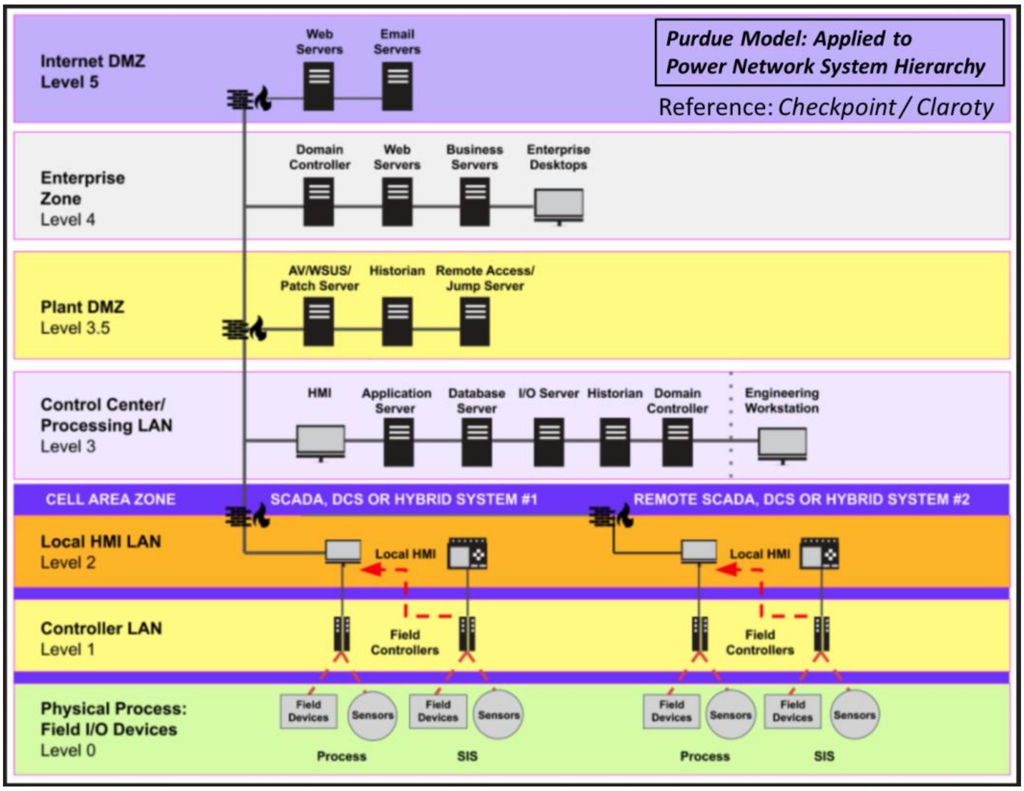


Figure 5: General Purdue Model for OT

At the heart of the Purdue model is IT/OT network segmentation. The model separates high impact environments such as process zone and supervisory control zones from higher risk zones such as corporate enterprise networks and the internet. IT/OT segmentation is a sensible approach to OT cybersecurity as it recognises threats are more likely to originate in enterprise networks that have many users with direct access to the internet. By carefully controlling and filtering the data interfaces between these zones risks to the critical OT environments can be mitigated. The general Purdue of Figure 5 can be translated into specific functional architecture of a power grid energy management systems of Figure 6.

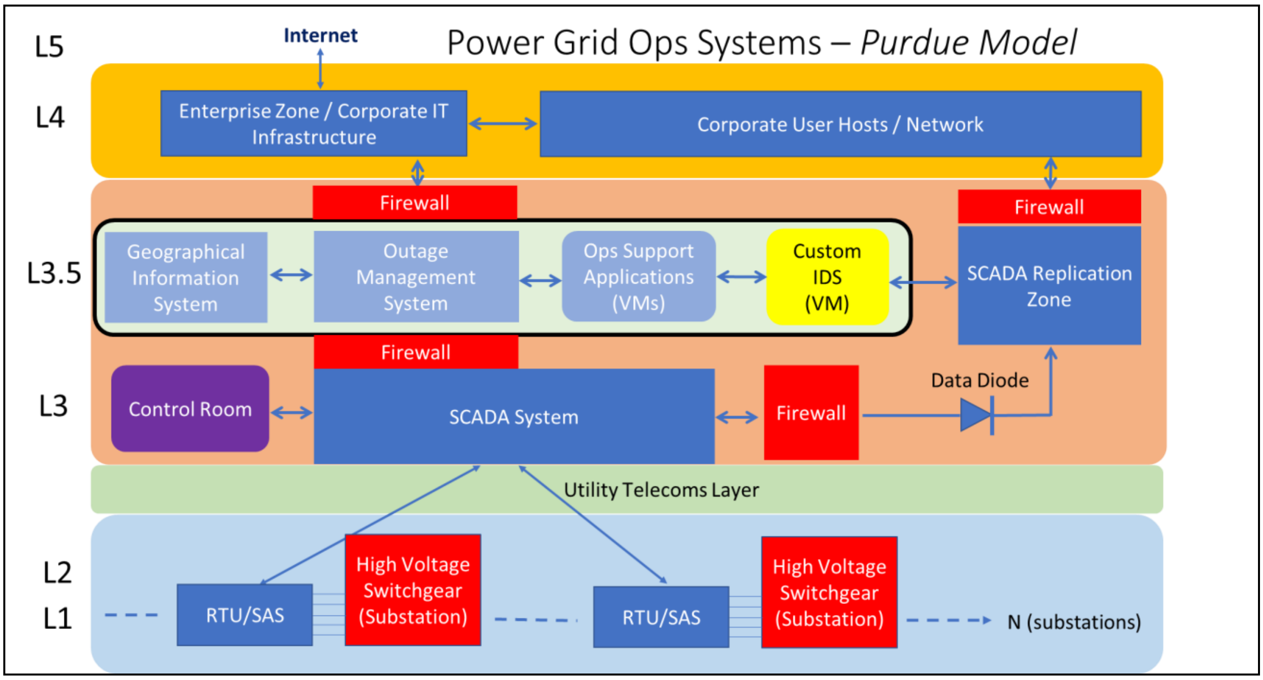

Power Grid Ops Systems – Purdue Model
L5
Internet
L4
Enterprise Zone / Corporate IT Infrastructure
Corporate User Hosts / Network
Firewall
Firewall
L3.5
Geographical Information System
Outage Management System
Ops Support Applications (VMs)
Custom IDS (VM)
SCADA Replication Zone
Firewall
L3
Control Room
SCADA System
Firewall
Data Diode
Utility Telecoms Layer
L2
L1
RTU/SAS
High Voltage Switchgear (Substation)
RTU/SAS
High Voltage Switchgear (Substation)
N (substations)

Figure 6: Purdue Model Applied to Power Grid OT

OT Intrusion Detection Systems

In Figure 6 the proposed OT IDS for this project has been indicated (yellow) to show the best logical location to take advantage of data flows from different zones. The OT IDS must interface with the SOC (level 4) but also have access to the OT zone OMS data in iDMZ zone (level 3.5) and SCADA mirror system (level 3.5).

Intrusion Detection is a key cybersecurity technology deployed to protect OT systems. There is a wide body of literature describing IDS. Host Based Intrusion Detection Systems (HIDS) - includes integrity checking mechanisms like Tripwire (Tripwire, 2018). Network Based Intrusion Detection Systems (NIDS) - includes traffic analysis and threat signature databases (SNORT, 2021). Non-signature-based analysis (anomaly and heuristic methods). Other IDS identify non-conformity from the protocol's specification. This is known as Specification-Based Inspection. (Yang *et al.*, 2013) developed an IEC60870-5-104 approach.

Most deployed IDS systems use a combination of HIDS and NIDS to provide a comprehensive security monitoring system. Traffic transiting the network is analysed using port spanning on network devices and the traffic is analysed with reference to either threat signature (ruleset) or unusual changes of traffic away from expected baseline. Both methods have advantages and disadvantages (Colbert and Kott, 2016).

Advantages of Signature-Based IDS

- Rulesets are available and easily integrated (via Snort or equivalent) for the known Threats. This is most useful to detect threats attempting to exploit vulnerabilities in commonly used IT protocols and systems.
- Provide specific feedback on the threat detected greatly aiding an investigation.

Disadvantage of Signature Based IDS

- Cannot defend against attacks deploying Zero-Day exploits. APTs and sophisticated criminal threat actors may defeat these types of systems by using novel approaches or purchase zero-day exploits.

Advantages of Non-Signature Based IDS (Anomaly)

- Can potentially detect Zero-Day based attacks. If properly configured and threats understood an anomaly-based IDS may defend against the most capable of attackers.

Disadvantages of Non-Signature Based IDS (Anomaly)

- False positives. If the operating environment changes, the traffic may change resulting in alerts. Dynamic network environments that constantly undergo change may not be well served by this IDS system. The system would need to constantly relearn the new operating environment.
- The Anomaly IDS may indicate an attack is taking place, but it does not illuminate the Who and the How.

Choice of IDS solutions for the Power Grid

An optimal solution may be to distribute *Anomaly* Based IDS in each substation as these OT systems do not change much after they are commissioned. We may deploy a *Signature*-Based IDS in the centralised SCADA that is likely to use IT centric technologies. Correlation between these 2 types of IDS can develop a robust security solution.

The best way to access important physical indications is to utilise the databases of the OT zone itself. This includes, but is not limited to, the SCADA system power system event database, the OT syslog event database, OT SNMP events databases, staff station/device login database. The OT IDS will utilise these data sources to provide rule-based alerts to the SOC enabling analysts to monitor the OT estate.

The above research has provided insights into how we may provide continuous security monitoring of the Utility IT/OT system. A comprehensive Utility IT/OT security model with IDS probes at security touchpoints was constructed.

3 Research Methodology

The project research methodology followed different phases. Initially, research was conducted to develop an understanding of the typical power grid OT system. The objective here was to develop a detailed interconnected model of how the power system protection, monitoring and control components and communication protocols fit together to make up a function transmission and distribution network. Further to this was some background research on enterprise IT systems. An important element of the research process was showing how the OT and IT systems fit together to make up a Utility OT/IT model. By adding the insights gathered from the Purdue model, it was possible to develop a segmented OT/IT Utility security model.

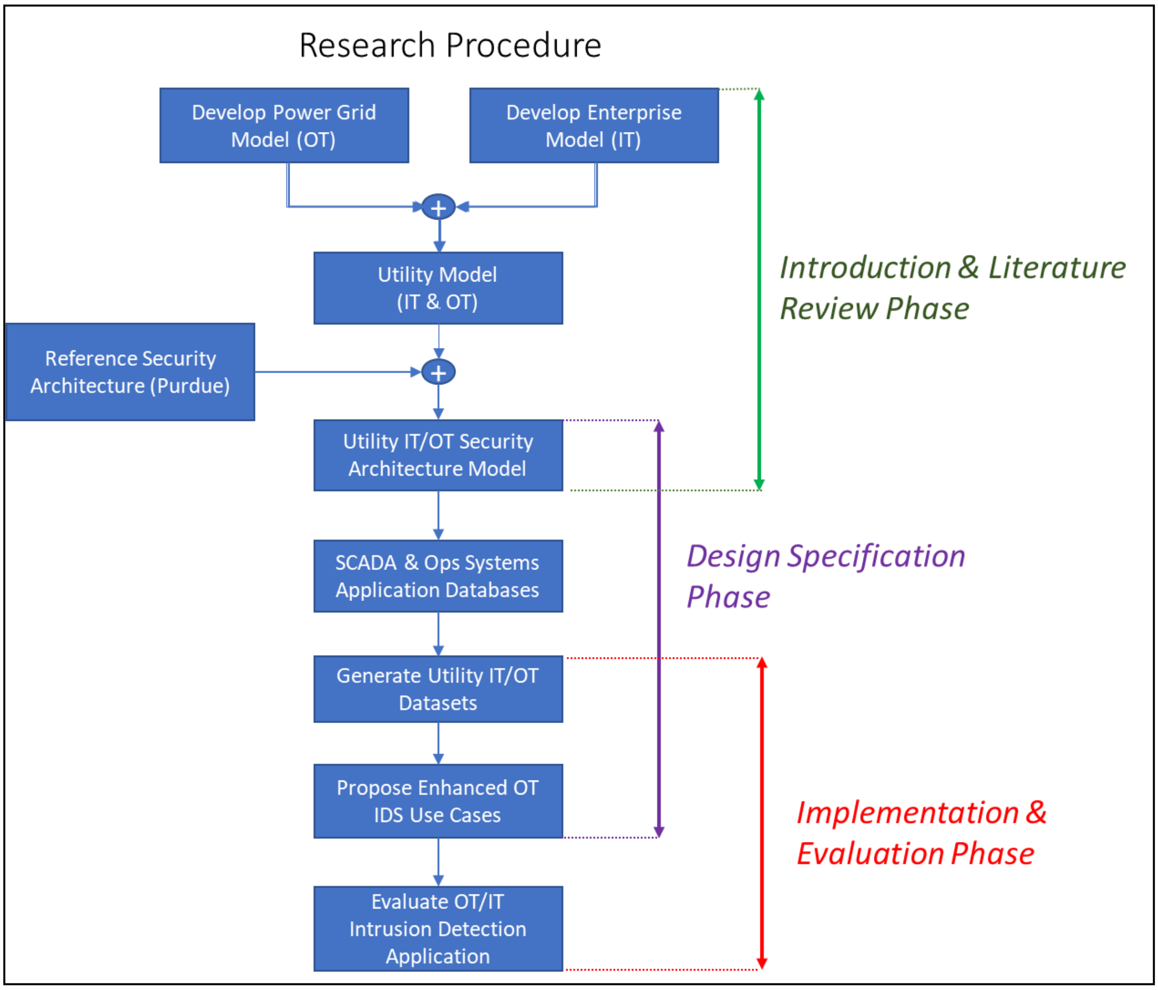

Research Procedure
Develop Power Grid Model (OT)
Develop Enterprise Model (IT)
Utility Model (IT & OT)
Reference Security Architecture (Purdue)
Utility IT/OT Security Architecture Model
SCADA & Ops Systems Application Databases
Generate Utility IT/OT Datasets
Propose Enhanced OT IDS Use Cases
Evaluate OT/IT Intrusion Detection Application
Introduction & Literature Review Phase
Design Specification Phase
Implementation & Evaluation Phase

Figure 7: Research Methodology

The Utility IT/OT Security Architecture Model can be referred in Figure 8.

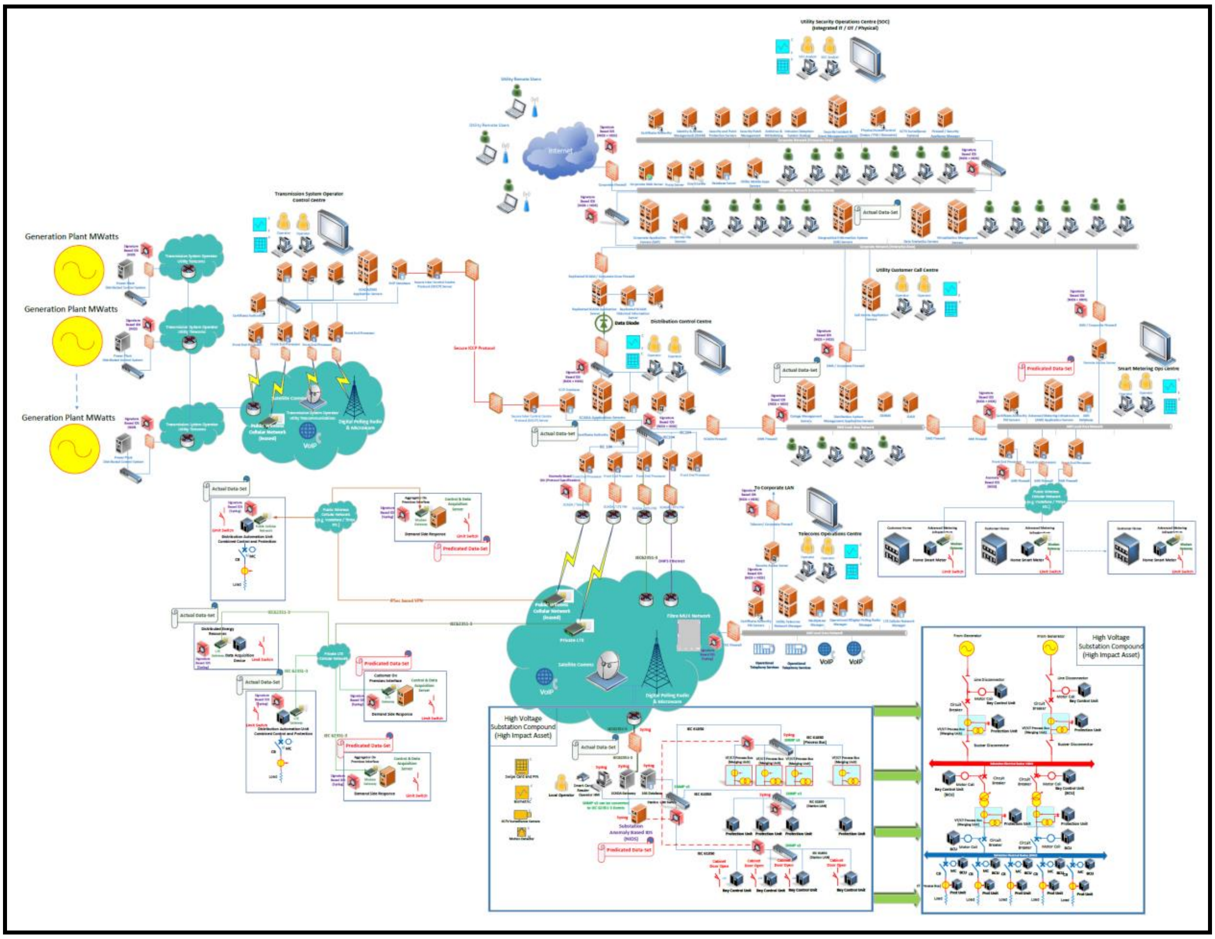

Utility Security Operations Centre (SOC) (Integrated IT / OT / Physical)
Transmission System Operator Control Centre
Generation Plant MWatts
Generation Plant MWatts
Generation Plant MWatts
Internet
Distribution Control Centre
Utility Customer Call Centre
Smart Metering Ops Centre
Actual Data-Set
Predicated Data-Set
Telecoms Operations Centre
To Corporate LAN
Public Wireless Cellular Network (leased)
Private LTE
Satellite Comms
Fibre MLPS Network
Digital Polling Radio & Microwave
VoIP
High Voltage Substation Compound (High Impact Asset)
High Voltage Substation Compound (High Impact Asset)
Data Diode

Figure 8: Utility IT/OT Power Grid Model with Security

The model in Figure 8 was used to devise the datasets that could be available for the proposed custom IDS application. Several datasets were inferred – these include:

- SCADA Power System Event Database (telemetry from all network plant systems)
- SCADA Analog Database
- OT Network Syslog & SNMP Databases
- Plant Staff Login application

For the next phase of the project, an OT IDS is proposed to parse the real time updating data and apply the ‘Use Cases’ to extract meaningful security events that can be passed to the SOC. Evaluation of the IDS application and consideration for future work was the last phase of the project.

4 Design Specification

For the design specification the key reference is the Utility IT/OT Security Model with integrated IDS probes at security touch points. Continuous security monitoring is a critical security control that, while common in IT networks, is relatively uncommon on the power grid OT network. Broadening IDS to the OT zone, especially to HV substations and Distribution Automation, provides the integrated IT/OT SOC with more visibility of threats to the OT estate.

Concept of Custom IDS Application

The OT IDS will leverage data from multiple OT datasets. SCADA real-time data is useful as it is directly monitoring HV plant. Substation or distribution automation devices are possible entry points for cyber attacks as the OT network is dependent on IP technologies. Monitoring both the physical security systems, staff presence on site and newly installed cybersecurity systems (*anomaly IDS*) provides an improved threat situational awareness. General concept of the custom IDS application is shown in Figure 9.

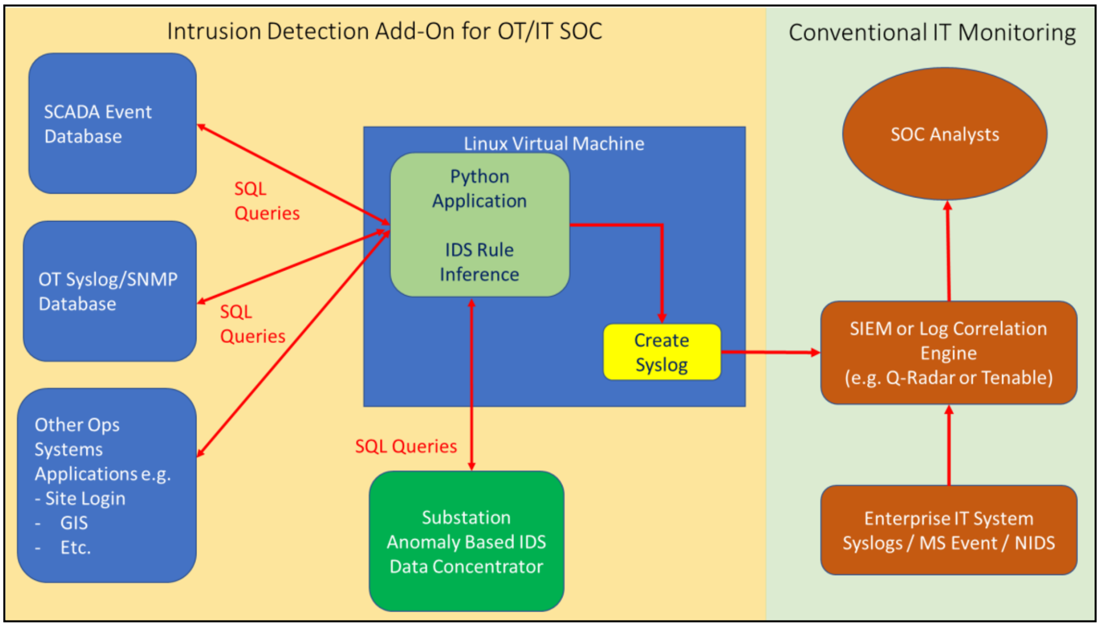
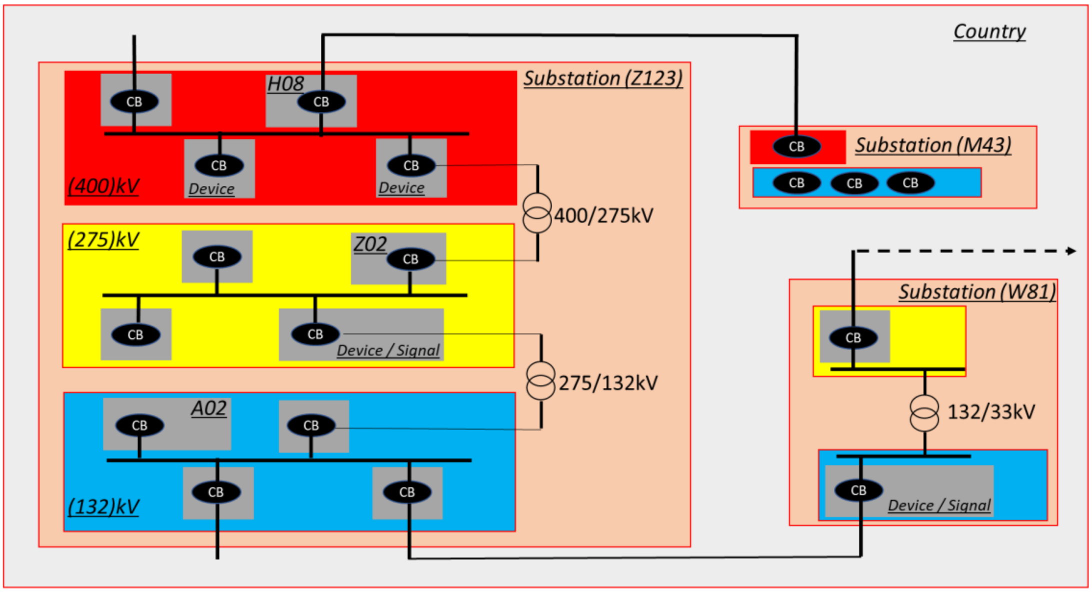

Intrusion Detection Add-On for OT/IT SOC
Conventional IT Monitoring
SCADA Event Database
OT Syslog/SNMP Database
Other Ops Systems Applications e.g.
- Site Login
- GIS
- Etc.
SQL Queries
SQL Queries
Linux Virtual Machine
Python Application
IDS Rule Inference
Create Syslog
SQL Queries
Substation Anomaly Based IDS Data Concentrator
SOC Analysts
SIEM or Log Correlation Engine (e.g. Q-Radar or Tenable)
Enterprise IT System Syslogs / MS Event / NIDS

Figure 9: Utility IT/OT Enhanced IDS Application

SCADA System Database Structure and Other Applications

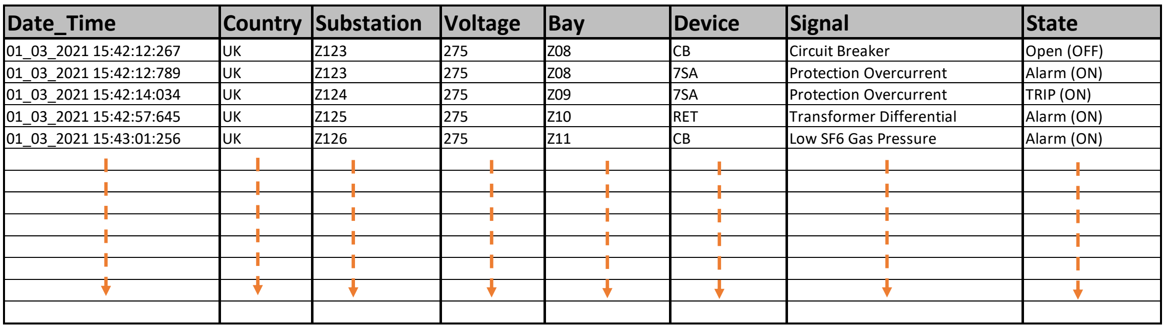
To parse the data contained with the SCADA power system event list, the database structure must be determined. A typical SCADA system may organise data tables from field devices according to Figure 10.



***Database Table:** *Countries / Country / Substation (Z123) / Voltage Level (kV) / Bay (Z02)/ Device (CB) / Signal (Protection Trip)*

Figure 10: A Typical SCADA Database Structure

A real-time (timestamped and constantly updating) power system event table is in Figure 11.



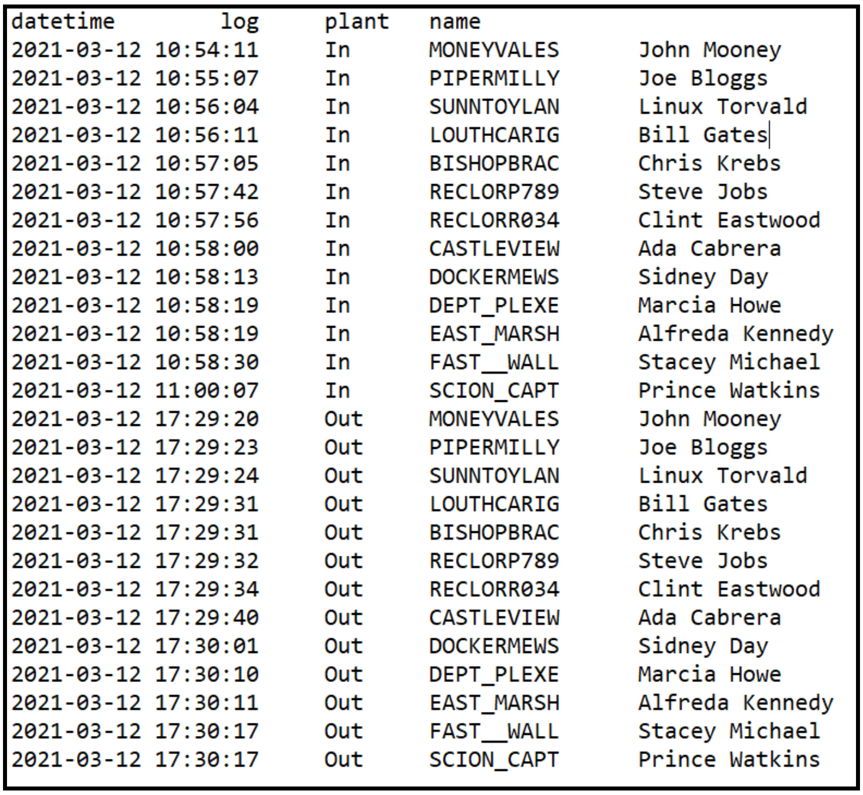
Date_Time	Country	Substation	Voltage	Bay	Device	Signal	State
01_03_2021 15:42:12:267	UK	Z123	275	Z08	CB	Circuit Breaker	Open (OFF)
01_03_2021 15:42:12:789	UK	Z123	275	Z08	7SA	Protection Overcurrent	Alarm (ON)
01_03_2021 15:42:14:034	UK	Z124	275	Z09	7SA	Protection Overcurrent	TRIP (ON)
01_03_2021 15:42:57:645	UK	Z125	275	Z10	RET	Transformer Differential	Alarm (ON)
01_03_2021 15:43:01:256	UK	Z126	275	Z11	CB	Low SF6 Gas Pressure	Alarm (ON)

Figure 11: Real-Time SCADA Power Event List

With this basic structure the dataset that the OT IDS will parse can be inferred. Refer to the constructed datasets samples in the Project Configuration Manual.

Safety Related Applications: Staff Site Presence Dataset

Utilities also require a means to know who is working at an OT site or device. As OT system are in hazardous environments, utilities deploy mobile applications that staff use to log their presence. This is useful from an IDS perspective, as alerts generated from a staffed site are unlikely to be a security incident – however if alerts occur in an unstaffed site, there is a higher risk of a security incident. This type of dataset is relatively straight forward to infer and the 'Site Login' dataset used by the IDS is in Figure 12.



```
datetime            log     plant       name
2021-03-12 10:54:11 In      MONEYVALES      John Mooney
2021-03-12 10:55:07 In      PIPERMILLY      Joe Bloggs
2021-03-12 10:56:04 In      SUNNTOYLAN      Linux Torvald
2021-03-12 10:56:11 In      LOUTHCARIG      Bill Gates
2021-03-12 10:57:05 In      BISHOPBRAC      Chris Krebs
2021-03-12 10:57:42 In      RECLORP789      Steve Jobs
2021-03-12 10:57:56 In      RECLORR034      Clint Eastwood
2021-03-12 10:58:00 In      CASTLEVIEW      Ada Cabrera
2021-03-12 10:58:13 In      DOCKERMEWS      Sidney Day
2021-03-12 10:58:19 In      DEPT_PLEXE      Marcia Howe
2021-03-12 10:58:19 In      EAST_MARSH      Alfreda Kennedy
2021-03-12 10:58:30 In      FAST__WALL      Stacey Michael
2021-03-12 11:00:07 In      SCION_CAPT      Prince Watkins
2021-03-12 17:29:20 Out     MONEYVALES      John Mooney
2021-03-12 17:29:23 Out     PIPERMILLY      Joe Bloggs
2021-03-12 17:29:24 Out     SUNNTOYLAN      Linux Torvald
2021-03-12 17:29:31 Out     LOUTHCARIG      Bill Gates
2021-03-12 17:29:31 Out     BISHOPBRAC      Chris Krebs
2021-03-12 17:29:32 Out     RECLORP789      Steve Jobs
2021-03-12 17:29:34 Out     RECLORR034      Clint Eastwood
2021-03-12 17:29:40 Out     CASTLEVIEW      Ada Cabrera
2021-03-12 17:30:01 Out     DOCKERMEWS      Sidney Day
2021-03-12 17:30:10 Out     DEPT_PLEXE      Marcia Howe
2021-03-12 17:30:11 Out     EAST_MARSH      Alfreda Kennedy
2021-03-12 17:30:17 Out     FAST__WALL      Stacey Michael
2021-03-12 17:30:17 Out     SCION_CAPT      Prince Watkins
```

Figure 12: Real-Time Site Login Dataset

OT Syslog and SNMP Dataset

The syslog/SNMP data produced by the OT system may be centrally stored in the Control Centre systems infrastructure. The substation anomaly-based IDS (*refer to Utility IT/OT model*) stores syslog's and SNMP messages generated by the substation control and protection network. There is also the ability to monitor syslog's of the DA devices installed all over the network. The relevant parts of the model are Figure 13.

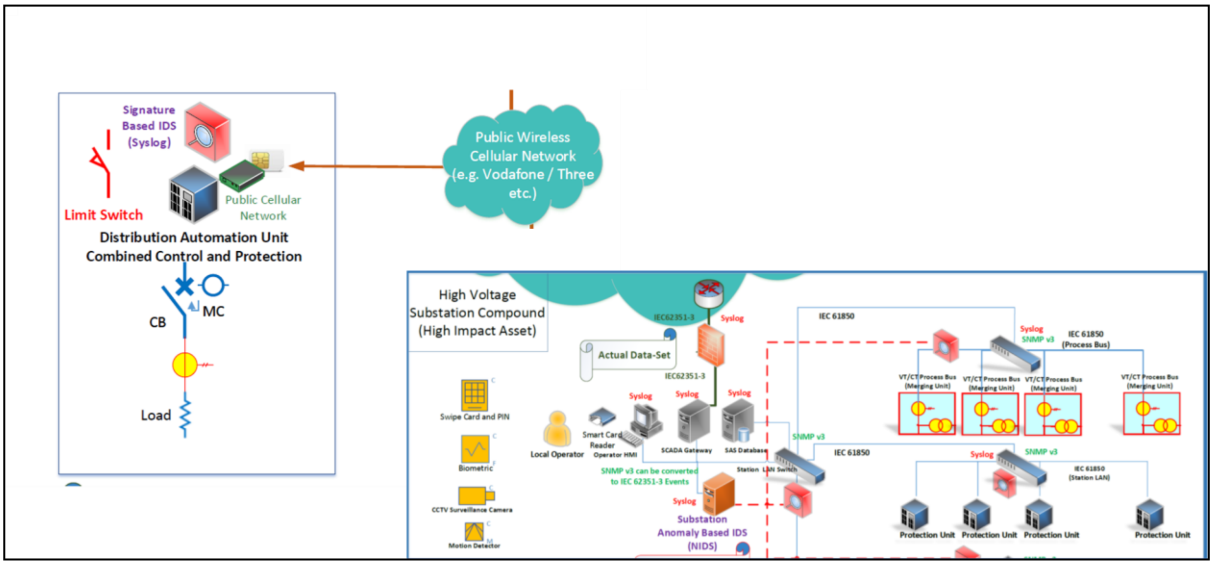


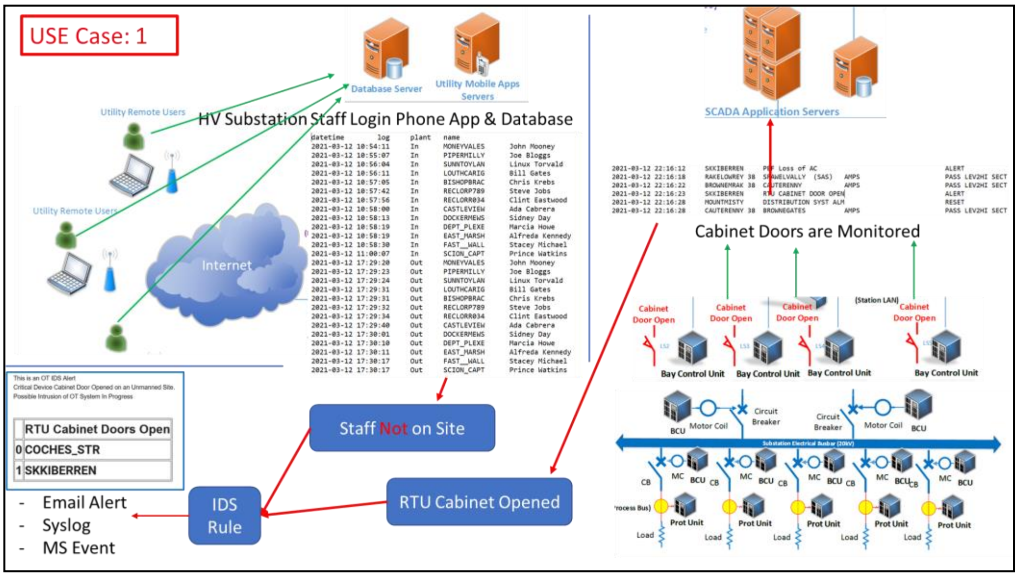
Figure 13: OT Systems Producing Syslog/SNMP Dataset

Use Cases for Implementation of Rules for the Custom OT IDS

A total of 9 custom rules were developed and implemented via coding for the custom OT IDS. The Use Cases rely on the Utility OT/IT Model previously discussed. Each Use Case is explained in terms of the security problem they address.

Rule 1: Alert the Risk of Physical Interference with Critical OT Systems in a Remote Site.

The SCADA system may routinely monitor access control to sensitive site equipment such as the control system, protection, and telecommunications equipment. These devices which are connected directly to the process are usually locked in equipment cabinets and limit switches on the cabinet doors may be in place. Open cabinets may be a safety risk to staff due to risks associated with meeting live apparatus. The SCADA system can alert the control centre if a cabinet is left open. This is useful information for the OT/IT SOC as it may also be indicative of an intrusion on site or some attempt to tamper with the equipment. However, it is only useful to the SOC if authorised staff are not present as open cabinets would indicate routine work. The custom OT IDS can parse the 'Site Login' database and search SCADA database for cabinet doors that are open in the reference timeslot. The IDS can alert the SOC via email or via Windows OS Event (automatically gathered by the SOC SIEM).



```
datetime            log     plant        name
2021-03-12 10:54:11    In      MONEYVALES      John Mooney
2021-03-12 10:55:07    In      PIPERMILLY      Joe Bloggs
2021-03-12 10:56:04    In      SUNNTOYLAN      Linux Torvald
2021-03-12 10:56:11    In      LOUTHCARIG      Bill Gates
2021-03-12 10:57:05    In      BISHOPBRAC      Chris Krebs
2021-03-12 10:57:42    In      RECLORP789      Steve Jobs
2021-03-12 10:57:56    In      RECLORR034      Clint Eastwood
2021-03-12 10:58:00    In      CASTLEVIEW      Ada Cabrera
2021-03-12 10:58:13    In      DOCKERMEWS      Sidney Day
2021-03-12 10:58:19    In      DEPT_PLEXE      Marcia Howe
2021-03-12 10:58:19    In      EAST_MARSH      Alfreda Kennedy
2021-03-12 10:58:30    In      FAST__WALL      Stacey Michael
2021-03-12 11:00:07    In      SCION_CAPT      Prince Watkins
2021-03-12 17:29:20    Out     MONEYVALES      John Mooney
2021-03-12 17:29:23    Out     PIPERMILLY      Joe Bloggs
2021-03-12 17:29:24    Out     SUNNTOYLAN      Linux Torvald
2021-03-12 17:29:31    Out     LOUTHCARIG      Bill Gates
2021-03-12 17:29:31    Out     BISHOPBRAC      Chris Krebs
2021-03-12 17:29:32    Out     RECLORP789      Steve Jobs
2021-03-12 17:29:34    Out     RECLORR034      Clint Eastwood
2021-03-12 17:29:40    Out     CASTLEVIEW      Ada Cabrera
2021-03-12 17:30:01    Out     DOCKERMEWS      Sidney Day
2021-03-12 17:30:10    Out     DEPT_PLEXE      Marcia Howe
2021-03-12 17:30:11    Out     EAST_MARSH      Alfreda Kennedy
2021-03-12 17:30:17    Out     FAST__WALL      Stacey Michael
2021-03-12 17:30:17    Out     SCION_CAPT      Prince Watkins
```

```
2021-03-12 22:16:12    SKKIBERREN     PEF Loss of AC                     ALERT
2021-03-12 22:16:18    RAKELOWREY 38  SPAWELVALLY  (SAS)   AMPS          PASS LEV2HI SECT
2021-03-12 22:16:22    BROWNEMRAK 38  CAUTERENNY           AMPS          PASS LEV2HI SECT
2021-03-12 22:16:23    SKKIBERREN     RTU CABINET DOOR OPEN              ALERT
2021-03-12 22:16:28    MOUNTMISTY     DISTRIBUTION SYST ALM              RESET
2021-03-12 22:16:28    CAUTERENNY 38  BROWNEGATES          AMPS          PASS LEV2HI SECT
```

This is an OT IDS Alert
Critical Device Cabinet Door Opened on an Unmanned Site.
Possible Intrusion of OT System In Progress

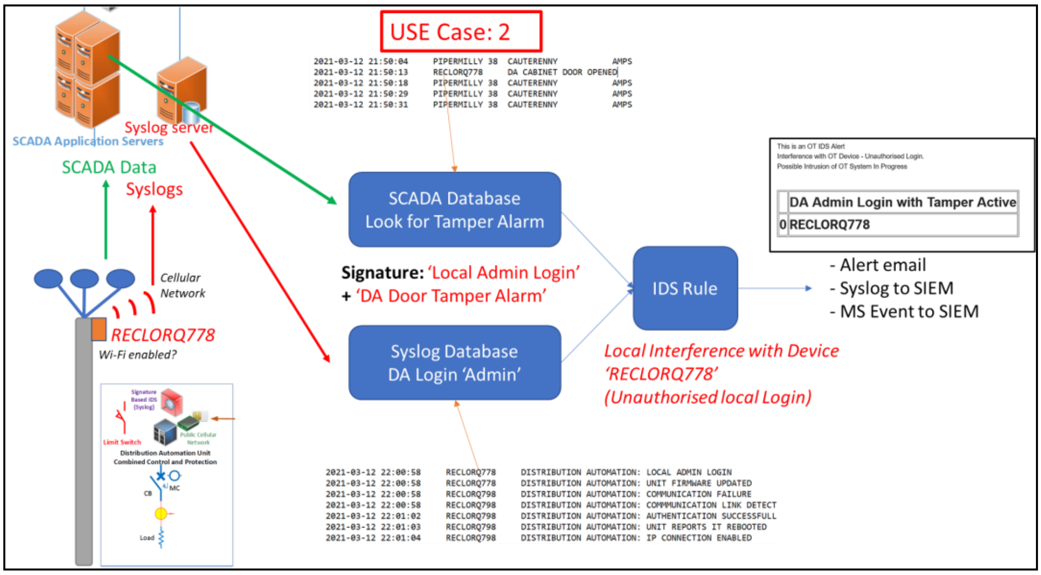
	RTU Cabinet Doors Open
0	COCHES_STR
1	SKKIBERREN

- Email Alert
- Syslog
- MS Event

Figure 14: Use Case 1 – Physical Intrusion to OT Systems

Rule 2: Alert the Risk of Unauthorised Access to OT system in a in secure location.

Field devices may be installed on the network in the vicinity of the public. For example, independent Distribution Automation units are installed to control and monitor MV overhead line network. There may be many 1000’s of these devices and some may be equipped with Wi-Fi, ZigBee or other communication technologies. The following Use Case seeks to alert if a DA device reports (via syslog or SNMP) that an Admin user has logged into the device. Combined with the enclosure open tamper alert, this maybe signature of unauthorised login. It is important to extend security monitoring to these end points as they may be networked with other OT systems over a WAN. If weakly secured it may present a vulnerable point for an attacker to exploit.


USE Case: 2
Syslog server
SCADA Application Servers
SCADA Data
Syslogs
Cellular Network
RECLORQ778
Wi-Fi enabled?
Signature Based IDS (Syslog)
Public Cellular Network
Limit Switch
Distribution Automation Unit Combined Control and Protection
CB
MC
Load
SCADA Database Look for Tamper Alarm
Signature: 'Local Admin Login' + 'DA Door Tamper Alarm'
IDS Rule
Syslog Database DA Login 'Admin'
Local Interference with Device 'RECLORQ778' (Unauthorised local Login)

```
2021-03-12 21:50:04    PIPERMILLY 38  CAUTERENNY             AMPS
2021-03-12 21:50:13    RECLORQ778     DA CABINET DOOR OPENED
2021-03-12 21:50:18    PIPERMILLY 38  CAUTERENNY             AMPS
2021-03-12 21:50:29    PIPERMILLY 38  CAUTERENNY             AMPS
2021-03-12 21:50:31    PIPERMILLY 38  CAUTERENNY             AMPS
```

This is an OT IDS Alert
Interference with OT Device - Unauthorised Login.
Possible Intrusion of OT System In Progress

	DA Admin Login with Tamper Active
0	RECLORQ778

- Alert email
- Syslog to SIEM
- MS Event to SIEM

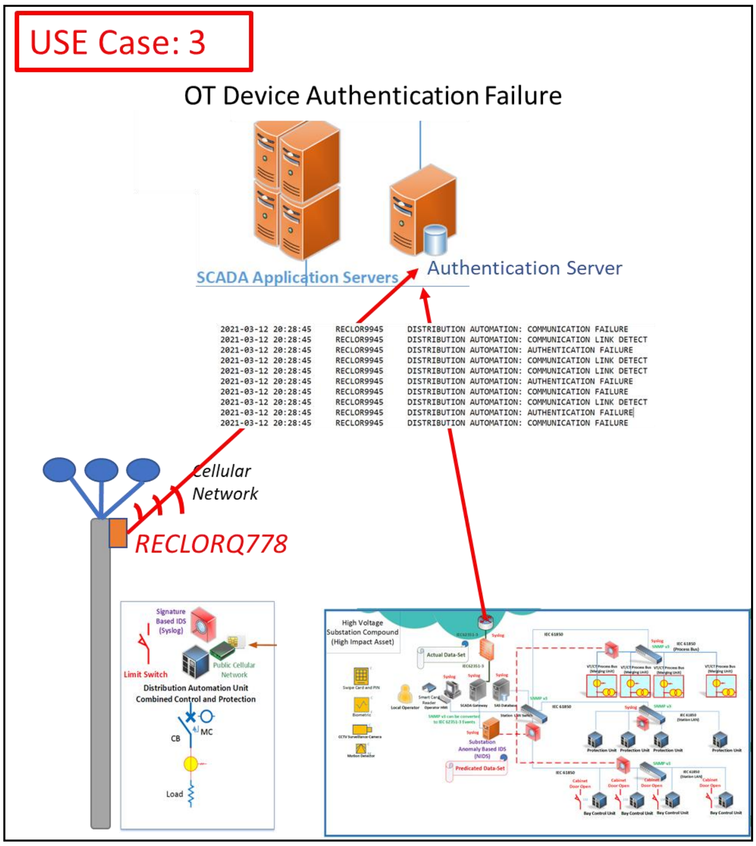
```
2021-03-12 22:00:58    RECLORQ778    DISTRIBUTION AUTOMATION: LOCAL ADMIN LOGIN
2021-03-12 22:00:58    RECLORQ778    DISTRIBUTION AUTOMATION: UNIT FIRMWARE UPDATED
2021-03-12 22:00:58    RECLORQ798    DISTRIBUTION AUTOMATION: COMMUNICATION FAILURE
2021-03-12 22:00:58    RECLORQ798    DISTRIBUTION AUTOMATION: COMMMUNICATION LINK DETECT
2021-03-12 22:01:02    RECLORQ798    DISTRIBUTION AUTOMATION: AUTHENTICATION SUCCESSFULL
2021-03-12 22:01:03    RECLORQ798    DISTRIBUTION AUTOMATION: UNIT REPORTS IT REBOOTED
2021-03-12 22:01:04    RECLORQ798    DISTRIBUTION AUTOMATION: IP CONNECTION ENABLED
```

Figure 15: Use Case 2 – Unauthorized Login to OT Systems

Rule 3: Alert the Failure of an OT Device to Properly Authenticate with SCADA.

Field devices such as Distribution Automation and Substation Automation Systems usually authenticate to a centralised authentication system to establish the IP connection.

Authentication can use different methods e.g., RADIUS, TACACS+ and/or PKI. A failed authentication could be a sign of a spoofing attack were a rogue device attempts to establish a connection with the centralised system. In the below example the device RECLORQ778 continuously fails to authenticate with the centralised authentication server.

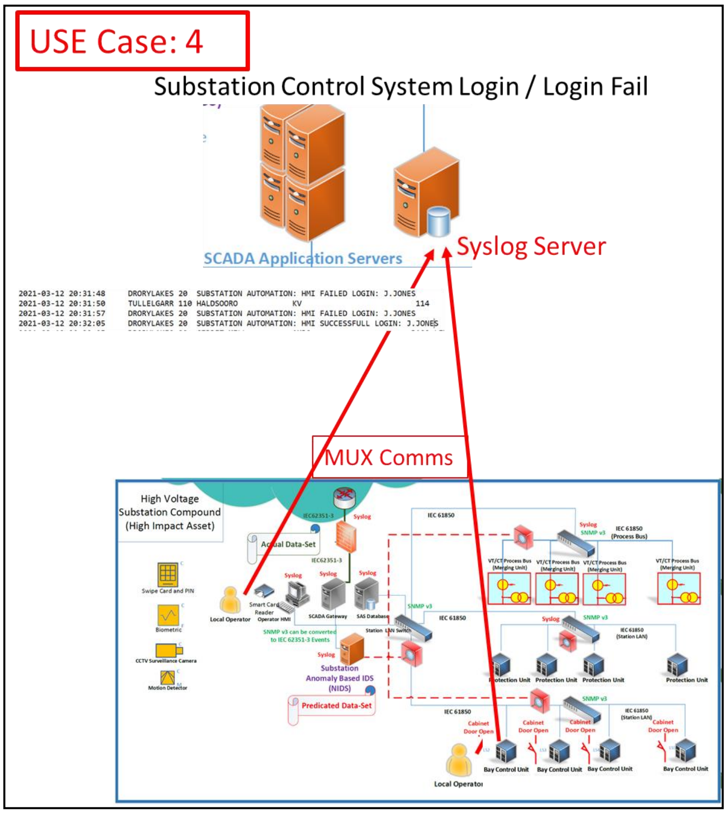


```
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION FAILURE
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION LINK DETECT
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: AUTHENTICATION FAILURE
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION LINK DETECT
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION LINK DETECT
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: AUTHENTICATION FAILURE
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION FAILURE
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION LINK DETECT
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: AUTHENTICATION FAILURE
2021-03-12 20:28:45    RECLOR9945    DISTRIBUTION AUTOMATION: COMMUNICATION FAILURE
```

Figure 16: Use Case 3 – OT Device Authentication Failure

Rule 4: Substation Automation System Login Successful / Login Failure.

The substation automation system is a sophisticated network of OT devices. Logins to the substation applications must be logged and monitored. Unauthorised access (either locally or remotely) may result in damage to the system, the plant or danger to staff or members of the public. Failed Logins to OT must be investigated by the SOC. The substation automation system can send back user authentication data via syslog protocol to the central syslog/SNMP database. The custom OT IDS can flag successful logins (with associated username) and failed logins.



```
2021-03-12 20:31:48     DRORYLAKES 20  SUBSTATION AUTOMATION: HMI FAILED LOGIN: J.JONES
2021-03-12 20:31:50     TULLELGARR 110 HALDSOORO            KV                          114
2021-03-12 20:31:57     DRORYLAKES 20  SUBSTATION AUTOMATION: HMI FAILED LOGIN: J.JONES
2021-03-12 20:32:05     DRORYLAKES 20  SUBSTATION AUTOMATION: HMI SUCCESSFULL LOGIN: J.JONES
```

Figure 17: Use Case 4 – Substation Automation System Login/Login Fail

Rule 5: SNMP Alert – Substation Ethernet Port Disconnected

The substation automation system utilises a sophisticated IP network (IEC61850) which uses SNMP protocol to supervise the network infrastructure. A disconnection of an ethernet cable from a network switch may indicate unauthorised action by intruder who may attempt to connect a rogue device to the network to further penetrate the OT system. The OT/IT SOC must investigate this disconnection event.

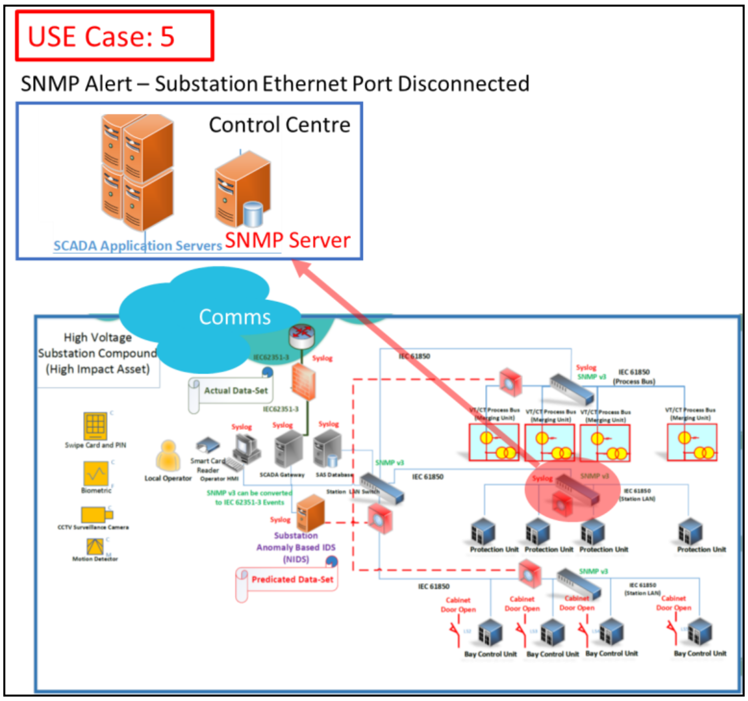


Figure 18: Use Case 5 – Substation Ethernet Port Disconnected

Rule 6: Syslog Alert – Substation IDS: Network Traffic Outside of Baseline

The substation Anomaly based IDS may detect traffic that is outside of baseline. As the substation traffic tends to remain the same due to the static nature of the network (i.e., configurations do not change much once commissioned), traffic outside of the baseline may indicate either incorrect operation or unauthorised influence by a threat actor. The substation IDS can provide the alert to the Control Centre Syslog server and the OT IDS can detect and relay the alert on to the OT/IT SOC.

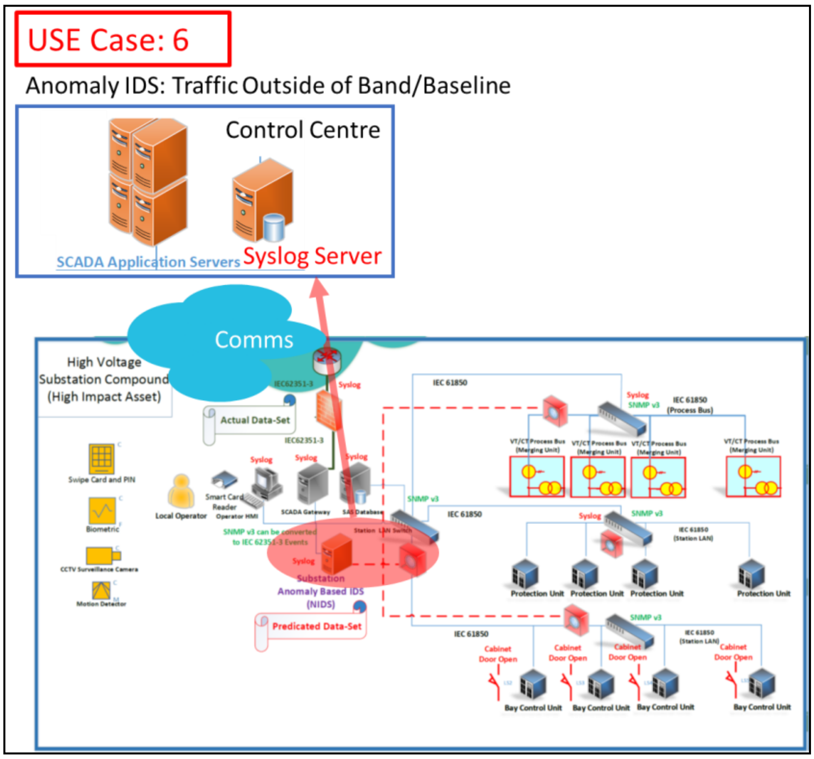


Figure 19: Use Case 6 – Substation Anomaly Based IDS: Traffic Outside of Baseline

Rule 7: Syslog Alert – Substation Application Whitelisting: Unauthorised Execution Blocked

The substation OT network has several conventional hosts industrially hardened to withstand the HV environment. These hosts run typical IT operating systems (Windows/Linux) to support local databases, HMIs, and engineering tools. Application Whitelisting may be deployed cybersecurity rather than antivirus due to isolation of OT from signature update servers and updates potentially degrading performance of control system software. The application whitelisting can be configured to provide syslog alerts when an unauthorised program (not on the Whitelist) attempts to execute. A blocking of this nature could be for example malware passed onto the OT host via USB stick.

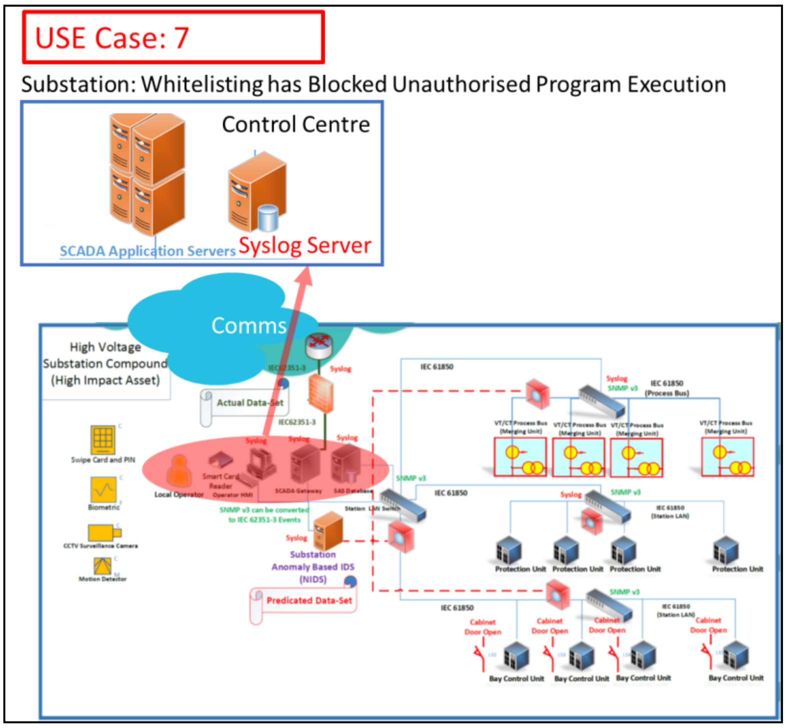


Figure 20: Use Case 7 – Substation App Whitelisting: Unauthorized Program Blocked

Rule 8: Syslog Alert – Layer 2 (802.1x Supplicant) Authentication Failed

The DA units may be equipped with additional security via Layer 2 authentication standard IEEE 802.1x (IEEE, 2021). This can be applied to both the wired ethernet connections and WI-FI connections. 802.1x is commonly used on Enterprise wireless networks via WPA2 Enterprise Wi-Fi. This may be useful in OT domain to secure the layer 2 connections of device LAN ports. Failure of authentication can be flagged to syslog server via the 802.1X authenticator. The failed authentication may indicate intrusion or unauthorised access to the OT device Layer 2 ports.

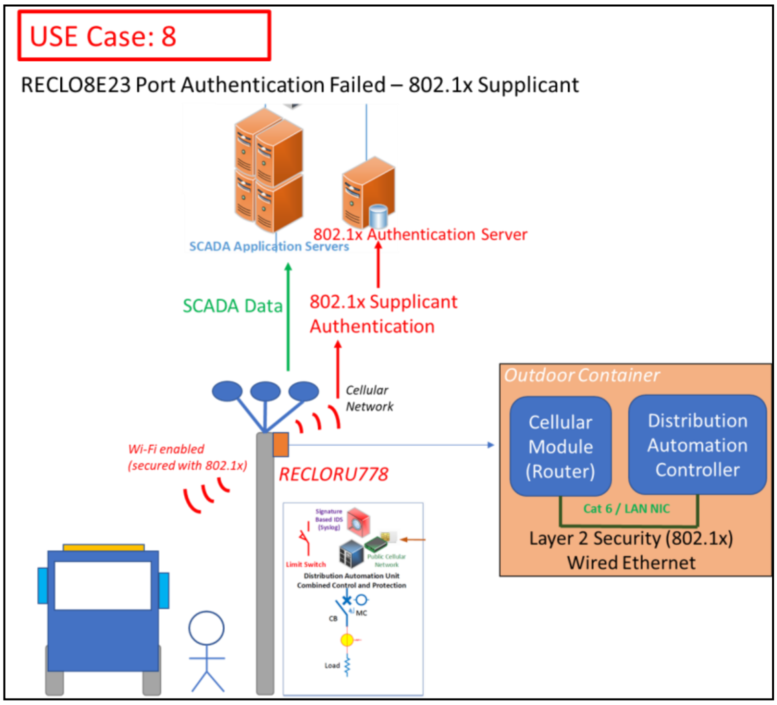

USE Case: 8
RECLO8E23 Port Authentication Failed – 802.1x Supplicant
SCADA Application Servers
802.1x Authentication Server
SCADA Data
802.1x Supplicant
Authentication
Cellular
Network
Wi-Fi enabled
(secured with 802.1x)
RECLORU778
Signature Based IDS (Syslog)
Limit Switch
Public Cellular Network
Distribution Automation Unit
Combined Control and Protection
CB
MC
Load
Outdoor Container
Cellular Module (Router)
Distribution Automation Controller
Cat 6 / LAN NIC
Layer 2 Security (802.1x)
Wired Ethernet

Figure 21: Use Case 8 – Medium Voltage Independent Device: Layer 2 Authentication

Software Flow Chart: The IDS software logical flow was implemented based on the Flowchart in Figure 22.

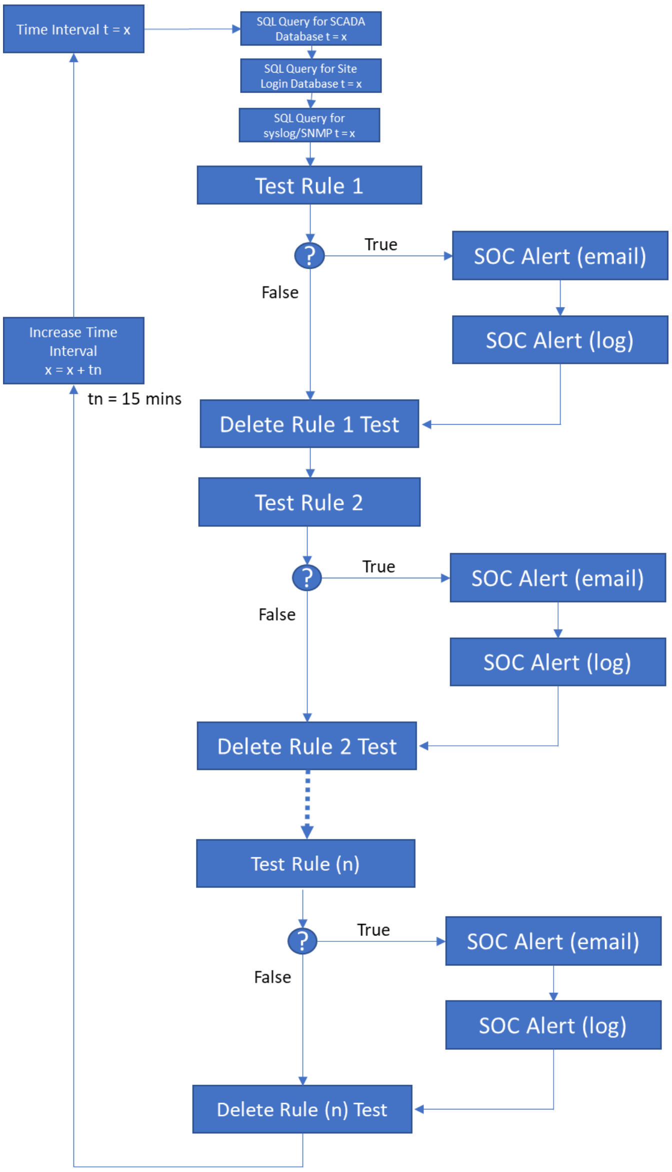


Figure 22: OT IDS Software Flow Chart

5 Implementation

The demonstration platform setup is shown in Figure 23. The primary system is a Windows 10 Professional running Hyper-V to enable the Guest *Lubuntu* VM to run (Lubuntu, 2021). A Gmail account was configured to allow the custom IDS to send the generated alerts to the SOC.

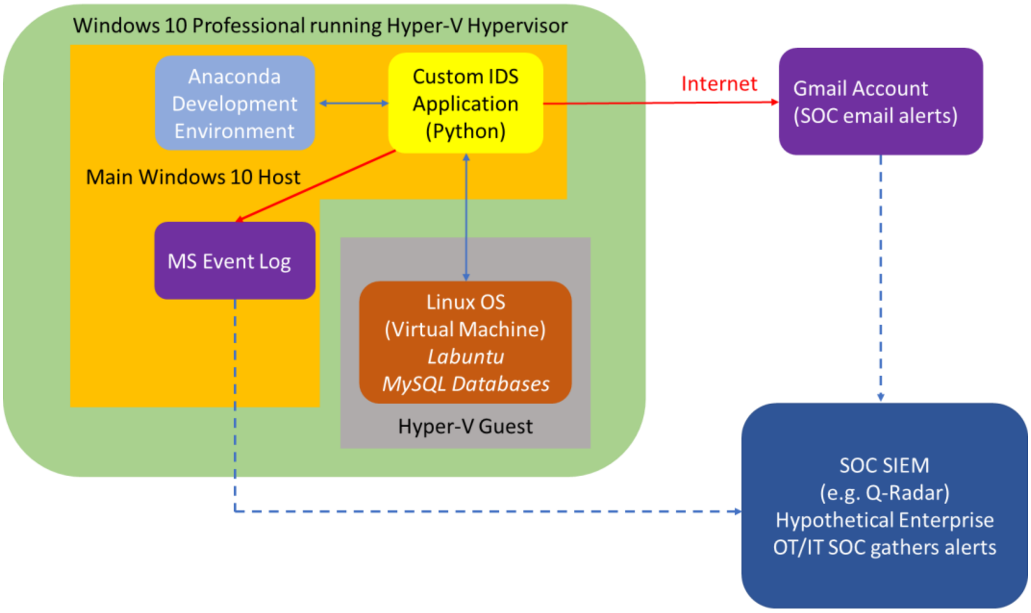

Windows 10 Professional running Hyper-V Hypervisor
Anaconda Development Environment
Custom IDS Application (Python)
Main Windows 10 Host
MS Event Log
Linux OS (Virtual Machine) *Labuntu* *MySQL Databases*
Hyper-V Guest
Internet
Gmail Account (SOC email alerts)
SOC SIEM (e.g. Q-Radar) Hypothetical Enterprise OT/IT SOC gathers alerts

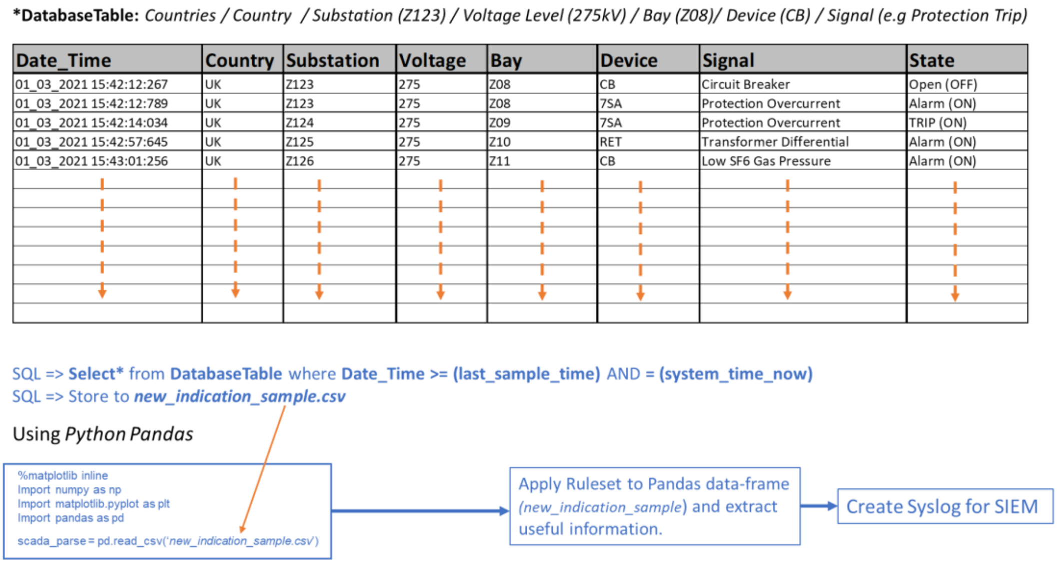
Figure 23: Implementation of Demonstration Platform

Programming Environment – Anaconda

Python scripts were prepared using the Spyder editor provided within the Anaconda environment (Anaconda, 2021). The Python scripts utilised the Pandas libraries. Pandas provides data-frame objects that are useful for processing large files of data that contain different types of information (e.g., time, text, numbers, other characters etc.).

Databases for Datasets – MySQL

The Lubuntu VM hosted MySQL Database (Oracle, 2021) to store the datasets used as proxies for the different OT Systems i.e., SCADA Database, Site Login database and Syslog/SNMP database. Each dataset is stored as a different table within MYSQL (*refer to Project Configuration Manual).* Data was acquired from the datasets by appropriate SQL queries – refer to Figure 24 below.



***DatabaseTable:** *Countries / Country / Substation (Z123) / Voltage Level (275kV) / Bay (Z08)/ Device (CB) / Signal (e.g Protection Trip)*

Date_Time	Country	Substation	Voltage	Bay	Device	Signal	State
01_03_2021 15:42:12:267	UK	Z123	275	Z08	CB	Circuit Breaker	Open (OFF)
01_03_2021 15:42:12:789	UK	Z123	275	Z08	7SA	Protection Overcurrent	Alarm (ON)
01_03_2021 15:42:14:034	UK	Z124	275	Z09	7SA	Protection Overcurrent	TRIP (ON)
01_03_2021 15:42:57:645	UK	Z125	275	Z10	RET	Transformer Differential	Alarm (ON)
01_03_2021 15:43:01:256	UK	Z126	275	Z11	CB	Low SF6 Gas Pressure	Alarm (ON)
↓	↓	↓	↓	↓	↓	↓	↓

SQL => **Select*** from **DatabaseTable** where **Date_Time >= (last_sample_time)** AND **= (system_time_now)**
SQL => Store to ***new_indication_sample.csv***

Using *Python Pandas*

```
%matplotlib inline
Import numpy as np
Import matplotlib.pyplot as plt
Import pandas as pd

scada_parse = pd.read_csv('new_indication_sample.csv')
```

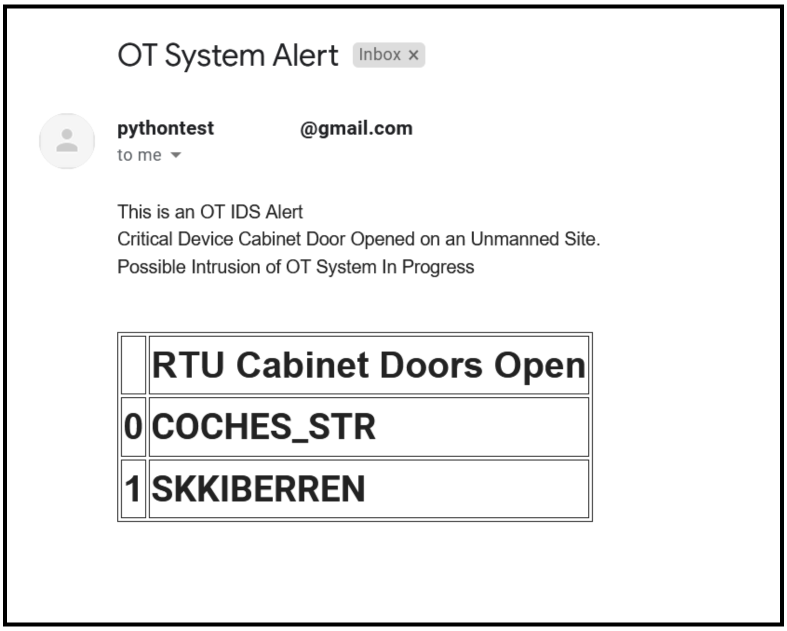
Apply Ruleset to Pandas data-frame (*new_indication_sample*) and extract useful information.

Create Syslog for SIEM

Figure 24: SQL Queries for Dataset 'SCADA'

OT IDS Alerting (emails)

Example 1: IDS email alert generated for Rule 1 i.e., Risk of Physical Interference with Critical OT Systems in a Remote Site. The email alert indicates that critical equipment cabinet doors have been opened (no staff present on site) in substations COCHES_STR and SKKIBERREN.



OT System Alert

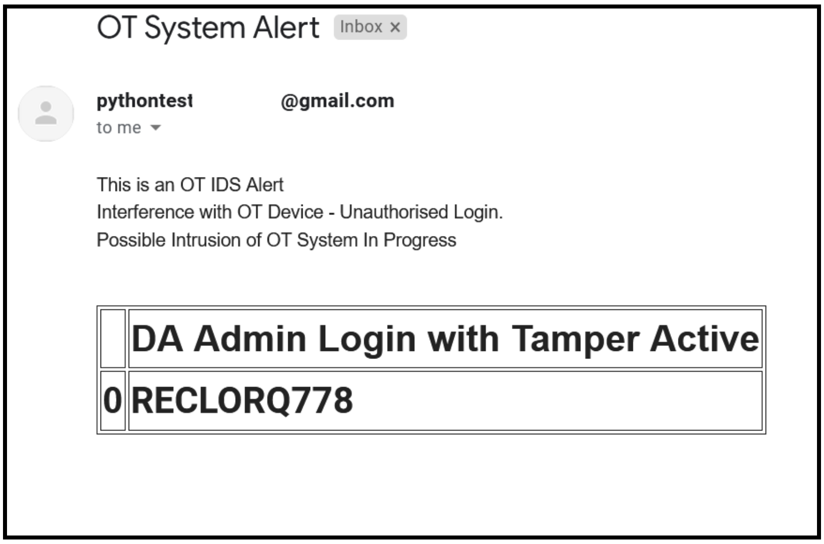
pythontest @gmail.com
to me

This is an OT IDS Alert
Critical Device Cabinet Door Opened on an Unmanned Site.
Possible Intrusion of OT System In Progress

	RTU Cabinet Doors Open
0	COCHES_STR
1	SKKIBERREN

Figure 25: Intrusion to Substation Control & Protection Cabinet

Example 2: IDS email alert generated for Rule 2: Risk of Unauthorised Access to OT system. The email alert indicates that OT equipment (i.e., device RECLORQ778) has a successful ‘Admin Login’ with the Tamper alarm (i.e., open enclosure) active.



OT System Alert

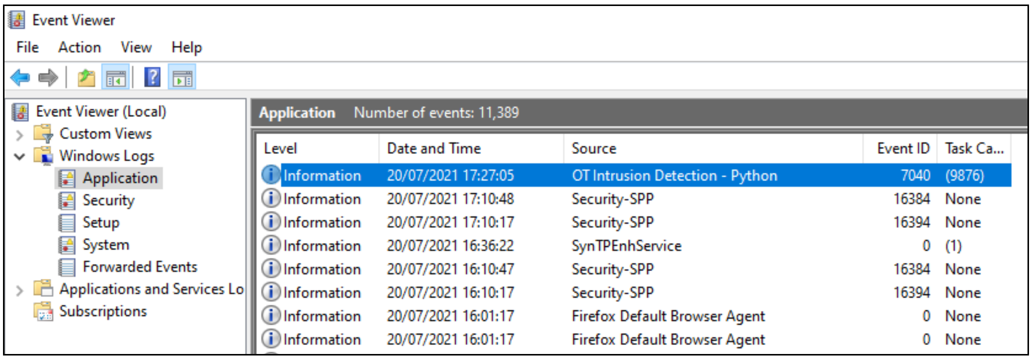
pythontest @gmail.com
to me

This is an OT IDS Alert
Interference with OT Device - Unauthorised Login.
Possible Intrusion of OT System In Progress

	DA Admin Login with Tamper Active
0	RECLORQ778

Figure 26: Unauthorized Access to OT Device

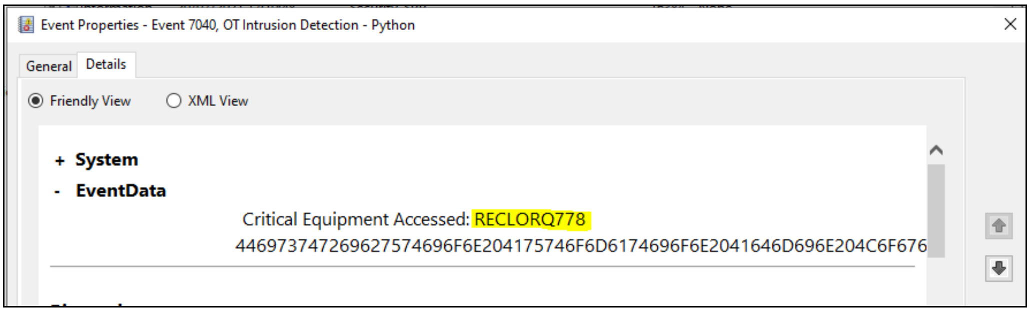
OT IDS Alerting (Windows OS Event)



Application Number of events: 11,389

Level	Date and Time	Source	Event ID	Task Ca...
Information	20/07/2021 17:27:05	OT Intrusion Detection - Python	7040	(9876)
Information	20/07/2021 17:10:48	Security-SPP	16384	None
Information	20/07/2021 17:10:17	Security-SPP	16394	None
Information	20/07/2021 16:36:22	SynTPEnhService	0	(1)
Information	20/07/2021 16:10:47	Security-SPP	16384	None
Information	20/07/2021 16:10:17	Security-SPP	16394	None
Information	20/07/2021 16:01:17	Firefox Default Browser Agent	0	None
Information	20/07/2021 16:01:17	Firefox Default Browser Agent	0	None

Detailed of Windows OS Event – provides the OT Device that is affected (RECLORQ778)

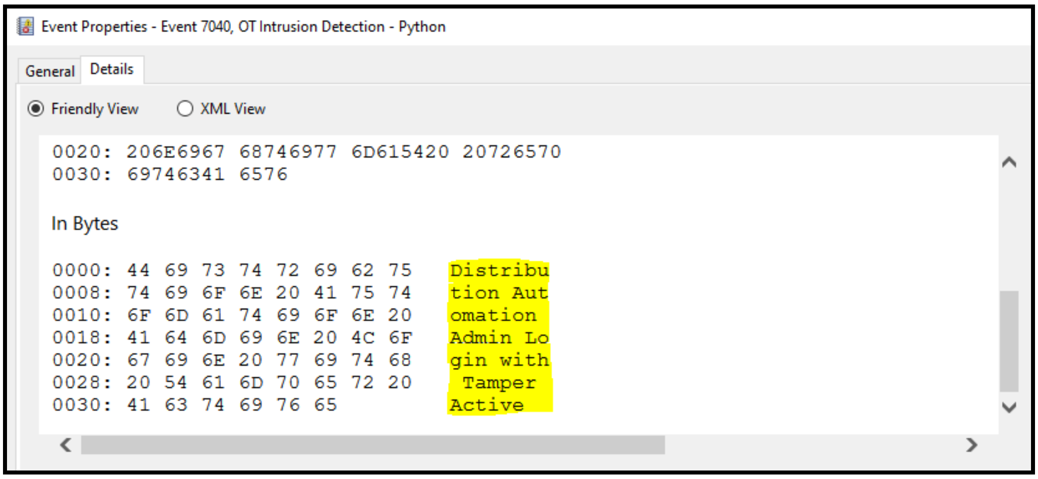


Event Properties - Event 7040, OT Intrusion Detection - Python
General
Details
● Friendly View
○ XML View
+ System
- EventData

Critical Equipment Accessed: RECLORQ778
4469737472696275746 96F6E204175746F6D6174696F6E2041646D696E204C6F676

Figure 27: Custom Generated System Log

Detailed of Windows OS Event – provides further explanation of security event. The description security event is 'Distribution Automation Admin Login with Tamper Alert'



Event Properties - Event 7040, OT Intrusion Detection - Python
General
Details
● Friendly View
○ XML View

```
0020: 206E6967 68746977 6D615420 20726570
0030: 69746341 6576
```

In Bytes

```
0000: 44 69 73 74 72 69 62 75   Distribu
0008: 74 69 6F 6E 20 41 75 74   tion Aut
0010: 6F 6D 61 74 69 6F 6E 20   omation 
0018: 41 64 6D 69 6E 20 4C 6F   Admin Lo
0020: 67 69 6E 20 77 69 74 68   gin with
0028: 20 54 61 6D 70 65 72 20    Tamper 
0030: 41 63 74 69 76 65         Active
```

Figure 28: Custom Generated System Log (Detailed Info)

6 Evaluation

As has been shown in the OT/IT Power Grid Model, there exists are very large amount of data in the OT zone that could potentially be a source of security information relevant to an enhanced OT/IT SOC. By developing Use Cases (examples provide 1 to 8) that are highly specific and unique to the characteristics of the power grid, it is possible to provide better cybersecurity situational awareness of real time threats.

As context specific rules with known positive signature formats have been developed as part of this project, the IDS developed program is therefore a type of *Custom Signature-Based IDS.* Formulation of the rules relies on a detailed understanding of how the power grid information system and its data is constructed and the types of communication and data flows that exist therein. A significant investment in time is required to develop the model, but a signature-based IDS is better at providing direct feedback to SOC about the type of security related event that is occurring.

The time required to develop a custom signature-based IDS is a drawback. Other options such as deployment of anomaly-based IDS may be quicker to deploy as they do not require a significant investment in time to develop a model. However, the lack of specific feedback as to the nature of the policy violation is a significant disadvantage of anomaly-based IDS.

Once the model is well developed, it is possible to be creative with respect to development of new rules that can detect new signatures. Given the importance of the power grid to our everyday lives, the investment of time to develop a custom signature-based OT IDS can be considered worthwhile and provide the traditional IT SOC with a much-enhanced situational awareness.

The developed program can be extended with new rules as required. The program is modularly designed and can implement logical checks on detected events i.e., it is possible to correlate information between different the OT datasets using AND, OR and NOT logic. In this project 8 use cases have been developed as proof of concept but there is no limit to number of rules and signatures that could be implemented but it is necessary to understand the OT/IT model thoroughly to be able to develop useful security use cases that can effectively detect unauthorised intrusions onto the OT estate.

Project and Dataset Limitations:

In real OT systems the datasets are very large and continuously updating. In the project only sample datasets have been used to drive the IDS program. This creates some limitations to assessing how well the IDS program would perform in the real world. Some of the recognised limitations include:

- The IDS program is a simulated platform, considering similar datasets that would be encountered in a real implementation. Deploying the IDS in the real-world application of OT security would be interesting future work.
- Python was useful coding language to develop the basic functionality, however if there was additional time, implementation of a Graphical User Interface (via Flask or PyCharm) to display and log the IDS information would be useful. In this respect other languages could also be considered (such as Java or Visual C++) which may be better suited to application development.
- Time slots for querying the SQL datasets was performed for the entire available dataset time. However, in a real implementation on an OT network the program would need to query specific time windows e.g., query each dataset every 10 minutes.

The overall system would be time synced with NTP so a common time would be available. The program would need to adjust its query time slot in 10-minute intervals in line with the overall system time.

- Given the limited size of the datasets, we cannot be sure that a real implementation of the is IDS would not through up some unexpected exceptions if it was to run continuously on data that is not fully characterised or known in advance.

7 Conclusion and Future Work

The objective of the project was to investigate ways to enhance continuous security monitoring of a Utilities OT/IT network. A demonstration platform was developed that shows how we might leverage useful OT data for improved security situational awareness. By implementing a simple IDS application that could search through these datasets, it was possible to provide an IT/OT SOC with up-to-date information enabling to assess cyber risks top the critical OT estate. By formulating a Utility OT/IT model, specific Use Cases could be developed that address security problems that may arise on the HV network. The research question posed is:

What enhancements can be made to traditional enterprise zone continuous security monitoring systems to accommodate the surveillance of the Power Grid OT estate?

The question has been positively answered by the research project as it has been shown that the existing OT systems (i.e., SAS, SCADA, OMS etc.) possess a wealth of information that may be correlated, by development of appropriate security use cases, to enhance the existing SOC continuous monitoring technologies and analytical skillsets. Intrusion detection of OT assets, that have traditionally not been subject to cybersecurity controls of this nature, can be easily integrated to the existing IT SOC function.

There are extensive areas for future work in this area. For example, simple use cases have been described in this proof of concept but more advanced computing technologies such as machine learning and artificial intelligence could be interesting areas of research. Only a few available datasets have been utilised here, but the OT network contains vast amount of information that could prove useful for security technologies.

As with any IDS, once deployed there is a tendency for the system to generate a lot of false positives. If the IDS was deployed onto a live OT network, there would be a need to conduct tuning to reduce the level of false positives. This tuning would be necessary if there are additional rules with their respective real-world use cased encoded in the IDS. The more rules encoded the longer the fine-tuning process.

References

Anaconda (2021) ‘Anaconda | The World’s Most Popular Data Science Platform’. Available at: https://www.anaconda.com/ (Accessed: 30 July 2021).

Assante, M. J., Lee, R. M. and Conway, T. (2017) ‘Modular ICS Malware’, *E-Isac Sans Ics*, (6), pp. 1–27. Available at: https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-

ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware Final.pdf?parent=64412.

Checkpoint Software (2020) *CLAROTY CONTINUOUS THREAT DETECTION & CHECK POINT NEXT-GENERATION FIREWALL*. Available at: www.claroty.com. (Accessed: 30 July 2021).

Chen, L. (2011) ‘Impacts of Digital and Networked Technologies Used in Smart Substation on Relay Protection’. IEEE, pp. 3947–3950.

Colbert, E. and Kott, A. (2016) *Cyber-security of SCADA and Other Industrial Control Systems*. Edited by E. Colbert and A. Kott. Springer. doi: 10.1007/978-3-319-32125-7.

Conklin, W. A. (2016) ‘IT vs. OT security: A time to consider a change in CIA to include Resilienc’, *Proceedings of the Annual Hawaii International Conference on System Sciences*.

IEEE, 2016-March, pp. 2642–2647. doi: 10.1109/HICSS.2016.331.

Cooney, K. and Lynch, K. (2012) ‘Developing a Roadmap for Introduction of IEC61850 based solutions for HV Substations in the Republic of Ireland’, in *Cigre*. Available at: http://www.cigre.org (Accessed: 2 November 2019).

DCCAE (2019) *NIS Compliance Guidelines for Operators of Essential Services*. doi: 10.1201/9781420072488.ch2.

Ernst & Young (2018) *Operational Technology Cyber Security, EY Consulting*.

HSE-UK (2017) ‘Cyber Security for Industrial Automation and Control Systems (IACS)’, p. Health and Safety Executive (HSE). Available at: https:/hse-guidance-for-iacs-security/.

Hughes, R. C. (2015) ‘DOCUMENTATION REQUIREMENTS THROUGHOUT THE LIFECYCLE OF DIGITAL SUBSTATION AUTOMATION’, in. Cigre. Available at: https://e-cigre.org/publication/628-documentation-requirements-throughout-the-lifecycle-of-digital-substation-automation-systems.

IANA (2010) *Service Name and Transport Protocol Port Number Registry*. Available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=IEC+104 (Accessed: 30 July 2021).

IEC (2009) ‘TECHNICAL SPECIFICATION Industrial communication networks-Network and system security-Part 1-1: Terminology, concepts and models’.

IEEE (2021) *IEEE 802.1X - Wikipedia*. Available at: https://en.wikipedia.org/wiki/IEEE_802.1X (Accessed: 30 July 2021).

Institute of Standards, N. (2014) ‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’. doi: 10.6028/NIST.CSWP.04162018.

ISA (2021) *Common ICS Cybersecurity Myth #1: The Air Gap*. Available at: https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap (Accessed: 30 July 2021).

Kerkers, M. (2017) *Assessing the Security of IEC 60870-5-104 Implementations using Automata Learning*. University of Twente. Available at: https://essay.utwente.nl/72277/1/Kerkers_MA_EEMCS.pdf (Accessed: 30 July 2021).

Knapp, E. D. and Samani, R. (2013) *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Elsevier Inc. doi: 10.1016/C2012-0-01113-1.

Kumar, R. (2010) 'Utility of SCADA in Power Generation and Distribution System'. IEEE, pp. 648–652. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5564689.

Langner, R. and Schneier, B. (2013) 'Stuxnet - To Kill a Centrifuge', *The Langner Group*, (November), pp. 1–37. Available at: www.langner.com.

Lubuntu (2021) 'lubuntu Linux OS – lightweight, fast, easier'. Available at: https://lubuntu.net/ (Accessed: 30 July 2021).

Lunden, K. (2021) *Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises | FireEye Inc*. Available at: https://www.fireeye.com/blog/threat-research/2021/05/increasing-low-sophistication-operational-technology-compromises.html (Accessed: 30 July 2021).

Ma, J. *et al.* (2010) 'Integration of Protection and Control Systems for Smart Substation'. IEEE.

Madonsela, B., Davidson, I. and Mulangu, C. T. (2018) 'Advances in Telecontrol and Remote Terminal Units (RTU) for Power Substations', (June). doi: 10.1109/PowerAfrica.2018.8521181.

Matoušek, P. (2017) *Description and analysis of IEC 104 Protocol Petr Matoušek*. Available at: http://www.fit.vutbr.cz/~matousp/grants.php.en?id=1101. (Accessed: 30 July 2021).

NERC (2009) *Catagorizing Cyber Systems*. Available at: https://www.nerc.com/docs/standards/sar/Concept_Paper_Categorizing_Cyber_Systems_2009July21.pdf.

NERC (2013) *Understanding the Grid*. Available at: https://www.nerc.com/AboutNERC/Documents/Understanding the Grid AUG13.pdf (Accessed: 30 July 2021).

Oracle (2021) *MySQL Database Software*. Available at: https://www.mysql.com/ (Accessed: 30 July 2021).

Robert M. Lee, Michael J. Assante and Tim Conway (2016) 'Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case', pp. 2–11. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Schlegel, R., Obermeier, S. and Schneider, J. (2017) ‘A security evaluation of IEC 62351’, *Journal of Information Security and Applications*, 34(June 2018), pp. 197–204. doi: 10.1016/j.jisa.2016.05.007.

Slowik, J. (2019) ‘Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack’, *Dragos Inc.* Available at: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Smart Grid Coordination Group (2014) *Report on Smart Grid Coordination Group: Smart Grid Information Security*. Available at: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

SNORT (2021) ‘Snort - Network Intrusion Detection & Prevention System’. Available at: https://www.snort.org/ (Accessed: 30 July 2021).

Tripwire (2018) *GitHub - Tripwire/tripwire-open-source: Open Source Tripwire®*. Available at: https://github.com/Tripwire/tripwire-open-source (Accessed: 30 July 2021).

Williams, T. J. (1994) ‘The Purdue Enterprise Reference Architecture and Methodology (PERA)’, *Computers in Industry*, 24(2–3), pp. 141–158.

Yang, Y. *et al.* (2013) ‘Intrusion Detection System for IEC 60870-5-104 based SCADA networks’, *IEEE Power and Energy Society General Meeting*, (May 2014). doi: 10.1109/PESMG.2013.6672100.