Segmenting a Network for Increased Reliability and Security

PH, PAUL HAUGHEY
BBA Engineering Ltd.
Canada

SUMMARY

We all have experienced browsing the internet at home when the connection speed has slowed to a crawl. This might be because your child has started a session of World of Warcraft or your spouse, or even the neighbor down the street, is streaming a movie. They have taken over all available bandwidth, leaving you waiting and wondering how long it will take to update your web page. Now imagine if this scenario were to happen on an industrial control system at a substation, a refinery or even a nuclear power plant. The results could be disastrous.

With the introduction of Ethernet to the plant floor, we should pay more attention to network design for industrial control systems. In the past, there were primarily vendor proprietary networks, so we did not commonly experience the same vulnerabilities and effects that multiple users or devices can have with Ethernet. It was not possible for someone to easily access Modbus Plus, Data Highway or a Field Bus network directly. With Ethernet implementation, we have seen companies combine operational control system network traffic with email and web browsing. I have even witnessed an open wireless connection to a programmable logic controller on-site without even a login or password. There is a trend for plant owners and operators to implement additional connectivity to field devices using ethernet. Bring your own device creates new challenges to networks and system administrators. Ethernet is more open than previous proprietary networks, which is great for interconnectivity and reduced cost, but can lead to real problems if not implemented and managed correctly.

There are numerous benefits to connected field devices with open architecture, such as the ability to monitor real time data, reduced equipment and cabling costs, access to machine data for advanced analytics, and troubleshooting. With the benefits of an interconnected plant come new operational risks and vulnerabilities. System owners need to pay more attention to the network design and security aspects. In the past, these networks were air gapped with limited access methods available for online attacks. All this has changed with ethernet at the plant industrial equipment. Automation and security professionals must ensure that all connected field devices are properly password protected, patched and meet regulatory requirements or minimum-security baselines. It only takes a single misconfigured device to have a weak link in the chain. This can put the company at risk for a remote attack or failure. An innocent mistake made by an employee could have a huge negative impact to the reliability of the system. Without effective segmentation of industrial control system networks, ransomware or other, cyber threats can easily access operational systems, enabling potential disruptions or damage to operational assets or human life.

Paul.Haughey@bba.ca

It is clear that cyber risk mitigation can directly impact the bottom line, not just in terms of potential business loss and penalties, but also in terms of future investment. Almost half (49%) of 600 global institutional investors identified cyberattacks as the number one risk expected to impact the investment landscape over the next five years. A further 75% will be raising data privacy and cybersecurity as the number one risk topic with executive boards in 2020 according to Edelman's annual Trust Barometer institutional investor special report.[1]

This paper is about a recent project that BBA completed to re-design a facility's electrical protection network from a flat network to a segmented network. The goal was to increase network reliability and security. The client was experiencing failures of network devices due to overwhelming broadcast messages flooding the network. This introduced potential safety concerns because the network was used to sending trip commands to open breakers located in remote substations. The increased load also restricted operations from monitoring the facility in real time. This paper will review the project requirements, design and process used to implement the changes.

KEYWORDS

Network, Segregation, Flat, Segmentation, Zoning

1. INTRODUCTION

Designing and deploying networks for industrial control system environments must be completed with due care and consideration of current equipment capabilities, vulnerabilities and future requirements. Due to potential operational consequences, there is no room for error should industrial networks fail. Designers and engineers face challenges with interoperability of legacy equipment, many of which were not originally designed for the network load demands and cyber threats encountered with modern facilities. The system integrator must work with limitations of equipment and budget constraints to provide a solution that is safe, robust and meets the requirements of the ever-changing threat landscape and evolving technology and business needs. Network segmentation cannot be accomplished in isolation without considering equipment connected to the network and applicable standards and regulatory requirements.

Technology is a key part of network segmentation but equally important are the challenges and constraints associated with restricting access to devices, reliable routing, and protecting the network from external adversaries while ensuring systems are available, fault tolerant and above all, safe.

2. WHAT IS A FLAT NETWORK?

A flat network is one where all stations can reach each other without going through intermediary hardware devices such as a bridge or router. A flat network is an approach to computer network design used to reduce cost, maintenance and administration. Flat networks are designed to use fewer switches on a computer network by connecting the devices to a single switch, instead of separate switches. Unlike a hierarchical network design, the flat network is not physically or virtually separated using different switches or VLANs. Flat networks were most commonly found in older facilities when demands for ethernet networks might be limited to a few Human Machine Interfaces (HMIs) or engineering workstations, with the process control and protection equipment running on proprietary networks. Topology of a flat network is not segmented or separated into different broadcast areas by using routers. Some such networks may use network hubs or a mixture of hubs and switches, rather than switches and routers, to connect devices to each other. Generally, all devices on the network are a part of the same broadcast area.

3. WHY FLAT NETWORKS CAN BE A PROBLEM?

There are increasingly new demands placed on industrial control networks today. In addition to traditional HMIs and programming workstations, it is now common to use ethernet networks to support the process control network, Supervisory control and data acquisition (SCADA), initiate equipment shutdowns, monitor machine health, support maintenance management systems, are used for distributed controller field I/O, real time trending, load shedding, intrusion detection systems, security information and event monitoring, and support of emerging Industry 4.0 technologies, such as Internet of Things, mobile technologies and Big Data to name a few.

These increased demands have led to concerns with flat networks: performance, reliability, operating, and maintenance for transmission and distribution facilities, including cybersecurity vulnerabilities that lead to operational risks. Other issues commonly encountered with flat networks include:

- Poor security – Because traffic travels through one LAN, it is not possible to prevent users from accessing certain parts of the network. It is easier for hackers to intercept data on the network.
- No redundancy – Since there is only one LAN, it is possible for the LAN to fail. Since there is no alternative path, the network will become inaccessible and computers may lose connectivity.
- Scalability and speed – One could be tempted to connect all the devices to one central switch, either directly or through hubs, which increases the potential for collisions (due to hubs), reduced data transmission speed and additional time for the central switch to process data. Flat networks also scale badly and increases the chance of network failure if excessive hubs are used and there are not enough switches to control data flow through the network.

4. WHAT IS AN ELECTRICAL PROTECTION NETWORK?

Electrical Protection networks consist of devices used in electric power systems to detect abnormal and intolerable conditions and initiate corrective actions. These devices are connected via an electrical protection network, commonly found in electrical facilities and substations and are used to:

- Help protect people against electrical hazards.
- Prevent equipment damage.
- Limit thermal, dielectric and mechanical stress on equipment.
- Maintain stability and service continuity in the power system.

If the electrical protection network fails to function as designed, faults could be introduced to the rest of the power grid causing instability. Flat networks are more susceptible to problems associated with overloaded network traffic than a segmented network. This can lead to:

- Unreliable operation.
- Missed alarms and trips.
- Clock synchronization out of sync.
- Introducing delays can create issues with breaker coordination affecting arc flash energy levels.

5. NETWORK SEGMENTATION

The solution to flat networks is network segmentation. Network segmentation involves splitting a computer network into subnetworks, each being a network segment. The advantages are primarily for boosting performance and improving security. This can be achieved by placing devices that commonly communicate with one another into the same zone or segment. There are several methods used to segment equipment, typically achieved with: firewalls, routers, switches, virtual local area network (VLANS), zones and electronic security parameter, mapping, and restricting data flows between devices.

Benefits of segmenting equipment:

- Enhanced performance: with fewer hosts per subnetwork, there is less signalling traffic and more bandwidth can be used for data communication.
- Improved security: with less signalling traffic going through all network segments, it is more difficult for an attacker to figure out the network structure; failures in one segment are less likely to propagate; and better access control can be established considering visitors' access or access to sensitive information/assets.
- Improved isolation: segmented networks allow companies to place more restrictive access controls for sensitive equipment such as safety instrumented systems or critical cyber systems.

5.1. DEFENCE IN DEPTH

Defense in depth is a critical strategy in having secure and resilient operational facilities. Most sites rely on a network infrastructure back bone. If this infrastructure is not designed properly, it is more difficult to expand on in a secure manner. Properly designed and configured firewalls and switches (often by using VLANs and network segmentation) can provide excellent defense strategies by creating the first line of defence in a layered approach to security. This makes it more difficult for unauthorized persons to gain access to systems, but also limits the potential lateral movements from occurring.

6. THE PROJECT

Our client had a network of 60 interconnected substations varying in voltage from 600 volts to 34.5 kV. The original electrical protection network (EPN) was designed as a flat network. As a result, they had experienced reliability issues when a single fault or cyber event on the network caused a partial or complete network failure. Broadcast messages overwhelmed the network due to the improper implementation of Generic object oriented substation event (GOOSE) messaging.

The client launched an initiative to strengthen the EPN architecture and design to mitigate current concerns with its performance and cybersecurity risks. The project involved segmenting the network into smaller logical sections, which would prevent network outages and focus network failure risks to smaller more distinct and controllable areas. The main objective was to fix the reliability issues.

7. IEC 61850 LAB AND PROOF OF CONCEPT TESTING

The first initiative was to use a test lab to reproduce the problem encountered on-site. This was accomplished with an IEC 61850 Smart Grid lab. It contained all of the client's equipment and supporting testing equipment to reproduce the problem. Once the problem was identified, the lab was used to perform a proof of concept test on the new design and equipment configuration prior to commencing detailed design.

The design team encountered a challenge with communications between devices. Goose messaging was a special challenge, it is a non-routable protocol. It uses VLAN and priority tagging as per IEEE 802.1Q to have separate virtual networks within the same physical network and sets the appropriate message priority level. We needed to find ways to reliably and consistently allow the messages to pass though the network. An undelivered GOOSE message could result in a missed trip command to a breaker or an alarm that did not make it to the operator console; this situation was unacceptable.

A proof of concept test was completed to confirm that key functionality, such as precision timing protocol, GOOSE message handling and clock synchronization performed as required within the network topology. These protocols were tested and verified inside every area/zone bounded by an internal segmented firewall. The proof of concept also sought to validate proper operation and communication between the new equipment and the existing switches.

This was an integral part of the project and reduced risk by verifying the preliminary design prior to spending hours on a detailed design solution.

8. DESIGN CRITERIA/SYSTEM DESIGN REQUIREMENTS

Several items were taken into consideration in the design phase and were part of the overall system requirements.

8.1. IEC 61850 STANDARD

IEC 61850 is an international standard defining communication protocols for intelligent electronic devices at electrical substations. This standard was a design requirement input for the project. The system architecture and design required supporting GOOSE high-speed protocol, with the large geographic location in mind. The main facility covered approximately four-square kilometers.

Other key network requirements included allowance of electrical protection relays to communicate with each other for high-speed system protection and coordination. This helped reduce arc flash energy levels by coordinating breaker trips. Another key network design requirement was to support operating status and control, alarms, trips, and metering information to the local automation controllers, HMIs and the main and backup control centres.

8.2. NORTH AMERICAN RELIABILITY CORPORATION (NERC)

The facility fell under NERC regulatory requirements, requiring adherence to Critical Infrastructure Protection (CIP) standards. Along with other requirements from the NERC standards, the following items were included in the design and the solutions were integrated: back-up/restore, password management, logical access, and malware protection. A Security and information event management (SIEM) solution was selected to monitor and correlate information and event log files from the various devices, such as relays, intelligent electronic devices, network equipment, and servers. A separate Proof of Concept test was completed to select a SIEM solution. These combined solutions helped improve the overall cybersecurity posture while meeting regulatory requirements. The design team included provisions to accommodate for future enhancements to the NERC standard and reused

existing processes and products/solutions, where possible. The information and events were integrated into the corporate SIEM solution.

8.3. SYSTEM ARCHITECTURE DESIGN REQUIREMENTS

The architecture of the electrical protection network segments took into consideration the need to define an electronic security perimeter (secure zone) addressed in the NERC CIP standards. Many industrial clients are familiar with the Purdue model identified in the ISA/IEC 62443 standard. There is no direct correlation between the ISA/IEC 62443 and NERC CIP standards when aligning the equipment locations. We worked with the client's technical team to integrate the NERC system architecture requirements into their design standard. It is recommended to keep only NERC CIP equipment grouped within the ESP. The reason for this is if other non-NERC equipment is located within the ESP, this equipment must follow all evidence gathering requirements. This creates additional regulatory activities.

The figures below show how the equipment was grouped to achieve the desired level of segmentation.

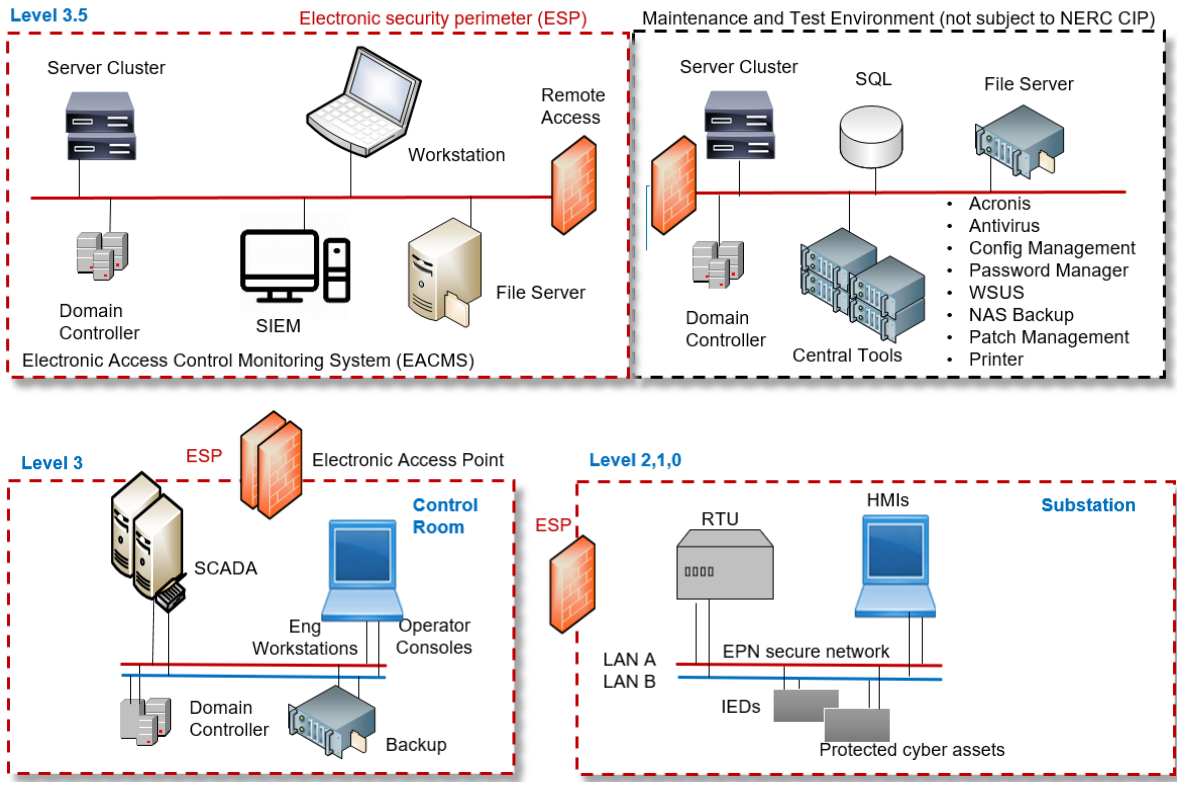

Figure 1: System Architecture

Design steps:

- Define an electronic security perimeter (secure zone) for each EPN segment.
- Define and enable access to each electronic security perimeter for each EPN secure network using an electronic access point (EAP).
- Deploy a firewall, which serves as the security device to establish the EAP for the site's EPN secure network.
- The EPN secure network contained all the essential cyber assets (HMIs, servers, Intelligent electronic device IEDs, network devices, etc.).

8.4. REQUIREMENTS FOR FIREWALLS

Firewalls played a very important role in segmenting the network. The following items listed are the requirements for the firewalls:

- The selected EPN firewalls were Precision Time Protocol (PTP) compatible. This allowed devices on the network to synchronize clocks.
- Firewalls required at minimum the features/capabilities to address/meet all applicable cybersecurity requirements for the NERC CIP v5 standards.
- The firewalls required the capabilities to perform routing to keep the GOOSE messages inside a contained location.
- A Proof of Concept was performed prior to beginning the migration process to determine the exact configuration to be deployed on the firewalls.

Network segmentation offered many advantages in performance and stability over the flat network. At the same time, new firewalls performed routing, which was critical for normal network operation. Dual firewalls were used to provide additional redundancy.

Internal segmented firewalls were installed in the substation electronic security perimeters (ESP) to segment LAN traffic inside the ESP. This also ensured that any problem or fault that occurred within the ESP would not affect any other location. The firewall was precision time protocol (PTP) compatible and it bridged through a switch to reach LAN A and LAN B. The switch supports redundancy protocols, parallel redundancy protocol (PRP) and high availability-seamless redundancy (HSR).

8.5. VLANS

Virtual LANs provide several advantages, such as ease of administration, confinement of broadcast domains, reduced broadcast traffic, and enforcement of security policies. VLANS and network switches were used for increased network separation, isolation and security. The project team identified and mapped all communications between the various applications and devices, and restricted communications to only those devices that needed to communicate. An increased visibility into the network traffic greatly improved the understanding of potential vectors for an attack.

8.6. ROUTING PROTOCOL

Configuring devices to consistently and reliably route messages was a challenge for this project. Open shortest path first (OSPF) routing protocol was used for the EPN segmented network. The main advantage of link state routing protocols, such as OSPF, is that they allow routers to calculate routes that satisfy quality of service requirements. This protocol was activated in all of the firewalls and created a mesh network between all firewalls. Thus, it enabled the Internal segmentation firewall (ISFWs) to determine the best route for each destination. Security rules were configured on each firewall to discard unauthorized traffic.

8.7. GPS CLOCK

A synchronized clock is essential in order to properly coordinate, analyze and track events and trips from the devices. This created challenges to ensure the clock synchronization made it to the destination. The following are requirements for implementing GPS clock capabilities and summarize the approach taken to meet performance objectives:

- The EPN network currently has five GPS clocks in different substations, connected via switches, to synchronize clock signals to end devices.
- Two of these clocks were moved to the new LAN D; this brought a clock to the new segmented network.
- The clock information (timestamp messages) was distributed over the entire LAN A and LAN B respectively; thus, all clock messages passed through the switches and ISFW/ESP firewalls to reach the ESP/Segments.
- The ISFW and switches were able to support the PTP protocol and distributed data synchronization across every substation.

We were forced to upgrade a master GPS clock as it could not support the requirements of the new system architecture.

8.8. SERVERS

Servers are a common target for adversaries and need to be protected. The two primary methods used to protect servers included:

- All servers needing access to or from the internet and the corporate network were installed in the electrical protection Demilitarized zone (DMZ) network.
- Operational Technology (OT) servers were physically connected to LAN D, but separated by VLANs, according to its application. All the inter-VLAN communications within these servers in LAN D automatically went through the OT bottom firewall, which served as the default gateway. All external communications went through the OT firewall for the routing and security process.

Numerous servers were deployed on virtual machines. Although standard for years in the Enterprise systems, virtualization can be new in some OT/ICS environments. Some benefits achieved:

- Drastically reduced hardware costs with fewer physical servers.
- Faster server provisioning, new servers can be spun up using a template in a matter of minutes.
- Improved disaster recovery ability, VMs can be backed-up and restored much easier than physical servers.
- Ability to dynamically adjust resources in real time. If a server needs more RAM or more CPU cores, it is a quick adjustment.

9. ON-SITE IMPLEMENTATION

The project required additional planning and careful consideration because the network changes were carried out on an active network and operating facility with limited planned outages. Unplanned system outages could cause disruptions to operations and would be very costly. This meant that detailed commissioning, deployment and contingency plans were developed to ensure a well defined and organized implementation, this included back-out planning sessions with the client. The team worked closely with site operations, maintenance and planning groups to ensure that all stakeholders' needs were considered, and risks identified.

10. CONCLUSION

There are several key items and takeaways that should be considered when improving flat network designs or when undertaking similar projects. This paper has covered a few of the design considerations and best practices that will help improve overall system reliability and cybersecurity posture. In summary:

- Segmented networks are less prone to system-wide failures than flat networks.
- Firewalls, switches and VLANS are used to isolate faults and protect against cyber-attacks.
- Use the IEC 61850 standard for smart grid designs.
- Include NERC CIP requirements early into the design phase, if required.
- Thoroughly test equipment and inter-connectivity in a lab environment prior to field rollout.

BIBLIOGRAPHY

[1] Edelman's annual Trust Barometer institutional investor special report. https://www.edelman.com/sites/g/files/aatuss191/files/2019-12/2019 Edelman Trust Barometer Special Report – Investor Trust.pdf

[2] Reference: Wikipedia https://en.wikipedia.org/wiki/Flat_network

[3] Reference: Electrical Engineering Guides - Electrical network protection guide https://electrical-engineering-portal.com/download-center/books-and-guides/electrical-engineering/electrical-network-protection-guide