Student Name: Jones Tobi Ogidiagba
Student ID: 2056237
Module Name: Proactive Network Defence
Module Code: 7CS017

Assessment Title: Targeted attacks on Critical National Infrastructure and Associated Risks

1.0 Executive Summary

This report explains how to protect key national infrastructure from targeted attacks and the risks that come with them. It looks at a converged integrated IT and industrial control system as an example case study (ICS). These SCADA (supervisory control and data acquisition) systems are examples of ICS. Other control system configurations include distributed control systems (DCS). PLCs (Programmable Logic Controllers) are common in industrial settings. Sectors of control ICS are mostly used in areas such as energy and transportation, water and wastewater, oil and gas, transportation, nuclear power, and electricity are only a few of the application areas. Automation and robotics in the chemical, pharmaceutical, paper, food, and beverage industries, among others control. SCADA systems are commonly used to control assets that are scattered. Using a centralized data collection system with supervisory control. In general, DCS are utilized to monitor and operate production processes in a small area as a plant that is subject to supervisory and regulatory oversight. PLCs are used in discrete control systems that have specific applications and provide regulatory control in general. These control systems are crucial for the operation of the country's critical infrastructures, which are frequently highly interconnected and mutually dependent. Numerous agencies operate numerous ICS, posing a considerable security risk to these systems. This research presents an overview of various industrial control systems, highlights common threats and weaknesses, and recommends security remedies to limit associated risks.

The Microsoft threat modelling technique is used in this report to represent the threats in the case study. The trust domains are initially defined within the confines of a generic trust border. Three trust domains inside a general trust border boundary are examined for the purposes of this work.

In order to identify threats, attacks, vulnerabilities, and countermeasures that could negatively impact the IT and ICS environments, the Microsoft threat modelling tool will be utilized. In order to achieve security objectives and reduce risk, this can be utilized to redesign the network and application design of the given case study.
The following approach is used to model the threat environment for the selected trust domains:

- The integrated IT and control system environment's security requirements are specified initially.

- After that, an application diagram is created using the security requirements.
- Then, the security threats are categorized.
- Then, options for mitigating identified threats are presented so that, the threat mitigation solution is validated to ensure that the threats have been eliminated.

1.1 Network Defence methodologies and tools

Each strategy and methodology for threat modelling enables security teams and companies to detect threats. The degree to which these strategies and methodologies are applicable varies in terms of their quality, consistency, and return on investment.

- OCTAVE

Known as the framework for evaluating Operationally Critical Threats, Assets, and Vulnerabilities [1]. It is heavily weighted and is geared toward analyzing organizational (non-technical) risks associated with data asset breaches. This technique is particularly effective when it comes to developing a risk-aware business culture. The method is extremely adaptable to the security objectives and risk environment of a particular company.

- Trike Threat Modelling

Trike threat modelling is an open-source threat modelling process that aims to satisfy security auditing requirements from a cyber security management perspective [2]. Users create a risk model based on assets, responsibilities, actions, and threat exposure using the finished threat model. Scalability, on the other hand, is a concern.

- P.A.S.T.A. Threat Modelling

This procedure is referred to as the Attack Simulation and Threat Analysis Process [3]. It varies according to platform. It produces asset-centric output and is optimal for firms seeking to connect threat modelling with strategic objectives, as it involves business impact analysis as a core procedure.

- STRIDE Threat Modelling

Spoofing Tampering Repudiation Information Message Disclosure Denial of Service and Privilege Elevation are the acronyms for STRIDE [4]. It is a threat modelling technique developed by Microsoft. The STRIDE threat modelling objective is to ensure that an application complies with the Confidentiality, Integrity, and Availability (CIA) security features, as well as Authorization, Authentication, and Non-Repudiation (AAN). It is well recorded.

- VAST Threat Modelling

It scales across infrastructure and the full DevOps portfolio, integrates smoothly into an Agile environment, and generates actionable, accurate, and consistent outputs for developers, security teams, and senior executives alike.

2.0 Thrust Domains and Data Flow Diagram (DFD)

The three trust domains examined in this report are depicted in Figures 1, 2 and 3. The threat analysis described in this report was conducted using the Microsoft threat modelling tool.

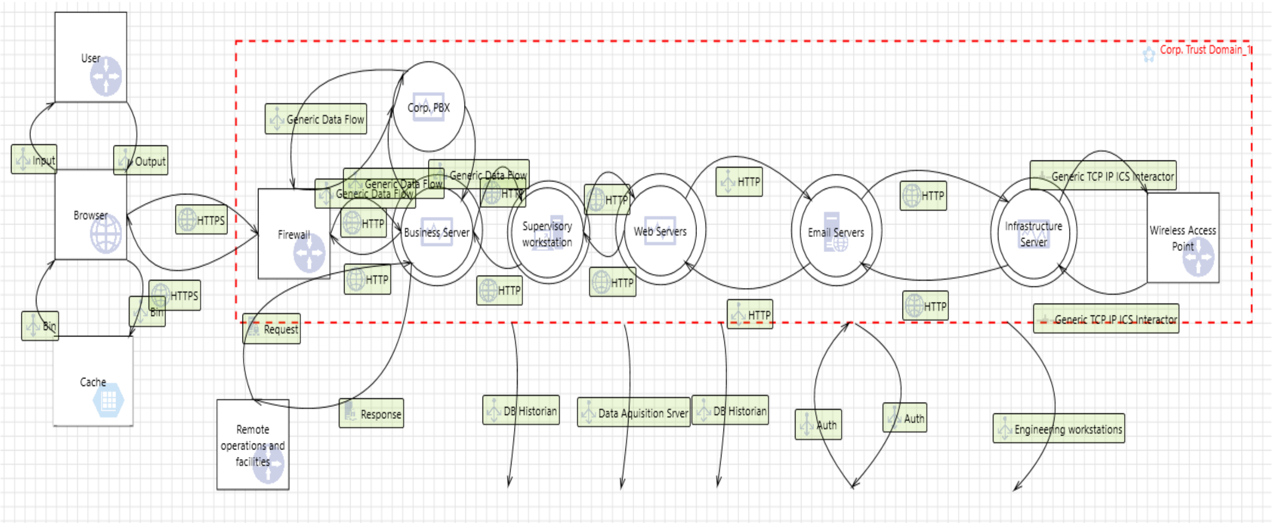


Figure 1: Trust Domain 1

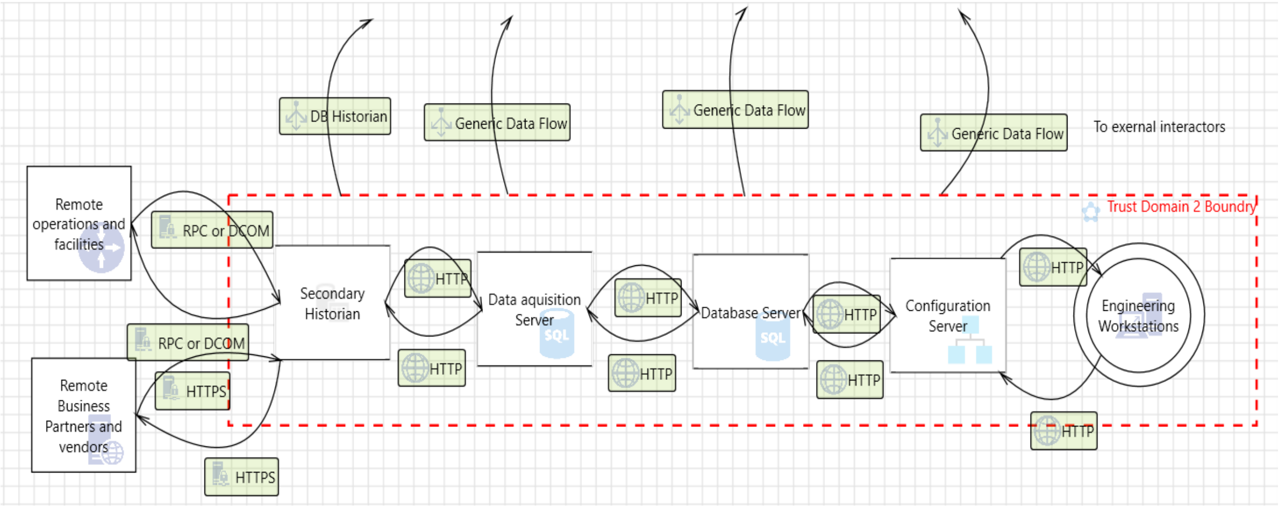


Figure 2: Trust Domain 2

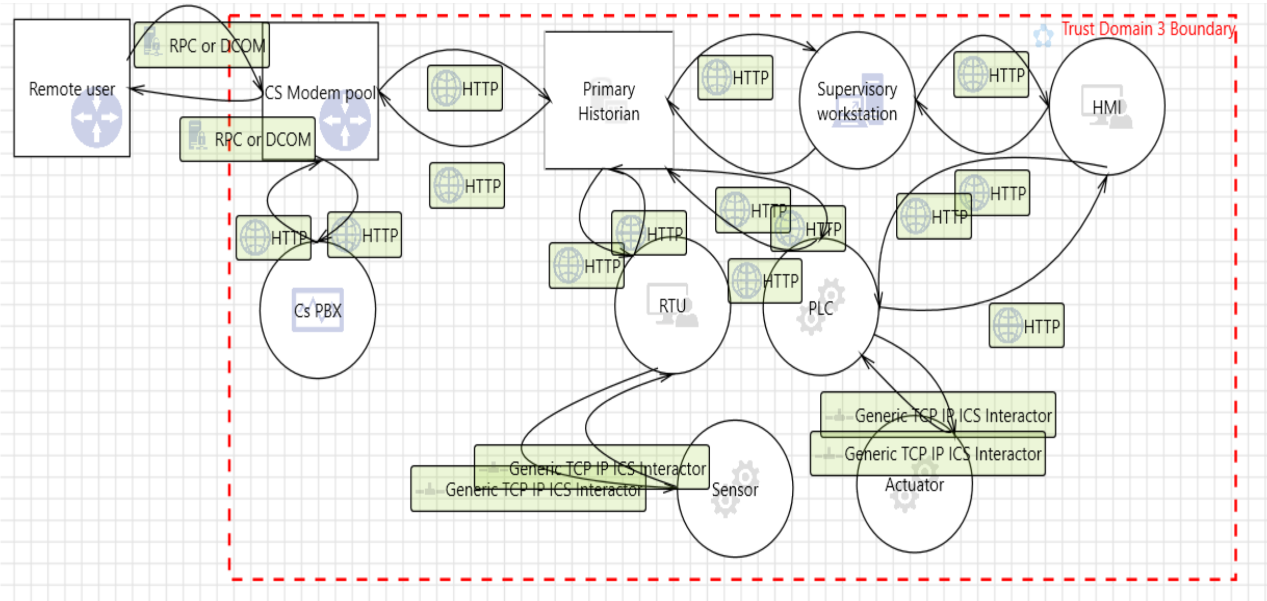
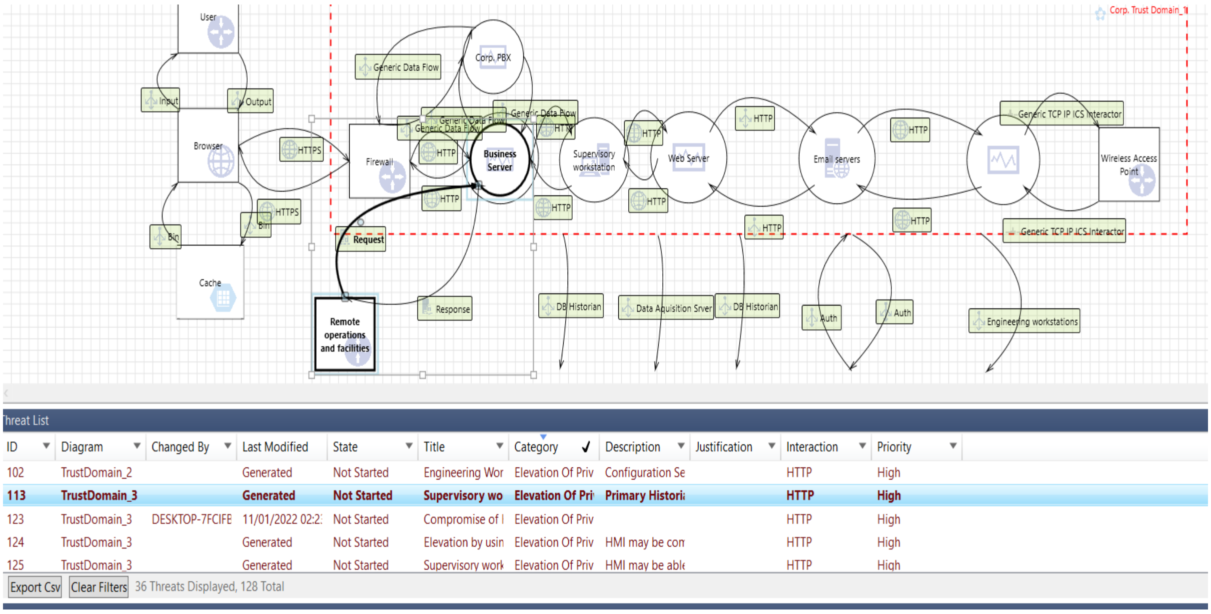


Figure 3: Trust Domain 3

2.1 Threat Identification

The STRIDE methodology was used to identify and categorize threats. The analysis panel in Microsoft's threat modelling tool is used to automatically identify and categorize risks based on each trust domain's data flow diagrams. Figure 4 illustrates a typical analysis pane.



hreat List

ID	Diagram	Changed By	Last Modified	State	Title	Category ✓	Description	Justification	Interaction	Priority
102	TrustDomain_2		Generated	Not Started	Engineering Wor	Elevation Of Priv	Configuration Se		HTTP	High
113	**TrustDomain_3**		**Generated**	**Not Started**	**Supervisory wo**	**Elevation Of Pri**	**Primary Histori**		**HTTP**	**High**
123	TrustDomain_3	DESKTOP-7FCIFE	11/01/2022 02:2	Not Started	Compromise of I	Elevation Of Priv			HTTP	High
124	TrustDomain_3		Generated	Not Started	Elevation by usin	Elevation Of Priv	HMI may be con		HTTP	High
125	TrustDomain_3		Generated	Not Started	Supervisory work	Elevation Of Priv	HMI may be able		HTTP	High

Export Csv | Clear Filters | 36 Threats Displayed, 128 Total

Figure 4: Section of Analysis pane

In this report, the threat for each trust domain is highlighted under each trust domain as follows:

2.2 Threat List for Trust Domain 1:

- **Spoofing threats:**
  - Spoofing of the Destination Data Store Cache: An attacker may spoof the Cache, resulting in data being written to the attacker's destination rather than the Cache.

  Mitigation:
  Consider utilizing a standard authentication mechanism to identify the destination data repository as a mitigation measure.

  - Spoofing the Firewall External Entity: An attacker can spoof the firewall, resulting in unauthorized access to the Business Server.

  Mitigation: This vulnerability can be mitigated by utilizing a well-known authentication process to identify the external entity.

  - Spoofing the Firewall External Entity: An attacker can spoof the firewall, granting unauthorized access to the Corp. PBX.

  Consider identifying the remote entity with a conventional authentication mechanism.

  - Using a Wireless Access Point as a Wi-Fi Spoofing Device External Entity: An attacker can fake a Wireless Access Point, granting unauthorized access to the Infrastructure Server.

  Consider identifying the remote entity with a conventional authentication mechanism.

  - Spoofing the Business Server Process: An attacker may spoof the Business Server process, resulting in the leakage of sensitive information by remote operations and facilities.

  Consider identifying the destination process with a common authentication technique.

  - Spoofing remote activities and infrastructure External Entity: An attacker may fake remote operations and facilities, which could result in unauthorized access to Business Server.

  Consider identifying the remote entity with a conventional authentication mechanism.

  - Remote operations and facilities impersonation External Destination Entity: An attacker may impersonate remote operations and facilities, resulting in data being transmitted to the attacker's target rather than to remote operations and facilities.

  Consider identifying the remote entity with a conventional authentication mechanism.

  - Spoofing the Firewall External Entity: An attacker may spoof the firewall, allowing unauthorized access to Business Server.

Mitigation: This issue can be mitigated by utilizing a standard authentication process to identify the foreign entity.

- Spoofing the Firewall External Entity: An attacker may spoof the firewall, allowing unauthorized access to the Corp. PBX.

Consider utilizing a standard authentication approach to determine the foreign entity's identity.

- Using a Wireless Access Point to Create a False Wireless Access Point External Entity: An attacker may fake a Wireless Access Point, granting unauthorized access to the Infrastructure Server.

Consider identifying the remote entity using a standard authentication procedure.

- Spoofing the Business Server Process: An attacker may spoof the Business Server process, resulting in the disclosure of information by Remote operations and facilities.

Consider identifying the destination process via a standard authentication technique.

- Remote operations and facilities spoofing External Entity: An attacker may fake remote operations and facilities, resulting in unauthorized access to Business Server.

Consider identifying the remote entity using a standard authentication procedure.

- Remote operations and facilities spoofing External Destination Entity: An attacker may spoof remote operations and facilities, resulting in data being transmitted to the attacker's target instead of remote activities and facilities.

Consider identifying the remote entity using a standard authentication procedure.

- **Tampering threats:**
  - It is possible that the web server 'Web Servers' is vulnerable to a cross-site scripting attack since it does not sanitize untrusted input.
  - The ability to verify input Business Server flaws: An attacker may interfere with data sent across Request if the server has vulnerabilities. Business Server could be subjected to a denial-of-service attack, a privilege elevation attack, or even the leaking of confidential data. A large number of exploitable flaws stem from the failure to verify that input fits expectations. Inquire about all available routes and the data handling that goes along with them. A list input validation strategy can be used to ensure that all input is correct.

- **Repudiation threats:**
  - If the firewall asserts that it did not receive data from a process that is on the other side of the trust boundary, this is feasible. Consider logging or auditing if you wish to keep track of the source, time, and summary of the data you receive.
  - Data from a process on the opposite side of trust has not been received by the browser, according to the browser. Logging or auditing can be used to keep track of where, when, and what data was used to create your output.
  - For whatever reason, Business Server refuses to accept data from a source outside of its trust boundary. It is important to keep track of the source, date, and summary of the data that is received.
  - Outside of the local neighborhood of the parent company's facilities and operations It's Possible for Remote Operations and Facilities to Deny Receiving Data from a Process Outside of the Trust Boundary. Use logging or auditing to keep track of the source, time, and summary of the data you receive.

- **Information Disclosure threat:**
  - The ability to sniff data flowing between Requests is a real possibility for an attacker. It is possible for an attacker to use the data they have access to attack other parts of the system or to simply reveal information that causes compliance concerns, depending on the data.

  - **Mitigation:** The data stream could be encrypted, as an option.
- **Denial of Service threats:**
  - HTTPS Data Flow Could Be Interrupted: An external agent could interrupt data moving in either way over a trust barrier.

  - Denial of Control attack against a Firewall: An attacker may attempt to deny control to the Firewall.

  - Flow of Data HTTPS Could Be Interrupted: An external agent could interrupt data moving in either way over a trust barrier.

  - Denial of Control of the target Browser: An attacker may attempt to deny control of the target Browser.

  - There is a high probability that the potential Process Business Server will fail to start, stop, terminate, or run slowly.
  - It is possible that an external actor could prevent data flowing in either direction across a trust border if a data flow request is made.

  - An attacker may deny access to Business Server through a denial of control assault.

- Denial of Control assault against remote operations and facilities: An attacker may deny access to remote operations and facilities.

- **Elevation of Privilege threat:**

  - To get greater rights, Business Server may be able to impersonate the context of the Firewall and gain access.
  - As a result of remote code execution, a firewall may be able to get elevated privileges.
  - To gain further privileges, a supervisory workstation may have to spoof a Business Server context.
  - If the Business Server can execute code on Supervisory workstations from a distance, this could lead to privilege escalation on the latter.
  - Imitating the context of the Supervisory workstation may allow Business Server greater rights by using impersonation as a ruse.
  - It's possible that web servers can use Supervisory workstation contexts to gain more access.
  - Web Server code may be remotely executed from a supervisory workstation.
  - Web Server contexts may be spoof-able by supervisory workstations to get further rights.
  - In some cases, web servers may be able to run Supervisory workstation code remotely.
  - To get further rights, email servers may be able to impersonate the context of web servers.
  - Email Servers' code may be executed remotely by Web Servers.
  - To gain further access, Web Servers may be capable of spoofing email servers' contexts.
  - For example, email servers might remotely run code on behalf of web servers.
  - It is possible that Infrastructure Servers can use Email Server context spoofing to get elevated access.
  - Changes in the Execution Flow of Programs in Business Server: An attacker can affect the execution flow of programs in Business Server by injecting data into the system.

2.3 Threat List for Trust Domain 2:

- **Spoofing threats:**

  - In this attack, data is written to the attacker's target instead of Secondary Historian because the attacker spoofs the Destination Data Store Secondary Historian. To find out where the data is stored, you might want to utilize a conventional authentication procedure.
  - For remote operations and facilities, an attacker's fake Secondary Historian could lead to the transmission of erroneous data. The source

data store's authenticity should be established by using a well-known authentication mechanism.
  - If an attacker impersonates Secondary Historian, data will be written to their target instead of Secondary Historian. To find out where the data is stored, you might want to utilize a conventional authentication procedure.
  - As a result, Remote Business Partners and Vendors may receive erroneous data from the Secondary Historian. The source data store's authenticity should be established by using a well-known authentication mechanism.
  - An attacker might spoof the Secondary Historian, resulting in the Data Acquisition Server receiving erroneous data. To verify the authenticity of the source data storage, consider using a well-known authentication mechanism.
  - As a result of an attacker posing as the Data acquisition Server, the attacker's target will receive data instead of the Data acquisition Server. The location of the data repository could be determined by using a normal authentication procedure.
  - Spying on the Database Server might lead to data being written to the attacker's server instead of the legitimate one. To find out where the data is stored, you might want to utilize a conventional authentication procedure.
  - Data can be written to an attacker's destination instead of Configuration Server by spoofing Configuration Server. To find out where the data is stored, you might want to utilize a conventional authentication procedure.

- **Tampering threats:**
  - An attacker may tamper with data traveling over RPC or DCOM. This could result in the corruption of the Secondary Historian. Ascertain the data's integrity as it flows to the data store.
  - An attacker may tamper with data transmitted through HTTPS. This could result in the corruption of the Secondary Historian. Ascertain the data's integrity as it flows to the data store.

- **Repudiation:**
- It's possible that you have trust levels, but is it OK for anyone than the highest level of trust to log updates? Allowing anyone to post to your logs can lead to concerns with attribution. Allow only trustworthy code to log.
- Logs from Unknown Sources: Do you accept logs from systems or people whose authentication is suspect? Authenticate the source of logs before receiving them.
- Secondary No trust boundary-crossing entity's data was written by the Historian, it claims. Keep track of the source, time, and summary of the data you get via logging or auditing.

- Facilities and operations outside the immediate vicinity of the parent entity Refusal to Receive Information: When a process on the other side of the trust boundary claims to have received data from a remote operation, the remote operation denies receiving it. Keep track of the source, time, and summary of the data you get via logging or auditing.
- In the presence of trust levels, is it possible for users other than those with the highest level of trust to log updates? If you allow anyone to write to your logs, you may have challenges with attribution. Enable the logging of only the most trusted code.
- Data may be withheld by the historian.

- **Information disclosure threats:**
  - Secondary Historian's poor data protection may allow an attacker to read information that was not intended for publication. - Weak Access Control for a Resource. Ensure that your permission settings are in order.
  - It is possible for an attacker to gain access to sensitive information in Secondary Historian due to a lack of effective data protection measures. Inspect your authorization options.
  - Inadequate data protection on Configuration Server may enable an attacker to read data that was not intended for public disclosure. Perform a review of the permissions you have been granted access to.

- **Denial of Service threats:**
  - An external agent can interrupt data traveling in either direction across a trust boundary if the flow of RPC or DCOM data is interrupted.
  - Unreachable Data Archive
  - It is possible that an attacker will seek to deny control of the Secondary Historian.
  - The remote activities and facilities of an opponent may be restricted.
  - Data traveling in either direction over a trust border can be interrupted by an external agent.
  - A Denial of Control (DoC) attack may be launched against Secondary Historian.
  - Denial of Control to Remote Business Partners and Vendors for Remote Businesses.
  - excessive resource consumption by engineering workstations or configuration servers: are efforts taken to manage resource consumption by engineering workstations or configuration servers? To guard against resource-consumption assaults, the operating system may be a better option. Make sure your resource requests don't get trapped and don't expire by being cautious.

- **Elevation of privilege:**
  - The Configuration Server may be able to execute code remotely on behalf of Engineering Workstations.

2.4 Threat List for Trust Domain 3:

- **Spoofing threats:**
  - Attackers can spoof Primary Historian to write data to the attacker's target instead of Primary Historian by spoofing the Destination Data Store Primary Historian. To find out where the data is stored, you might want to utilize a conventional authentication procedure.
  - An attacker can pose as the Primary Historian and supply the Supervisory workstation with bogus data. To verify the authenticity of the source data storage, consider using a well-known authentication mechanism.
  - The Primary Historian can be spoofed by an attacker, resulting in the PLC receiving erroneous data. To verify the authenticity of the source data storage, consider using a well-known authentication mechanism.
  - In the event of a PLC spoofing attack, the HMI will get incorrect data. It exploits the inherent security flaws of ICS network protocol, particularly the lack of message authentication, for this vulnerability. Network isolation should be considered in order to prevent the use of false control platforms A trust barrier should prevent this type of traffic from leaving an enclave.

- **Tampering threats:**
  - Risks associated to log files: Log readers can be hacked through logs. Think about canonicalizing your log data. To reduce the attack surface area, utilize a single log reader if at all possible. Check to make sure you understand and document information in log files that comes from unreliable or questionable sources.
  - It is possible for an attacker to modify the supervisory workstation's command and control. You could want to use security enclaves and make their operations more visible.
  - Windows CE and Windows XP operating systems may be subject to general system breach and may run compromised code, making HMI susceptible to manipulation of sensors and instruments. There is a possibility that these targets could be used to launch industrial malware.
  - It's possible for an attacker to alter the data sent by the PLC in order to get access to the system.
  - HMI safety can be jeopardized by a denial-of-service attack.

- **Repudiation:**
  - Updates Logs for Less Trusted Subjects
  - Unidentified Source Data Logs
  - Auditing is insufficient Is their sufficient data in the log to deduce what occurred in the past? Are your logs sufficiently detailed to allow for post-incident analysis? Is this type of capture sufficiently light that it may be

left on indefinitely? Are your data sufficient to defend against repudiation claims? Ascertain that you have logged adequate and relevant data to deal with a repudiation claim. You may wish to consult with both an audit and a privacy professional over your data selection.

- Potential Audit Data Is Not Protected Properly: Consider what happens if the audit mechanism is attacked, such as through an attempt to destroy the logs or through an attack on the log analysis tools. Ascertain that access to the log is controlled separately via a reference monitor. Indicate which filters, if any, readers, or writers can rely on.
- Disclosing Information
- Inadequate Data Protection for a Resource: Inadequate data protection for Primary Historian can let an attacker to read information that was not intended for dissemination. Re-evaluate your authorizations.

- **DDOS attack:**

  - When it comes to possible overconsumption of resources, does the Supervisory workstation or the Primary Historian take any special precautions? There are times when it makes sense to let the operating system manage resource-consumption attacks, which are notoriously tough to deal with. Make sure that your requests for resources do not get trapped or expire before they are completed.
  - Elevation of privileges:
  - For the Supervisory workstation, the Primary Historian may be able to remotely run code.
  - Industrial endpoint attributes documented as compromise for HMI Elevation: Industrial endpoint features can be exploited by an attacker to get access to an HMI. The target's security may be jeopardized if this file contains default passwords, known backdoors, or other system codes.
  - Supervisory workstation code may be executed remotely by the HMI.
  - An attacker can get access to a PLC by using known ways for escalating their privileges. Default credentials, well-known backdoors, and unique system codes can all be found in this file, putting the target's security at risk.

2.5 Threat Mitigation Plan(s)

In order to summarise the strategy of mitigating threats, security entities/components are first categorized, and then mitigation strategies are applied to each of the numerous trust domains in which they exist.

2.5.1 Network

ICS communication protocols such as Modbus and DNP3 are utilized; network protocols such as TCP/IP are used; and ICS sublayers such as the device layer, the monitoring and control layer, and the management layer are used in this case study. The following precautions should be taken:

- ICS communication traffic should be encrypted.

- TCP/lP communication should also be encrypted within VPN tunnels.

- Shielded twisted pair wires should be used in delicate settings.

- Security measures in place to prevent illegal entry.

In order to reduce the risk of insider attacks, employ role-based logical access control and personnel vetting.

- Avoid using disposable storage media that have a low level of integrity.

Give crucial network components a fail-over option.

Encryption and authentication of Wi-Fi traffic are a must.

Use port blocking on your network switch.

Use honeypots and honeynets in a demilitarized zone (DMZ) between the ICS and the corporate network.

2.5.2 Processes

It is important to note that all of these devices are examples of processes. As a precautionary measure, the following are some of the options:

- Background checks on employees can help avoid insider attacks.
- ICS should have an incident response mechanism installed.
- The establishment of a plan for disaster recovery and business continuity is a must.
- There needs to be an archivist in the DMZ and environmental controls put in place.
- There should be a regular schedule for applying software fixes.
- A wide range of defensive options
- Use of antimalware software

3.0 Legal and Ethical considerations(s)

Many countries have developed legislation to avoid catastrophic assaults on ICSs because of their vulnerability and importance as a national asset. When suggesting mitigating measures, it is certain that these regulations would be considered. Several regulations, such as the Passport to Good Security [6] and the National Information Assurance Directives [5]

4.0 Conclusions

This paper included an overview of vital national infrastructures and a security analysis. The case study used a converged IT and ICS infrastructure as its backdrop. The system was analysed using the Microsoft threat modelling tool and the STRIDE methodology. The highlighted threats and suggested mitigations were obtained from the case study's data flow diagram.

References

1. OCTAVE: Method Implementation Guide
2. Octotrike: Trike, available at: http://www.octotrike.org/
3. Ucedavélez, Tony & Morana, Marco. (2015). Intro to Pasta. 10.1002/9781118988374.ch6.
4. The STRIDE Threat Model. Microsoft. Microsoft.
5. CPNI: Passport to Good Security, accessed on 11/01/2022: https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport

6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, p. 1–30 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV) available at: http://data.europa.eu/eli/dir/2016/1148/oj