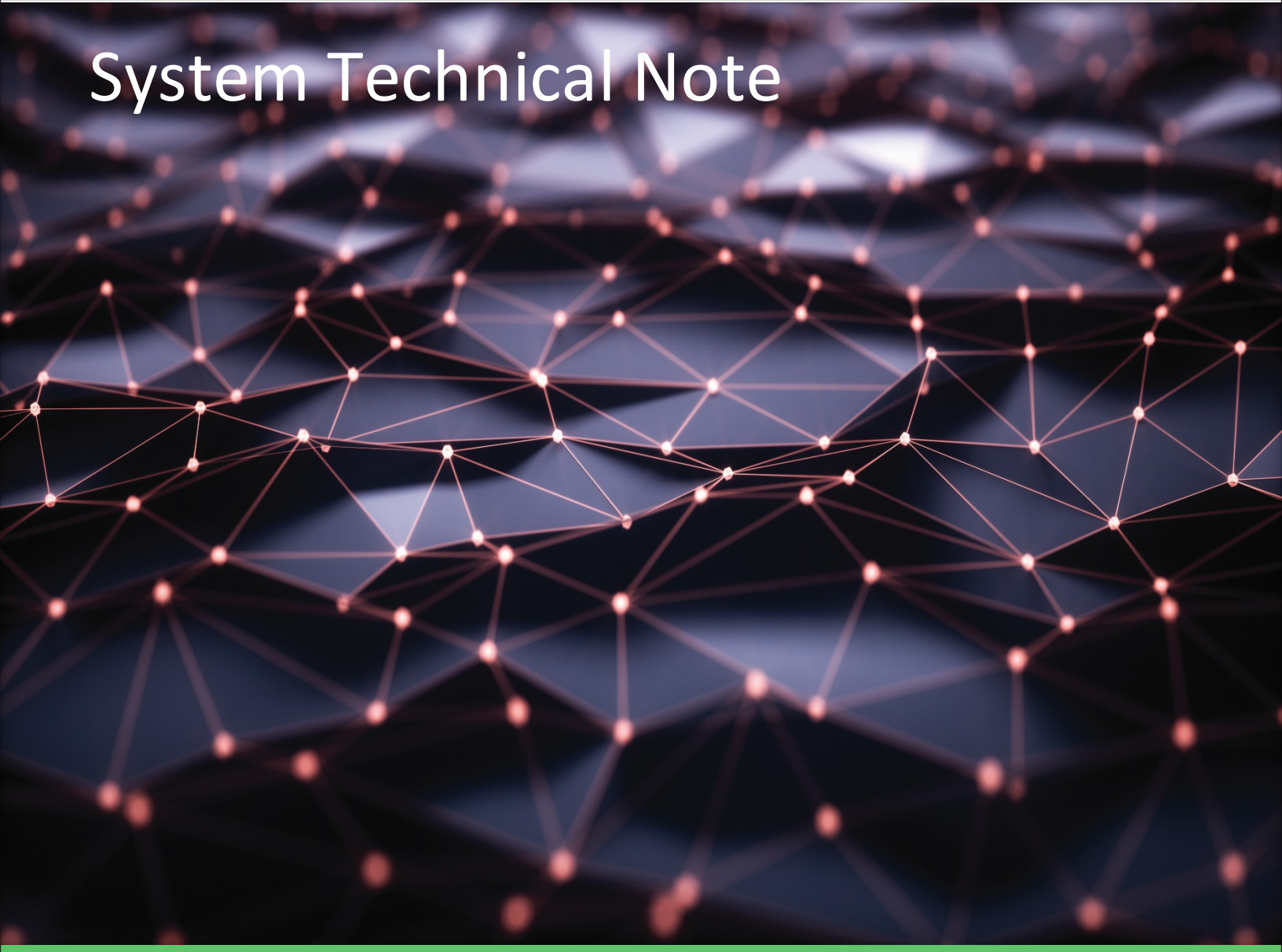
System Technical Note



How can I...

Reduce Vulnerability to Cyber Attacks v3.0

Cybersecurity

Develop your project

schneider-electric.com

Life Is On Schneider Electric

Important information

People responsible for the application, implementation and use of this document must make sure that all necessary design considerations have been taken into account and that all laws, safety and performance requirements, regulations, codes, and applicable standards have been obeyed to their full extent.

Schneider Electric provides the resources specified in this document. These resources can be used to minimize engineering efforts, but the use, integration, configuration, and validation of the system is the user's sole responsibility. Said user must ensure the safety of the system as a whole, including the resources provided by Schneider Electric through procedures that the user deems appropriate.

Notice

This document is not comprehensive for any systems using the given architecture and does not absolve users of their duty to uphold the safety requirements for the equipment used in their systems, or compliance with both national or international safety laws and regulations.

Readers are considered to already know how to use the products described in this document.

This document does not replace any specific product documentation.

The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING
WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury. **Failure to follow these instructions can cause death, serious injury or equipment damage.**

⚠ CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury. **Failure to follow these instructions can result in injury or equipment damage.**

NOTICE
NOTICE is used to address practices not related to physical injury. **Failure to follow these instructions can result in equipment damage.**

Note: Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, operation and installation of electrical equipment, and has received safety training to recognize and avoid the hazards involved.

Before you begin

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions and government regulations etc. In some applications more than one processor may be required when backup redundancy is needed.

Only the user can be aware of all the conditions and factors present during setup, operation and maintenance of the solution. Therefore, only the user can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, the user should refer to

the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual also provides much useful information.

Ensure that appropriate safeties and mechanical/electrical interlocks protection have been installed and are operational before placing the equipment into service. All mechanical/electrical interlocks and safeties protection must be coordinated with the related automation equipment and software programming.

Note: Coordination of safeties and mechanical/electrical interlocks protection is outside the scope of this document.

START UP AND TEST

Following installation but before using electrical control and automation equipment for regular operation, the system should be given a start up test by qualified personnel to verify the correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

⚠ WARNING

EQUIPMENT OPERATION HAZARD

- Follow all start up tests as recommended in the equipment documentation.
- Store all equipment documentation for future reference.
- Software testing must be done in both simulated and real environments.

Failure to follow these instructions can cause death, serious injury or equipment damage.

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the USA, for example). If high-potential voltage testing is necessary, follow recommendations in the equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

Remove tools, meters, and debris from equipment

Close the equipment enclosure door

Remove ground from incoming power lines

Perform all start-up tests recommended by the manufacturer

Operation and adjustments

The following precautions are from NEMA Standards Publication ICS 7.1-1995 (English version prevails):

Regardless of the care exercised in the design and manufacture of equipment or in the selection and rating of components; there are hazards that can be encountered if such equipment is improperly operated.

It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.

Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

⚠ WARNING

UNEXPECTED EQUIPMENT OPERATION

- Only use software tools approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can cause death, serious injury or equipment damage.

Intention

This document is intended to provide a quick introduction to the described system. It is not intended to replace any specific product documentation, nor any of your own design documentation. On the contrary, it offers information additional to the product documentation on installation, configuration and implementing the system.

The architecture described in this document is not a specific product in the normal commercial sense. It describes an example of how Schneider Electric and third-party components may be integrated to fulfill an industrial application.

A detailed functional description or the specifications for a specific user application is not part of this document. Nevertheless, the document outlines some typical applications where the system might be implemented.

The architecture described in this document has been fully tested in our laboratories using all the specific references you will find in the component list near the end of this document. Of course,

your specific application requirements may be different and will require additional and/or different components. In this case, you will have to adapt the information provided in this document to your particular needs. To do so, you will need to consult the specific product documentation of the components that you are substituting in this architecture. Pay particular attention in conforming to any safety information, different electrical requirements and normative standards that would apply to your adaptation.

It should be noted that there are some major components in the architecture described in this document that cannot be substituted without completely invalidating the architecture, descriptions, instructions, wiring diagrams and compatibility between the various software and hardware components specified herein. You must be aware of the consequences of component substitution in the architecture described in this document as substitutions may impair the compatibility and interoperability of software and hardware.

⚠ CAUTION
EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT Read and thoroughly understand all hardware and software documentation before attempting any component substitutions. **Failure to follow these instructions can result in injury or equipment damage.**

This document is intended to describe cybersecurity risks and abatement strategies in control and automation.

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, BURN OR EXPLOSION

- Only qualified personnel familiar with low and medium voltage equipment are to perform work described in this set of instructions. Workers must understand the hazards involved in working with or near low and medium voltage circuits.
- Perform such work only after reading and understanding all of the instructions contained in this bulletin.
- Turn off all power before working on or inside equipment.
- Use a properly rated voltage sensing device to confirm that the power is off.
- Before performing visual inspections, tests, or maintenance on the equipment, disconnect all sources of electric power. Assume that all circuits are live until they have been completely de-energized, tested, grounded, and tagged. Pay particular attention to the design of the power system. Consider all sources of power, including the possibility of back feeding.
- Handle this equipment carefully and install, operate, and maintain it correctly in order for it to function properly. Neglecting fundamental installation and maintenance requirements may lead to personal injury, as well as damage to electrical equipment or other property.
- Beware of potential hazards, wear personal protective equipment and take adequate safety precautions.
- Do not make any modifications to the equipment or operate the system with the interlocks removed. Contact your local field sales representative for additional instruction if the equipment does not function as described in this manual.
- Carefully inspect your work area and remove any tools and objects left inside the equipment.
- Replace all devices, doors and covers before turning on power to this equipment.
- All instructions in this manual are written with the assumption that the customer has taken these measures before performing maintenance or testing.

Failure to follow these instructions will result in death or serious injury.

The STN collection

The implementation of an automation project includes five main phases: Selection, Design, Configuration, Implementation and Operation. To help you develop a project based on these phases, Schneider Electric has created the Tested, Validated, Documented Architecture and System Technical Note.

A Tested, Validated, Documented Architecture (TVDA) provides technical guidelines and recommendations for implementing technologies to address your needs and requirements, This guide covers the entire scope of the project life cycle, from the Selection to the Operation phase, providing design methodologies and source code examples for all system components.

A System Technical Note (STN) provides a more theoretical approach by focusing on a particular system technology. These notes describe complete solution offers for a system, and therefore support you in the Selection phase of a project. The TVDAs and STNs are related and complementary. In short, you will find technology fundamentals in an STN and their corresponding applications in one or several TVDAs.

Development environment

Each TVDA or STN has been developed in one of our solution platform labs using a typical EcoStruxure Plant architecture.

EcoStruxure Plant, the process automation system from Schneider Electric, is a collaborative architecture that allows industrial and infrastructure companies to meet their automation needs while at the same time addressing their growing energy efficiency requirements. In a single environment, measured energy and process data can be analyzed to yield a holistically optimized plant.

Table of contents

1. Introduction[1]

1.1. Purpose

This STN will help the reader understand what constitutes cybersecurity in the industrial market. Readers will become more familiar with the methods of malicious network penetration, the risks caused by system vulnerabilities, and Schneider Electric's recommendations to mitigate those risks. It provides a common, readily understandable reference point for end users, system integrators, OEMs, sales people, business support, and other parties.

1.2. What is Cybersecurity?

Cybersecurity is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions. The objective of cybersecurity is to provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users. Cybersecurity is an ongoing process that encompasses procedures, policies, software, and hardware.

1.3. Why is Security Important in Industrial Controls Today?

Cybersecurity is no longer a secondary requirement in the industrial controls world. It is as important as safety or high availability.

Industrial control systems based on computer technology and industrial-grade networks have been in use for decades. Earlier control system architectures were developed with proprietary technology and were isolated from the outside world. In many cases, physical perimeter security was deemed adequate and cybersecurity was not a primary concern.

Today many control systems use open or standardized technologies such as Microsoft Windows operating systems and Ethernet TCP/IP to reduce costs and improve performance. Many

[1] Some of the content in this section is based on or clarifies content available on the US-CERT Industrial Control Systems Emergency Response Team Web page located at https://ics-cert.us-cert.gov/ Electric recommends reviewing all the materials at this Web site to gain a better understanding of control system vulnerabilities and potential threats. This link is provided for informational purposes only and does not represent an endorsement by or affiliation with the US-CERT (DHS).

systems also employ direct communications between control and business systems to improve operational efficiency and manage production assets more cost-effectively.

This technical evolution exposes control systems to vulnerabilities previously thought to affect only office and business computers. Control systems are now vulnerable to cyberattacks from both inside and outside of the industrial control system network.

Security challenges for the control environment include:

- Diverse physical and logical boundaries.
- Multiple sites and large geographic spans.
- Adverse effects of security implementation on process availability.
- Increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open.
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and from the enterprise network.
- Direct impact of control systems on physical and mechanical systems.

No longer are fences and security guards adequate to protect industrial assets. Companies must be diligent in the steps they take to help secure their systems. A successful cyberattack can result in lost production, damaged company image, environmental disaster, or loss of life. The controls industry and its customers must apply cybersecurity lessons learned from the IT world.

1.4. Cyber Threat Profile

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated from within the physical facility or from an external location. Experts estimate that nearly half of all cyber incidences occur from within the enterprise. With the proliferation of email phishing schemes and ransomware attacks. This number is likely to rise.

A cybersecurity plan needs to account for various potential sources of cyberattacks and accidents, including:

- Internal:
  - Inappropriate employee or contractor behavior
  - Disgruntled employees or contractor
  - Opening an email or attachment from an unknown or spoofed sender
  - Inadvertently launching a virus by downloading a file or font
- External opportunistic (non-directed):
  - Script kiddies (slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding how the script works or its potential impact on a system)

  - Recreational hackers
  - Virus writers
- External deliberate (directed):
  - Criminal groups
  - Activists
  - Terrorists
  - Agencies of foreign states
- Accidents

A deliberate cyberattack on a control system may be launched to achieve a variety of malicious results, including:

- Disrupt the production process by blocking or delaying the flow of information.
- Damage, disable, or shut down equipment to negatively impact production or the environment.
- Modify or disable safety systems to cause intentional harm.

1.5. How Attackers Can Gain Access to the Control Network

A cyber attacker must bypass the perimeter defenses to gain access to the control system network. The most common points of access include:

- Poorly configured firewalls
- IT controlled network products
- Phishing control network employees
- Database links
- Supplier access points (such as technical support access points)
- Dial-up access to RTU devices
- Corporate virtual private network (VPN)
- Peer utilities

1.5.1. Dial-up Access to RTU Devices

Many control systems include a modem, like the one shown in Figure 1, for backup use if the main network becomes unavailable. An attacker must know the protocol of the remote terminal unit (RTU) to gain access via dial-up. Most RTUs do not employ strong authentication or other security mechanisms.

Many modems accept and respond to any caller. This allows an attacker to gain access to the control network, the field network and possibly the enterprise network. Take care when connecting a modem to this environment. One interesting technology is telephony authentication. With this technology, hardware keys reside on the public switched telephone network (PSTN)

side of the modem, not between the modem and serial device as is typically done with inline encryption/authentication devices known in the industry as "bump-in-the-wire." When two phones attempt to connect, the master key validates the slave key before a PSTN connection is allowed. Because authentication is performed on the PSTN side, it should block modem discovery during a war-dialing exercise[2]. The US Department of Homeland Security has published a document, Recommended Practice for Securing Control System Modems, to provide guidance when using a modem in a control system.

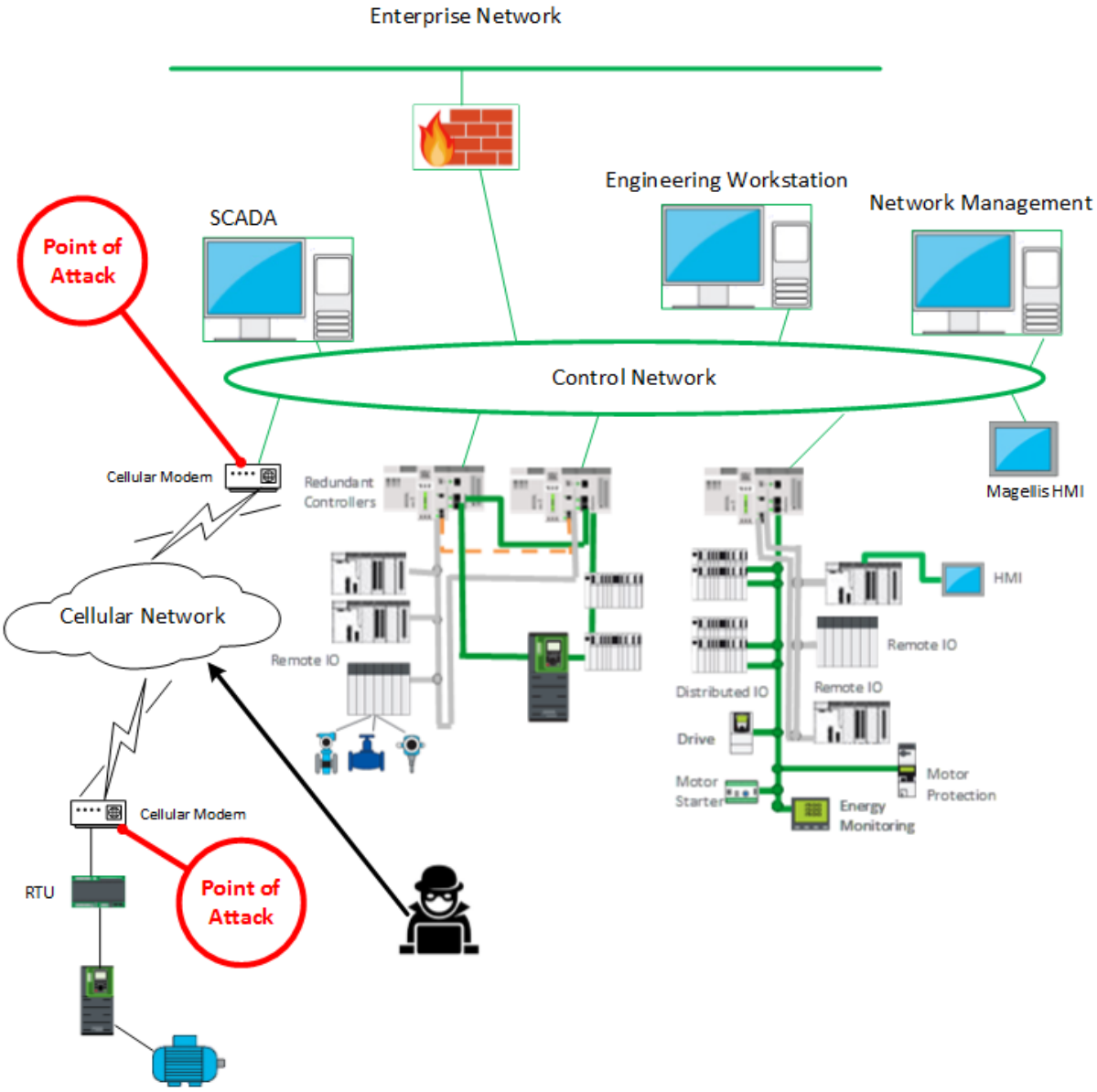


Figure 1: RTU Dial-Up Modem Backup Connection

[2] https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_SecuringModems_S508C.pdf

1.5.2. Supplier Access

To reduce down-time and costs, organizations often grant access to suppliers for remote diagnostics or maintenance through dial-up, as shown in Figure 2, or through a VPN. These suppliers sometimes leave ports open on the equipment to simplify their tasks, giving the attacker access to the equipment and links to control system networks. This scenario is similar to the RTU dial-up modem case mentioned earlier (see page 17), with the same impacts and mitigation recommendations.

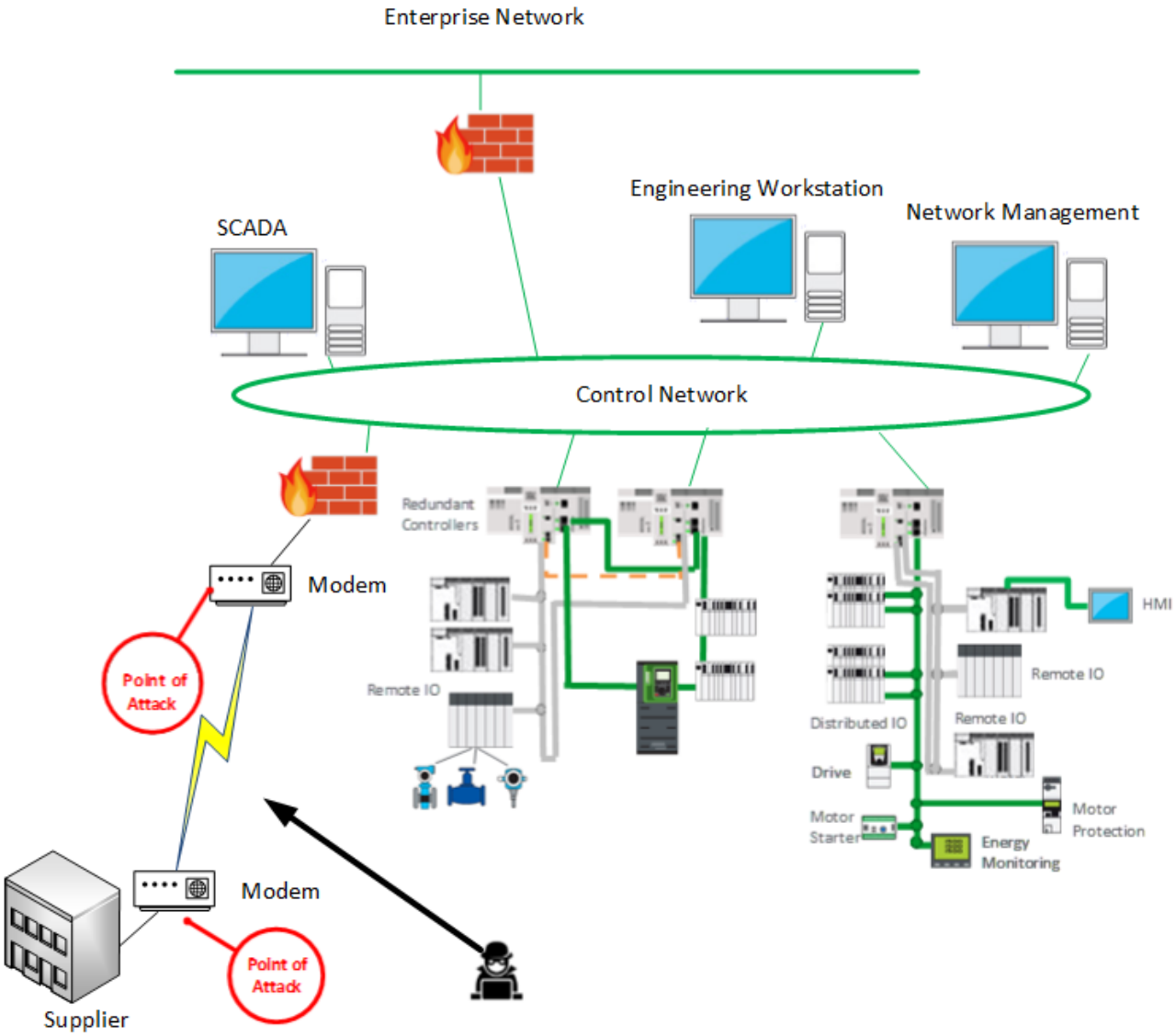


Figure 2: Vendor Access Vulnerabilities

1.5.3. IT Controlled Communication Equipment

The automation department's network authority is often limited to the control network within the facility. The IT department assumes responsibility for the organization's long-distance communication. As shown in Figure 3, a skilled attacker can access the control network through the communication architecture and reconfigure or compromise communications to the field control devices. In this scenario, the hacker has breached the firewall and now has gained access to the control and field networks. It is recommended that you monitor log files from the firewall on a regular basis to identify unusual events or unauthorized devices attempting to access the control or field networks. Test and verify that firewall rules are functioning properly.

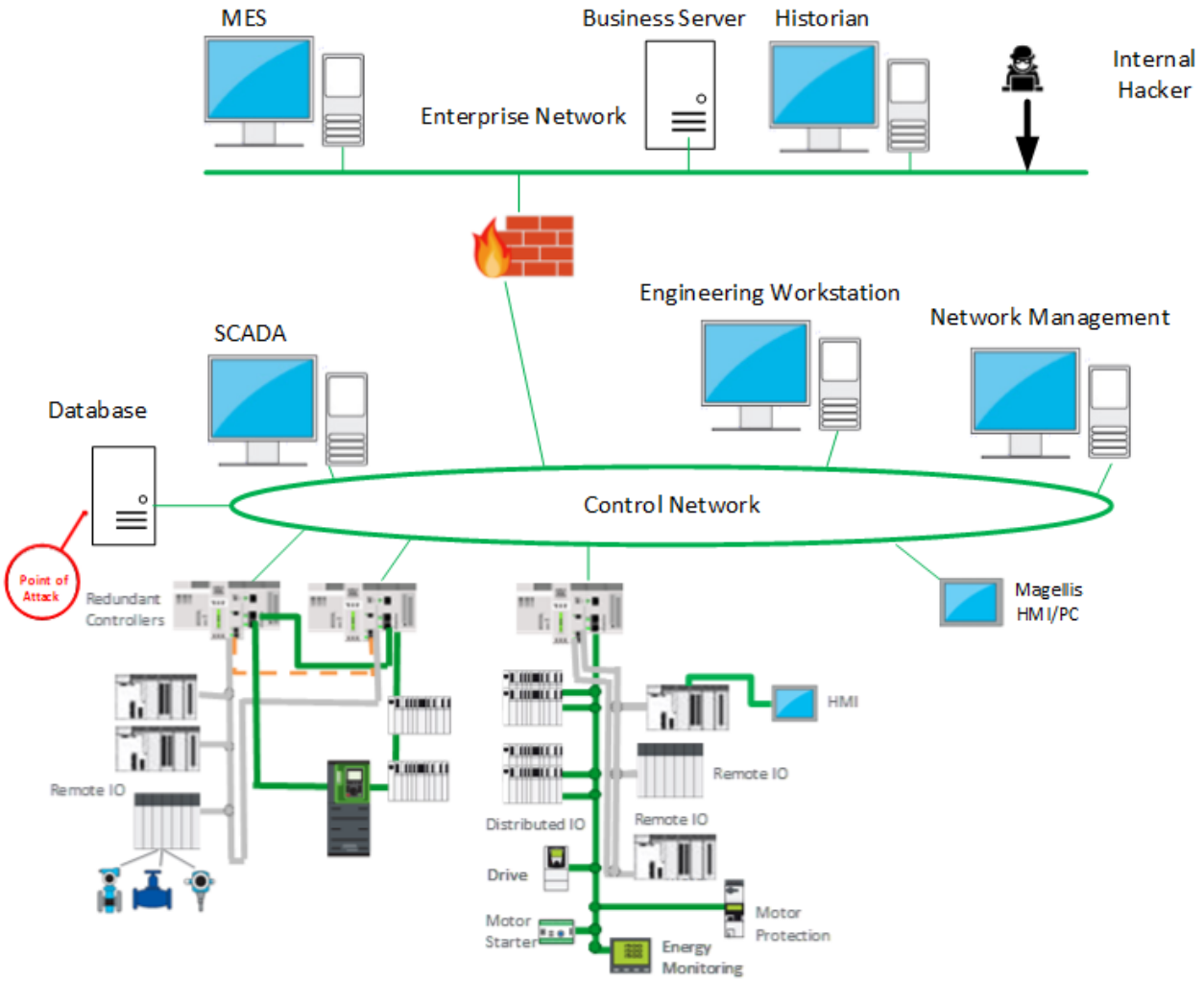


Figure 3: IT Controlled Equipment

1.5.4. Corporate VPNs

Engineers working in the corporate offices often use VPN connections to gain access to the control network, as shown in Figure 4.

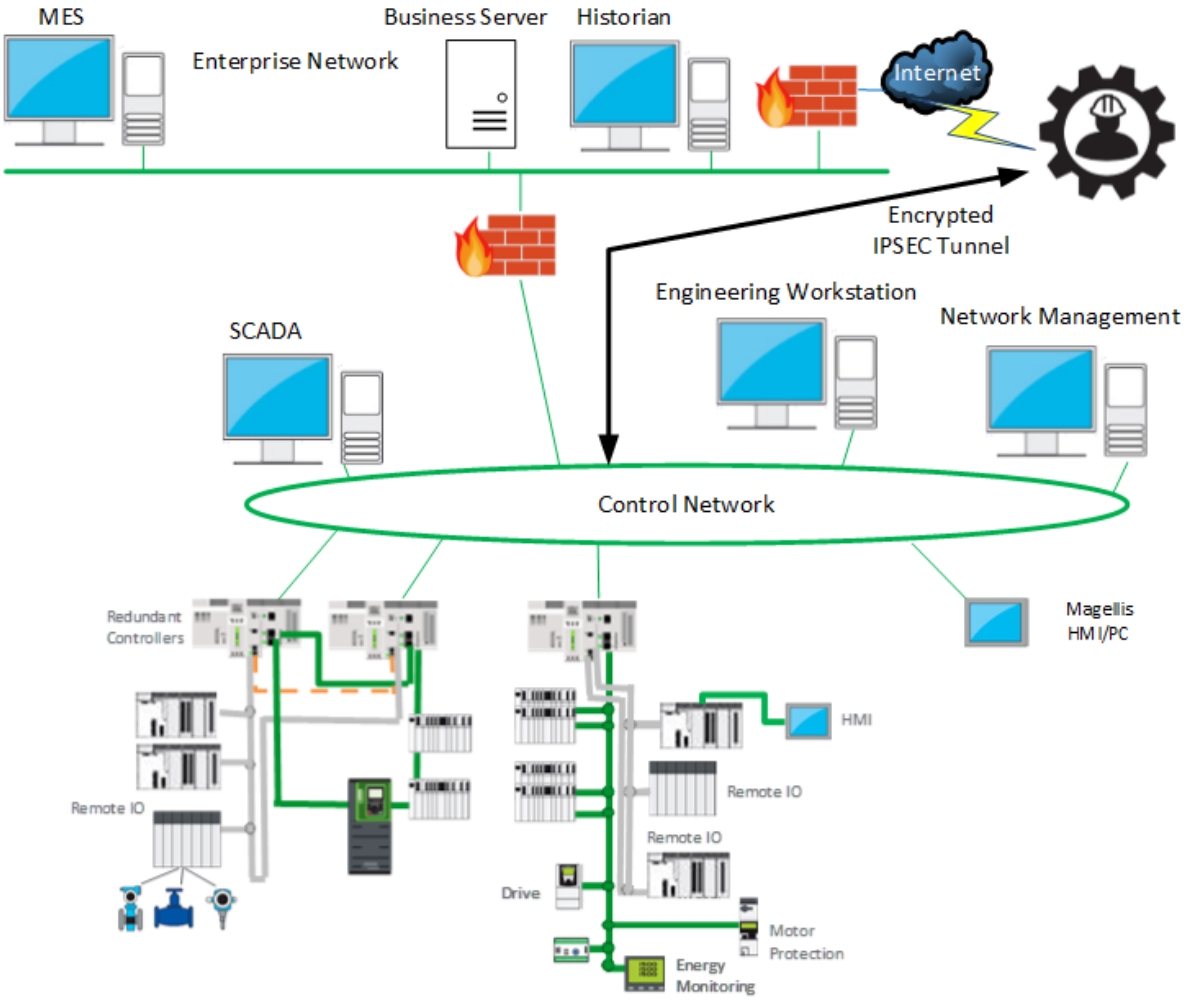


Figure 4: Corporate VPN Connections

An attacker can compromise the VPN server, wait for a legitimate user to establish a VPN connection into the control system network, and piggyback on the legitimate connection. Once successful the hacker has unlimited access to the network. It is recommended that you monitor log files from the VPN server on a regular basis for any abnormality. Grant VPN access only to personnel who need this access to provide service and support to the control and field network.

1.5.5. Database Links

Most control systems use real-time databases, configuration databases, and multiple historian databases. If the firewall or the security on the database is not configured properly, a skilled attacker can gain access to the database from the business network, as shown in Figure 5, and generate SQL commands to take control of the database server on the control system network.

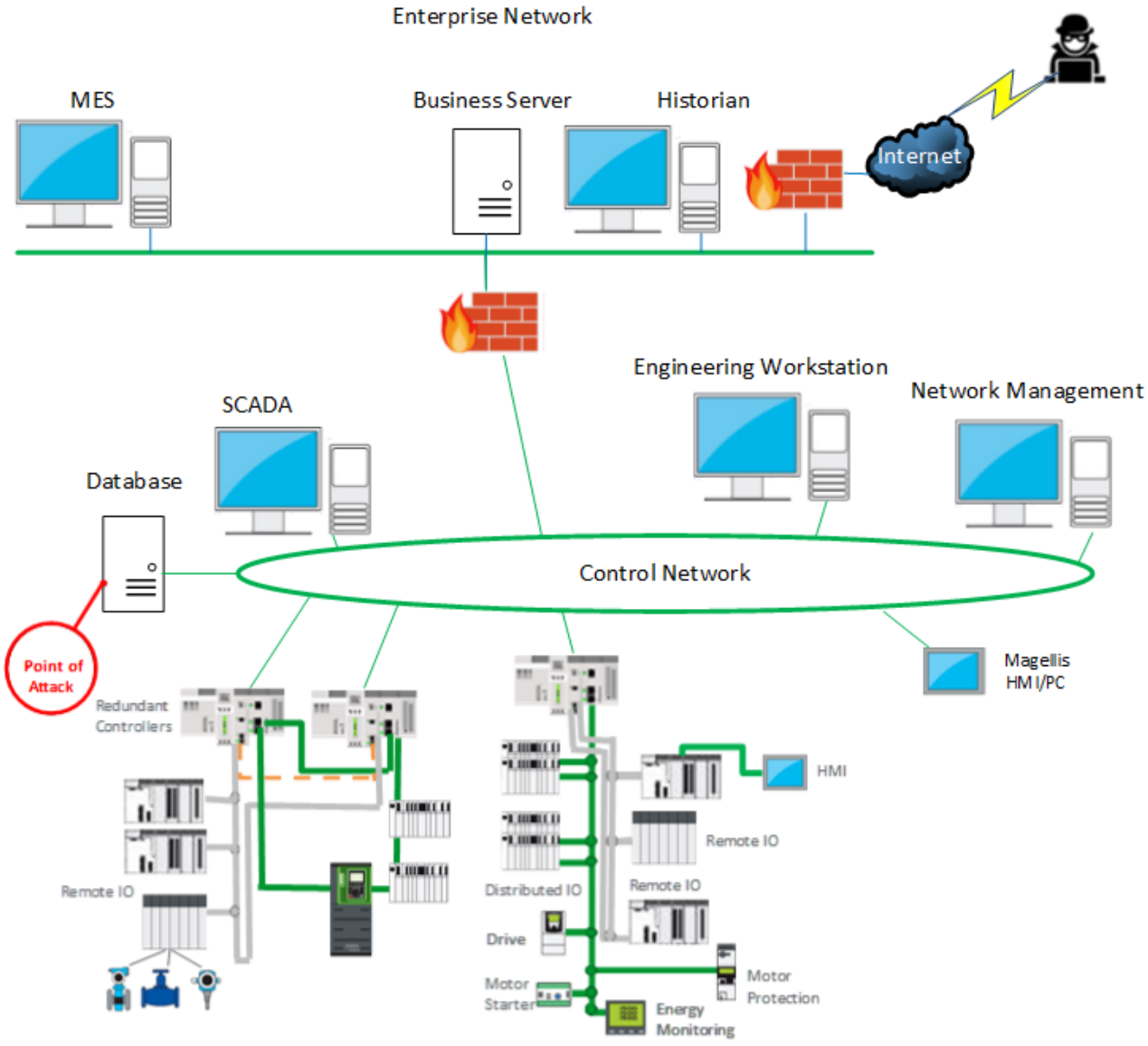


Figure 5: Database Links

1.5.6. Peer Utility Links

Partners and peers are sometimes granted access to information located on either the business or control network, as shown in Figure 6. With the peer-to-peer link, the security of the system is only as strong as the security of the weakest member. A network breach from one of these sites can provide access to the control and field network. It is recommended that you closely monitor and manage firewall connections between these sites. If these connections are through the Internet, employ and monitor a secure VPN connection.

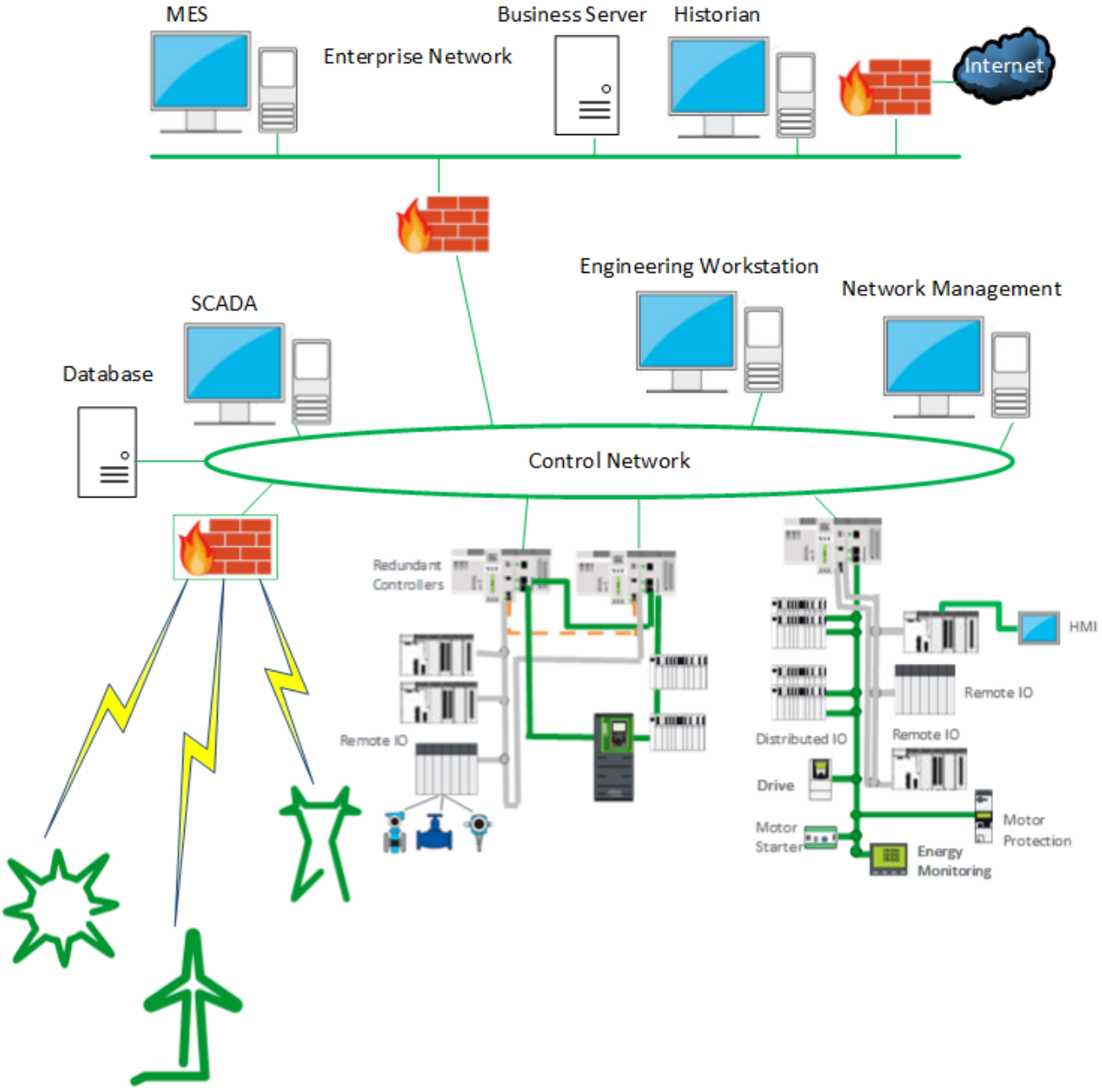


Figure 6: Peer Utility Links

1.5.7. How Attackers Attack

Depending on motives and skills, the attacker may or may not need to know details of the control process to disrupt operations. For example, if the motive is simply to shut down the process, very little knowledge is needed. However, if the attacker wants to attack a specific machine or process, he or she needs to understand how the application program is written.

Highly vulnerable processes include:

- **Data acquisition databases**. Names of databases vary from supplier to supplier but most use a common naming convention with a unique number such as pump1, pump2, breaker1, breaker2, and so on. On the communications protocol level, the devices are simply referred to by number (memory location or register address). For a precise attack, the attacker needs to translate the numbers into meaningful information.
- **HMI or SCADA display screens**. Gaining access to the HMI screens is one method for understanding the process and the interaction between the operator and the equipment. The information on the screen allows the attacker to translate the reference numbers into something meaningful.
- **PC systems**. PCs can be infected with viruses and worms that attach to and corrupt software and data.

1.5.8. Control of the Process

Once an attacker has enough information about the process, the next step is to manipulate it. One way to gain control of the process is to connect to a data acquisition device, such as a programmable automation controller (PAC) that has access to field devices and send it properly formatted commands. Many PACs, gateways, and data acquisition servers use weak authentication or no authentication and will accept any commands that have been formatted correctly.

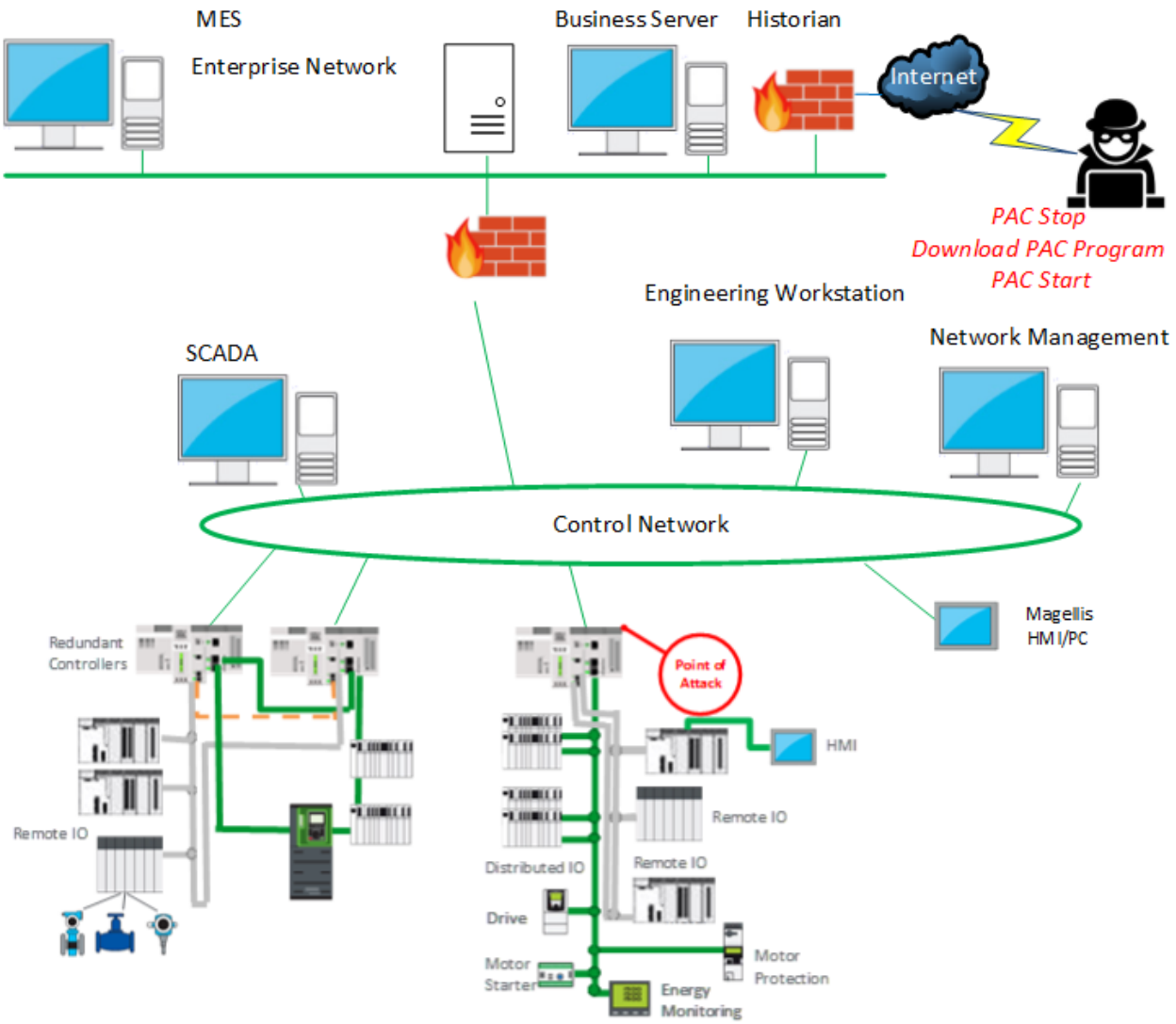


Figure 7: Attacker Commands

1.5.9. Exporting the HMI Screen

Another method of attack is to export the HMI screen to gain control of the operations. If the attacker succeeds, the operator's HMI screen can be viewed and controlled on the attacker's screen. A sophisticated attacker may also modify the operator's screen to display normal operations in order to disguise the attack. This could cause a plant shutdown or equipment malfunction. An example of this is the Stuxnet virus that destroyed centrifuges separating nuclear material for Iran's nuclear program in 2005. To help defend against this form of attack, constantly monitor system access, and use authentication to grant access or download configuration changes to a device.

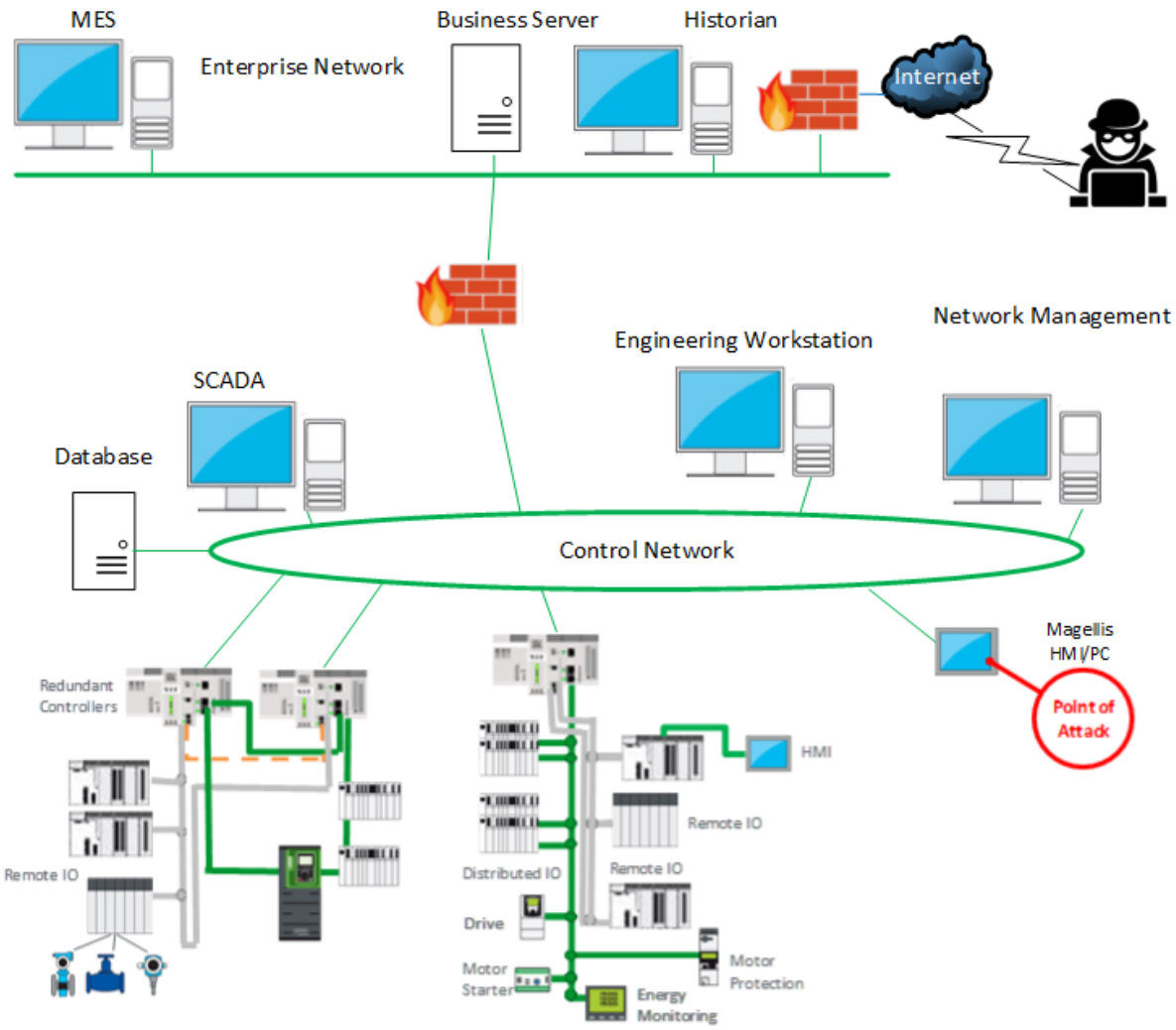


Figure 8: HMI Vulnerabilities

1.5.10. Changing the Database

A successful attacker can access the database and modify the data to disrupt normal operation of the control system or change stored values to affect the system's integrity. This can cause plant operators to make costly decision errors, based on the modified data in the database. Again, persistent log file examination can help mitigate this vulnerability.

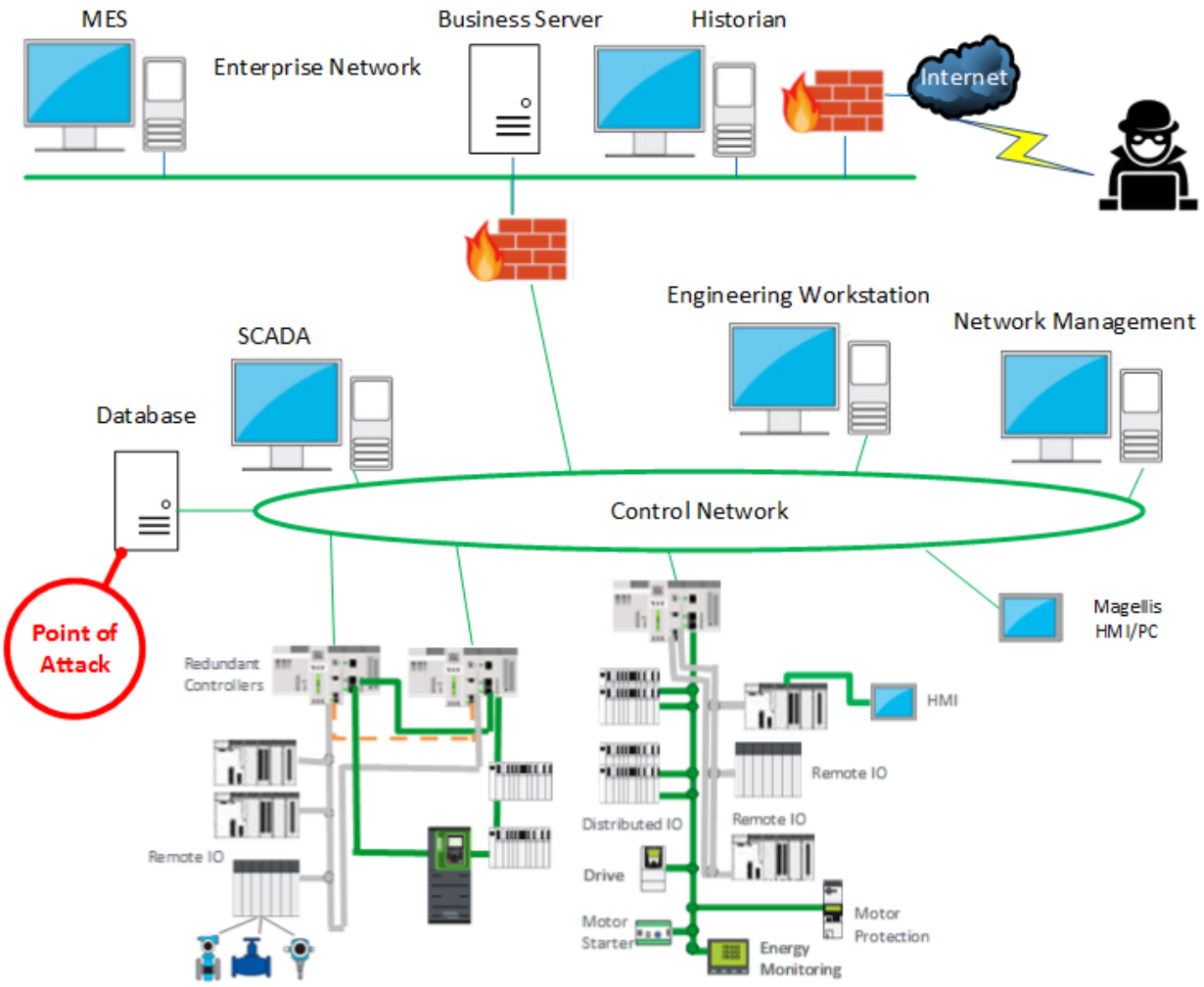


Figure 9: Database Change Attacks

1.5.11. Man-in-the-Middle Attacks

Man-in-the-middle is a type of attack where the attacker intercepts messages from one computer (Host A), manipulates the data, and then forwards it to the intended computer (Host B), as shown in Figure 10. Both computers appear to be communicating with each other and neither system detects the presence of an intruder in the middle. The intruder then can modify data, which can cause many problems at the site.

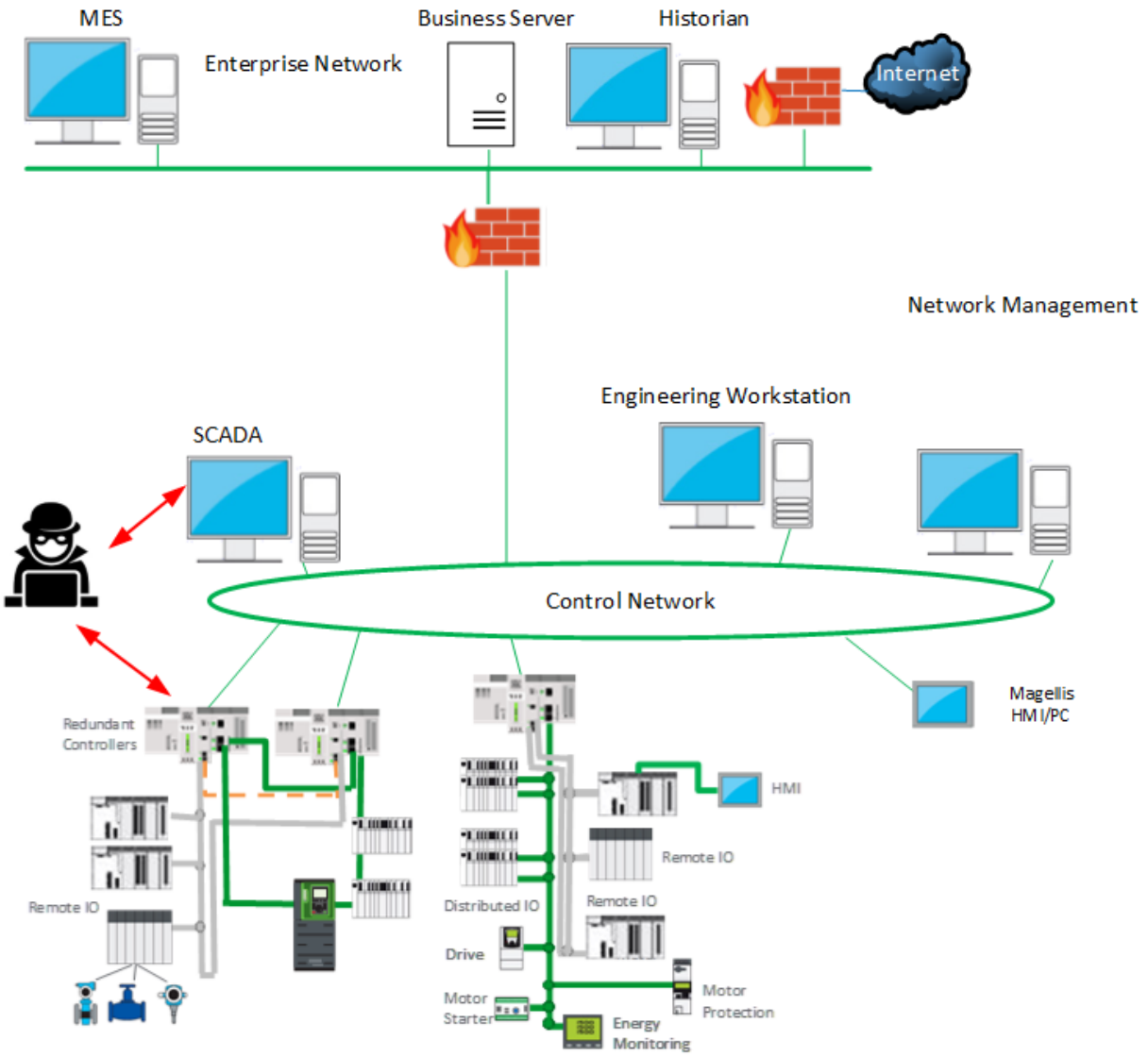


Figure 10: Man-in-the-Middle Attacks

A man-in-the-middle attack can even allow the attacker to spoof the operator HMI screens (that is, display a fake HMI screen) and take control of the control system, as shown in Figure 11. For the attack to succeed, the attacker needs to know the protocol of the targeted exchange. Again, careful examination of logs and system behavior can help detect an attack.

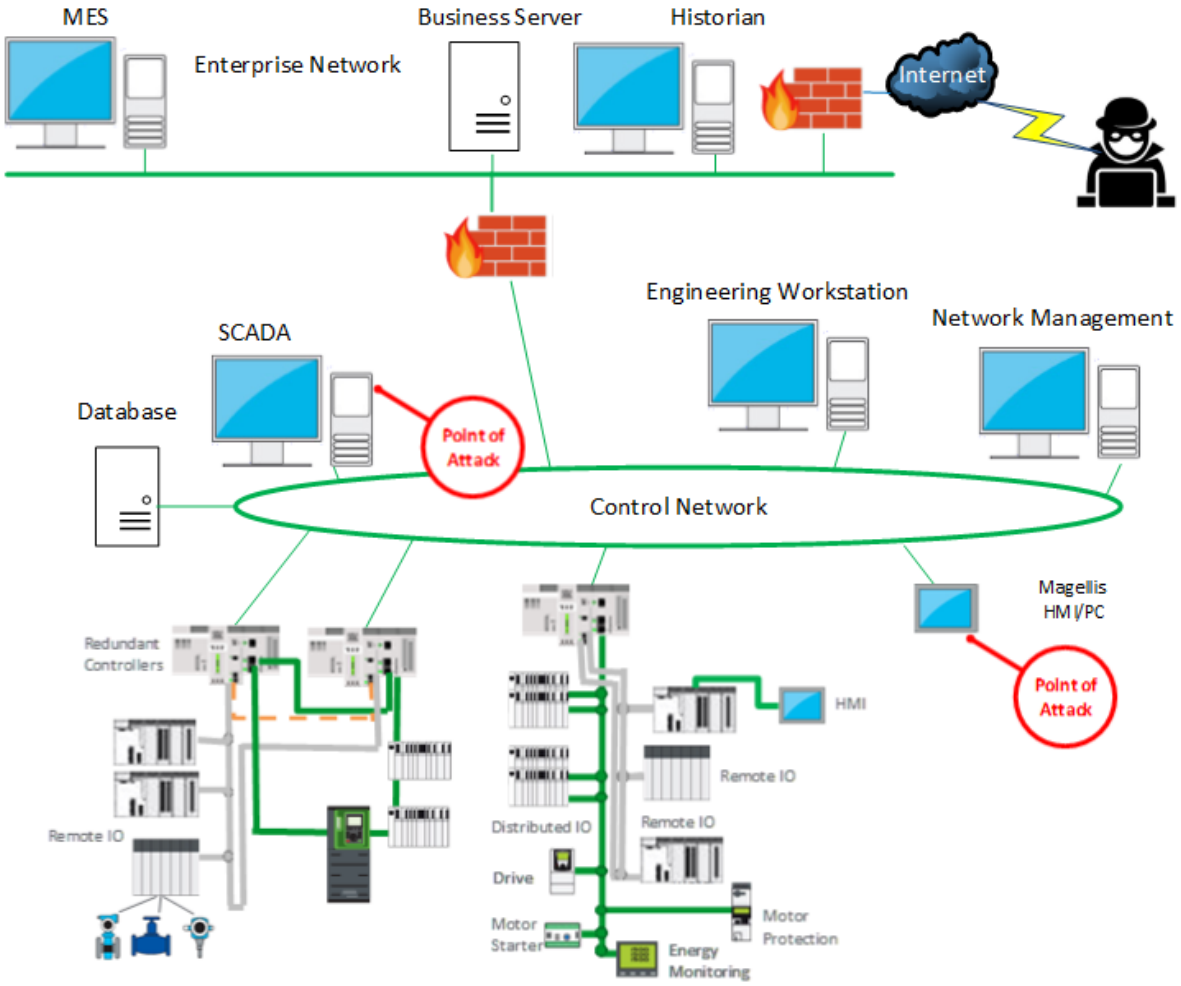


Figure 11: Attacker Spoofs HMI Operator Screens

1.5.12. Denial of Service

Denial of service (DoS) attacks attempt to block legitimate access to network or device services. One common type of DoS attack floods a device with requests so that its response times are slowed to the point where the system is unusable. Another type of DoS attack floods the network with traffic such as TCP SYN, affecting network response times to the point where legitimate use is severely impacted.

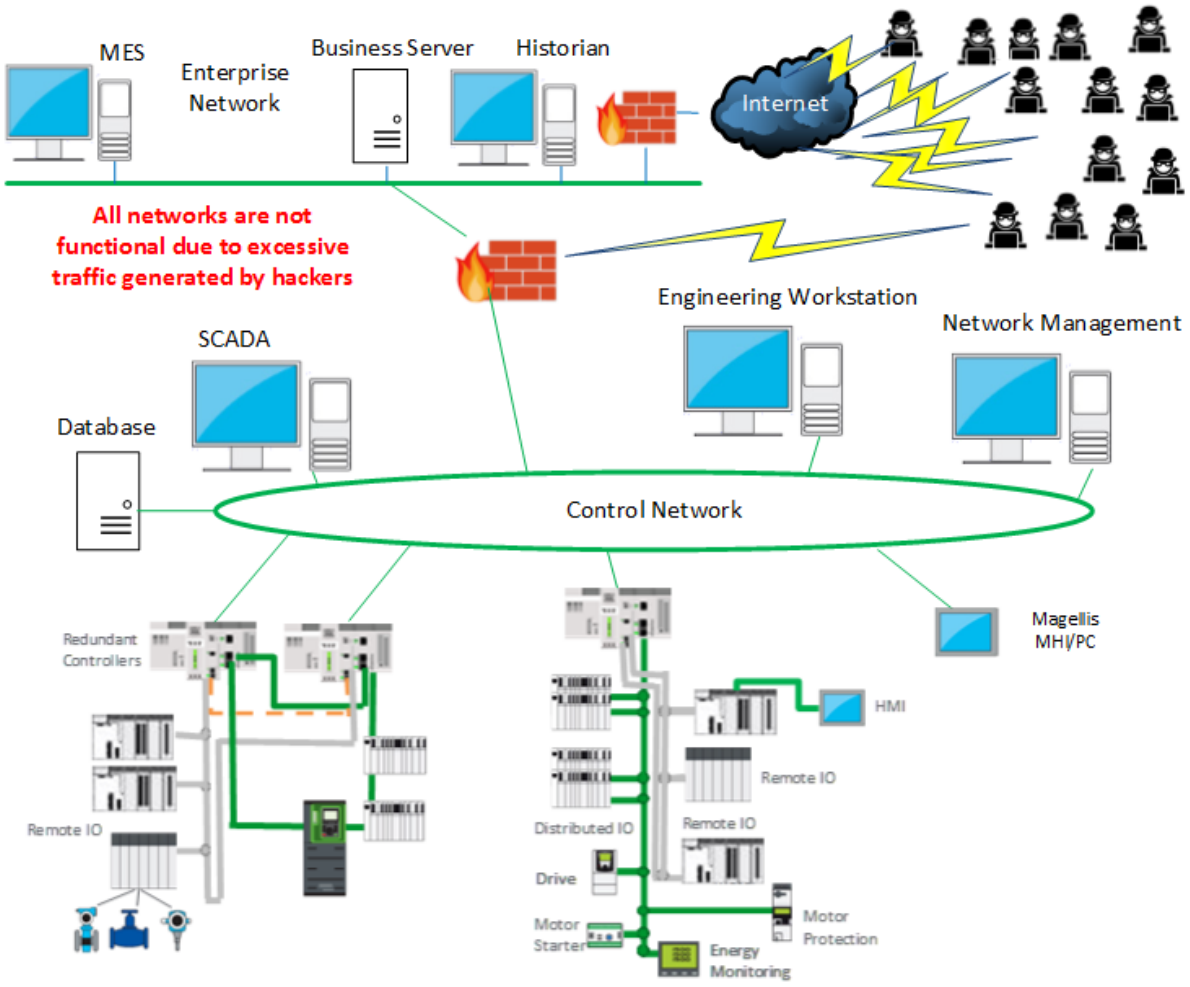


Figure 12: Denial of Service

1.6. Accidental Events

Experts attribute more than 75% of network-related system outages to accidental events. Causes of these accidents can include poor network design, programming errors, improperly functioning network devices, non-compliance with procedures, or human error such as accidentally connecting network cables in wrong ports. Many of the security features and processes discussed in this document can also mitigate accidental events.

In many cases, contractors contribute directly to system design, commissioning, or maintenance. Operational procedures should be refined so that contractors cannot introduce malware or vulnerabilities into the control network. For instance, automatically scan contractor equipment for malware infection before allowing access to any control network equipment. USB keys are another common source of malware infection and should be carefully screened before permitting their use.

Individuals who inadvertently connect a network cable into the wrong port on a multi-port switch can create outages or broadcast storms that could disable the network or severely affect its performance.

In general, the cause might be accidental, but the features, practices, and procedures used for cybersecurity work equally well against accidental system outages.

Incident recovery methods should be developed and tested so that recovery from an outage or other events can be quickly and reliably managed. High availability and redundant architectures play a role in this area when even short system outages cannot be tolerated.

1.7. NERC Top Ten Control System Vulnerabilities

The Control System Security Working Group of the North American Electric Reliability Corporation (NERC) publishes a report identifying the top 10 vulnerabilities of control systems. The published list contains the following vulnerabilities:

1. **Inadequate policies, procedures, and culture that govern control system security**.
   - IT and OT have different perspectives, which can cause a culture clash that is often challenging to resolve.
   - It is often difficult to gather the required people and resources to design and implement all levels of security planning. Nevertheless, it is a mistake not to persist until these tasks are accomplished!
2. **Rely on "security through obscurity".**
   - With the proliferation of scanning tools on the Internet it is no longer viable to "hide" from unwelcome Internet intrusions.
   - Internet access is often required as more cloud based solutions evolve.
   - Firewalls, and intrusion detection and prevention systems are now necessary.
3. **Untimely implementation of software and firmware patches, inadequate testing of patches prior to Implementation.**
   - Patch management is vital in today's industrial networks.
4. **Use of inappropriate wireless communication. Lack of authentication in the 802.11 series of wireless communication protocols. Use of unsecured wireless communication for control system**.
   - With the emergence of the "Internet of things" (IoT), wireless solutions are essential in today's industrial networks. Authentication in necessary especially with Bring Your Own Device (BYOD) that is common today.
5. **Use of nondeterministic communication for command and control such as Internet based SCADA. Inadequate authentication of control systems communication protocol traffic.**

- Stateful firewalls and deep packet inspection can help protect the control network from unsolicited network requests.

6. **Poor password standards and maintenance practices. Limited use of virtual private networks (VPN) configurations in control system networks.**
   - Make it a practice to change the initial password of every device upon installation.
   - Secure VPN connections are commonly used for remote access by equipment servicers.
7. **Lack of quick and easy tools to detect and report on anomalous on inappropriate activity among the volumes of appropriate control system traffic.**
   - Employ network management systems in your industrial networks. SNMP enabled devices can communicate to the network manager providing real-time notification of detected network issues.
   - Send a history of logs and events to a Security Information and Event Manager (SIEM).
8. **Dual use of critical control systems low bandwidth network paths for noncritical traffic or unauthorized traffic**.
   - Telemetry systems rely on low bandwidth solutions. Network intrusion, detection and prevention (NIDS) systems can help prevent unauthorized access.
9. **Lack of appropriate boundary checks in control systems that could lead to "buffer overflow" in the control system software itself**.
   - Understanding which devices need to communicate with each other is indispensable. Understand whether communication is unidirectional or bidirectional. Firewalls and Access Control Lists can help prevent unnecessary communication.
10. **Lack of appropriate change management and control of control system software and patches.**
    - IT organizations have long used methods to push updates and patches to help protect against cyber threats. These same systems can be used for workstations and SCADA systems. PACs and field device require vendor based solutions, but all these systems should have a change control process and methodology.

Schneider Electric understands these issues and offers services including:

- Risk Assessment
- Security Plan (guidelines, consultancy services)
- Training
- Ethernet/Cybersecurity Network Audit

Information about these services is available at http://software.schneider-electric.com/services/security-and-compliance-services/cyber-security-services/

Schneider Electric and our CAPP partners provide specific cybersecurity offerings that include the following:

- ConneXium Firewall offerings (Industrial Firewall and Tofino Firewall)
- Network Access Control system (Cisco/Extreme Networks/Hirschmann)
- SIEM partnership with McAfee
- 802.1X certificate services
- VPN capabilities

These will be discussed in detail later in this document.

1.8. Glossary

A glossary is available in the appendix chapter of this document. Please refer to it whenever necessary.

2. Schneider Electric Defense in Depth

Schneider Electric recommends a defense-in-depth approach to cybersecurity. No single approach is adequate. The defense-in-depth approach layers the network with security features, appliances, and processes.

As shown in Figure 13, this defense-in-depth approach integrates a set of related process and systems components to provide higher levels of security in an EcoStruxure plant network.

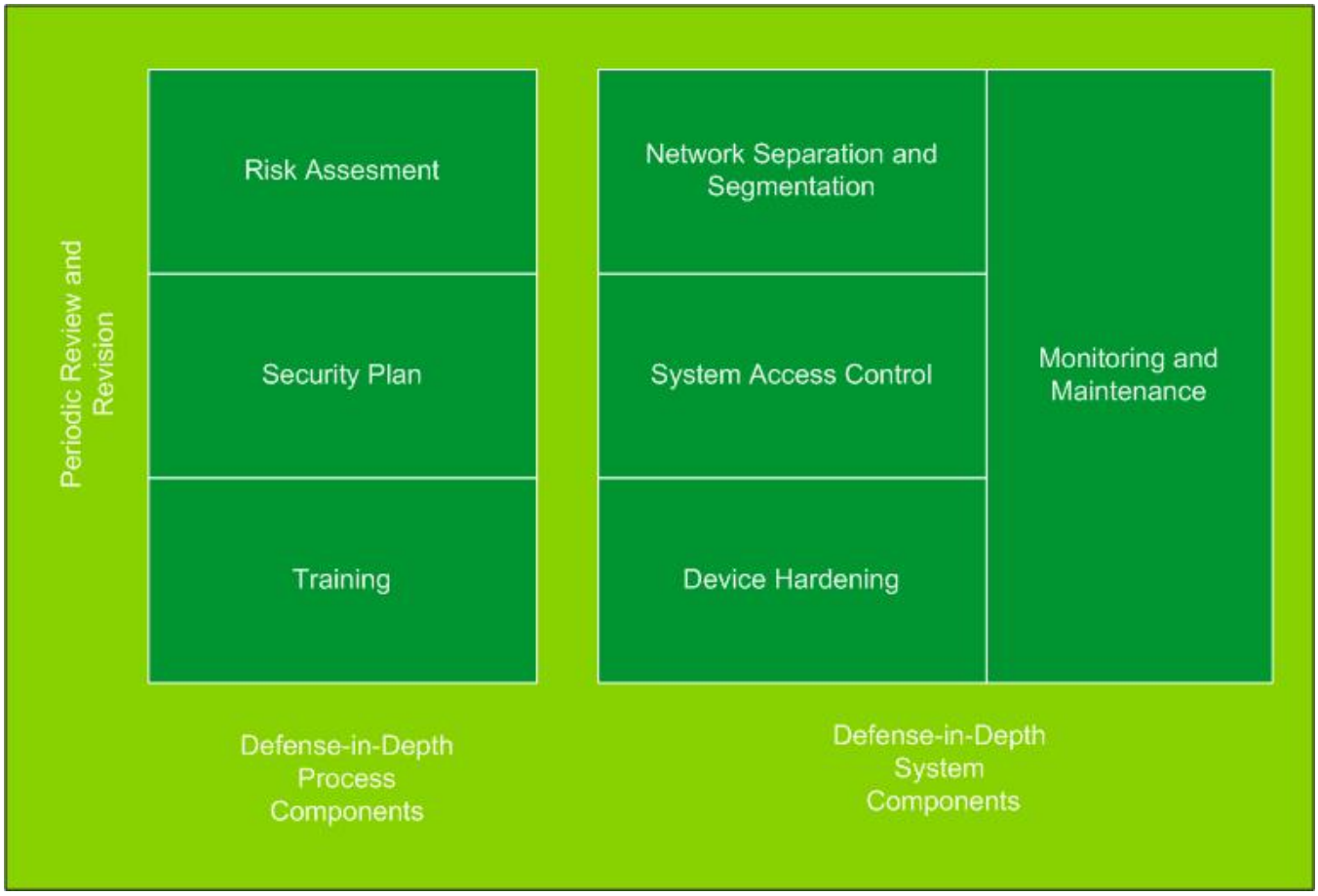


Figure 13: EcoStruxure Plant Network Defense-in-Depth Components

The basic components of Schneider Electric's defense-in-depth approach are:

1. Risk assessment. A systematic security analysis of the EcoStruxure Plant environment and related systems.
2. A security plan built on the results of the risk assessment.
3. A multi-phase training campaign.
4. Network separation and segmentation. Physical separation of the control network from other networks using a demilitarized zone (DMZ), and the division of the control network itself into segments and security zones.

5. System Access Control. Controlling logical and physical access to the system with firewalls, authentication, authorization, VPN, and antivirus software. This effort also includes traditional physical security measures such as video surveillance, fences, locked doors and gates, and locked equipment cabinets.
6. Device hardening, the process of configuring a device against communication-based threats. Device hardening measures include disabling unused network ports, password management, access control, and the disabling of all unnecessary protocols and services.
7. Network monitoring and maintenance. An effective defense-in-depth campaign requires continual monitoring and system maintenance to meet the challenge of new threats as they develop.

Schneider Electric supports defense-in-depth with a wide selection of devices, including:

- ConneXium Industrial Firewalls to provide a higher level of control network perimeter security and support components such as VPN and DMZ.
- ConneXium Tofino Firewall to help secure communication zones within the control network using basic firewall rules, stateful packet inspection, and deep packet inspection.
- ConneXium infrastructure devices to limit internal access to areas of responsibility and act as a second line of defense in the event of a firewall breech.
- PACs, SCADA, HMI devices, and Ethernet modules hardened with password protection, access control, and the ability to turn off unneeded services.

Details of the Schneider Electric defense-in-depth approach are in the chapters that follow.

3. Risk Assessment, Security Planning, and Training

This section describes the interrelated process components of Schneider Electric's defense-in-depth. They include risk assessment, security planning, and training.

3.1. Risk Assessment

Risk assessment is the process of analyzing and documenting the EcoStruxure Plant environment and related systems to identify, and prioritize potential threats.

The goals of this phase are to:

- Identify and document all potential threats.
- Prioritize these threats by severity, business impact, and safety criteria.
- Decide the order in which to address the threats and how to distribute resources to the effort.

The assessment examines possible threats from internal sources such as disgruntled employees and contractors and external sources such as hackers and vandals. It examines potential threats to continuity of operation and assesses the value and vulnerability of assets such as proprietary recipes and other intellectual properties, processes, and financial data.

Use the outcome of this assessment to prioritize cybersecurity resource investments. Address the processes, devices, and networks with the highest risk and highest business and safety implications.

Infrastructure Diagrams

Infrastructure diagrams like the example shown in Figure 14 show communication paths into and out of areas, processes, and control systems. They can help identify weaknesses, potential threats, and origins of threats to the devices and processes.

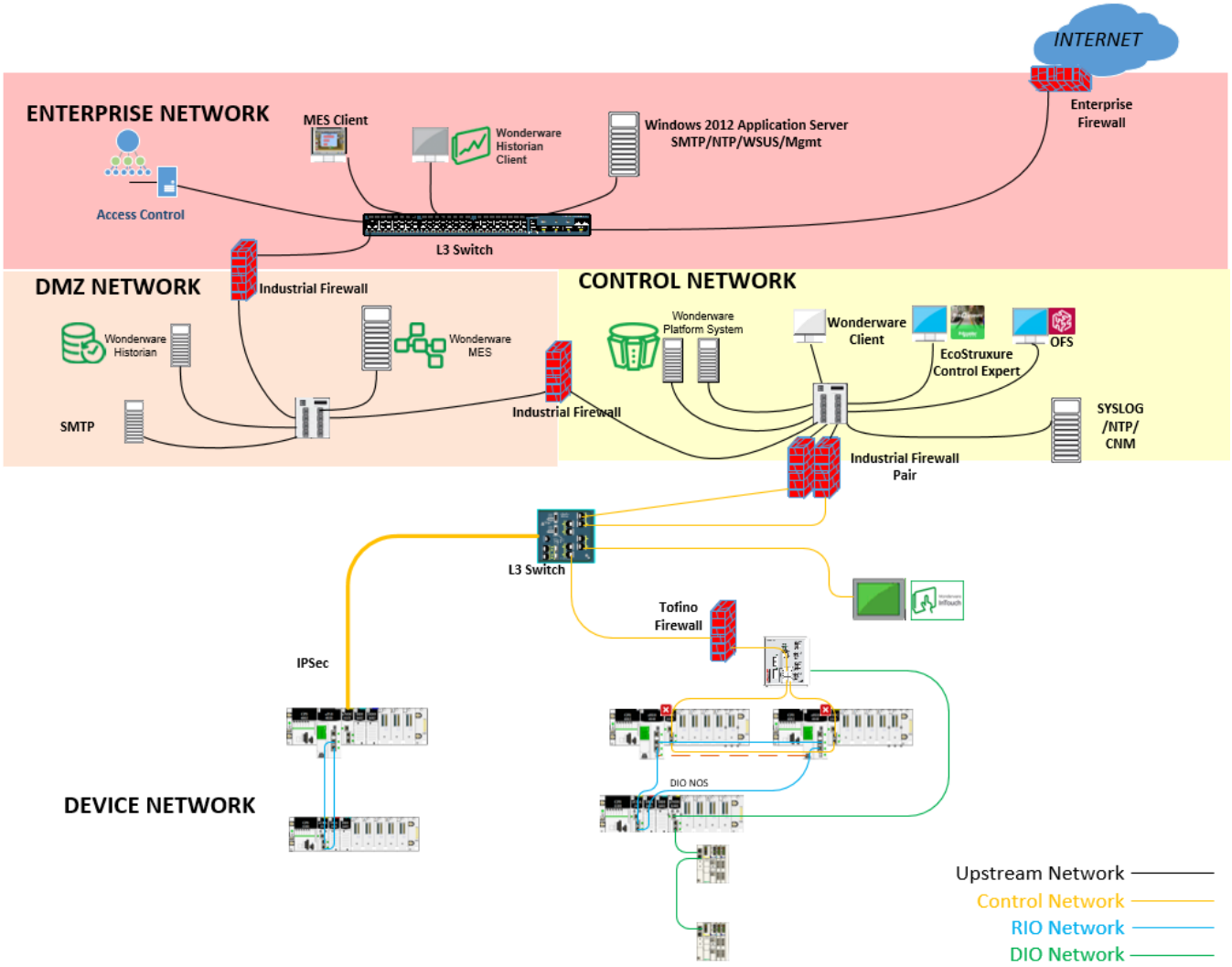


Figure 14: Sample Control Systems Diagram

3.2. Security Plan

The security plan defines the policies on which the defense-in-depth implementation is based and the job- and role-specific procedures to execute those policies. The security policies and procedures define:

- Roles and responsibilities of those affected by the policy and procedures.
- Actions, activities, and processes that are allowed and not allowed.
- Consequences of non-compliance.
- Incident response policies and procedures. These define the steps to take if a cyber-attack or accident occurs and should include:
    - Incident response plan. Who to notify and what actions to perform to contain the incident.
    - Incident recovery plan. Role-specific procedures for restoring devices and process to known good operating state.

The security plan also details the equipment, software, protocols, procedures, and personnel involved in implementing the components of the defense-in-depth program.

The security plan summarizes the findings of the risk assessment phase and includes detailed network diagrams. It also includes the training plan.

Develop and maintain the security plan with a team representing management, IT staff, control engineering, operation, and security experts.

Review the security plan periodically for changes in threats, environment, and adequate security level.

3.3. Training

Awareness plays a foundational role in the success of a defense-in-depth campaign and the development of a security conscious culture. Schneider Electric recommends the establishment of a two-phase training program for employees and other agents.

The first training phase is a cybersecurity awareness program that educates stakeholders on the organization's security policies, procedures, and standards. Schneider Electric offers an online academy that will help close the knowledge gap. Go to Schneider Electric Cybersecurity Academy for most up to date on demand videos, white papers and blogs. This is an ongoing program that is updated regularly.

The second training phase includes job- and role-based training classes that detail the relevant security policies, procedures, and standards that pertain to a particular job or function. These classes provide specific steps for applying the security policies and procedures. They also include specific instructions to follow if a cyberattack or accident has occurred.

Also, consider providing training classes for vendors, outside repair personnel, and other visitors. These classes provide an overview of company security policies and procedures with a special emphasis on the privileges and restrictions that apply to the visitor.

3.3.1. Training available to the public

Many organizations offer cybersecurity training to the public. Organizations such as the SANS Institute (SysAdmin, Audit, Network, Security) offer extensive training courses on cybersecurity. SANS was organized in 1989 as a non-profit that specializes in information security and cybersecurity training. SANS offers online training as well as traditional classroom courses. Its web site provides a wealth of information including whitepapers, tips and other resources.

The United states and most nation states have organizations to tackle cybersecurity threats. Check your home country web site for cybersecurity information and training. For example, in

Europe The European Cyber Security Organization (ECSO) ASBL is a fully self-financed not-for-profit organization under Belgian law, established in June 2016.

ECSO represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and start-ups, research centers, universities, end-users, operators, clusters and associations as well as European Member States' local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA), and H2020 associated countries.[3]

The US Department of Homeland Security US-CERT (United States Cybersecurity Emergency Response Team) responds to major incidents, analyzes threats, and exchanges privileged cybersecurity information with trusted partners around the world. It has a section – The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) – that works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share information regarding control systems-related security incidents and mitigation measures.

ICS-CERT publishes cybersecurity alerts, advisories and awareness documents. It also publishes a bi-monthly newsletter, critical alerts (see Appendix A), whitepapers and provides web based and instructor lead training. ICS-CERT has created a self-assessment tool, The Cyber Security Evaluation Tool (CSET®), which provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It is a desktop software tool that guides asset owners and operators through a step-by step process to evaluate their industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations. ICS-CERT offers this tool at no cost to end users.[4]

[3] https://www.ecs-org.eu/
[4] https://ics-cert.us-cert.gov/Assessments

4. Network Separation and the DMZ

A dual-firewall DMZ separates the industrial control networks from the enterprise and other external communication paths. Bounded by two firewalls as shown in Figure 15, the DMZ provides a security layer to help protect the control room's operations network and the deeper control and device networks.

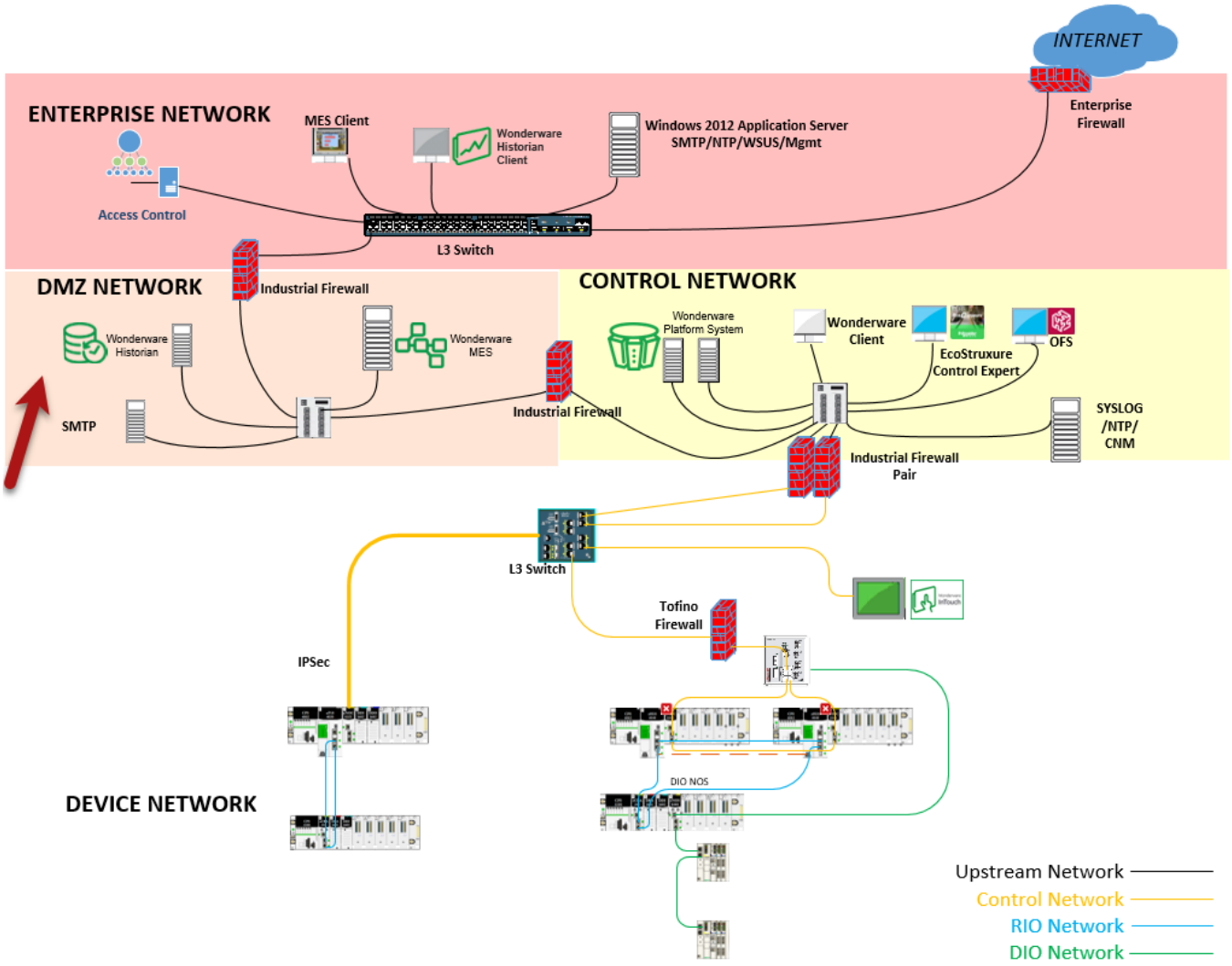


Figure 15: DMZ in EcoStruxure Plant Architecture

External requests and data terminate at controlled and dedicated servers and services within the DMZ. Requests and data from the control and operations networks terminate at servers and services in the DMZ. Allow no direct path of communication between the industrial control systems and the enterprise networks. For instance, industrial commands cannot travel from the enterprise to the control network, and industrial messages cannot travel from the control to the enterprise network.

Servers and services within the DMZ can include:

- Data servers such as Wonderware Historian that collect data from the SCADA systems and share it with MES or other reporting systems
- Patch management servers
- Proxy servers for web-connectivity or other protocols
- RADIUS and VPN servers

Some variations of the DMZ approach include a dedicated server or proxy within the DMZ to function as the sole conduit for communications between internal and external networks.

4.1. DMZ Guidelines

Take the following measures to provide higher levels of security with DMZs:

- Filter inbound traffic to the control room through a firewall before allowing a connection to a server or service in the DMZ. Likewise, filter outbound traffic from the control room to external network. This traffic should be minimal and tightly controlled on a per protocol, per host and per user basis. Filter traffic destined to the control network from the operations network. Filter traffic from the control network to the operations network. For example, multicast traffic cannot enter or leave the control network.
- Establish security policies limiting outbound traffic to required communications only. Devices on any industrial control systems network, including the operations, control, or device networks, cannot have Internet access.
- Configure the firewalls so that outbound traffic to the corporate network is source- and destination-restricted by service and port.
- Configure firewalls with outbound filtering to stop forged IP packets from leaving the control network or the DMZ.
- Configure firewalls to accept IP packets only if those packets have a correct source IP address for the control network, operations, or enterprise networks. The firewalls should drop any packet that comes in from the enterprise network with a source IP address that matches the address range of any of the control networks. This scenario is indicative of a spoof or errant route.
- Harden servers in the DMZ. See *Hardening Citect SCADA Systems* (p. 81) for examples of relevant server and client hardening methods.
- Perform security patches and antivirus software updates on a documented, monitored schedule.

5. Network Segmentation

Divide the control network into logical segments and establish security zones. For instance, in Figure 15 the control network itself is a security zone, and the field network level is divided into three separate device network security zones.

Network segments can be established using devices such as managed Ethernet switches, which provide virtual LAN (VLAN) and access control list management capabilities, firewalls, and routers.

As a first level of defense, ConneXium managed Ethernet switches can block unwanted traffic from going to all devices.

Additionally, the rate limiter feature on ConneXium switches can help reduce the risk of denial of service (DoS) and other flood attacks. The rate limiter allows the user to specify the maximum amount of traffic allowed in or out of each port.

VLAN functionality can be used to further restrict traffic by segmenting the physical network into multiple logical networks. Note that interoperability between VLANs requires Layer 3 routing capability. Routers or Layer 3 switches are generally used for this. The Modicon BMENOC0321 module includes an IP Forwarding feature, which allows 3 VLANs to interoperate. The module is installed in the M580 Ethernet backplane, and enables data to pass between the control network and a functional unit. It is less costly than standard Layer 3 switches or routers.

Segmentation facilitates the establishment of security zones. A security zone can consist of one or more network segments. Traffic into and out of a zone is subject to a zone-specific set of rules, enforced, monitored, and supported by means of devices such as ConneXium Industrial Firewalls. The organization of zones can be influenced by many factors including function, location, and security requirements. For instance, a zone may consist of network segments and devices located near each other that serve a related functional task. Another network zone may contain devices that share a common set of security requirements.

Network segmentation and the establishment of security zones can help to:

- Contain malware infections to one network segment.
- Improve security by limiting node visibility.
- Stop intruder scans at the network level before they reach a potential target system.
- Limit the impact of a security breach on a network.
- Restrict broadcasts and multicasts to specific VLANs.
- Improve network performance and reduce network congestion.
- Control communication access between segments providing high-priority devices or systems get a higher level of security.

5.1. Virtual LANs

One common method of network segmentation is the use of virtual LANs (VLANs). VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, simplify network design, and provide another layer of security. For instance, in the architecture shown in Figure 15, a separate VLAN could be established for each of the three device network security zones.

VLAN is an OSI Layer 2 broadcast domain configured on ConneXium managed Ethernet switches and other switches on a port-by-port basis. Traffic on each VLAN segment is isolated from other VLANs. The switch does not filter traffic between two devices on the same VLAN. VLANs can limit the impact of a security breach if a system in one VLAN becomes compromised.

ConneXium managed Ethernet switches provide port-based VLANs per IEC 802.1 Q standard.

5.1.1. VLAN Guidelines

VLAN grouping strategies vary greatly, but common strategies include grouping by:

- Functional or cell/area zone: Each VLAN carries only that traffic which is necessary for the operation of a particular function or cell/area zone.
- Access requirements: VLANs are grouped according to the access requirements of different types of users such as operators, engineers, and vendors.
- Security: VLANs are grouped to support the control of access to sensitive information, devices, and processes.
- Traffic: VLANs are grouped to balance traffic load in support of the required throughput.

Segmentation guidelines include:

- Use one VLAN per ring topology for all manufacturing traffic per cell/area zone.
- Contain voice over Internet protocol (VoIP) on a dedicated VLAN.
- Contain video on a dedicated VLAN.
- Assign a restricted VLAN identifier (ID) to packets entering the DMZ from the enterprise network so those packets can access only specific devices in the DMZ.
- Remove all unnecessary traffic from each VLAN.
- Apply quality of service (QoS) access control lists (ACL) to rate-limit the amount of ping traffic allowed.
- Avoid protocols such as telnet and FTP that send passwords in clear text. Use secure shell (SSH) and SFTP sessions if the device supports those protocols. If telnet or FTP is needed, use ACLs or firewall rules to allow connections only between specific hosts.
- Connect untrusted devices to untrusted ports, trusted devices to trusted ports.
- Disable unused ports or put them into an unused or untrusted VLAN that has very restricted access.

- Avoid the use of VLAN 0 Transparent Mode. In this mode, the packets are sent without VLAN membership.
- Avoid using VLAN 1 as this VLAN is generally used for network device communication. Network management packets use this VLAN.

5.1.2. Communication Between VLANs

Once the network is segmented into VLANs, users need restricted communications between VLANs. This can be achieved by use of a Layer 3 switch/router that maps traffic from one VLAN to another. Schneider Electric recommends the Hirschmann MICE range of Layer 3 switches or the ConneXium Industrial Firewall configured in routing mode for this purpose.

5.2. Firewalls

Firewalls help protect network security zone perimeters by blocking unauthorized access and permitting authorized access. A firewall is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy traffic between different security zones based upon a set of rules and other criteria.

Process control devices require fast data throughput and often cannot tolerate the latency introduced by an aggressive security strategy inside the control network. Firewalls play an essential role in a security strategy by providing levels of protection at the perimeters of the network. As illustrated by the redundant stateful firewalls that bound the DMZ in Figure 15, a control system relies heavily on perimeter protection to block unwanted and unauthorized traffic.

Common firewall types include the following:

- **Packet Filtering Firewalls**. A packet filtering firewall is a first-generation, basic firewall that exerts minimal impact on network performance. Packets are filtered based on basic information in each packet, such as IP address (source and destination) and port number. Rules based on this information are established to determine if a packet will be forwarded, dropped, or rejected. However, first generation firewalls that provide only packet filtering are not recommended for use in control systems. They lack authentication and do not conceal the shielded network's architecture.
- **Application-Proxy Gateway Firewalls**. An application proxy gateway firewall examines packets at the application layer and filters traffic based on rules that regulate access by applications such as browsers or protocols such as FTP. It also acts as a gateway for client requests, determining the final server address. Application proxy gateway firewalls provide a high level of security, but can cause overhead delays that slow down network performance. These firewalls are suitable for systems located in the control room operations network, but not for the performance-sensitive networks of the control system.

- **Host Firewalls**. A host firewall is a software-based firewall that resides on a host device and helps protect its ports and services. Most laptops, servers, and workstations today feature integrated host firewalls. Host firewalls support the creation of customized rules to help protect ports and services. Host firewalls are a valued feature of laptops, mobile devices, engineering workstations, and HMIs in industrial networks.
- **Stateful Inspection Firewalls**. Stateful multilayer inspection firewalls, such as the ConneXium Industrial Firewall, combine features of all the other firewall types. They filter packets at the network layer and validate that the session packets and their contents at the application layer are legitimate. A stateful multilayer inspection firewall also keeps track of the network connections (such as TCP and UDP connections) that traverse the firewall. It allows packets that match known good connections and rejects those that do not match. Stateful inspection checks that inbound packets are the result of an outbound request. Stateful inspection firewalls provide a high level of security and good performance. They tend to cost more than other types of firewall and may require more configuration effort.
- **Deep Packet Inspection Firewalls**. Deep packet inspection firewalls, such as the ConneXium Tofino, typically offer the same benefits as stateful firewalls but also offer the ability to interrogate and make forwarding decisions based on the analysis of application packets. For instance, the Tofino can filter based on Modbus and extended Modbus protocols. These firewalls can block certain message types, control application traffic from specific hosts, and help stop application traffic from flooding high-priority devices. A potential disadvantage of deep packet inspection firewalls is that they can have a greater negative impact on performance than stateful firewalls.

5.2.1. NIST Firewall Guidelines

The National Institute of Standards and Technology (NIST) published the following firewall guidelines in its Special Publication 800-82: Guide to Industrial Control Systems:

- *By default, "deny all, permit none." [When defining explicit or implicit deny rules, Schneider Electric recommends implementing a drop action rather than a reject action. This helps prevent system interrogation from external sources.]*
- *Ports and services between the control system network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.*
- *All "permit" rules should be both IP address and TCP or UDP port specific.*
- *All rules should restrict traffic to a specific IP address or range of addresses.*
- *Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in a DMZ.*

- *Any protocol allowed between the control network and the DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).*
- *All outbound traffic from the control network to the operations network should be source and destination-restricted by service and port.*
- *Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.*
- *Control network devices should not be allowed to access the Internet.*
- *Control networks should not be directly connected to the Internet, even if protected via a firewall.*

These are only guidelines. Carefully assess each control environment before implementing any firewall rule.[5]

5.2.2. Other Firewall Risk Mitigation Guidelines

Packet Filtering

Packet filtering provides network security based on unique applications and protocols. It filters packets based on IP protocol and the packet source IP address, source port, destination IP address, and destination port. Schneider Electric's ConneXium Industrial Firewall is a packet-filtering device.

With packet filtering, access to a device can be restricted to allow only specific protocols (ports).

In Figure 16, the PC communicates with the PLC via port 80, but port 69 messages are blocked by the firewall.

[5] Guide to Industrial Control Systems (ICS) Security NIST special publication 800-82 revision 2 May 2015

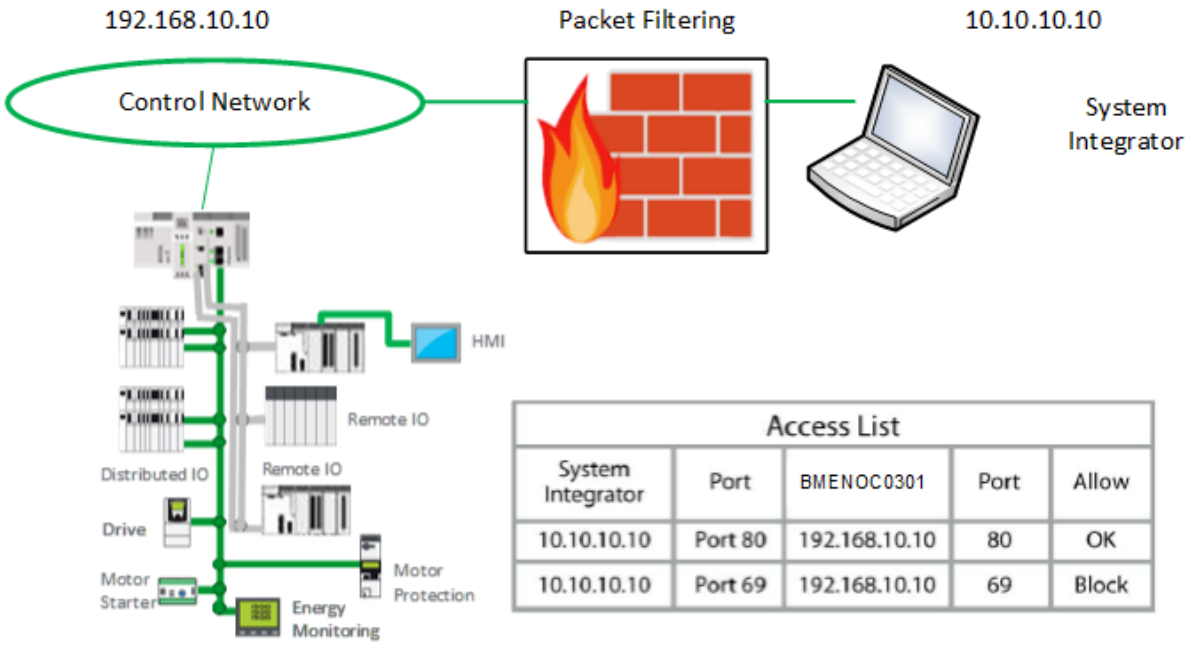


Figure 16: Packet Filtering

Ports that need extra protection due to inadequate built-in security include:

Non-Secure Protocols		
Internet Protocol	**Service Protocol**	**Port #**
TCP	Telnet	23
TCP/UDP	HTTP	80
TCP/UDP	SNMP v1 & V2	161
TCP	FTP	20: Data 21: Command
UDP	TFTP	69
TCP/UDP	DNS	53
TCP	POP3	110
TCP/UDP	SMTP	25
TCP	Modbus TCP	502

Table 1: Non-Secure Protocols

Schneider Electric recommends that packet filtering be implemented on incoming connections (untrusted ports) and on outgoing connections (trusted ports).

Some firewalls can inspect the protocol to make intelligent decisions about allowing or restricting specific messages. These firewalls can examine a protocol such as Modbus TCP (port 502) and

allow certain function codes to pass while blocking others. An example is the ConneXium Tofino Firewall.

Flood Protection

DoS attacks are a common form of flood attacks. If a DoS attacker penetrates the control network, the impact can be minimized using flood protection provided in the firewall. The sample ConneXium firewall configuration screen in Figure 17 lets you set limits on certain traffic types, such as a high number of incoming or outgoing TCP connections per second that could indicate a DoS attack.

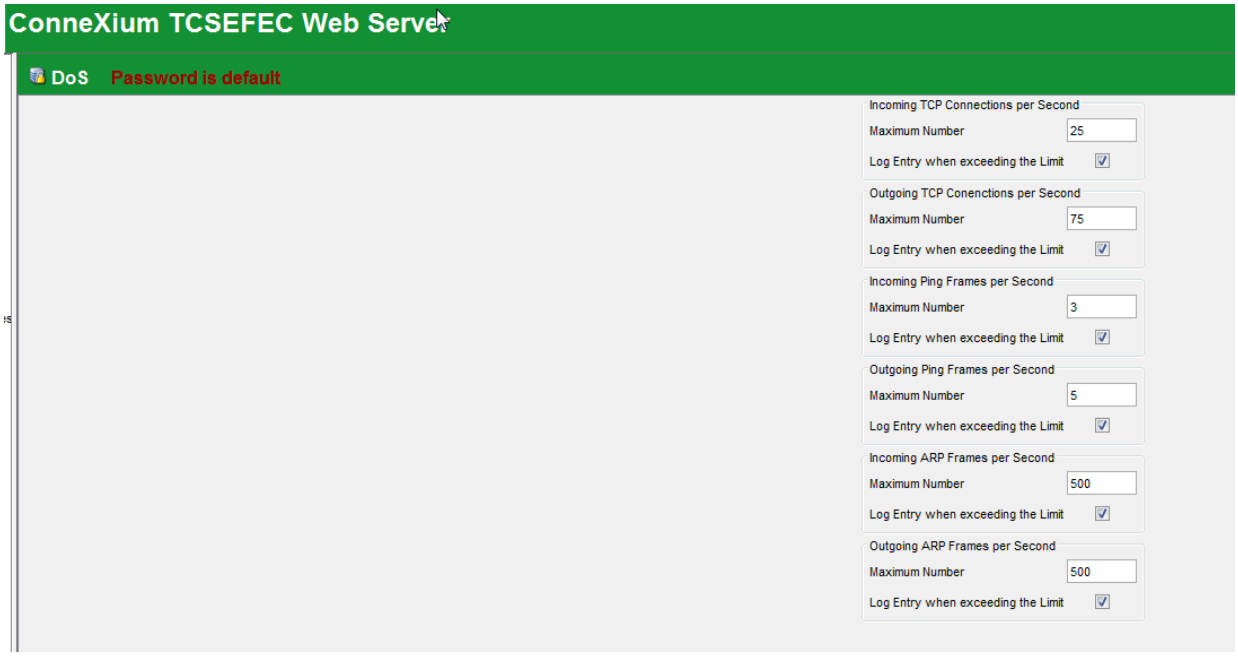


Figure 17: Sample ConneXium Firewall DoS Protection Configuration Screen

6. Firewalls and Specific Services

This section expands on the network segmentation component of Schneider Electric's defense-in-depth approach. It describes how firewalls process and help manage many of the protocols and services used in industrial control systems, including DNS, HTTP, DHCP, FTP, TFTP, telnet, SMTP, POP, SNMP, and NAT.

6.1. Firewalls and Domain Name System (DNS) Server

A Domain Name System (DNS) server is a database used to translate domain names to IP addresses. Many Internet services rely on DNS, but DNS is not commonly used by control systems. According to the NIST, "In most cases there is little reason to allow DNS requests out of the control network to the corporate network and no reason to allow DNS requests into the control network."

6.1.1. DNS Vulnerabilities

DNS servers are vulnerable to many exploits, including DNS cache poisoning and DNS amplification attack.

DNS cache poisoning is initiated by replacing the intended domain IP address with the attacker's domain IP address. Web traffic, e-mail, and other network data can then be redirected to systems under the attacker's control.

DNS amplification attack is a type of DoS attack that generates traffic overload.

6.1.2. DNS Risk Mitigation

Avoid DNS requests from the control network to the corporate network whenever possible. Address exceptions on a case-by-case basis.

Design your network so that DNS requests are not allowed to enter the control network.

If DNS is required, configure the firewall to use specific DNS servers instead of those allocated by an ISP. For instance, on the ConneXium Industrial Firewall DNS Server screen, set DNS Client Configuration to User and enter the IP addresses of up to four DNS servers. Queries will be sent to those servers, and queries will not be sent to any DNS server addresses allocated by an ISP.

6.2. Firewalls and Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol is the underlying protocol used by the World Wide Web. It is used in control systems to support embedded Web servers in control products. Schneider Electric Web servers use HTTP communications to display data and send commands via Web pages.

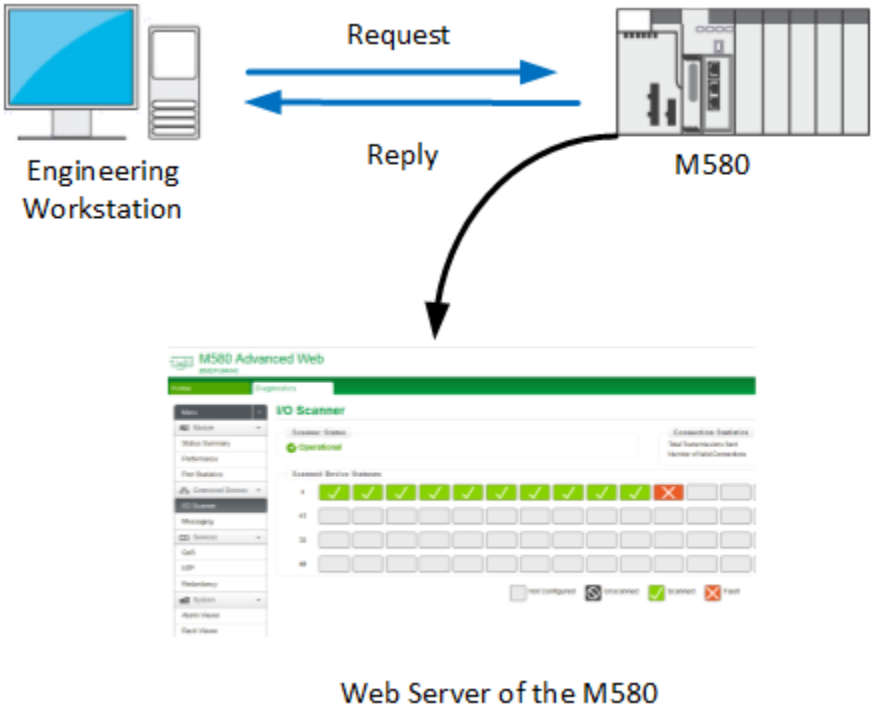


Figure 18: Sample HTTP Exchange

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the HTTP and a cryptographic protocol. By default, HTTP uses port 80 and HTTPS uses port 443.

HTTPS transmits normal HTTP with encryption, commonly using either Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL).

6.2.1. HTTP Vulnerabilities

HTTP has little inherent security and can be used as a transport mechanism for attacks and worms. Common attacks are man-in-the-middle and eavesdropping.

6.2.2. HTTP Risk Mitigation

If the HTTP server is not needed, disable it. Otherwise, use HTTPS instead of HTTP if possible and only to allow traffic to specific devices.

6.3. Firewalls and DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol based on BootP. It is used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. DHCP is an unauthenticated protocol. The DHCP service works by using the DORA (Discover, Offer, Request, and Acknowledgment) grants.

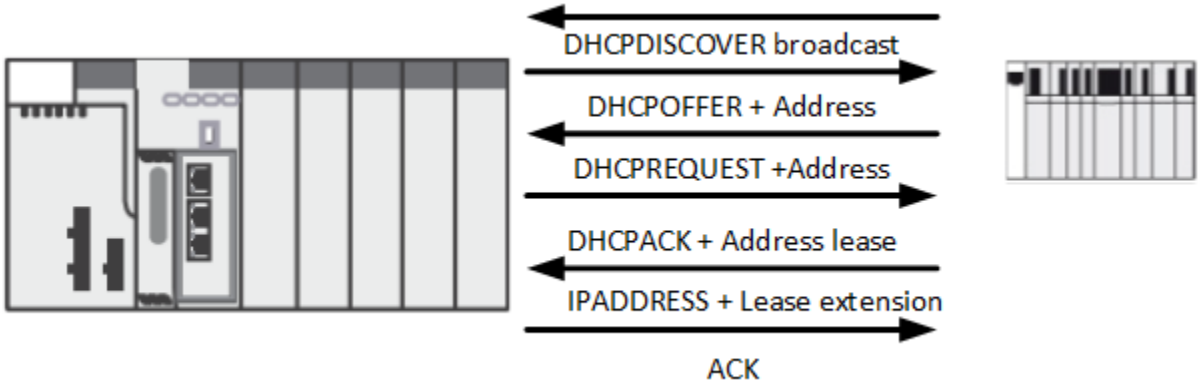


Figure 19: Sample DHCP Exchange

DHCP service uses port 67/UDP in the DHCP server, and 68/UDP in the DHCP clients.

Schneider Electric uses DHCP for Fast Device Replacement (FDR).

6.3.1. DHCP Vulnerabilities

There are two common types of DHCP attacks:

- DHCP starvation attack: The DHCP server is inundated with requests from different MAC addresses. The DHCP server eventually runs out of IP addresses blocking legitimate users from obtaining or renewing their IP addresses.
- DHCP rogue attack: The attacker disguises itself as a DHCP server, responds to a DHCP request with false IP addresses, and then launches a man-in-the-middle attack.

6.3.2. DHCP Risk Mitigation

Allow only authorized persons to have physical or wireless access to the device.

If DHCP is not needed, disable it in the firewall or any device supporting DHCP.

Some Schneider Electric PAC and network communication modules have built-in DHCP servers. The DHCP server uses the device's MAC address or device name to serve the IP configuration and the name and location of the configuration file.

6.4. Firewalls and FTP or TFTP

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. TFTP a simplified unidirectional protocol commonly used for special purpose file transfers such as the transmission of boot files between devices.

Schneider Electric Ethernet devices use FTP for various tasks including to firmware loading, display of custom Web pages, and the retrieval of event logs.

6.4.1. FTP Vulnerabilities

FTP uses a login password that is not encrypted. TFTP requires no authentication. FTP is vulnerable to buffer overflow and FTP Bounce attacks. The FTP bounce attack uses an FTP server in passive mode to transmit information to any device on the network. To begin the bounce attack process, the attacker logs into the FTP server that will be used as the middleman. Once connected to the FTP server, the attacker sends the PORT command to direct all data connections to the illegitimate destination IP address and TCP port.

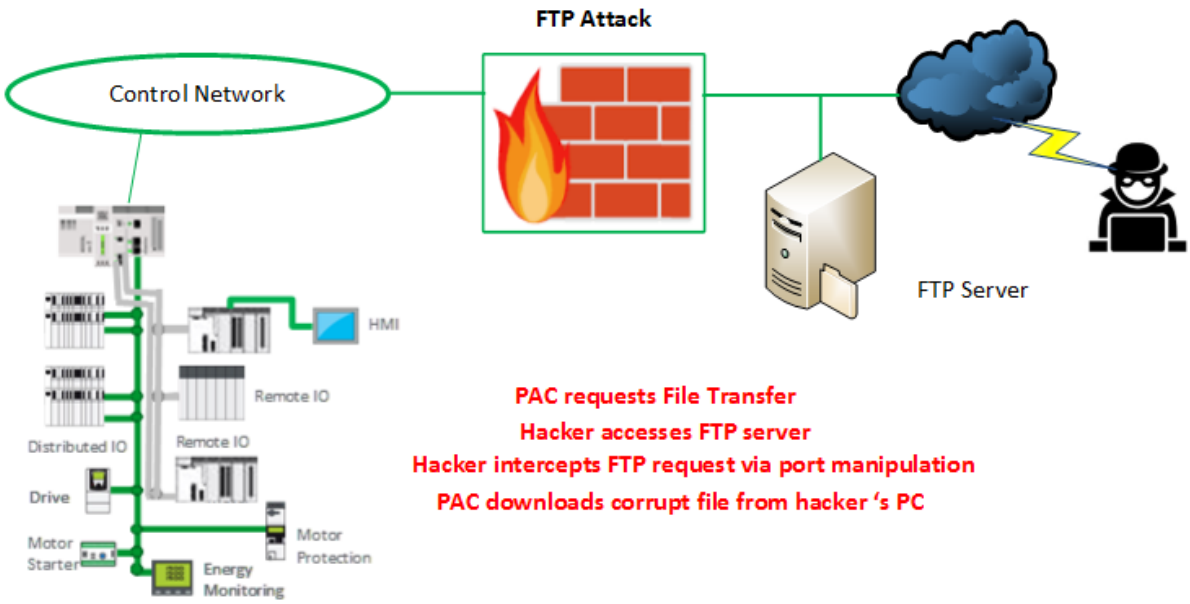


Figure 20: Sample FTP Attack

6.4.2. FTP Risk Mitigation

Allow FTP communications for outbound sessions only, unless additional security is provided by means of token-based multi-factor authentication and an encrypted tunnel.

If possible, use more secure protocols such as Secure FTP (SFTP) or Secure Copy (SCP).

Configure each server connection individually.

Use packet filtering to allow access only to the FTP server.

Block TFTP communications if they are not required.

6.5. Firewalls and Telnet

The telnet protocol provides interactive, text-based communications between a client and a host. Telnet provides access to a command-line interface, typically via port 23. It is mainly used for remote login and simple control services to systems with limited resources or to systems with limited needs for security. Due to security risks, Schneider Electric has limited the use of telnet in its products.

6.5.1. Telnet Vulnerabilities

Telnet is a severe security risk. All telnet traffic, including passwords, is unencrypted. This can allow an attacker considerable control over a device.

6.5.2. Telnet Risk Mitigation

Inbound telnet sessions from the corporate to the control network should be prohibited, unless additional security is provided by means of authentication and an encrypted tunnel such as a VPN tunnel.

Outbound telnet sessions should be allowed only over encrypted tunnels to specific devices as described in Remote Access (p. 64).

The ConneXium managed switches provide the option to disable the telnet interface. Disable the telnet interface when not using the command line interface to configure the switch.

6.6. Firewalls and Simple Mail Transfer Protocol (SMTP) & Post Office Protocol (POP3)

Email notification in the automation industry is becoming more prevalent as plants increasingly rely on off-site personnel to troubleshoot and fix detected problems. Schneider Electric Ethernet devices send e-mail but do not receive it. However, there is potential that non-Schneider Electric devices residing on the network can receive e-mail. Use antivirus software to scan e-mail for viruses. No email client should be enabled on any dedicated control room workstation or server. If receiving email is required, the mail should be received on dedicated business machines connected on the enterprise network.

The Simple Mail Transport Protocol (SMTP) is an Internet standard used by e-mail clients or mail transfer agents (MTA) to send e-mails. An SMTP server performs two functions:

- Verifies that the configuration is valid and grants permission to the computer sending the message.
- Sends the outgoing message to a predefined destination and validates the successful transfer of the message. If the message is not successfully transferred, a message is sent back to the sender.

Post Office Protocol v3 (POP3) or Internet Message Access Protocol (IMAP) is used by local e-mail clients to download e-mail from a remote server. The POP3 server receives the e-mail message and retains the e-mail message until it is retrieved by the local client. POP3 uses port 110.

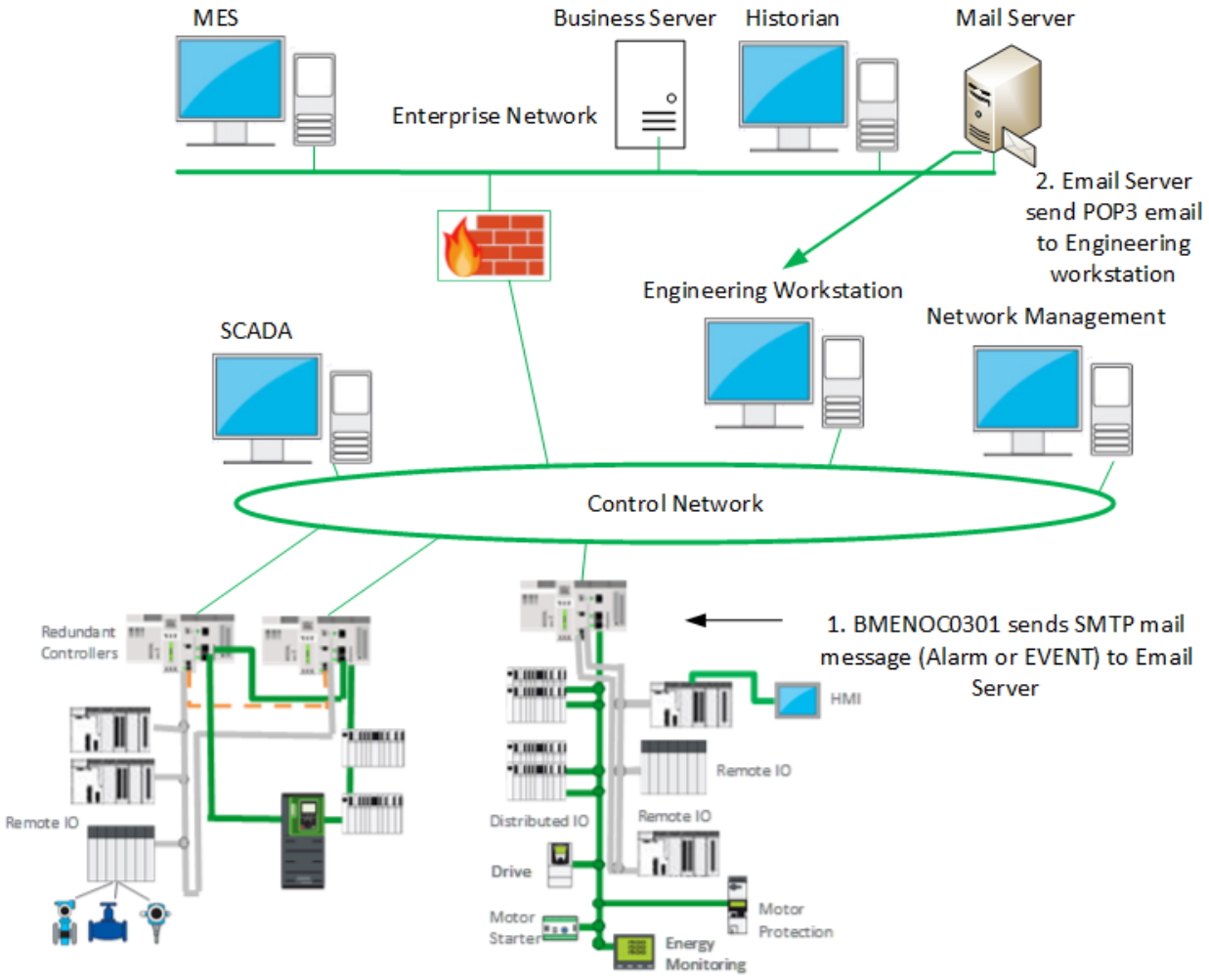


Figure 21: Sample SMTP & POP3 Exchanges

6.6.1. SMTP & POP3 Vulnerabilities

Directory harvesting is a common form of e-mail attack. The attack relies on invalid e-mail addresses being rejected by the e-mail system either during the SMTP conversation or afterwards via a Delivery Status Notification (DSN). When the attacker receives a rejection from an invalid e-mail address, the e-mail address sent is discarded. When no rejection or DSN is

received, the e-mail address is considered valid and is added to a spam database. The attacker typically uses two methods:

- Brute force: an approach that sends messages with all possible alphanumeric characters and waits for a valid response.
- Selective: an approach sending an e-mail using a likely username in hopes of finding a valid one, as shown in Figure 22.

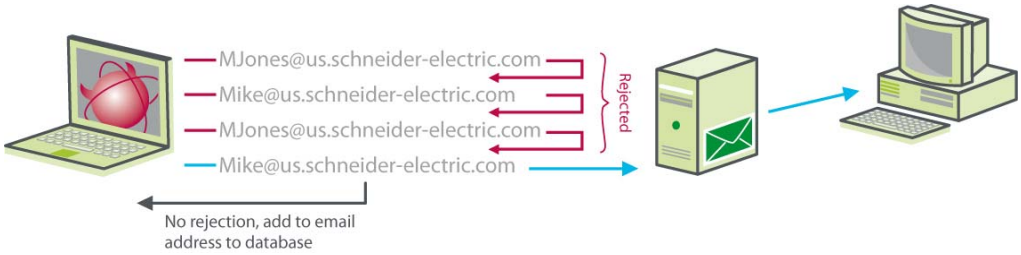


Figure 22: Selective Mail Attack

6.6.2. SMTP and POP3 Risk Mitigation

Design your network so inbound e-mail cannot be sent to any control network device.

Allow outbound e-mail only when necessary. For instance, a device may send an alert by e-mail.

6.7. Firewalls and Simple Network Management Protocol (SNMP)

SNMP provides network management services between a central management console and network devices such as routers, Ethernet devices, and PACs.

SNMP consists of three parts:

- Manager: an application that manages SNMP agents on a network by issuing requests, getting responses, and listening for and processing agent-issued traps.
- Agent: a network-management software module that resides in a managed device. The agents allow configuration parameters to be changed by managers. Managed devices can be any type of device: routers, access servers, switches, bridges, PACs, drives.
- Network management system (NMS): the terminal through which administrators can conduct administration tasks.

Schneider Electric Ethernet devices have SNMP service capability for network management. Many Schneider Electric Ethernet devices use SNMP v1, which does not use encryption and is therefore considered unsecure.

ConneXium switches are an exception. They use SNMP v3, which uses encryption, authentication, and security features to enhance message integrity. Inherently they also support SNMP v1 and v2.

6.7.1. SNMP Vulnerabilities

SNMP in general is weak in security. Versions 1 and 2 of SNMP use unencrypted passwords to both read and configure devices. Passwords may not be able to be changed. Version 3 is more secure but is still limited in use.

Often SNMP is automatically installed with public as the read string and private as the write string. This type of installation provides an attacker the means to perform reconnaissance on a system to create a denial of service.

SNMP also provides information about the system that may allow the attacker to piece together the network system with the interconnection.

6.7.2. SNMP Risk Mitigation

- When possible, deactivate SNMP v1 and v2 and use SNMP v3, which encrypts passwords and messages.
- Change the default passwords of all devices that support SNMP.
- Block all inbound and outbound SNMP traffic at the boundary of the enterprise network and operations network of the control room.
- Filter SNMP v1 and v2 commands between the control network and operations network to specific hosts or communicate them over a separate, secured management network.
- Control access by identifying which IP address has privilege to query an SNMP device.
- If SNMP v1 or v2 is needed, use access settings to limit the devices (IP addresses) that can access the switch. Assign different read and read/write passwords to devices.

6.8. Firewalls and Network Address Translation (NAT)

Network Address Translation (NAT), also known as IP masquerading, is a service that conceals a device's true IP address from the outside world to keep outside agents from accessing the device directly. As illustrated in Figure 23, IP addresses used on one side of a device network are mapped to a different set on the other side.

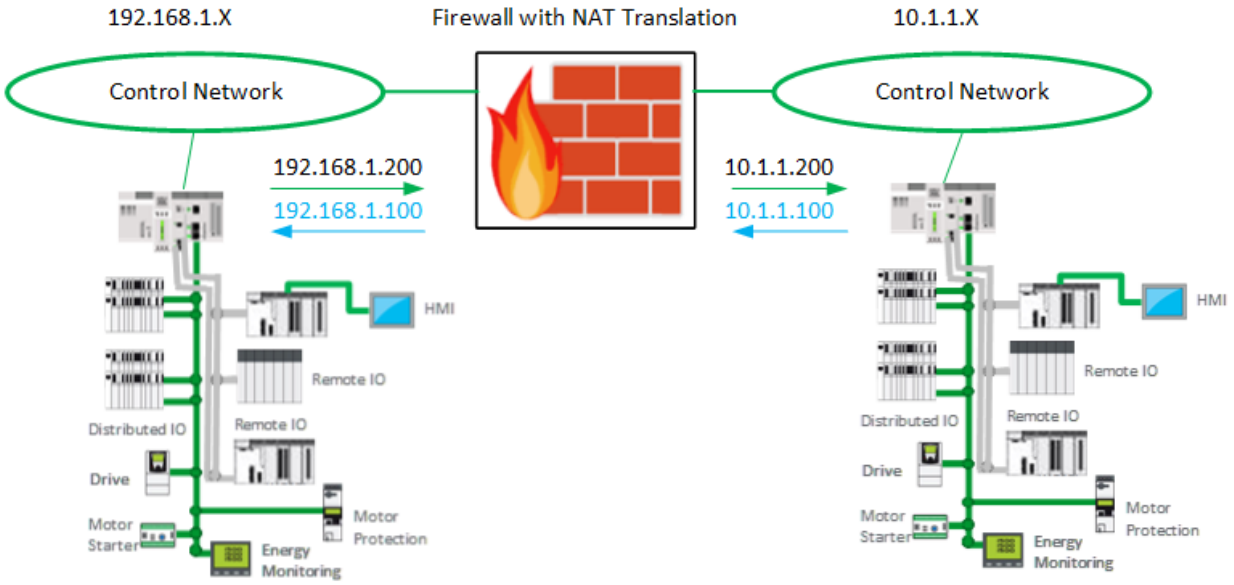


Figure 23: Simple NAT Exchanges

NAT maps the entire network to a single IP address prior to transmitting. NAT relies on the premise that not every internal device is actively communicating with external hosts at any given moment. The firewall tracks the state of each connection and how each private internal IP address and source port was remapped. When the response is received by the firewall, the IP address mapping is reversed and the packets forwarded to the proper internal host.

Although NAT routers are not technically firewalls because they do not filter the packets, NAT does offer devices a level of protection from external networks. NAT blocks inbound packets that were not sent in response to a request from accessing the device directly.

6.8.1. NAT Vulnerabilities

None known.

6.8.2. ConneXium Industrial Firewall NAT Features

NAT features supported by the ConneXium firewall include:

- 1:1 NAT can be used when setting up identical internal production cells that use the same IP addresses but need to be connected to an external network. The firewall replaces the source IP address of a data packet from the internal network with an IP address of the external network.
- Inverse 1:1 NAT allows devices in an internal network to communicate with devices in an external network as if the devices in the external network were in the internal network. With inverse 1:1 NAT, the firewall replaces the destination IP address of a data packet from the internal network with an IP address of the external network

- Double NAT allows devices in an internal network to communicate with devices in an external network as if the devices in the external network were in the internal network, and vice versa.

To devices in the internal network, the firewall allocates a different IP address in the external network (1:1 NAT function). To devices in the external network, the firewall allocates a different IP address in the internal network (inverse 1:1 NAT function).

- NAT–IP Masquerading hides the internal network structure (IP addresses) from an external network. The firewall replaces the source IP address of a data packet from the internal network with the external IP address of the firewall.
- NAT Port-Forwarding hides the internal network structure from the outside but allows a communication connection to be set up from the outside in. External devices can set up a communication connection to the internal network, and send data packets to a specific port with the external IP address of the firewall.

6.8.3. NAT Configuration Recommendation

Use NAT whenever possible. NAT does not support producer-consumer protocols such as EtherNet/IP or Foundation Fieldbus.

Since NAT is usually used on routers and network gateways, its use requires enabling IP forwarding so that packets can travel between networks.

7. System Access Control

Regulating access to the control system is another indispensable component of the defense-in-depth approach. This section describes external authentication and authorization with RADIUS, providing secure access with remote access services (RAS) and Network Access Control (NAC) and Virtual Private Networks (VPN), and providing security while allowing access for remote control.

7.1. External Authentication with RADIUS

Authentication, authorization, and accounting (AAA) protocols authenticate users before granting access to network assets, authorize them for certain assets, and account for use of those assets. AAA is commonly used for access into trusted networks.

Remote Authentication Dial in User Service (RADIUS) is an AAA protocol commonly used in control systems.

RADIUS is a client-server protocol that provides centralized and scalable user management where network devices might number in the hundreds or more. When embedded devices such as switches, PACs, or firewalls have the storage capacity to handle only a few user accounts, RADIUS can substantially increase the number of supportable user accounts. RADIUS also helps to enforce consistency in security policy and user access.

RADIUS clients are used in many VPN servers, remote access servers, wireless access points, switches, routers, and other network access devices. Presently, RADIUS authentication is supported in ConneXium Industrial Firewalls.

A RADIUS server is typically a process running on a Windows or UNIX system. For instance, Windows Server 2012 R2 offers a RADIUS server called Network Policy Server (NPS). In an EcoStruxure Plant architecture, locate any dedicated RADIUS servers within the DMZ.

Transactions between the RADIUS client and the RADIUS server are authenticated with a shared secret, which is typically a password or pass code. Figure 24 illustrates a sample RADIUS exchange.

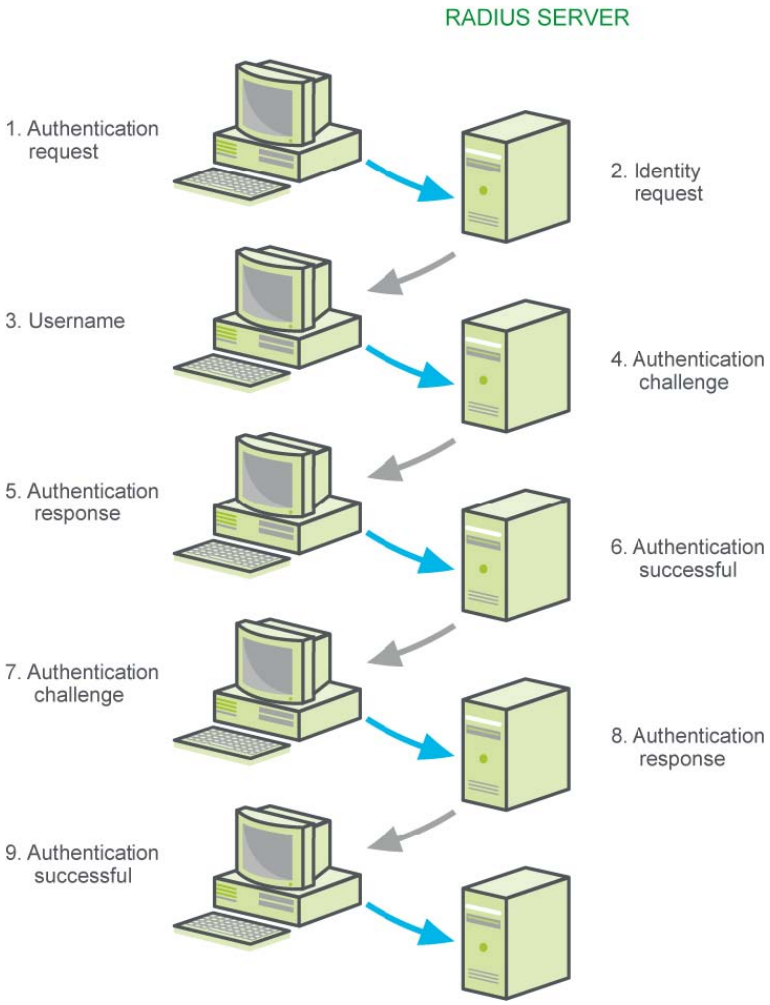


Figure 24: Sample RADIUS Authentication Exchange

Alternatives to RADIUS include Microsoft Windows Active Directory, Terminal Access Controller Access-Control System (TACACS), TACACS+ and Diameter protocols. These protocols are more commonly found on PC servers and clients than on embedded devices such as switches, PACs, and firewalls. TACACS+ and Diameter are TCP-based and support IPSec and TLS protocols, whereas TACACS uses UDP.

7.1.1. RADIUS Authentication Vulnerabilities

The communication of user credentials between the RADIUS client and the RADIUS server is not strongly encrypted. The impact of the weak encryption is mitigated by a strong perimeter if the RADIUS server and client reside on the same internal network and that network is separated by a DMZ.

RADIUS does not encrypt transferred attribute values. This can potentially expose identifiable network elements. If the RADIUS server needs to proxy requests through untrusted networks or if the client and server are separated by untrusted networks, then use IPsec VPNs as described in Remote Access (p. 64).

7.1.2. RADIUS Authentication Guidelines

- Use a different shared secret for each RADIUS server-RADIUS client pair.
- If possible, configure shared secrets with a minimum length of 16 characters consisting of a random sequence of upper and lower case letters, numbers, and punctuation.
- Implement RADIUS authentication on ConneXium firewalls if there are many devices supporting RADIUS.
- For the ConneXium firewall use group authentication:
  - Group authentication allows the assignment of multiple users to groups via a RADIUS server. If the group authentication is active and an unknown person logs in to the user firewall, the firewall checks the user's authenticity via the RADIUS server. If the authentication is successful, and if the firewall has a user firewall account with this group name, the firewall gives the user access. This is particularly convenient when vendors might perform maintenance on the networks. Using external authentication with groups enabled provides a more secure way of allowing temporary bypass of normal firewall rules. This is also useful for defining user-based rules so software or firmware can be downloaded to high-priority equipment without the need to open high-risk ports in the normal firewall table.
  - Authentication will be successful only if the credentials of the externally authenticated user are entered and present in the user firewall accounts.

7.2. Network Access Control

Network Access Control (NAC) performs a useful role in a plant network. It provides admission and compliance control on any device accessing the network. Most NAC systems are offered by network vendors. They can be an appliance, a server or a virtual machine. Cisco and Extreme Networks, our technology partners, offer very sophisticated NAC solutions. NAC systems:

- Enforce policies to control access to devices.
- Provide integration to authentication sources.
- Quarantine devices that are not compliant to plant policy.
- Remediate non-compliant devices with software updates.
- Monitor devices.

A NAC solution can use policies to permit, deny, prioritize, rate-limit, tag, re-direct and audit network traffic based upon user identity, time, location, device type, and other variables. A NAC system can manage both wired or wireless Ethernet networks.

NAC usually ties to an authentication system. A RADIUS server, explained in Section 7.1, is an example of an authentication system. Other authentication systems, for example Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), Kerberos, or S/Ident, may also be used.

A noteworthy feature is the quarantining of non-compliant devices. This feature denies access to any device that has not been granted permission to access the network. This helps stop unwanted malware from entering the network. For example, NAC would help protect your system against a service technician showing up at your plant site with a laptop that contains a virus. NAC helps prevent a spread of infection.

These systems can provide software updates to devices in non-compliant systems. It will automatically check the current software on a device accessing the network and push updates including Microsoft security updates or recent anti-virus updates.

A NAC system also constantly checks and logs all the permitted devices. It can be an indispensable tool to provide a forensic audit trail in the event of a cyberattack.

7.3. Remote Access Control with RAS or VPN

Many organizations allow engineers and support personnel to monitor and control the system from remote locations across the public Internet. Remote access to the control network can be susceptible to cyberattacks if not configured correctly.

Methods for providing and managing remote access include remote access servers and VPNs.

7.3.1. RAS

In the RAS model, a remote client uses the telecommunications infrastructure (dial-up) to create a temporary physical circuit to a port on a remote access server. After the physical circuit is made, connection parameters are negotiated.

For additional security, the remote access server can be configured to call back users at a predefined number. This works well for static users but not for mobile users. Remote access servers typically offer asynchronous serial interfaces connected to external analog modems, ISDN terminal adapters, or direct analog/ISDN connections. Remote access servers are application-specific computer systems dedicated to the support of LAN to WAN connections.

Proprietary remote access servers are designed to handle a mix of protocols and remote node capabilities, and some offer remote control capabilities. Clients dial in using point-to-point protocol (PPP) and serial line internet protocol (SLIP) encapsulation while the RAS handles the user's attachment, control, and protocol assignment.

RAS implementations typically provide user credential authorization services. Common industry standard security features include password authentication procedure (PAP), challenge

handshake authentication protocol (CHAP), and other feature-enhanced proprietary authentication capabilities.

Many RAS systems support security software protocols such as RADIUS. Other RAS security features include password encryption and data encryption.

7.3.2. VPN

A VPN provides security through encryption and authentication, helping to protect the data as it moves over the public Internet. A VPN client uses the Internet to create a virtual point-to-point connection with a remote VPN server. VPN servers are found in many different devices. They can be a network appliance designed exclusively to perform this function. Many network routers offer this feature, and even Microsoft Windows and Linux servers can function as VPN servers. The ConneXium Industrial firewall includes a VPN feature. Once a VPN session is established, a VPN client can access a system in the control network such as an engineering workstation or SCADA client. Microsoft Windows incorporates a remote desktop feature that allows connection to a remote system via the remote desktop protocol (RDP). Other software packages are also available for Windows, Linux, Android and iPhone devices. Here are some examples:

- Teamview
- Splashsoft
- LogMeIn
- Chrome Desktop
- VNC

Schneider Electric recommends that you use network access control (NAC) when using a VPN.

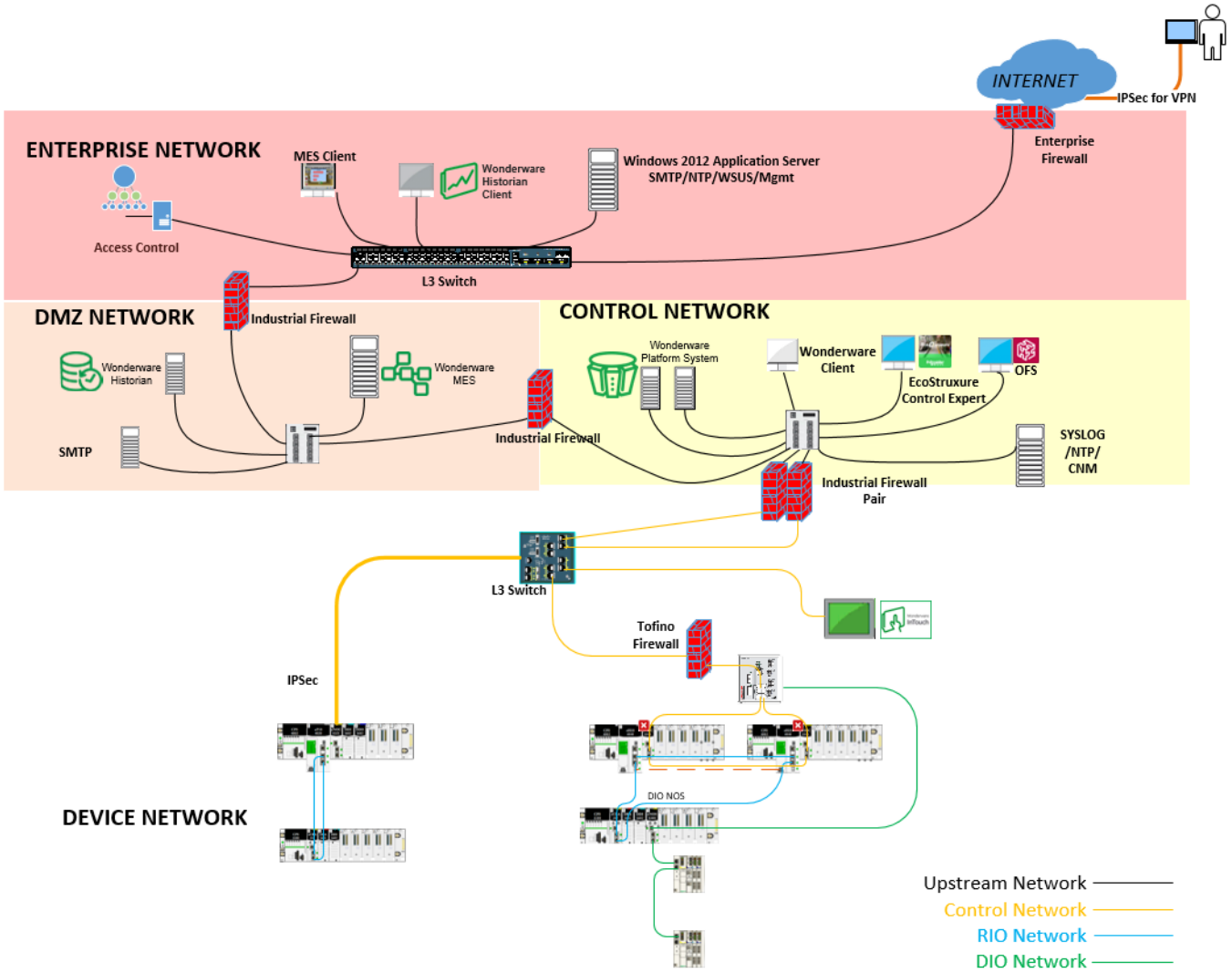


Figure 25: IPsec VPN Access Point in EcoStruxure Plant Architecture

Commonly used VPN technologies include transport layer security (TLS), secure socket layer (SSL) and the open standard Internet protocol security (IPsec).

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of a reliable transport protocol (e.g., TCP), is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- The connection is private. Symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.
- The connection is reliable. Message transport includes a message integrity check.

The TLS Record Protocol is used for encapsulation of various higher- level protocols. One such encapsulated protocol, the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties:

- The peer's identity can be authenticated using asymmetric, or public key, cryptography. This authentication can be made optional, but is generally required for at least one of the peers.
- The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.
- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.[6]

SSL is the predecessor to TLS and is a common protocol built into most Web browsers. SSL is easier to configure than IPsec and it does not require special client software. However, SSL only works for Web-based (TCP) applications and only supports Digital Signature.

VPN with IPsec provides more of the security features required for remote access to industrial control systems. IPsec is transparent to the application and uses IP network-layer encryption to provide private, secure communications over Internet Protocol (IP) networks. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection.

IPsec supports both digital signature and secret key algorithm.

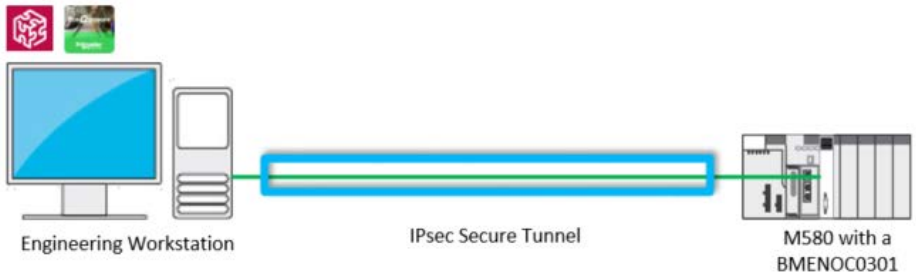


Figure 26: IPsec

IPsec is a suite of standards for performing encryption, authentication, and secure tunnel setup. IPsec essentially creates private end-to-end tunnels out of the public bandwidth available on the Internet. IPsec uses the following components:

- Internet key exchange (IKE and IKEv2)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

[6] https://tools.ietf.org/html/rfc5246

IPsec can be used in transport mode or, as recommended by Schneider Electric, in the tunnel mode.

Transport mode connections are host-to-host. Only the data payload of the IP packet is encrypted and/or authenticated.

In tunnel mode, connections can be established using gateway-to-gateway, gateway-to-host, or host-to-host architectures. The entire IP packet is encapsulated to provide a virtual secure hop between two gateways and a secure tunnel across an untrusted Internet.

IPsec VPN tunnel uses algorithms to encrypt and decrypt user information. The three common encryption protocols are:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- Triple-DES (3DES) - effectively doubles encryption strength over DES.

A one-way encryption algorithm known as a hash takes an input message of arbitrary length and produces a fixed-length output message. Hash algorithms are used by Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP) to authenticate data. Popular hash algorithms include:

- Message Digest 5 (MD5): 160-bit key. Although still widely used today it is not recommended for use. This messages digest has been susceptible to multiple vulnerabilities.
- Secure Hash Algorithm 2 (SHA-2): generates a variable length message digest. SHA-2 message digest lengths can vary from 224 to 512 bits. Sites using SHA-1 should look to migrate to SHA-2. Due to the ever-increasing computing power of attacking devices, a SHA-1 160 bit message digest can be susceptible to being cracked.

7.3.3. ConneXium Industrial Firewall VPN Features

The ConneXium Industrial Firewall supports the following VPN functions:

- Multipoint VPN: Router Mode
- VPN protocols: IPsec
- Encryption algorithms:
  - DES-56
  - 3DES-168
  - AES-128, AES-192, AES-256
- Authentication:
  - Pre-shared key (PSK)
  - X.509v3 certificates
- NAT-T support

7.3.4. Remote Access Vulnerabilities

- Inadequate access restriction.
- Firewall filtering deficiencies.
- Services allowed into the control system network.
- War dial-ups (computer dialing consecutive telephone numbers seeking a modem).
- Connection passwords programmed with vendor's default password.
- Access links are not authenticated and/or encrypted.
- Wireless has additional challenges because radio waves propagate outside the intended area:
    - Attackers who are within range can hijack or intercept an unprotected connection.
    - Wardriving is a common form of attack where a person in a moving vehicle uses a portable computer or PDA to search for a wireless device.

7.3.5. Remote Access Guidelines

- Approve and install remote access enabling hardware and software in strict accordance with security policies.
- Disable remote access when not needed. Enable it only when the access is required, approved, and authenticated. Consider risk to the process when allowing remote access.
- Change the password immediately after a remote maintenance session has terminated.
- For remote connections via dial-up modem or over the Internet, use an encrypted protocol such as IPsec. Once connected, require a second authentication at the control network firewall using a strong mechanism, such as a token-based multi-factor authentication scheme.
- Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts.
- Change or delete any default passwords or User IDs. Change passwords periodically.
- For remote access modems, change default settings as appropriate:
    - Set dial-out modems to not auto answer.
    - Increase ring count before answer.
    - Use inactivity timeout if available.
    - Use callback whenever possible.
- Weigh the benefits of VPN usage against potential impacts.
- Configure the firewall for a VPN connection using a tunnel network-to-network configuration.

7.4. Access for Remote Control

Some applications require remote control, and in some cases, the latency introduced by a firewall can be unacceptably high for the remote-control application. Therefore, remote access for remote control is sometimes allowed without going through a firewall. A security risk analysis by the organization is required to balance risk versus functionality.

Remote control with wireless brings additional security challenges. When remote control via wireless is needed, the recommended approach is to use VPN tunnel with IPsec as shown in the following figure. Configure firewall rules in ConneXium switches to allow connection via a VPN tunnel. For instance, to allow a VPN dial-in to the switch acting as VPN gateway, configure a firewall rule allowing incoming messages from a client to the network.

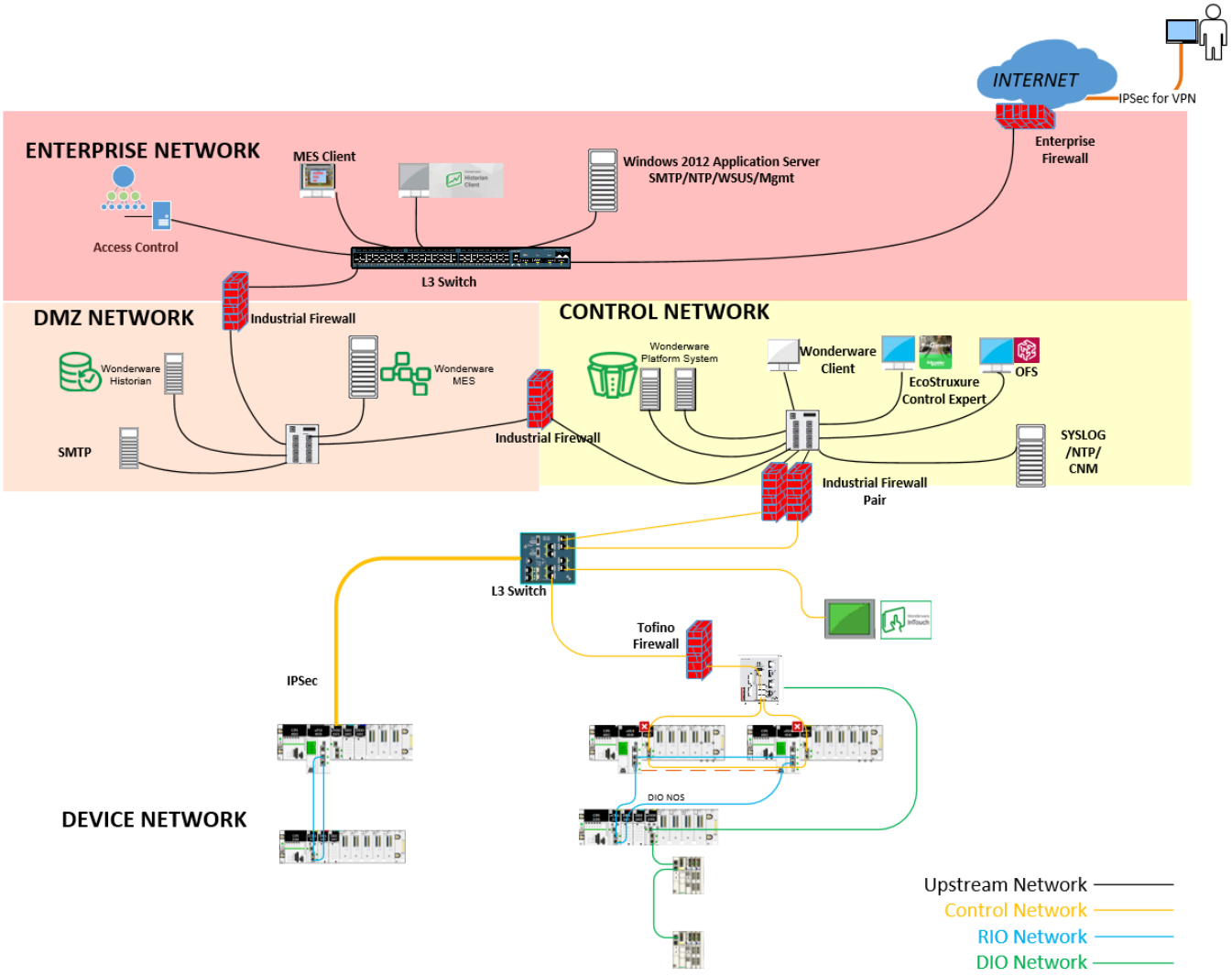


Figure 27: VPN Tunnel and IPsec to Help Mitigate Remote Control Risks

7.4.1. VPN Access with a ConneXium Industrial Firewall

A virtual private network (VPN) refers to the part of a public network that someone uses for their private purposes. The special feature of a VPN, as the name “private” suggests, is that it is closed off from the public network. Different measures help protect the data of the virtual private network from spying, data falsification and other attacks from external subscribers.

In the industrial environment, for example, a VPN serves to connect two plant sections with each other via the public Internet.

The ConneXium Industrial Firewall (TCSEFEC) includes a VPN feature that can permit a secure VPN session to multiple plant networks over the Internet. This is accomplished in a secure way by using Internet Protocol Security encryption (IPsec) and Internet Key Exchange authentication (IKE). IPsec is the most commonly used VPN protocol. IPsec regulates the configuration of a VPN connection and the methods for secure data transmission in the virtual private network.

Secure data transmission in a VPN involves:

- Integrity protection

  Integrity protection seeks to limit transmissions to only genuine data, i.e. that it comes from a trustworthy sender (is authentic) and that the recipient receives the data in an unfalsified form.

- Encryption

  Encryption limits the ability to view data to only authorized subscribers. Encryption procedures encode the data to be transmitted using an identifier (key) that is exclusively available to the authorized communication subscribers.

- Traffic flow confidentiality

  Traffic flow confidentiality hides the identity of a data packet's sender and recipient, so that no unauthorized party can obtain this knowledge. IPsec performs this function in tunnel mode by encrypting the complete IP packet.

  IPsec uses IKE for authentication, for exchanging keys, and for agreeing on additional parameters for the creation of a secure VPN connection.

- Authentication

  Use authentication as part of the security arrangement. During authentication, the connection partners show each other their ID cards, so to speak.

  This ID card can consist of:

  - A pre-shared key, which is a character string previously exchanged via a different communication channel.
  - A digital certificate, which was issued by a certification authority (CA). Certificates based on the X.509 standard contain, for example:
    - Information about the certification authority itself.

- Validity period of the certificate.
- Information describing the permitted usage.
- The identity of the person to whom the certificate is assigned (X.500DN).
- The public key associated with to this identity.
- The digital signature for verifying the connection between this identity and the related public key.

- Encryption

To help protect the data, IKE uses various cryptographic algorithms to encrypt the data. The endpoints of the VPN connection require the key to code and decode the data.

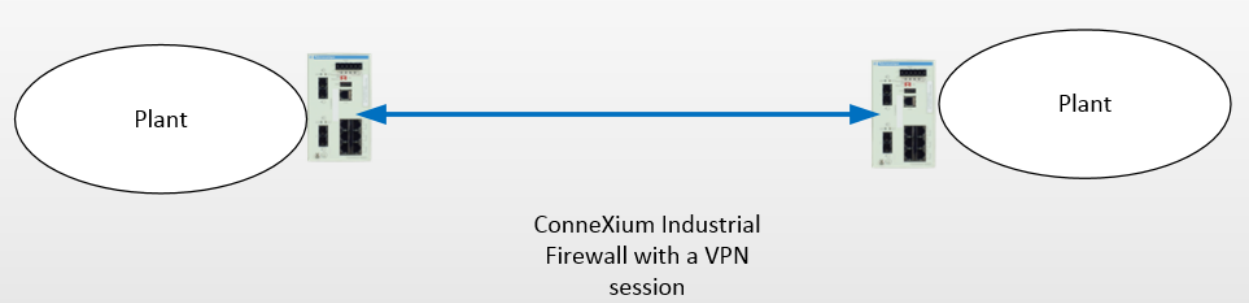


Figure 28: VPN Tunnel for Plant to Plant Secure Communication

The TSCEFEC has 3 modes of operation, Transparent, Router or Point to Point Protocol over Ethernet (PPPoE).

- When Transparent mode is used, the network is based upon layer 2 of the ISO/OSI 7-layer model. The IP address ranges before and after the firewall are in the same subnetwork.
- When Router mode is used, the network is based on Transmission on layer 3 of the ISO/OSI 7-layer model. The IP address ranges before and after the firewall are in different subnetworks.
- In PPPoE mode VPN access via the public telephone network using a device from a telco or service provider.

7.4.2. WiFi Remote Control Vulnerabilities

Vulnerabilities associated with IEEE 802.11 wireless include:

- Security settings either not configured or configured for poor security.
- Radio waves that propagate outside the intended area.
- Vulnerability to eavesdropping.
- Physical locations that permit easy access.
- Lack of security polices for setting up a wireless network.
- Attackers who are within range can hijack or intercept an unprotected connection.

- War driving - a common form of attack where a person is searching for a wireless device in a moving vehicle, using a portable computer or PDA.

Consider installing an NAC control system to help protect against WiFi vulnerabilities.

7.4.3. NIST Wireless Guidelines

The following wireless LAN guidelines were published by the National Institute of Standards and Technology (NIST) in its Special Publication 800-82: Guide to Industrial Control Systems as they are quoted below:

- *Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas.*
- *Wireless users' access should use IEEE 802.1x authentication using a secure authentication protocol (e.g., Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via a user certificate or a Remote Authentication Dial In User Service (RADIUS) server.*
- *The wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible) connections to the ICS network.*
- *Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, and enable MAC filtering at a minimum.*
- *Wireless devices, if being used in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain.*
- *Wireless device communications should be encrypted and integrity-protected. The encryption must not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.*
- *For mesh networks, consider the use of broadcast key versus public key management implemented at OSI Layer 2 to maximize performance. Asymmetric cryptography should be used to perform administrative functions, and symmetric encryption should be used to secure each data stream as well as network control traffic. An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible supporting rapid network recovery in*

the event of a detected failure or power loss. The use of a mesh network may provide fault tolerance thru alternate route selection and pre-emptive fail-over of the network. [7]

7.5. Internal Access for Service or Vendor Personnel

Before allowing any computer to communicate in an industrial control network, check that it is properly configured, including cybersecurity settings and software, and free of malware.

At a minimum, manually check that all applications, operating systems, and antivirus software are at the latest patch levels.

Consider the use of Network Access Control (NAC) systems to perform security checks automatically. A NAC can control access to a network by applying a set of rules to a device when the first attempts to access the network. These rules typically regulate antivirus protection level, applications, operating system patch levels, and configuration. NAC systems may also integrate the automatic remediation process (fixing non-compliant computers before allowing access) into the network systems before communication is allowed.

NAC systems control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

NAC systems are used mainly for endpoint health checks and are often used with role-based access policies. Depending on a person's profile and the result of a posture or health check, access to the network is granted or denied.

A major benefit of using a NAC solution is the ability to block access by devices that lack appropriate antivirus software, application patch levels or host intrusion prevention software. Such devices would otherwise place other devices on network at risk of cross-contamination.

NAC support is available in many current operating systems such as Windows 7 and Windows Server 2012 R2.

[7] Guide to Industrial Control Systems (ICS) Security NIST special publication 800-82 revision 2 May

8. Device Hardening

Device hardening is the process of configuring various settings to strengthen security on devices such as those shown in Figure 29.

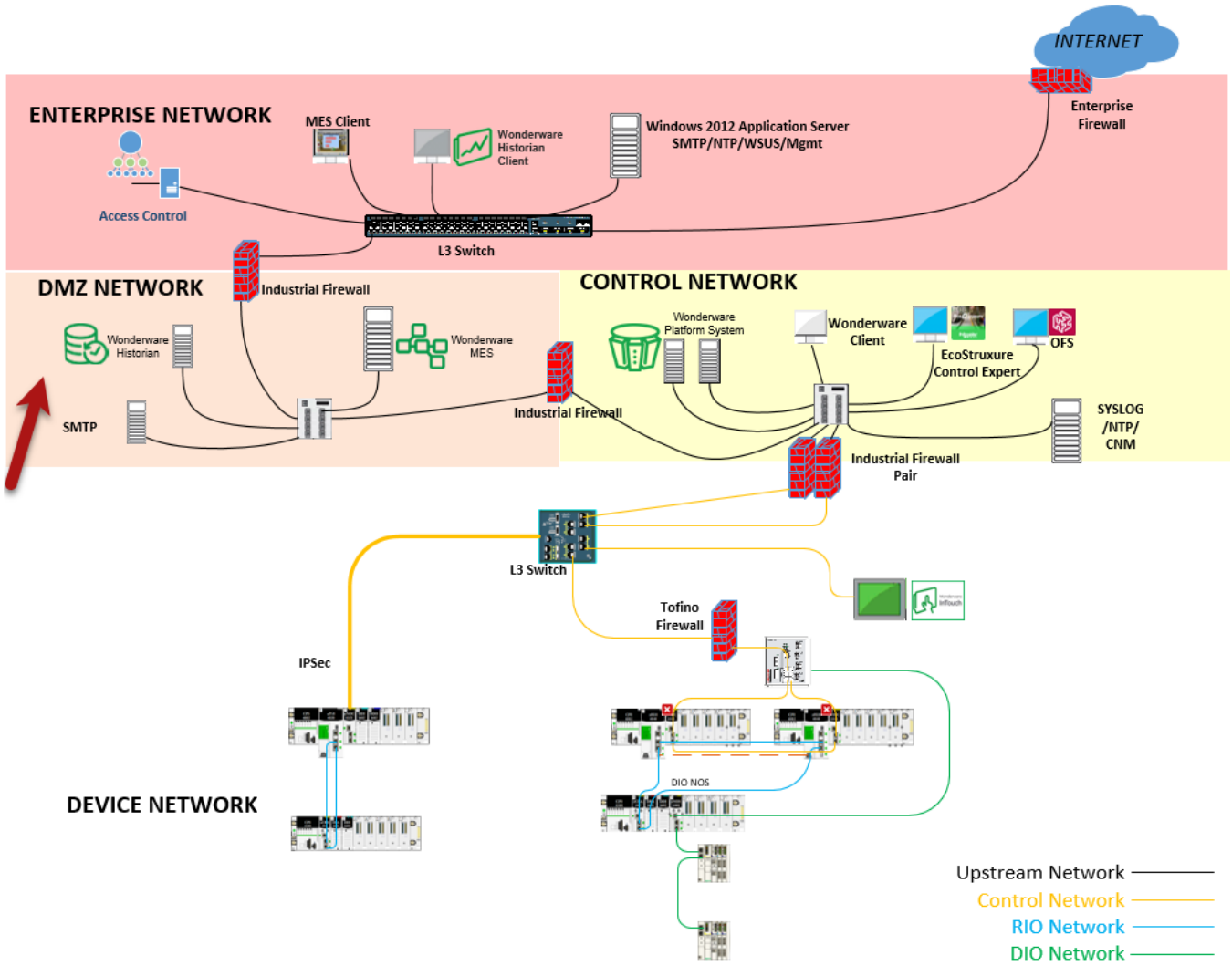


Figure 29: Device Hardening in EcoStruxure Plant Architecture

Device hardening applies to all devices below the DMZ including routers, firewalls, switches and other devices on the network such as SCADA and PACs. Examples of device hardening actions, tools, and methods include:

- Password management including encryption
- Disabling of unused services
- Access Control
- Patches, hot fixes, application updates
- Strong authentication

The following sections describe how some of these activities, tools, and methods are used in an EcoStruxure Plant environment.

8.1. Password Management

Password management is one of the fundamental tools of device hardening. Passwords are often neglected in industrial control systems. Policies and procedures on password management are often inadequate or missing entirely.

8.1.1. Password Management Guidelines

- Enable password authentication on all e-mail and Web servers, PACs, Ethernet interface modules, and embedded Web servers.
- Change all default passwords immediately after installation, including those for:
  - User and application accounts on Windows, SCADA, HMI and other systems
  - Scripts & source code
  - Network control equipment
  - Devices with user accounts
  - FTP Servers
- Grant passwords only to people who need access. Prohibit password sharing.
- Passwords should be hidden, and not displayed during password entry:
  - Require passwords that are difficult to guess. They should contain at least 8 characters and should combine upper and lowercase letters, digits, and special characters when permitted.
- Require users and applications to change passwords on a scheduled interval.
- Remove employee access account when employment has terminated.
- Require use of different passwords for different accounts, systems, and applications.
- Maintain a secure master list of administrator account passwords so that they can quickly be accessed in the event of an emergency.
- Implement password management in a way that does not interfere with the ability of an operator to respond to an event such as an emergency shutdown.
- Passwords should not be transmitted via e-mail or in any other way over the insecure Internet.

8.2. Device Access Control

Another aspect of device hardening is device-level access control. For instance, a Schneider Electric device might maintain an access control table with a list of approved addresses, and the

device would accept only access requests that originate from those addresses. This type of access control is useful in controlling access between different areas of the plant.

8.2.1. Access Control Guidelines

Access control should be implemented at all levels: servers, workstations, firewalls, switches, and devices.

Use access control lists such as the one shown in the following Schneider Electric Ethernet module configuration screen to list the addresses from which a TCP connection request will be allowed.

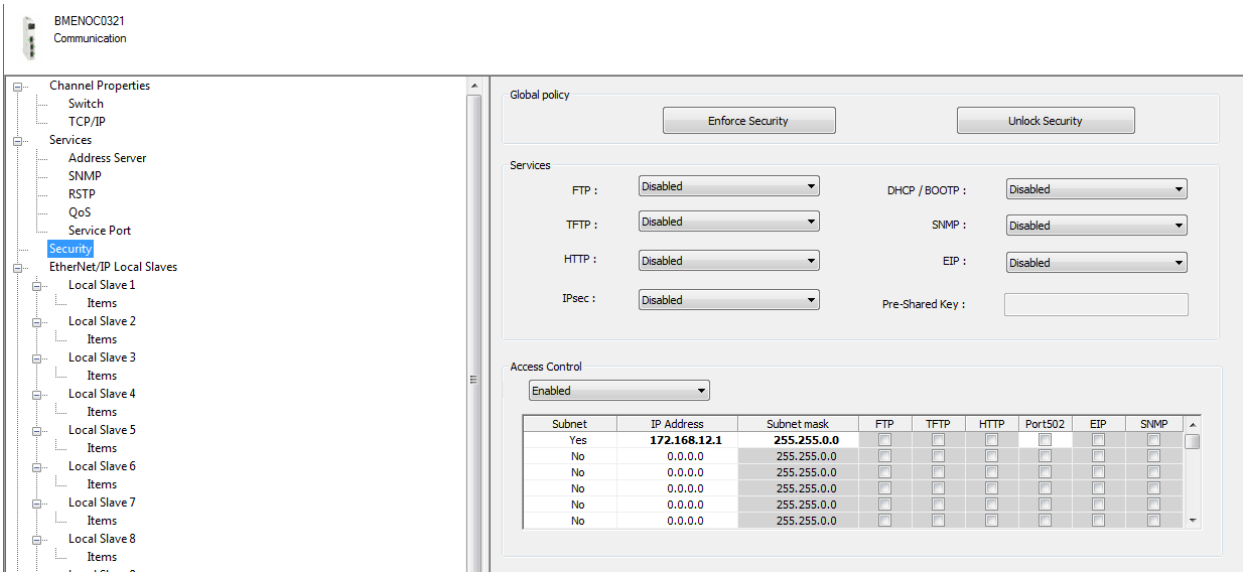


Figure 30: Sample TCP Connection Access Configuration

8.3. Hardening Modicon M580

8.3.1. M580 Security

The Modicon M580 PAC platform is cybersecurity ready. It has embedded security that conforms to the ISA/IEC 62443 standard. ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). In addition, the Modicon M580 PAC has achieved an Achilles Level 2 certification. With this certification, firmware integrity is checked at every start-up, and is compiled and stored in memory, helping to prevent its decompilation by a third party. Within the M580 platform:

- Unused services can be disabled (FTP, HTTP, SNMP).
- Remote access can be controlled.
- IPsec security protocol can be used between the control network and the end device.

- Program software provides an integrity check with EcoStruxure Control Expert application suite.
- Traceability of system events via syslog.

Please see the Security Tab of the M*odicon M580 Hardware Reference Manual* for further details.

8.3.2. Security Settings from EcoStruxure Control Expert:

You enable or disable the following Modicon M580 Ethernet services using the **Security** tab in EcoStruxure Control Expert:

Field	Parameter	Value	Comment
FTP	-	Disabled	Disables firmware upgrade, CD memory card remote data access, and. Note: Data storage is optional
TFTP	-	Disabled	Disabled the ability to read RIO drop configuration and device configuration management using the FDR service.
HTTP	-	Disabled	Disables the web service access
Achilles Level 2	-	Enabled	Setting the feature to Enabled increases Ethernet frame filtering to improve the level of security and robustness. Setting the feature to Disabled increases system performance by reducing the Ethernet frame filtering capability.
Access Control	-	Enabled	Deny Ethernet access to the Modbus and IEP server by unauthorized network devices.
Enforce Security and Unlock Security	-	-	See the following paragraph for details.
Unauthorized addresses	IP Address	0.0.0.0…. 255.255.255.255	You can modify this field when you set Address Control to Enabled
	Subnet	YES/NO	
	Subnet mask	0.0.0.0…. 255.255.255.255	

Table 2: M580 Security Settings

Schneider Electric recommends disabling services that are not being used.

Set the **Security** tab parameters before you download the application to the CPU. The default settings (maximum security level) reduce the communication capacities and port access.

Using the Enforce Security and Unlock Security Fields:

Click **Enforce Security** (the default setting) to set the fields in the **Security** tab to their maximum security level:

- **FTP**, **TFTP**, and **HTTP** are set to **Disabled**.
- **Achilles level 2** and **Access Control** are set to **Enabled**.

Click **Unlock Security** to set these fields to their minimum security level:

- **FTP**, **TFTP**, and **HTTP** are set to **Enabled**.
- **Achilles level 2** and **Access Control** are set to **Disabled**.

Note: You can set each field individually after the global setting is applied.

Defining the List of Authorized Addresses:

The list of authorized addresses applies only to the devices that can communicate with the M580 CPU via the port 502 server or the EtherNet/IP server. The list also applies to CPU firmware downloads.

When access control is enabled, add the IP addresses of the authorized addresses. Devices can communicate only with authorized addresses. To define the list of authorized addresses, enter one of the following:

- an IP address in the **IP Address** table column with **NO** selected in the **Subnet** column.
- a subnet address in the **IP Address** table column with **YES** selected in the **Subnet** column and a subnet mask entered in the **Subnet Mask** column.

The subnet in the IP Address column can be the subnet itself or any IP address of the subnet. If you enter a subnet without a subnet mask, a detected error is displayed stating that the screen cannot be validated.

You can enter up to 128 authorized IP addresses.

Refer to the TDVA *How Can I Reduce Vulnerability to Cyberattacks in an M580 Functional Unit*? which contains detailed information on Cybersecurity for the Modicon M580 PAC.

8.3.3. Modicon M580 IPsec via BMENOC03x1

The Internet Engineering Task Force (IETF) developed and designed Internet Protocol Security (IPsec) as an open set of protocol standards that make IP communication sessions private and secure. The IPsec functionality of the BMENOC03x1 modules supports the data integrity and origin authentication of IP packets.

Additional functionality of the BMENOC03x1 module include the following:

- The module operates in a network that uses the RSTP protocol.

- The module configures IP parameters and device configuration files for I/O devices in the control network.
- The module supports Hot Standby functionality.
- The module scans I/O devices in the control network.

Follow the steps from the Modicon M580 BMENOC03x1 Control Network Module Installation and Configuration Guide to create a specific IPsec configuration on a Windows 7 PC. For more information about IPsec, refer to the Internet Engineering Task Force website (www.IETF.org). Client-initiated communications are not supported from the BMENOC03** Ethernet communication module when IPsec is enabled. For example, peer-to-peer (BMENOC03x1-to-BMENOC03x1) communications are not supported when IPsec is enabled.

Note:

- You cannot enable the IPsec protocol and the IP Forwarding service at the same time. (You cannot build a EcoStruxure Control Expert project when both are enabled.)
- Use Unity Pro 11.1 (and higher) with DTM v3.6.x (and higher) to run IPsec.

8.4. Hardening ConneXium Ethernet Managed Switches

The following ConneXium managed Ethernet switch features can be configured to harden the switch and help protect against unauthorized users:

- SNMP
- Telnet or Web access
- Ethernet Switch Configurator Software
- Port access control via IP or MAC address

8.4.1. SNMP

SNMP v1, v2 and v3 are supported by the ConneXium managed Ethernet switches. By default, SNMP v1 and v2 are activated with default passwords public for read access and private for read/write access. For SNMP guidelines, see SNMP Risk Mitigation (p.58).

8.4.2. Telnet and Web Access

The ConneXium managed Ethernet switch telnet server supports device configuration via command line interface over telnet and by access to the switch's embedded Web pages. On delivery, both servers are activated. To harden the switch:

- Change the default read and read/write passwords for the telnet and Web servers
- Deactivate the telnet server if not using the command line interface to configure switch.
- After configuration and operational verification, disable the Web server.

Note: If both the telnet server and the Web server are disabled, the switch's V.24 port will be the only remaining access port.

8.4.3. Ethernet Switch Configurator Software Protection

The Ethernet Switch Configurator Software protocol allows users to assign an IP address, net mask, and default gateway IP to a switch. As part of device hardening, after assigning the IP parameters to the device, disable the Ethernet Switch Configurator Software function in the Ethernet Switch Configurator Software Protocol frame or limit the access to read-only.

8.4.4. Ethernet Switch Port Access

A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall to defeat its incoming filtering protection.

Ethernet switches maintain a table called the Content Address Memory (CAM) that maps individual MAC addresses on the network to the physical ports on the switch. In a MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses filling the CAM table. Once the CAM table is full, the switch becomes an Ethernet hub allowing all incoming packets to be broadcast on all ports. The attacker then could use a packet sniffer (such as Wireshark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and instant messaging conversations), which would not be accessible were the switch operating normally.

The following device hardening methods help to mitigate these vulnerabilities:

- Disable unused ports.
- Lock specific MAC addresses to specific ports on the Ethernet switch.
- Lock specific IP addresses to specific ports on the Ethernet switch.

8.5. Hardening Wonderware SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems are used in industrial control for data collection, human interface, and data analysis. Schneider Electric's Wonderware ArchestrA platform is an example of this functionality. SCADA systems, due to their typical PC-based architecture, simple access to process control functions, and criticality to the process, are vulnerable devices on the control system network.

Steps required to harden the SCADA system include:

- Grant physical access to the hosting server only to system administrators or similar authorized personnel.

- Keep logical access to the physical server within a dual-firewall DMZ, along with other systems such as workstations, Wonderware Historian and OFS. Use industrial stateful firewalls, such as the ConneXium Industrial Firewall devices.
- Provide dedicated operator and developer access to the server via Wonderware InTouch. Install developer tools only on dedicated Integrated Development Environment (IDE) workstations, and not on a running production ArchestrA Automation Object Server (OAS).
- Harden the PC server and its operating system via strong and unique user and administrative account passwords. Use enterprise grade operating systems, such as Windows 2012R2 Standard Server, for the data execution prevention (DEP) and user account controls (UAC) capabilities provided by these operating systems. Patch operating system to current required levels on a documented, monitored schedule.
- Disable or remove unused programs and services. Run Wonderware InTouch with non-administrative privileges only. The Integrated Development Environment (IDE) can be installed but not on production servers.
- Hardening of servers, particularly user account management and patching, should be a continuous improvement process. All file systems should be NTFS.
- Limit information access by configuring roles within the Galaxy security model.
- Web and e-mail access on systems directly on or accessing any ArchestrA system is not recommended. That includes the Galaxy Repository (GR) Server, IED workstations and OAS servers. Disable or severely restrict Web and e-mail access for any system in the control room.
- Use multiple digital signatures.
- When possible, test any changes such as patching and installation in a dedicated closed test environment prior to production rollout.
- Implement Microsoft Windows authentication. Use Active Directory for central management if possible.
- Routinely track and monitor audit trails to identify suspicious activity and remedy the activity immediately.
- Configure mirrored servers such as the historian in the DMZ for external access, and not for direct access on the control system network.
- Validate that there are no IP addresses for non-required devices on the access list.
- When possible, use white listing products on all servers and clients instead of antivirus products. White list products tend to be less resource-intensive than antivirus tools and they offer stronger protection against zero-day threats.
- If antivirus products are used, keep the software and virus definitions current. Because antivirus updates can affect production, consider a risk-benefits assessment to help determine appropriate scheduling.

- ArchestrA security is designed to help prevent users from gaining unauthorized access. The system is not designed to stop malicious access. Use Microsoft Windows authentication to restrict users from accessing any application on an ArchestrA server. Use systematic password maintenance procedures like those used in IT-managed systems.
- Allow no e-mail or Web access on the Citect server or on machines that connect to the server.
- If the server cannot be placed in a secure physical location, establish some form of access control process.
- Disable or remove CD-ROM drives.
- Disable USB ports not used by the keyboard or mice.
- Close all remote units when not in use. Establish and enforce procedures to log out of or screen-lock any clients.
- Use dual stateful firewalls such as ConneXium Industrial Firewalls.

8.6. Hardening Wonderware Historian

Wonderware Historian is a centralized reporting tool for industrial control environments. Because it has many touch points to other industrial systems like the Wonderware Historian Client or SmartGlance, it is vulnerable to cyberattacks. Use the following steps to help harden the system:

- Locate client, server, and database components on separate machines if possible.
- Patch MS SQL databases on a documented, monitored schedule to check that MS SQL SA passwords are strong and differ from other passwords.
- Harden all hosting servers and client workstations. See Hardening Wonderware SCADA Systems (p.81) for examples of relevant server and client hardening methods.
- Locate the database server and Historian server within the same DMZ as the Wonderware SCADA.
- Use ACLs to control client access to the Historian Web portal in the ConneXium Industrial Firewall that separates the control network from the enterprise network.

8.7. Hardening OPC Factory Server (OFS)

The OFS product provides computer client applications with a group of services (methods) for access to variables of target PAC devices. Because OFS has networked access to control systems, it is a target vector for attacks against industrial assets.

- Patch the hosting server on a documented, monitored schedule.
- Harden the server. See Hardening Wonderware SCADA Systems (p. 81) for examples of relevant server and client hardening methods.

- Locate the server and client in the same DMZ, and if possible, on the same host. OFS requires DCOM services to operate if the client and the server are remote. DCOM requires many ports to be open if the client and server are separated by a firewall. Locating client and server on same host reduces exposure to DCOM vulnerabilities.
- If Wonderware SCADA is present, install OFS on the same physical server.
- Allow only specific hosts and/or accounts to connect to the IIS server.
- Allow only specific hosts and/or accounts to connect to the FTP server.

8.8. Device Hardening for Legacy Drives

In many cases, industrial control systems include older devices that are not equipped with sufficient device hardening features. In this case, an external device can be applied in combination with the installed end device to improve the hardening.

Schneider Electric recommends use of the ConneXium Tofino Firewall to provide these features. Configure the firewall to use the same IP address as the internal device so the combination of the two units appears as a single end device to the rest of the network.

The single combined unit can also take advantage of the firewall's ability to limit network traffic, restrict access to allow only data requests from specific originating devices and even limit access to specific data register areas or use of specific function codes.

8.9. Industrial PCs for Enhanced Security

Industrial PCs, such as the Magelis Box PCs, can host software applications such as SCADA servers, MES Clients, and EcoStruxure Control Expert development environments. These are hardened PCs running Windows 7 or Windows 10 64-bit operating systems designed for the rigors of industrial environments. These systems were designed for low maintenance and can be installed in electrical enclosures for additional physical security. When such systems are enclosed, the keyboard, mouse, and display access can be implemented using an IP based KVM, such as the APC KVM2G.

Industrial PCs can also be used as platforms to host network intrusion detection systems such as Snort. Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. It combines the benefits of signature, protocol, and anomaly-based inspection.

These PCs can also host proxy server applications such as SQUID. Proxy servers can control traffic into and out of the DMZ, thereby providing additional isolation of the control room infrastructure from the enterprise. These systems are also suitable for hosting network management applications such as ConneXium's Configuration Manager.

8.10. Hardening Engineering Workstations

Customers may choose from a variety of commercial PC systems for their engineering workstation needs. Harden and manage these PCs using the same methods used to harden industrial PC systems. Key hardening techniques include:

- Strong password management
- User account management
- Methods of least privilege applied to applications and user accounts
- Removal or disabling unneeded services
- Removing remote management privileges
- Systematic patch management

Unlike the Schneider Electric industrial PC systems, which might be located in the more trusted control or device networks, these engineering workstations should be located within the operations network.

8.11. Patch Management

To reduce vulnerability to attacks, systems should be patched to the latest vendor-recommended software and firmware levels. This is particularly true with computer systems, such as SCADA hosts, that provide an element of control for the deeper layers of the industrial control networks. It is also true of devices on the control and field level networks.

Patch management and deployment approaches include automatic, semi-automatic, and manual. In all cases patch updates should be systematically planned, tested, and executed. Before releasing any patch to a production system, create a system backup with the ability to roll back configurations rapidly. Backups can be accomplished using tools such as Backup and Restore embedded within Windows. These tools are available from the Control Panel. Alternatively, software backup systems are available that have additional features like automated scheduling or using the cloud.

There are numerous ways to keep informed about the availability of new patches. These include subscriptions to free security bulletin services such as http://www.microsoft.com/security/ and http://www.sans.org/newsletters. In addition, vendor Websites for devices, application software, and operating systems can be monitored for updates.

More advanced server patching can be accomplished by hosting a patch management server in the DMZ supporting Windows Server Update Services (Microsoft WSUS server). This is local a repository of Microsoft hot fixes and service packs for operating systems and applications such as MS SQL Server. Local machines within the control room would connect to this server for patch management. Groups of patches would be predefined, tested, and authorized by system administrators prior to deployment.

EcoStruxure Control Expert includes an automatic update feature for downloading and installing the latest patches from a secure Schneider Electric site.

Firmware patching of other industrial control systems devices such as PACs, network switches, routers, firewalls, and distributed I/O may require system down time and should be performed on a carefully planned schedule. Some patches may address urgent issues and should be installed as soon as possible, regardless of the planned patch management schedule. The patch management plan should have specific guidelines for such exceptions. Even in these exception cases, include testing and backup procedures in the release plan.

Several utilities allow firmware to be deployed from the control room to the field level devices. These include OS Loader, Unity Loader and Web-based access. Use a dedicated machine in the operations network to deploy firmware. Some field devices cannot be remotely patched and will require local access. In these cases, connect only with a security-approved laptop free of malware with the latest OS updates installed.

9. Monitoring and Maintenance

Cybersecurity is a continual process. Monitoring and maintenance are necessary components of a defense-in-depth approach.

9.1. Monitoring

Through proactive monitoring, intrusion attempts can be detected and stopped before they can do any damage. There are several methods of monitoring the network for suspicious activity. They include:

- Routine examination of log files
- SNMP authentication traps
- Network load monitoring
- Use of an Intrusion detection system (IDS)

9.1.1. Log File Monitoring

- Monitor device event logs for unusual activity.
- Monitor MS Windows Event Viewer (Control Panel/Administrative tools/Event Viewer/Application Log) for unusual activity.
- Monitor log files produced by devices. For example:
    - M580 PAC log files
    - Alarm log files from PACs and other devices
    - Diagnostic log files such as those produced by ConneXium managed Ethernet switches
    - Syslog files such as those produced by ConneXium Industrial Firewalls

9.1.2. Simple Network Management Protocol (SNMP)

- Enable SNMP authentication traps on all devices that support SNMP to monitor for unauthorized login attempts.
- Use network diagnostic tools like ConneXium Network Manager to monitor and immediately investigate unusual traffic load. ConneXium Network Manager also provides alarms for notification if a new device connects to the network.

9.1.3. Intrusion Detection Systems

An intrusion detection system (IDS) monitors activity on the network for malicious traffic, and logs and reports traffic anomalies. A typical IDS monitors traffic patterns, file access, changes in port status, invalid password entries, and inoperable equipment.

Types of IDS include:

- Network intrusion detection system (NIDS). NIDS monitor traffic to and from all devices on the network by analyzing individual packets for malicious traffic. NIDS are often located at demilitarized zones or network boundaries. Snort is a NIDS.
- Host intrusion detection system (HIDS). A HIDS is an agent that runs on an individual host or device on the network and monitors traffic in and out of the host or device. It analyzes system calls, application logs, file system modifications and other host activities and states to identify intrusions. The agent is usually a software application. Tripwire and OSSEC are HIDS that are free open source solutions.

9.1.4. Security Information Event Management (SIEM)

Security Information Event Management (SIEM) systems are very advanced security products that not only provide network and host intrusion detection and protection, but also are combined with security event management. SIEM features include:

- Consolidation of log files – correlates disparate log files form multiple source/systems.
- Advanced analytics – examines events from multiple sources and identifies trends, possible threats, and solutions.
- Dashboard – tracks alerts and incidences in real time.
- Governance – monitors compliance to standards, generates reports, and provides auditing trails.
- History – long term data is retained for trends, auditing and forensics.

SIEM solutions are available from many system and network management companies. McAfee – a Schneider Electric CAPP partner – has been selected to provide security solutions, which include their SIEM product McAfee Security Enterprise manager.

9.2. Maintenance

Continual maintenance of the control system includes the routine, scheduled updating of antivirus software with the latest signatures and installing the latest patches for software and firmware used on devices in the network.

A periodic assessment and test of the control system network for security risks should be performed. Check that device configurations are appropriate for security. Use the latest security standards and practices and update as needed.

10. Mitigation Strategies

Mitigation is an approach to reduce the risk of a cyberattack. Most of the practices discussed in this document are part of a mitigation strategy. The Australian Department of Defense published a document named “Top 4” Strategies to Mitigate Targeted Cyber Intrusions. The four strategies are:

- Application Whitelisting
- Patch Applications
- Patch the Operating System
- Minimize Administrative Privileges

The document states that implementing the Top 4 will mitigate at least 85% of the intrusion techniques that the Australian Cyber Security Operation Center (CSOC) responds to.[8]

Application whitelisting is a security approach designed to help protect against unauthorized or malicious code executing on a system. Its aim is that only authorized applications (e.g., programs, software libraries, scripts and installers) can be executed.

While application whitelisting is primarily designed to help prevent the execution, and spread of malicious code, it can also help prevent the installation or use of unauthorized applications.

Implementing application whitelisting across an entire organization can be a daunting undertaking. However, implementation on systems used by high-value or often-targeted staff members, such as executive officers and their assistants, human resources staff, Freedom of Information staff or public relations staff, can be a valuable first step.[9]

Microsoft introduced a feature, in Windows 7 and Windows Server 2012 R2, called AppLocker. AppLocker allows you to specify the users or groups that can run specific applications in your organization based on unique identities of files. If you use AppLocker, you can create rules to allow or deny applications from running.

Today's organizations face several challenges in controlling application execution, including the following:

- Which applications can a user access and run?
- Which users should be allowed to install new software?
- Which versions of applications should be allowed?
- How are licensed applications controlled?

[8] https://www.asd.gov.au/publications/protect/top_4_mitigations.htm
[9] https://www.asd.gov.au/publications/protect/application_whitelisting.htm

To meet these challenges, AppLocker provides administrators with the ability to specify which users can run specific applications. AppLocker allows administrators to control the following types of applications: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.msi and .msp), and DLL files (.dll and .ocx). This helps reduce the organization's cost of managing computing resources by decreasing the number of help desk calls from users running inappropriate applications.[10]

The other 3 strategies (Patch Applications, Patch Operating Systems and Minimize Administrative Privileges) are discussed throughout this document.

Checkpoint Software Technology Limited lists the ASD (Australian Signals Directorate) Top 35 Mitigation Strategies.[11] They are:

Rank	Strategy
1	Application whitelisting
2	Patch applications
3	Patch operating system vulnerabilities
4	Restrict administrative privileges
5	User application configuration hardening
6	Automated dynamic analysis
7	User application configuration hardening
8	Host-based Intrusion Detection/Prevention System
9	Disable local administrator accounts
10	Network segmentation and segregation
11	Multi-factor authentication
12	Software-based application firewall, blocking incoming network traffic
13	Software-based application firewall, blocking outgoing network traffic
14	Non-persistent virtualized sandboxed trusted operating environment
15	Centralized and time-synchronized logging of successful and failed computer events

[10] https://technet.microsoft.com/en-us/library/dd759117(v=ws.11).aspx
[11] https://www.checkpoint.com/asd-top-35-mitigation-strategies/

Rank	Strategy
16	Centralized and time-synchronized logging of allowed and blocked network activity
17	Email content filtering
18	Web content filtering
19	Web domain whitelisting for all domains
20	Block spoofed emails
21	Workstation and server configuration management
22	Antivirus software using heuristics and automated Internet-based reputation ratings
23	Deny direct Internet access from workstations
24	Server application configuration hardening
25	Enforce a strong passphrase policy
26	Removable and portable media control
27	Restrict access to Server Message Block (SMB) and NetBIOS
28	User education
29	Workstation inspection of Microsoft Office files
30	Signature-based antivirus software
31	TLS encryption between email servers
32	Block attempts to access websites by their IP address
33	Network-based Intrusion Detection/Prevention System
34	Gateway blacklisting
35	Capture network traffic

Table 2: 35 Top Mitigation Recommendations

Click on an underlined recommendation, above, to link to the Checkpoint web site for additional information.

The US ICS-CERT organization also published a document on Malware Threats and Mitigation Strategies.

10.1. SE Cybersecurity Support Portal

Schneider Electric's vulnerability management policy is to address cybersecurity vulnerabilities affecting Schneider Electric products and systems for the purpose of supporting the security and safety of our installed solutions, and helping to protect our customers and the environment.

We work collaboratively with researchers, Cyber Emergency Response Teams (CERTs), and asset owners to provide accurate information in a timely fashion to help protect their installations. Schneider Electric's Corporate Product CERT (CPCERT) is responsible for managing and providing alerts relating to vulnerabilities and mitigations affecting products and solutions. The CPCERT coordinates communications between relevant CERTs, independent researchers, product managers, and all affected customers.

All public notifications and postings relating to vulnerability management released by Schneider Electric are located at the following URL:

http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp

Schneider Electric follows an ISO 30111-conformant vulnerability handling process:

- Receive information regarding a potential vulnerability.
- Evaluate the potential vulnerability and, if confirmed, identify affected products.
- Mitigate the vulnerability.
- Disclose the vulnerability.

Receive

Schneider Electric provides a web site form to permit anyone aware of a potential vulnerability or a cyber incident to securely submit a report to Schneider Electric's CPCERT. The contact form is available by clicking on the "Report an incident or vulnerability" button on the Schneider Electric Global web site.

Alternatively, interested parties are free to send the same information via email to:

cybersecurity@schneider-electric.com.

Schneider's CPCERT will respond to confirm receipt and follow-up with any questions. Schneider Electric provides a PGP public key to support secure submission of information by email. Schneider Electric strongly encourages reporting of all product or system vulnerabilities, regardless of the stage of a product's lifecycle. We value all such information and respect the confidentiality of the reporting entity. We strive to maintain active and secure communications with the reporting entity and coordinate the disclosure to help protect asset owners, the public, and the environment. We encourage reporting entities to support our disclosure policy to provide asset owners adequate time to protect their systems with the mitigation strategies we define.

Evaluate

Schneider Electric's CPCERT will analyze the potential vulnerability. The CPCERT will report back to the reporting entity with our conclusion or a request for more information. If a submitted vulnerability is determined to be valid, Schneider Electric will perform an assessment of the vulnerability to determine the risk to customers; products affected, field population, and severity.

Mitigate

Schneider Electric will assess all affected Schneider Electric products and prepare a mitigation plan. Schneider Electric identifies all affected products, determines the root cause of the issue, and develops a resolution or remediation. During this phase, the CPCERT strives to maintain active and secure communications with the reporting agency regarding any mitigations, potentially including advisories, patches, or updates.

Disclose

Once a mitigation is available, Schneider Electric will prepare and release a disclosure. General disclosures are published on the Schneider Electric corporate web site, unless the disclosure is limited to a specific group of customers, in which case customers may be contacted directly to support remediation. Each disclosure announcement contains: ·

- Overall description of the vulnerability and its severity (based on CVSS score).
- Identification of products and versions affected.
- Availability of patches or mitigating actions to reduce the risk of exploitation, including patch download instructions where applicable.

Schneider always encourages customers to take advantage of these updates and/or instructions and patch their installations appropriately. With the consent of the reporting party, Schneider Electric will identify the researcher to give credit for their discovery.

You can contact Schneider Electric's Corporate Product CERT Website at:

http://www.schneider-electric.com/b2b/en/support/cybersecurity/overview.jsp

Or email us at: Cybersecurity@schneider-electric.com

11. EcoStruxure Plant Security Architecture

This section builds on the defense-in-depth recommendations provided in the previous sections of this document. It shows how to apply these recommendations to an EcoStruxure Plant architecture by providing expanded detail on:

- Security zones
- Location and function of firewalls
- Data flow between security zones
- Device security settings

The EcoStruxure Plant security architecture recommendations in this section are limited to single-site communications with no plant-to-plant or external to plant communications. Specific EcoStruxure Plant wireless and remote access security recommendations are beyond the scope of this section.

The wireless and remote access security discussions in other sections of this STN are general in nature and provided for informational purposes only.

This STN describes general security settings for devices in the EcoStruxure Plant security architecture.

11.1. EcoStruxure Plant Security Architecture Overviews

Figure 31 shows a baseline EcoStruxure Plant architecture. Figure 32 shows the same architecture with defense-in-depth security recommendations.

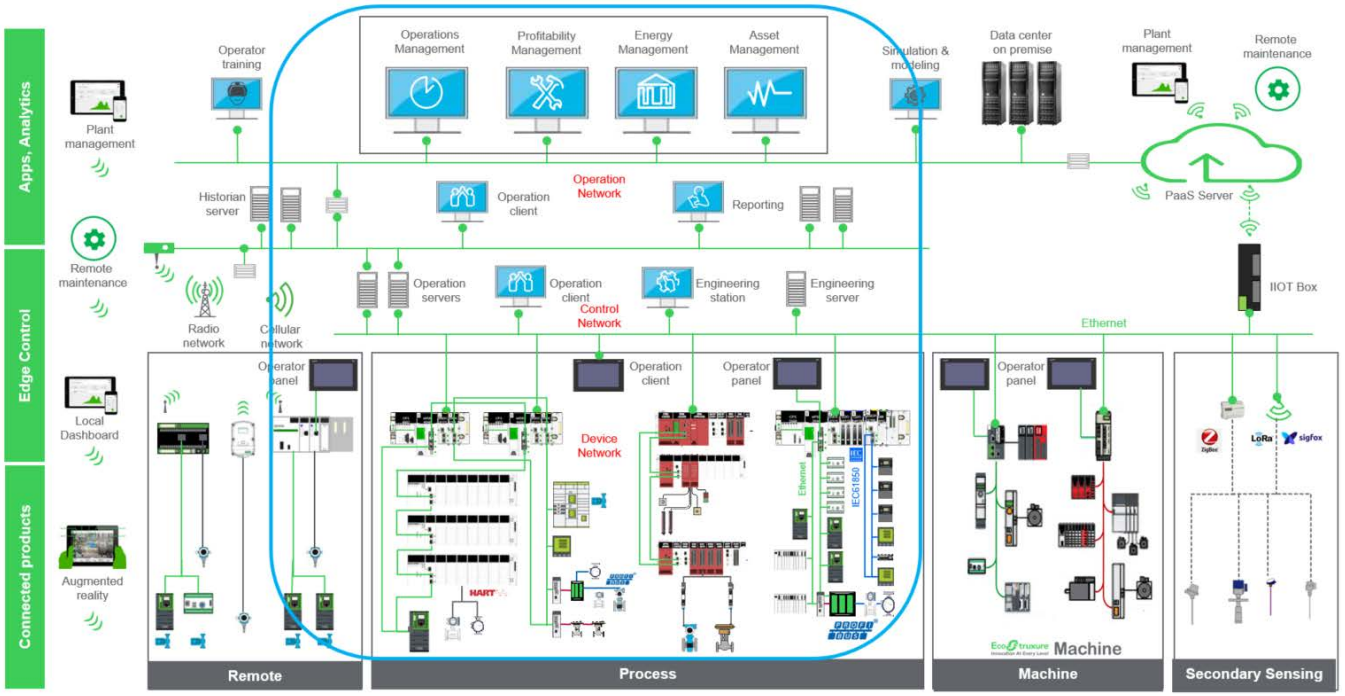


Figure 31: Sample EcoStruxure Plant Architecture

The baseline sample architecture is separated into the following networks: operations network, control network, and all device networks. In the EcoStruxure Plant security architecture (Figure 32), each of these networks is defined as a security zone. Each of the functional units in the device network security zone is a different subnet. The functional unit subnet netmask is sized slightly higher than the actual number of host device in the functional unit. Security Zones

Security zones are established by locating and configuring the appropriate firewalls at the zone boundaries as shown in Figure 32.

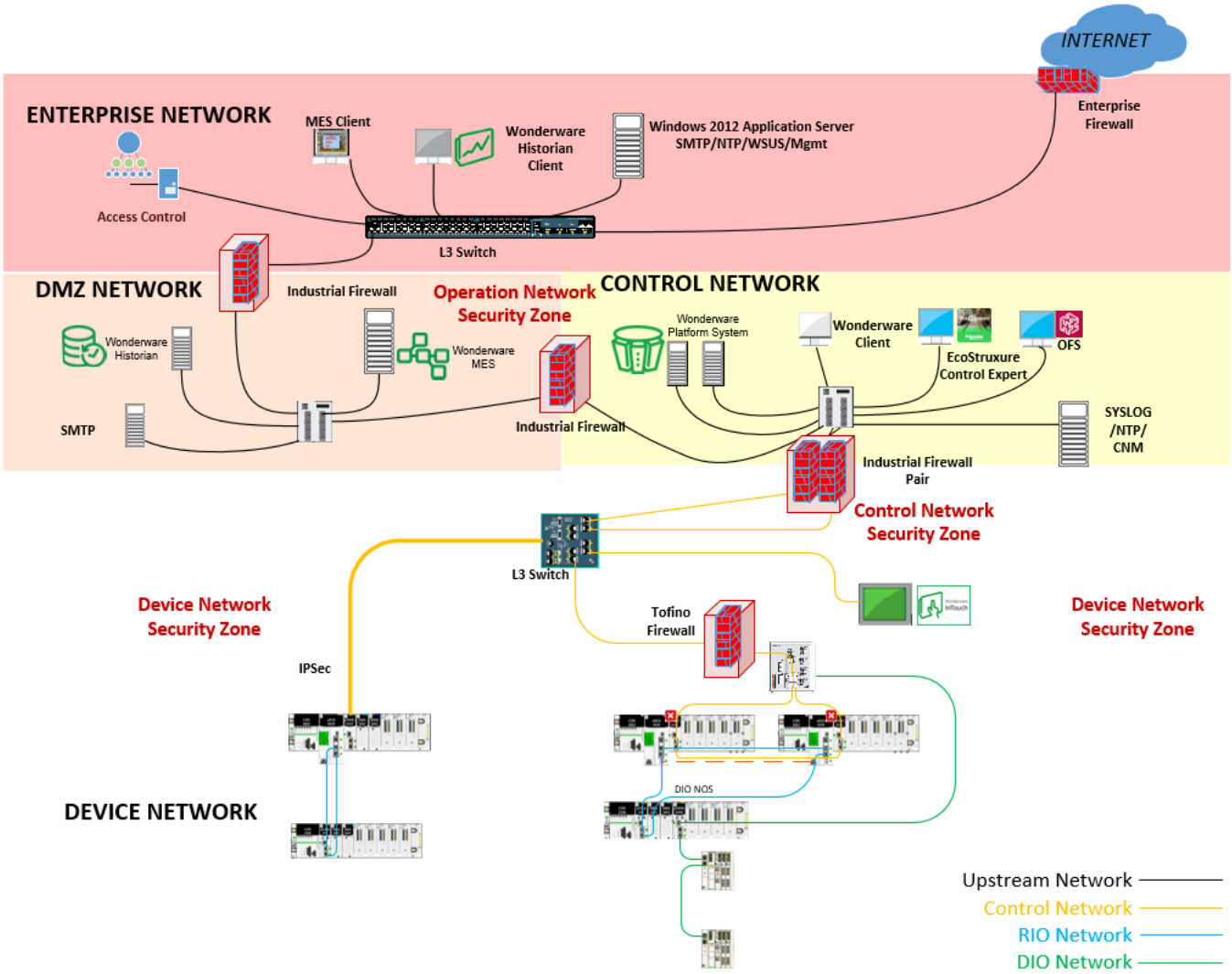


Figure 32: Sample EcoStruxure Plant Architecture with Defense-in-Depth Recommendations

Communication between the different zones happens through pathways or conduits in which the firewalls reside. The conduits allow control over access to zones, limit propagation of malware, resist denial of service attacks, and maintain the integrity and confidentiality of network traffic.

Place the stateful ConneXium Industrial Firewalls at the demarcations between the enterprise network and the DMZ, between the DMZ and operations network and between the operations network and the control network.

For the boundaries between the control network and the device network, use the ConneXium Tofino Firewall. Tofino provides the additional deep packet inspection of the industrial protocols.

The firewalls are used to restrict the network traffic between the security zones. Figure 33 shows the types of network traffic that are permitted to traverse between the different networks.

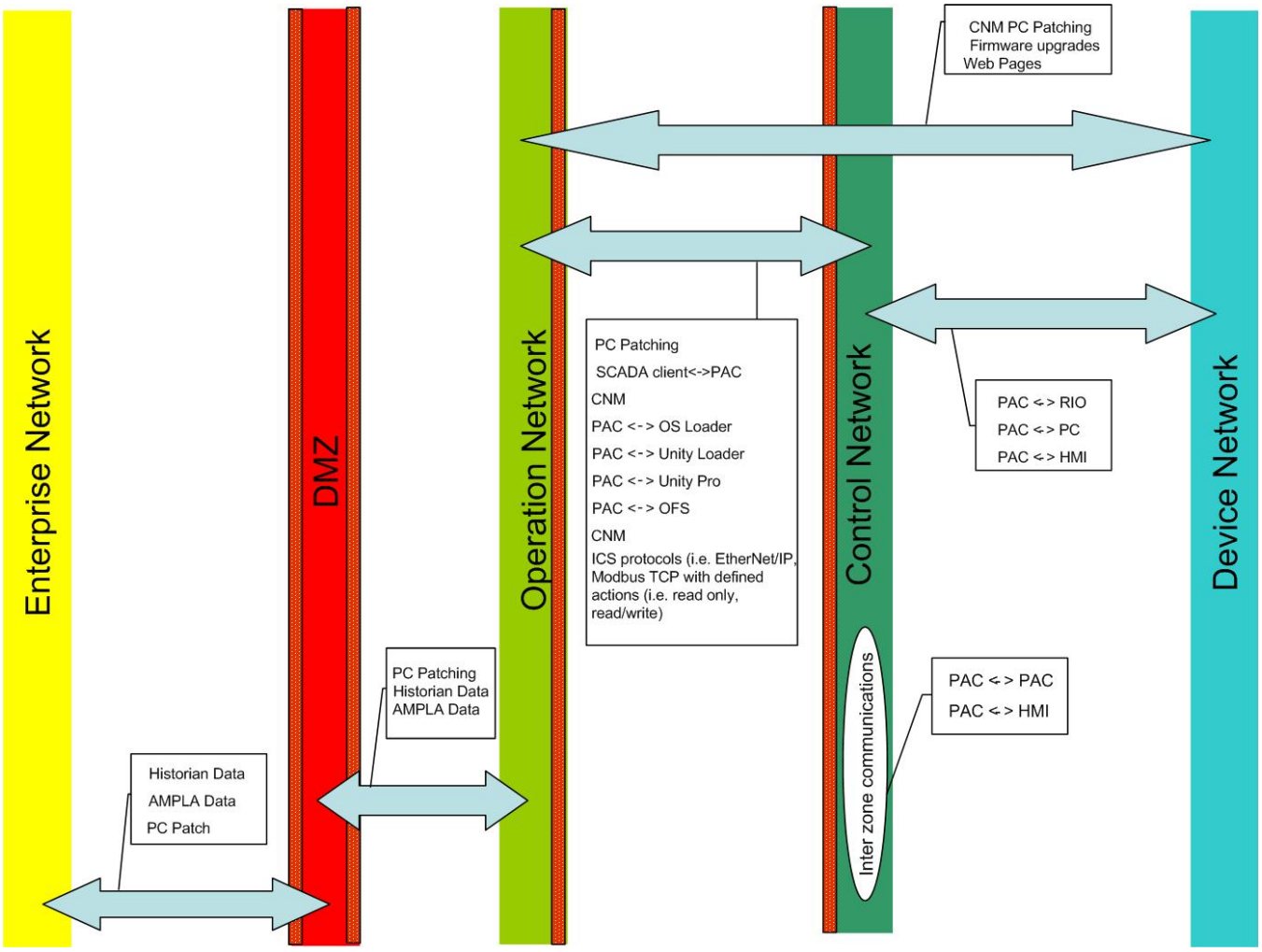


Figure 33: Network Data Flow

11.2. ConneXium Industrial Firewalls

The ConneXium Industrial Firewalls should be configured to allow only traffic that is mandatory between the immediately adjacent zones. Deny all other traffic.

For the firewalls located at the enterprise network and the DMZ, use the router feature of the firewall to route traffic between the enterprise network and the DMZ.

For the firewalls located at the DMZ and operations network, use the firewall's router feature to route traffic between the DMZ and the operations network.

For the firewalls located at the operations network and control network, use the firewall's transparent mode to relay traffic from the operations network to the control network. Routing of the multiple functional area subnetworks is performed by the Hirschman Power MICE router located in the operations network.

For high availability, the ConneXium Industrial Firewalls and MICE routers should be configured for redundancy.

The following table lists basic ingress and egress recommendations for specific firewall locations.

Firewall Location	Ingress Rules	Egress Rules
Enterprise & DMZ*	• Allow source- destination-, and protocol-specific traffic such as HTTP, SQL, network time protocol (NTP), and DNS, to any DMZ machines • Drop all ICS protocols • Drop any internal ICS source • Drop all defaults	• Allow source- destination-, and protocol-specific traffic from DMZ machines. • Explicitly drop any ICS protocols • Drop all defaults
DMZ & Operations Network*	• Allow only operation hosts with specific protocol to communicate with DMZ network hosts • Drop all defaults	• Allow only DMZ hosts with specific protocol to communicate with operations network hosts • Drop all defaults
Operations Network and Control Network*	• Allow source- destination-, and protocol-specific traffic for ICS protocol • Allow user/vendor time-based ACLs for FTP, TFTP, patching, and other maintenance needs • Reject all multicasts • Drop all defaults	• Allow source- destination-, and protocol-specific traffic for ICS protocol • Allow user/vendor time-based ACLs for FTP, TFTP, patching, and other maintenance needs • Reject all multicasts • Drop all defaults
*Allow only defined hosts within the operations network to configure the firewall.		

Table 3: ConneXium Industrial Firewall Ingress and Egress Rules

11.3. ConneXium Tofino Firewalls

Use the deep packet inspection feature of the ConneXium Tofino Firewall to regulate which devices have read access and read/write access.

The following table lists basic ingress and egress recommendations for a Tofino Firewall located between the control and device networks.

Ingress Rules	Egress Rules
• Allow source- and destination-specific Modbus, extended Modbus, Class 1 or Class 3, EtherNet/IP traffic • Allow source- and destination-specific traffic for function codes such as 3, 5, 23, 90 • Allow specific hosts to read from specific devices • Allow specific hosts to read from or write to specific devices • Allow multicasts (RTPS, IGMP) • Drop all defaults	• Allow source- and destination-specific Modbus, extended Modbus, Class 1 or Class 3, EtherNet/IP traffic • Allow source- and destination-specific traffic for function codes such as 3, 5, 23, 90 • Allow specific hosts to read from specific devices • Allow specific hosts to read from or write to specific devices • Allow multicasts (RTPS, IGMP) • Drop all defaults
Allow only defined hosts within the operations network to configure the firewall.	

Table 4 – ConneXium Tofino Firewall Ingress and Egress Rules

11.4. ConneXium Managed Ethernet Switches

Take the following actions to enhance the security of ConneXium managed Ethernet switches:

- Change default passwords.
- Disable unused ports.
- Disable telnet access (used for configuration via CLI).
- After IP assignment, disable the Ethernet Switch Configurator.
- After configuration, disable the device's Web pages. If both the telnet server and the Web server are disabled, the switch's V.24 port will be the only remaining access port.
- Use IP or MAC access control list to allow access to ports.
- Allow only defined hosts from the operations network to configure the switches.

11.5. Device and Application Security Recommendations

Schneider Electric recommends using all available device and applications security features. The following are general recommendations for using security features found in devices and applications.

11.5.1. Login IDs and Passwords

Use login ID and password authentication on devices and applications that support it.

Use a unique password for each such device and application.

Change all default passwords to unique passwords.

11.5.2. SNMP Community Names

Change all SNMP default community names to unique names.

11.5.3. Access Control Lists

Use access control to manage communication to and from specific IP addresses on all Ethernet modules that support access control (for instance, the BMENOC03x1).

11.5.4. Programming and Configuration Software

- Configure logins, password, and user groups. Create profiles with different access rights such as the ability to open project, create new project, and modify sections. For example, the EcoStruxure Control Expert
- Security Editor supports these functions.
- Lock sections and derived function blocks (DFBs) to make them read only or no read/write. For example, EcoStruxure Control Expert programming software supports these functions.

11.5.5. SCADA

SCADA systems incorporate features that restrict access to runtime systems and areas. Roles can be assigned to individual user accounts.

ArchestrA security is designed to help prevent users from performing unauthorized activities. There are four types of security authentication modes in the Galaxy:

- NONE
- Galaxy
- OS User Based
- OS Group Based

When using the Galaxy security authentication mode, passwords are encrypted but they are stored in a database that is accessible. So, the system is not designed to stop determined programmers from accessing it.

If your application requires a higher level of security, this can be typically achieved by IT departments using tools provided by Microsoft®. To facilitate a higher level of security, the security model can be configured to support operating system authentication. In that case, the configuration and runtime permissions can be mapped to the external operating system account.

This project implements the **Galaxy Security model**, for further information about the OS-based security models please refer to the ArchestrA documentation.

11.5.6. Device Web Pages

Some devices with Web pages provide Web page password, access restriction features and the ability to configure variables, symbols, and direct address data as read-only or write-enabled. Use these security features when they are available.

11.5.7. PACs

Use the following methods to provide increased security on PACs:

- Change SNMP default community names for PACs that incorporate a built-in Ethernet ports (for instance, the Modicon M580 series).
- Use ACLs to manage communication to and from specific IP addresses for PACs built-in Ethernet ports (for instance, the Modicon M580 series).
- Disable all unused Ethernet services such as FTP, TFTP, HTTP, and so forth.

11.5.8. Ethernet Communication Modules

- Change SNMP default community names on all Ethernet modules that support SNMP (for instance, the Modicon M580 series).
- Use access control to manage communication to and from specific IP addresses on all Ethernet modules that support access control (for instance, BMENOC03x1).
- Disable all unused Ethernet services such as FTP, TFTP, HTTP, etc.

11.5.9. Log Files

Enable and configure device and application logging features when available.

Schneider Electric recommends systematic monitoring of all log files for changes, unintended behavior, and unauthorized access. See Log File Monitoring (p.87) for more information.

11.5.10. General Recommendations

Use the following methods on devices and or applications that support them:

- Disable unused ports on devices.
- Disable unused USB ports.
- Disable or lock keyboards, touch screens, and PCs when unused or unmanned.
- Remove unused device and application user accounts.

11.6. Patch Management Recommendations

The patching of systems should be a systematic procedure governed by corporate policy. It should be closely aligned with security, scheduled downtimes, backup, change control, verification, and incident management procedures.

There are several ways to deploy patches for PC systems. Schneider Electric recommends the following:

- Prior to patching, create baselines and backups of all production systems.
- Test all patches prior to deployment to production systems.
- Use a dedicated patching server located in DMZ that can either replicate from a patch repository upstream or serve as its own WSUS (Windows Server Update Service) server directly.
- Configure Client PCs to have their MS Windows Server point to dedicated server.
- Have the assigned administrator push patches to PC clients after the patches are tested.

There may be situations in which a patch needs to be manually installed. In these situations, only the assigned administrator should install the patch, using a PC known to be free of malware.

Depending on the device, patching of industrial control systems (firmware upgrades) may be done via network connectivity or may require local connection of a PC to the device. Schneider Electric recommends the following:

- Prior to upgrading any production devices, perform backups and make previous release firmware available.
- If locally connecting to any industrial control device, use a PC that is known to be free of malware.
- When updating industrial devices through the network, verify that the firewall rules and user accounts permit the necessary protocols, such as TFTP and FTP, to pass from source to destination and destination to source.

11.7. Conclusions

The defense-in-depth recommendations described in this document can decrease the risk of successful attacks on typical EcoStruxure Plant architectures. No single component provides an adequate defense. Schneider Electric recommends that you consider all the defense-in-depth strategies described in this document to mitigate risk.

12. Methods of Attack

This section describes common methods of cyberattack, including:

- Malware
- Phishing
- SQL injection on SCADA
- Cross Site Scripting (XSS)
- DoS
- Session Hijacking (Man-in-the -Middle)

12.1. Malware

Malware refers to various types of malicious software. malware is used to gain unauthorized access to your computer, server or mobile device.

Adware: The least dangerous and most lucrative malware. Adware displays ads on your computer.

Spyware: Spyware is software that spies on you, tracking your Internet activities in order to send advertising (Adware) back to your system.

Virus: A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.

Worm: A program that replicates itself and destroys data and files on the computer. Worms work to “eat” the system operating files and data files until the drive is empty.

Trojan: The most dangerous malware. Trojans are written with the purpose of discovering your financial information, taking over your computer’s system resources, and in larger systems creating a “denial-of-service attack”, which is an attempt to make a machine or network resource unavailable to an authorized user attempting to reach it. Example: Google or your business network becoming unavailable.

Rootkit: This one is likened to the burglar hiding in the attic, waiting to steal from you while you are not home. It is the hardest of all malware to detect and therefore to remove. Many experts recommend completely wiping clean your hard drive and reinstalling everything from scratch. It is designed to permit the other information gathering malware to enter your computer and obtain identity information without you realizing anything is going on.

Backdoors: Backdoors are much the same as Trojans or worms, except that they open a "backdoor" onto a computer, providing a network connection for hackers or other malware to enter or for viruses or SPAM to be sent.

Keyloggers: Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program. Keyloggers are often used by corporations and parents to acquire computer usage information.

Rogue security software: This one deceives or misleads users. It pretends to be a good program to remove malware infections, but all the while it is the malware. Often it will turn off the real Anti-Virus software. Figure 34 shows the typical screen for this malware program, Antivirus 2010

Ransomware: Ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are told that unless a ransom is paid, access will not be restored. The ransom demanded from individuals varies greatly but is frequently $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. For example, vulnerable Web servers have been exploited as an entry point to gain access into an organization's network. [12]

For example, the WannaCry attack of May 12, 2017 infected approximately 230,000 computers in over 150 countries.

[12] https://www.us-cert.gov/ncas/alerts/TA16-091A

Figure 34: WannaCry screenshot

Browser Hijacker: When your homepage changes to one that looks like those in the images inserted next, you may have been infected with one form or another of a Browser Hijacker. This dangerous malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not removing the malware lets the source developers capture your surfing interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in every case, they allow other more infectious malware programs to be installed on your PC. [13]

[13] http://www.malwaretruth.com/the-list-of-malware-types/

Figure 35: Browser Hijacker screenshot

12.2. Phishing[14]

Phishing, the act of stealing personal information via the Internet for the purpose of committing financial fraud, has become a significant criminal activity on the Internet. Recently the definition of phishing has grown to encompass a wider variety of electronic financial crimes. In addition to the widespread use of fake email messages and web sites to lure users into divulging their personal information, there has been an increase in the amount of malicious code that specifically targets user account information. Once installed on a victim's computer, these programs use a variety of techniques to spy on communications with web sites and collect account information. This method differs from the technical subterfuge generally associated with phishing scams and can be also included within the definition of spyware.

Just as with real fishermen, phishers today have a large tackle box of tools available to them. These tools serve a variety of functions, including email delivery, phishing site hosting, and specialized malware:

- Bots/Botnets

[14] https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf

- Phishing Kits
- Technical Deceit (URL obfuscation)
- Abuse of Domain Name Service (DNS)
- Specialized Malware

Bots/Botnets

"Bots" refer to programs that reside on a computer and provide remote command and control access via a variety of protocols, including IRC, HTTP, instant messaging, and peer-to-peer protocols. When several of these bots are under common control, it is referred to as a botnet. Bots provide the controller with features that can be used to support illicit activity, including:

- Relays for sending spam and phishing emails.
- Web servers or redirectors for spam/phishing sites or malware distribution.
- Updates for existing malware.
- Installation of additional malware.
- Distributed denial of service (DDoS).
- Proxy services.
- Pay-for-click services.
- Vulnerability scanning and exploitation.
- Surveillance.

In addition to the ability of most bots to infect new hosts through built-in scanning and exploitation of vulnerabilities, bots can also be deployed through social engineering techniques. These include mass mailing, file-sharing programs, and instant messaging networks.

Phishing Kits

The criminals performing phishing attacks have become more organized. One indication of increased organization is the development of ready-to-use phishing kits containing items such as pre-generated HTML pages and emails for popular banks and online commerce sites, scripts for processing user input, email and proxy server lists, and even hosting services for phishing sites. These hosting services usually advertise themselves as being impossible to shut down. Traditionally these kits are bought and sold by criminals within the underground economy; however, versions of these kits have been found to be available for anyone to download at no cost in the dark web. Phishing kits lower the barrier for criminals to enter into the marketplace, reducing the amount of technical knowledge required to conduct a phishing scam.

Technical Deceit

As users have become more aware of phishing and better educated about the signs for detecting fake emails and web sites, criminals are developing techniques to counter this awareness. These techniques include URL obfuscation that make phishing emails and web sites appear more

legitimate, and exploitation of vulnerabilities in web browsers that allow the download and execution of malicious code from a hostile web site.

Basic URL Obfuscation

URL obfuscation misleads the victims into thinking that a link and/or web site displayed in their web browser or HTML-capable email client is that of a trusted site. These methods tend to be technically simple yet highly effective, and are still used to some extent in phishing emails today. HTML redirection, one of the simplest techniques for obscuring the actual destination of a hyperlink, uses a legitimate URL within an anchor element but has its href attribute point to a malicious site.

Clicking on a legitimate-looking URL instead sends the user to a phishing site. This deception can be detected because web browsers display the actual destination of a hyperlink when a user moves the mouse pointer over the link; this information is typically displayed in the web browser's status bar. Use of JPEG images Electronic mail rendered in HTML format is becoming more prevalent. Phishers are taking advantage of this by constructing phishing emails that contain a single image in JPEG format. When displayed, this image appears to be legitimate email from an online bank or merchant site. The image often includes official logos and text to add to the deception. However, when users click on this image, they are directed to a phishing site. As with the previous example, phishing emails using this technique can often be detected by observing the actual destination URL when moussing over the image.

Abuse of Domain Name Service

Criminals often take advantage dynamic DNS providers, which are often used for providing a static domain name mapping to a dynamic IP address. This service can be useful to phishers by providing them with the ability to easily redirect traffic from one phishing site to another if the initial site is shut down. With ISPs and law enforcement becoming more proactive in shutting down phishing sites, the use of dynamic DNS and registration of multiple IP addresses for a single fully qualified domain name (FQDN) is becoming more prevalent to increase the resilience of phishing sites.

Specialized Malware

There has been an emergence of malware being used for criminal activity against users of online banking and commerce sites. This type of specialized malware (which can be considered a class of spyware) greatly increases the potential return on investment for criminals, providing them with the ability to target information for as many or as few sites as they wish. One benefit for criminals is that most malware can easily be reconfigured to change targeted sites and add new ones. Malware also provides several mechanisms for stealing data that improve the potential for successfully compromising sensitive information.

12.3. SQL Injection on SCADA

SCADA systems are vulnerable to SQL Injection attacks. SQL injection is a code injection technique that occurs in the database layer of an application. The attacker executes unauthorized SQL commands by taking advantage of poorly secured code on a system connected to the Internet. Vulnerable points include the login and URL string.

SQL injection attacks are used to steal information from a database and/or to gain access to an organization's host computers through the computer that is hosting the database.

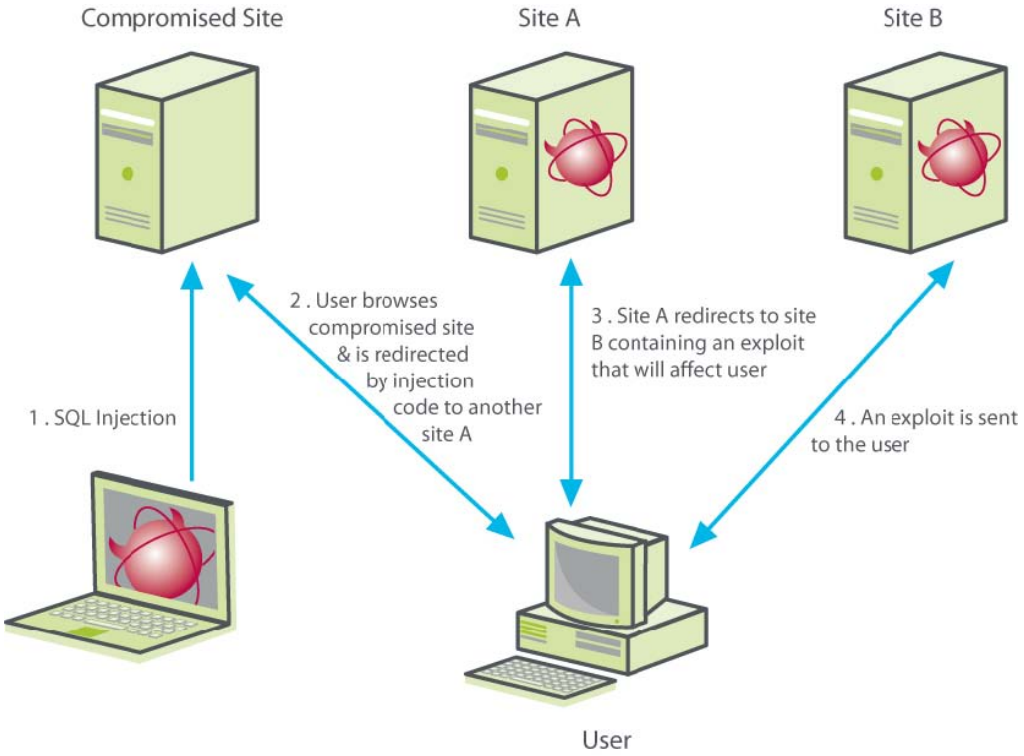


Figure 36: Sample SCADA SQL Injection Risk

12.4. Cross Site Scripting

Cross-site scripting (XSS) attacks can occur in programs on web sites that accept user input. If the program does not properly sanitize the input data, the vulnerable program may process input or even execute code that the original program was not intended to do. For example, a phisher could construct a URL that uses a vulnerable program on a legitimate commerce site. This URL would also contain (probably obfuscated) code, such as JavaScript, that could target account credentials. There have been reports that this type of attack was used in a phishing scam against a bank. A more common XSS attack that has been used in phishing involves the exploitation of vulnerable URL redirector programs. URL redirectors are often used by web sites to perform custom processing based on attributes such as web browser or authentication status or even just to display a message when clicking on a link to an external site. There have been multiple

incidents of commerce sites using URL redirectors that allowed a user to input any external URL they wanted to. As a result, phishers were able to send phishing emails with URLs that used the vulnerable redirectors on the legitimate sites to trick people into visiting phishing sites.

12.5. Session Hijacking

Sometimes referred to "man-in-the-middle attacks", IP spoofing is a method used to disguise the identity of an attacker who is attempting to perform malicious attacks. Session hijacking is accomplished by manipulating the IP address.

IP is the main protocol used to communicate data across the Internet. The IP header of the data contains the information necessary to transport data from the source to the destination. The header contains information about the type of IP datagram, how long the datagram remains active on the network, special flags indicating any special purpose the datagram is supposed to serve, such as whether or not the data can be fragmented, the destination and source addresses, and several other fields.

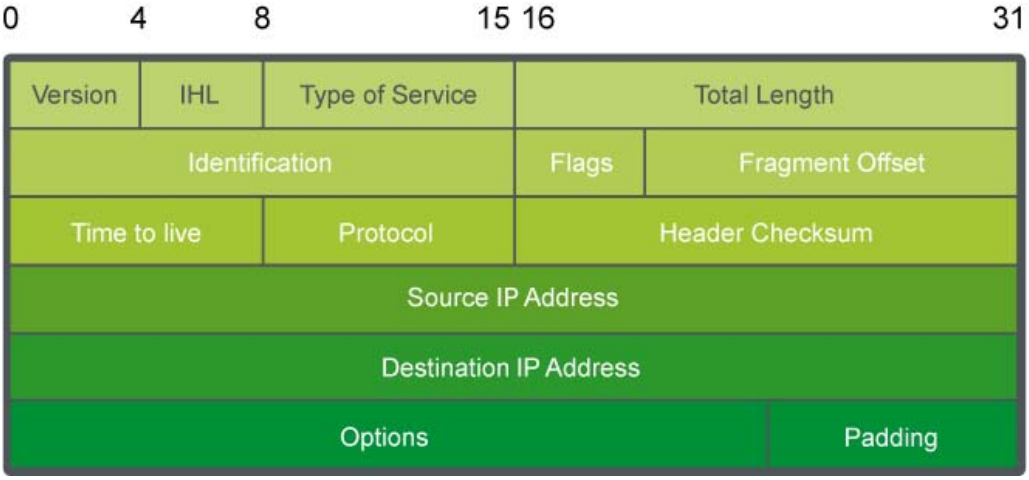


Figure 37: IP Datagram Header

The receiver of the packet is able to identify the sender by the source IP address. IP does not validate the source's IP address. In session hijacking, the attacker manipulates the datagram. The most common manipulation is creating a false source IP address to hide identity.

The primary motives of the attack are to:

- Gather information about open ports, operating systems, or applications on the host. For example, a port 80 response may indicate that the host is running a Web server. Using telnet, the attacker can see the banner and determine the Web server version and type. Now the attacker can try to exploit any vulnerability associated with that Web server.
- Uncover the sequence-number. TCP requires the use of sequence number for every byte transferred and an acknowledgment from the recipient. An attacker can send several

packets to the victim in an attempt to determine the algorithm. Once the algorithm is determined, the attacker tricks the target in believing its legitimacy and launches attacks.

- Hijack an authorized session by monitoring a session between two communicating hosts and injecting traffic that appears to be coming from one host. By doing so, the attacker steals the session from one host and terminates its session. The attacker continues the same session with the same access privileges to the other legitimate host.

12.6. Denial of Service Attacks

DoS is an attempt to deny legitimate users access to computer services either temporarily or permanently. One common method involves saturating the victim's computer with external communications requests to either block responses or respond so slowly that the system becomes ineffective. The attacker usually accomplishes this by:

- Crashing the system.
- Denying communication between systems.
- Bringing the network or the system down or have it operate at a reduced speed affecting productivity.
- Hanging the system. This is more disruptive than crashing it because there is no automatic reboot. Productivity can be disrupted indefinitely.

Today, Distributed Denial of Service (DDoS) is more common. A DDoS attack is where multiple systems are compromised with some trojan malware and then simultaneously launch a DoS attack against the same target.

For example, DYN the DNS service provider of hundreds of companies, some of which include, Amazon, Comcast, HBO, The New York Times, BBC and the Swedish government was attacked on September 21, 2016. The attack was caused by the DNS service receiving DNS lookups for tens of millions of IP addresses. Though it is unknown who launched the attack, the attack originated from a botnet that infected thousands of residential cable routers, printers, home IP cameras and baby monitors. The attack occurred 3 times that day starting at 07:00 with DYN finally resolved the issue at 18:11 that evening.

DDoS variations include:[15]

[15] https://www.rivalhost.com/12-types-of-ddos-attacks-used-by-hackers

UDP Flood

User Datagram Protocol is a sessionless networking protocol. One common DDoS attack method is referred to as a UDP flood. Random ports on the target machine are flooded with packets that cause it to listen for applications on those ports and report back with a ICMP packet.

SYN Flood

A “three-way handshake”, which refers to how TCP connections work, are the basis for this form of attack. The SYN-ACK communication process works like this:

- First, a “synchronize”, or SYN message, is sent to the host machine to start the conversation.
- Next, the request is “acknowledged” by the server. It sends an ACK flag to the machine that started the “handshake” process and waits for the connection to be closed.
- The connection is completed when the requesting machine closes the connection.

A SYN flood attack will send repeated spoofed requests from a variety of sources at a target server. The server will respond with an ACK packet to complete the TCP connection, but instead of closing the connection the attackers allow the connection to timeout. Eventually, and with a strong enough attack, the host resources will be exhausted and the server will go offline.

Ping of Death

Ping of death (”PoD”) is a denial of service attack that manipulates IP protocol by sending packets larger than the maximum byte allowance, which under IPv4 is 65,535 bytes. Large packets are divided across multiple IP packets – called fragments – and once reassembled create a packet larger than 65,535 bytes. The resulting behemoth packet causes servers to reboot or crash.

Note: *This was a real problem in early years (think 1996), but doesn't have the same effect these days. Most ISPs block ICMP or “ping” messages at the firewall. However, there are many other forms of this attack that target unique hardware or applications. Some other names are “Teardrop”, “Bonk”, and “Boink”.*

Reflected Attack

A reflected attack is where an attacker creates forged packets that will be sent out to as many computers as possible. When these computers receive the packets, they will reply, but the reply will be a spoofed address that routes to the common target. When the computers simultaneously attempt to communicate, they cause the target site to be bogged down with requests until the server resources are exhausted.

Peer-to-Peer Attacks

Peer-to-Peer servers present an opportunity for attackers. Instead of using a botnet to siphon traffic towards the target, a peer-to-peer server is exploited to route traffic to the target website.

When executed successfully, people using the file-sharing hub are instead sent to the target website until the website is overwhelmed and sent offline.

Nuke

Corrupt and fragmented ICMP packets are sent via a modified ping utility that repeatedly sends the malicious packets to the target. Eventually, the target machine goes offline. This attack focuses on compromising computer networks and is an old distributed denial of service attack.

Slowloris

This type of distributed denial of service attack can be especially difficult to mitigate. Its most notable use was in the 2009 Iranian Presidential election. Slowloris is a tool that allows an attacker to use fewer resources during an attack. During the attack connections to the target machine will be opened with partial requests and allowed to stay open for the maximum time possible. It will also send HTTP headers at certain intervals. This adds to the requests, but never completes them – keeping more connections open longer until the target website is no longer able to stay online.

Degradation of Service Attacks

The purpose of this attack is to slow server response times. A DDoS attack seeks to take a website or server offline. That is not the case in a degradation of service attack. The goal here is to slow response time to a level that essentially makes the website unusable for most clients. Zombie computers are leveraged to flood a target machine with malicious traffic that will cause performance and page-loading issues. These types of attacks can be difficult to detect because the goal is not to take the website offline, but to degrade performance. They are often mistaken for a simple increase in website traffic.

Unintentional DDoS

Unintended distributed denial of service happens when a spike in web traffic renders a server unable to handle all incoming requests. The greater the traffic, the greater the amount of resources used by the server. This causes pages to timeout when loading and eventually the server will fail to respond and go offline.

Application Level Attacks

Application level attacks target areas that have more vulnerabilities. Rather than attempt to overwhelm the entire server, an attacker will focus their attack on one – or a few – applications. Web-based email apps, WordPress, Joomla, and forum software are good examples of application specific targets.

Multi-Vector Attacks

Multi-vector attacks are the most complex forms of distributed denial of service (DDoS) attack. Instead of utilizing a single method, a combination of tools and strategies are used to overwhelm

the target and take it offline. Often, multi-vector attacks will target specific applications on the target server, and will also flood the target with a large volume of malicious traffic. These types of DDoS attacks are the most difficult to mitigate because the attack comes in different forms and simultaneously targets different resources.

Zero Day DDoS

A “Zero Day” based attack is an attack method that to date has no patches. This is a general term used to describe new, exploitable vulnerabilities.

13. Appendix

13.1. Appendix A

National Cyber Awareness System:

TA17-163A: CrashOverride Malware

06/12/2017 05:44 PM EDT

Original release date: June 12, 2017

Systems Affected

Industrial Controls Systems

Overview

The National Cybersecurity and Communications Integration Center (NCCIC) is aware of public reports from ESET and Dragos outlining a new, highly capable Industrial Controls Systems (ICS) attack platform that was reportedly used in 2016 against critical infrastructure in Ukraine. As reported by ESET and Dragos, the CrashOverride malware is an extensible platform that could be used to target critical infrastructure sectors. NCCIC is working with its partners to validate the ESET and Dragos analysis, and develop a better understanding of the risk this new malware poses to the U.S. critical infrastructure.

Although this activity is still under investigation, NCCIC is sharing this report to provide organizations with detection and mitigation recommendations to help prevent future compromises within their critical infrastructure networks. NCCIC continues to work with interagency and international partners on this activity and will provide updates as information becomes available.

For a downloadable copy of IOCs, see:

- IOCs (.csv)
- IOCs (.stix)

To report activity related to this Alert, please contact NCCIC at NCCICCustomerService@hq.dhs.gov or 1-888-282-0870.

13.2. Glossary

The following table describes the acronyms and defines the specific terms used in this document.

Term	Description
BootP	(bootstrap protocol) A TCP/IP network protocol that lets network nodes request configuration information from a BootP server node.
broadcast	A message that is sent out to all devices on the network.

Term	Description
broadcast domain	A collection of devices that receive a broadcast sent on an Ethernet network. The broadcast domain ends at a router positioned in the network. If any device in a broadcast domain broadcasts information, that information is received by all devices in the same domain. It is not received by devices connected through a router.
control network	The portion of the control system network where process data is transferred. It includes SCADA-to-PAC traffic and PAC-to-PAC traffic.
DMZ	In computer networking, a De-Militarized Zone (DMZ) is a special local network configuration designed to improve security by segregating computers on each side of a firewall.
encapsulation	Wrapping a data set in a protocol header. For example, Ethernet data wrapped in a specific Ethernet header before network transit. Also, a method of bridging dissimilar networks where the entire frame from one network is enclosed in the header used by the link-layer protocol of the other network.
FDR	(fast device replacement) service allows a central device (the FDR server) to store configuration parameters for remote devices on the network. If a remote device requires replacement, the server automatically passes the stored configuration parameters on to a replacement device so that it can operate using the same configuration parameters as the replaced device. The replacement is accomplished without manually configuring the parameters. The FDR service should be used for all on the automation network that support it. It reduces the need for service personnel to keep configuration records on hand, and it reduces the chance of human error in entering the new configuration.
forwarding	Process whereby an Ethernet switch or bridge reads the contents of a packet and passes the packet on to the appropriate attached segment.
field network	The portion of the control system network in which field device monitoring and control traffic is primarily transferred. It includes PAC-to-I/O, PAC-to-drive, and primary-to-hot-standby-PAC traffic.

Term	Description
FIO	Freedom of Information. Nearly 70 countries had freedom of information legislations applying to information held by government bodies and in certain circumstances to private bodies. Access to information was increasingly recognized as a prerequisite for transparency and accountability of governments, as facilitating consumers' ability to make informed choices, and as safeguarding citizens against mismanagement and corruption.
gateway	A combination of hardware and software that interconnects otherwise incompatible networks or networking devices. Gateways include packet assembler/disassembler and protocol converters. Gateways operate at layers 5, 6, and 7—the session, presentation, and application layers, respectively—of the OSI model.
header	The control information added to the beginning of a transmitted message. It contains required information such as the packet or block address, source, destination, message number, length, and routing instructions.
HMI	(human-machine interface) The keypad and screen or other user interface of a device.
host	Generally, a node on a network, such as a computer, that can be logged into and used interactively.
ISO layered model	The open systems interconnection (OSI) reference model, which specifies how dissimilar computing devices such as NICs, bridges and routers exchange data over a network. The model is defined by the International Standards Organization. It consists of 7 layers. From lowest to highest, they are physical, data link, network, transport, session, presentation, and application. Each layer performs services for the layer above it (see OSI reference model).
LAN	(local area network) A data communications system consisting of a group of interconnected computers, sharing applications, data, and peripherals. The geographical area is usually a building or a campus.
LAN segmentation	Dividing local area network bandwidth into multiple independent LANs to improve performance and/or security.
latency	The delay incurred by an Ethernet switching or bridging device between receiving the frame and forwarding the frame.

Term	Description
layer	The software protocol levels that comprise a network's architecture, where each layer performs functions for the layer(s) above it (see ISO layered model).
MES	(manufacturing execution system) A computerized system that aids in managing data and communications for production flow.
MICE	(mechanical, ingress, climatic, environmental) An international standardization effort by IEC TC65, TIA TR-42.9, and CENELEC TC215 WG1 to establish environmental standards for industrial Ethernet.
NOE	Quantum140 NOE 771 xx Ethernet communication module
OSI	(open systems interconnect/interconnection) A structure for Internetworking heterogeneous devices for distributed application processing per international standards (see ISO layered model).
OSI reference model	A 7-layer network architecture model of data communication protocols developed by ISO and CCITT. Each layer specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer (see ISO layered model).
packet	A series of bits containing data and control information, formatted for transmission from one node to another. It includes a header with a start frame, the source and destination addresses, control data, the message itself, and a trailer with error control data (called the frame check sequence).
PAC	Programmable automation controller
port	A physical or logical connector on a device enabling the connection to be made.
process level network	The portion of the control system network in which process data is transferred. It includes SCADA-to-PAC and PAC-to-PAC traffic.
QoS	(quality of service) A performance specification for measuring and improving the transmission quality and service availability of a communications system.

Term	Description
router	Device capable of filtering and forwarding packets based on data link layer information. Whereas a bridge or switch may read only MAC layer addresses to filter, a router can read data such as IP addresses and route accordingly. Unlike bridges, routers operate at level 3 (the network layer) of the OSI model. Also unlike bridges, routers are protocol-specific, acting on routing information carried by the communications protocol in the network layer. Bridges pass layer 2 (data link) packets directly onto the next segment of a LAN, whereas a router can use information about the network topology and so can choose a better route for a Layer 3 packet. Because routers operate at level 3, they are independent of the physical layer and so can be used to link a number of different network types. Routers need to exchange information between themselves so that they know the conditions on the network, such as which links are active and which nodes are available.
SNMP	(simple network management protocol) Standard Internet protocol used to manage Ethernet network devices such as switches and routers. A 3-part protocol comprising: structure of management information (SMI), management information base (MIB) and the protocol itself. The SMI and MIB define and store the set of managed entities; SNMP itself conveys information to and from these entities. A TCP/IP host running an SNMP application can query other nodes for network related statistics and detected error conditions. The other hosts, which provide SNMP agents, respond to these queries and allow a single host to gather network statistics from many other network nodes.
VLAN	(virtual local area network) An implementation in some managed Ethernet switches to group ports and nodes based on 802.1Q protocol tags. This allows isolating network traffic and reducing Ethernet collision domains, resulting in better performance and deterministic system behavior.

Table 3: glossary

13.3. Reference Documents

The following table is a list of documents you might want to refer to when more details are needed.

Source	Reference
US Department of Commerce	National Institute of Standards and Technology Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
US Department of Homeland Security and US Department of Commerce	HTTP://www.us-cert.gov/control_systems/ Catalog of Control Systems Security: Recommendations for Standards Developers - 2008 Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security - National Institute of Standards and Technology (NIST), Keith Stouffer, Joe Falco, Karen Scarfone – 2008 Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program - U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed (NSTB) - 2008 Control Systems Cyber Security: defense-in-depth Strategies – Idaho National Laboratory – May 2006
The Instrumentation, Systems and Automation Society (ISA)	Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks -2004 Mitigations for Security Vulnerabilities Found in Control System Networks -2006 2008 CSI Computer Crime & Security Survey - Robert Richardson, CSI Director Design Secure Network Segmentation Approach - SANS Institute InfoSec Reading Room – 2005 VLAN Best Practices – White paper FLUKE networks -2004 OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts - Digital Bond,
British Columbia Institute of Technology, Byres Research – 2007	HTTP://www.vicomsoft.com/knowledge/reference/firewalls1.html

Table 4: Reference documents

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centres, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.
www.schneider-electric.com

Schneider Electric Industries SAS
Head Office
35, rue Joseph Monier
92506 Rueil-Malmaison Cedex
FRANCE

Version 3.0 – 2 2019