EcoStruxure™ Innovation At Every Level Power

EcoStruxure™ Power Guide for Designing and Implementing a Cyber Secure Digital Power System

Technical Guide

10/2021
ESXP2TG003EN

se.com/ww/ecostruxure-power

Life Is On Schneider Electric

Purpose of the Document

Target Audience

This technical guide is intended for those responsible for designing digitalized electrical distribution systems; such as electrical design consultants, as well as system integrators and application engineers responsible for configuration and implementation of EcoStruxure™ Power systems.

Objective

The objective of this document is to support the EcoStruxure™ Power Digital Application Design Guide, in which we introduce the digital applications and describe their implementation for large buildings and critical facilities.

All the digital applications embedded in EcoStruxure™ Power Edge Control Software need to collect data from the electrical installation to enable applications, for example: Cost Allocation, Energy Usage Analysis, Power Event Analysis, etc., as well as to perform general trending or diagnostics.

For information about EcoStruxure™ Power courses, contact: Cybersecurity.Academy@se.com

Digital Applications for Large Buildings and Critical Facilities
EcoStruxure™ Power Design Guide for North America
Ref: 0100DB1802R11/20

Important Information

This document is intended to provide an introduction for designing and implementing a secure digital power system. It is not intended to replace any specific product documentation or site-specific design documentation.

The architectures and services described in this document are 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.

It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein.

When devices are used for applications with technical safety requirements, all pertinent state, regional, and local safety regulations must be observed when deploying and using the automation architectures recommended in this documentation.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Table of Contents

1

2

3

4

5

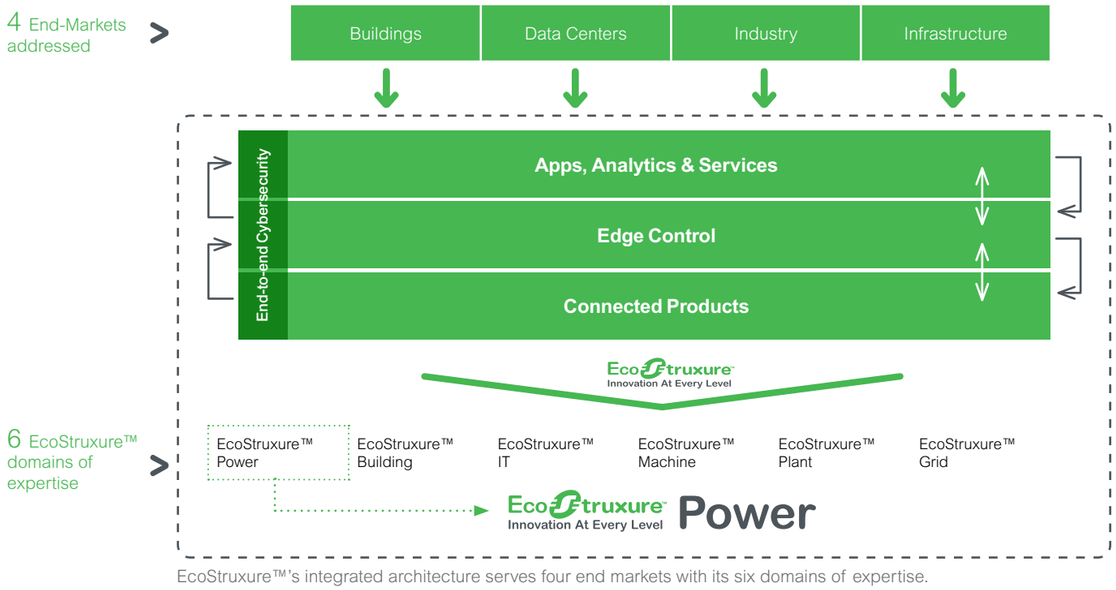
6

Overview of EcoStruxure™ Power (1/3)

Introduction

As shown in the diagram below, and indicated by the green arrows, EcoStruxure™ Power is one of the six domains of EcoStruxure™, our IoT-enabled architecture and platform.

EcoStruxure™ Power plays a key role in all four End-Markets (Building, Data Center, Industry and Infrastructure). This involves bringing the world of electrical distribution to those End-Markets.



EcoStruxure™'s integrated architecture serves four end markets with its six domains of expertise.

OUR VISION OF A NEW ELECTRIC WORLD

The world is becoming more electric and digital, and power is becoming more distributed, more complex to manage, and more integrated into our everyday lives. We envision a New Electric World where building staff and occupants are safer, with zero electrical safety incidents. Where power is 100% available, with zero unplanned downtime. Where energy and operations are more efficient, with zero energy waste. And where operational systems are resilient, with zero cyber intrusions.

We strive to make this vision a reality with our IoT-enabled EcoStruxure™ architecture and platform, which we deliver through our connected energy management ecosystem – a collective of partners and industry experts who are openly collaborating with us to push innovation, enhance productivity, reduce risk, and unlock new growth opportunities.

Overview of EcoStruxure™ Power (2/3)

EcoStruxure™ Power

- **EcoStruxure™ Power digitizes and simplifies low and medium voltage electrical distribution systems.** It provides essential data to aid the decisions that help protect people, safeguard assets, maximize operational efficiency and business continuity, and maintain regulatory compliance.

- **EcoStruxure™ Power is an open architecture and platform** designed with the intention of making it easy to add, upgrade, and swap components. The world is full of electrical distribution systems in various stages of maturity; from a variety of manufacturers. Interoperability with EcoStruxure™ Power is essential to making these power distributions systems future ready. The added benefit of a holistic Schneider Electric system is the plug-and-play connectivity to achieve faster and lower risk integration and commissioning.

- **EcoStruxure™ Power architectures are cost-optimized** to deploy, using only the right technology to deliver the desired business outcomes for our customers – no more, no less. However, customer needs or demands change over time.

- **The EcoStruxure™ Power system is scalable** from light commercial and industrial buildings to critical facilities such as hospitals data centers or infrastructure like airports, rail and oil and gas. Scalability of EcoStruxure™ Power also extends to growing and evolving with changing needs or demands through its modular architecture.

- **EcoStruxure™ Power architectures are fully flexible power distribution systems** with the ability to adapt to dynamic and ever-changing conditions, such as balancing supply and demand by the hour or minute or adding and then scaling on-site renewable generation capabilities over time. Connecting IT and OT systems into a single, easy-to-manage Ethernet IP network is at the heart of our digitization story. With EcoStruxure™ Power, facility managers can use the data they collect to make real-time decisions to maximize business continuity and optimize operations.

More about EcoStruxure™ Power
https://www.schneider-electric.com/en/work/campaign/innovation/power-distribution.jsp

www.se.com

Overview of EcoStruxure™ Power (3/3)

Reference Documents

ID	Document
R1	IEC62443-2-4: Security program requirements for IACS service providers
R2	IEC62443-3-3: System security requirements and security levels
R3	Power Operation System Guide
R4	Power Monitoring Expert (PME) System Guide
R5	Cybersecurity Admin Expert (CAE) User Guide
R6	Wireless Personal Area Network Security Recommendations

Terms and Abbreviations

Term	Description
CAE	Cybersecurity Admin Expert
DMZ	Demilitarized Zone
DPI	Deep Packet Inspection
HMI	Human Machine Interface
HP	Host Protection
IACS	Industrial Automation and Control Systems
IDS	Intrusion Detection System
NAT	Network Address Translation
NSA	National Security Agency
NTP	Network Time Protocol
OT	Operational Technology
PME	Power Monitoring Expert (Software)
PTP	Precision Time Protocol
SIEM	Security Information and Event Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

About the Guide (3/3)

Structure of the Document

Section 1 explains why Cybersecurity is important while designing an EcoStruxure™ Power digital architecture and introduces the sample architecture.

Section 2 provides information about the methodology for designing the network for security, design requirements and suggestions to achieve a proper defense.

Section 3 provides deeper information about the configuration of devices.

Section 4 provides deeper information about the configuration of servers.

Section 5 provides deeper information about the configuration of software products.

Section 6 provides information about the integration and hardening of servers and workstations.

The Bibliography quotes the sources of the information embedded in this guide and provides links to useful documentation.

SECTION 1

Introducing Cybersecurity

Introduction

Why Read this Section?

The objective of this section is to introduce the notion of cybersecurity, which is fundamental when implementing EcoStruxure™ Power Applications.

Contents of this Section

First, we explain the importance of cybersecurity.

Then, we explain the background and recommendations to understand it, its process and pillars.

Additionally, to illustrate why applications require different levels of security, we will review a sample architecture diagram.

Why Is Cybersecurity Important?

Introducing Cybersecurity

By using smart connected devices to collect and share data, teams manage their processes and assets on premises or remotely. The Internet of Things is helping buildings and facility organizations to improve productivity and profitability by unlocking the power of data from the edges of their electrical distribution systems.

With IoT enabled systems, users can reach deeper into their electrical distribution to gain insights into operational performance, as well as reliability of energy supply. As a result they are improving safety, increasing efficiency and reducing downtime.

So, while implementing connected devices eases processes and improves efficiency, it also creates a security concern that must be addressed.

Cybersecurity threats are rising and operational systems with IoT and connectivity to enterprise software and the cloud are a new vector cyber intrusions. Strong cybersecurity strategies are needed to mitigate the impact of cyber incidents (down time, data loss).

Additionally, cyber vulnerabilities can vary and aren't necessarily performed by external hackers. Education, security process and technology are all required for a strong cybersecurity strategy.

Cybersecurity is an enabler for the Industrial Internet of Things and is central to EcoStruxure™ solutions, helping enhance resilience against cyber threats through an end-to-end approach to security.

Background

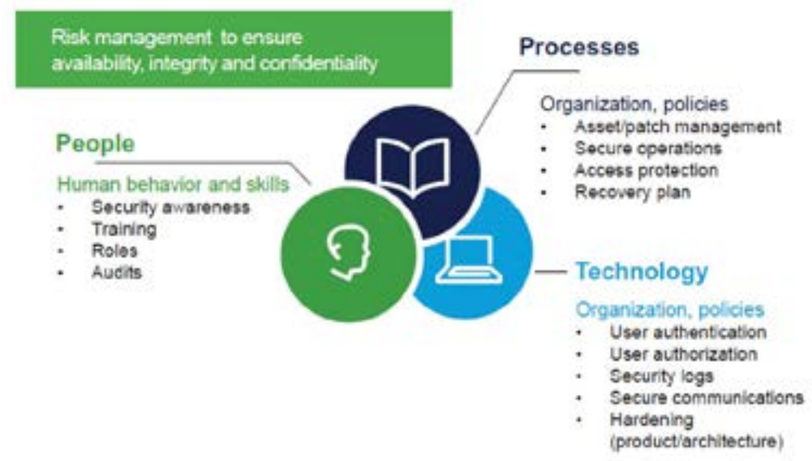
Project Scope

This document will focus on the technical architecture methodology of the system as well as the configuration of hardware and software components.

Description

Cyber attacks on power monitoring and control systems are becoming more prevalent. These systems are generally easy targets for attackers due to their extended life expectancy and their dependence on legacy technologies. Many systems did not consider cybersecurity during their conceptual definition wich makes them vulnerable to even the most basic of attacks.

Cybersecurity consists of three basic pillars: people, processes, and technology. This guide focuses on the technology pillar. It is strongly recommended to understand the people (social engineering) and process pillars as they are fundamental to secure integration, deployment, and maintenance.



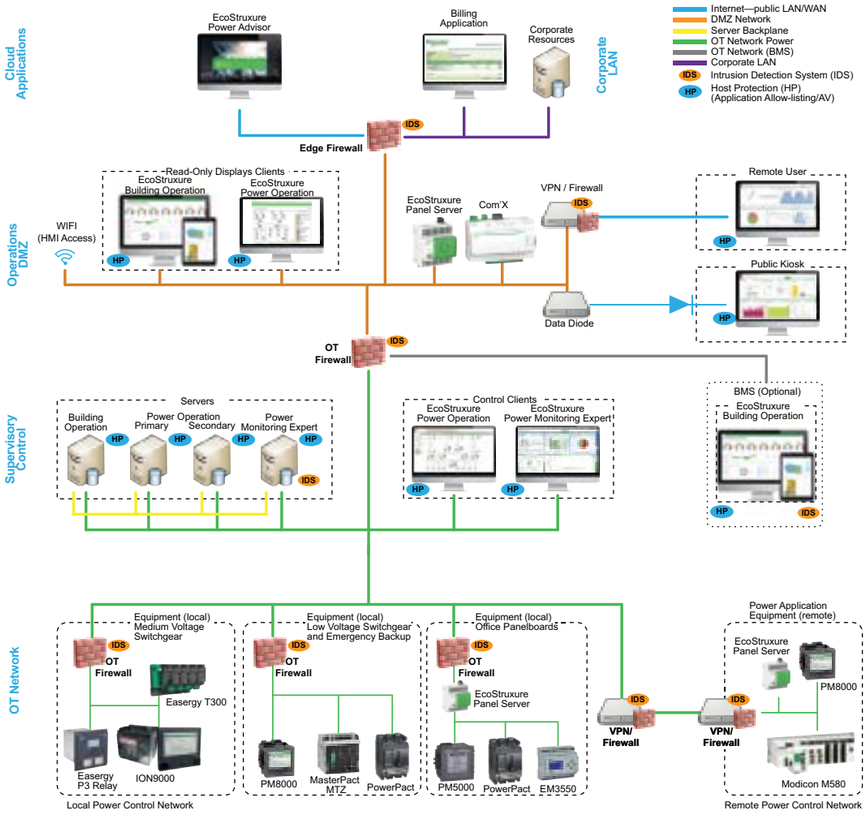
Background

Architecting a system designed to protect and power critical infrastructure takes considerable effort on many fronts. Many markets have regulatory requirements and standards that must be met when designing, implementing and maintaining a system This document is not designed to replace such standard; however it is designed to create alignment with the IEC 62443 family of standards. Note that this document does not concentrate on Cybersecurity policies and procedures (including those referred to in IEC 62443). Further, this document should not be considered a replacement of the official standard documentation. The concepts presented in this document will assist in preparing for a certification, but it is not a complete list of the standards (and not all standard requirements are listed in this document).

Note that this technical reference does not cover the necessary testing required to meet many regulations of deployed systems. For instance, many deployments require periodic risk assessments. This testing should be done in accordance with the risk tolerance for each specific customer and all relevant regulatory requirements.

Sample Architecture

The following architecture is presented as a reference to be used during discussion in the document. It is intended to be sufficiently broad to cover many network architectures. While the network is represented as a star design in this example, the implemented architecture may take other forms (for example: redundant ring).



1 2 3 4 5 6

SECTION 2

Designing the Network for Security

Introduction

Why Read this Section?

In Section 2, the purpose is to detail a security architecture methodology. We also discuss the protection mechanisms in detail.

Contents of this Section

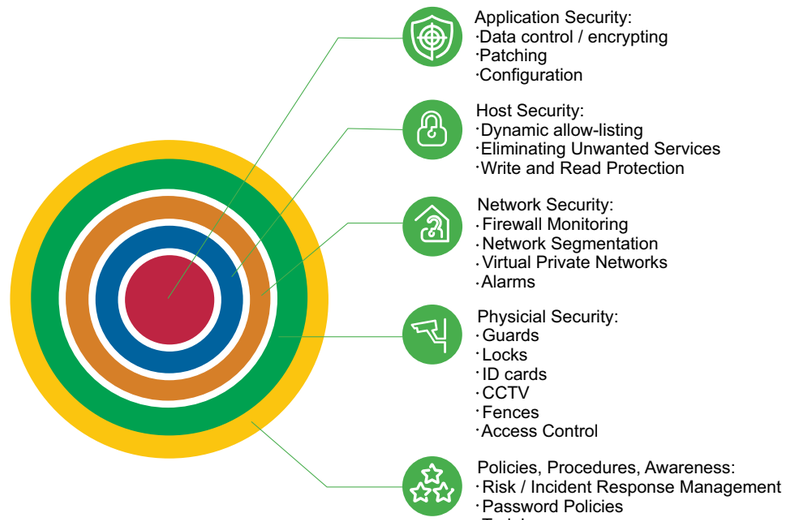
This section will follow the security architecture methodology as follows:

- Policies and Procedures
- Physical Security
- Network Security
- Host Security
- Application and Security
- Network Provisioning and Isolation
- Demilitarized Zone (DMZ)
- Virtual Private Network (VPN)
- Secure Network Integration
- Virtual Local Area Networks (VLANs)
- Server Network Backplanes
- Firewalls
- Perimeter Firewalls
- OT Firewalls
- Wireless Networks
- Application-level usage (HMI, Historian, Client Apps)
- Device Communication (Low-Level Protocols)
- ZigBee-Specific Security Measure
- Network Binding
- IPv4 and IPv6 Considerations
- OT Network Protocols
- Intrusion Detection System
- Unidirectional Gateways (Option)

Designing the Network for Security

Security Architecture Methodology

Designing a system for cyber security should involve a Defense in Depth approach. Also called the Castle Approach, this is a military strategy adapted by the United States National Security Agency (NSA) for use in cyber security.



Networks for critical facilities have the potential for many layers of protection. The following sections detail specific design requirements and suggestions to achieve a proper defense in depth implementation.

A description of each layer of this approach subsequent. Later sections of this document discuss the protection mechanisms in detail.

Designing the Network for Security

Defense in Depth

Policies and Procedures

The outermost layer, or the perimeter, includes policies and procedures related to accessing the network (these policies and procedures fall outside the scope of this document and will not be discussed; refer to IEC 62443 for more information). This is an important layer of the defense system and should be carefully designed. For example, implementing training for IT and OT managers on proper practices for managing the digital OT infrastructure should be provided. Specialists in OT cybersecurity like Schneider Electric can help the organization organize and implement such training

Physical Security

Physical security is the next defense against eavesdropping or other unauthorized connections. Firewalls and other security appliances are rendered useless if physical defenses are not properly designed to prevent access to the internal network.

All communicating devices must be physically protected from unauthorized access.

It is possible to provide these protections using secured networking closets or server racks with alarmed sensors to provide visibility and logging at the SCADA (supervisory) level. Additionally all Ethernet cable that is outside of the secured area (for example, a cable leading to an external device such as a generator control panel) must be enclosed in conduit or some similar tamperproof enclosure.

It is recommended to use tamperproof medium such as fiber-optic cable for exterior runs (fiber-optic cable should be enclosed in conduit when present outside of a secure area).

Network Security

This layer concentrates on the traditional network appliance-type of protection, namely firewalls, VPNs and network intrusion detection systems.

Host Security

This layer includes protections specifically available on the host (including computers and hardware devices). This includes anti-virus, application allow-listing and host-based intrusion detection software.

Application and Security

The inner-most layer includes the timely patching of operating systems and applications as well as any protections offered by the software running on the host. Common protections offered by application software is encrypting data in transit or at rest and two-factor authentication. This layer also includes setting security permissions on files and processes as well as setting access to data on hardware devices (for example, allowing or restricting access to specific Modbus registers on a device).

www.se.com
SECTION 2 | Designing the Network for Security
Designing the Network for Security

Protection Mechanisms

Network Provisioning and Isolation

While complete network planning is outside the scope of this document, this section will focus on cybersecurity-specific design elements such as network security appliances (firewalls, etc.).

There is no "one size fits all" approach to secure network design and there are many different network designs used in critical infrastructure. A redundant ring design is a popular choice to build a resilient architecture, offering high availability on a backbone and individual star networks spanning out to support downstream devices. Some deployments do not offer redundant networking architectures.

Regardless of the network architecture selected, it is imperative to consider how the Operational Technology (OT) network will be integrated with other networks (if at all), based on the risk tolerance deemed acceptable by the customer. Note that this includes performing a zone and conduit analysis (as required by IEC 62443-3-2).

Demilitarized Zone (DMZ)

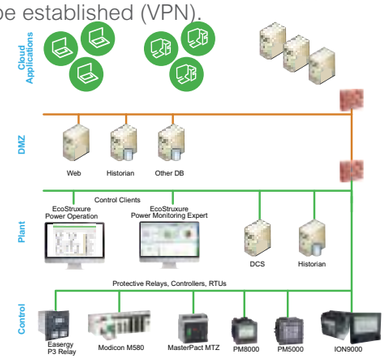
A DMZ is a subnetwork that provides a way to expose an organization's external-facing services to an untrusted network. Part of the defense-in-depth strategy, the DMZ allows for appropriate data access protecting sensitive networks and systems with firewalls.

If the OT network will be connected to any less secure network (corporate network or Wide Area Network (WAN)), it must connect through a properly configured DMZ. Deploying a DMZ consists of at least two firewalls and a server to provide the data to the less secure network.

Keep in mind that IT departments may consider the corporate network to be more secure than the "legacy based" OT network. However, a connection to the corporate network expands the attack surface providing additional access to the OT network. Additionally, OT network protocols might be invisible to IT network infrastructure (due to the limitations of IT infrastructure understanding low-level OT network protocols). For the purposes of this discussion, corporate networks are considered less-secure when compared to OT networks.

Connections to less secure networks must be through a DMZ.

As shown in the following figure, web servers and database servers may be placed in the DMZ to allow access to less secure networks. Of note, it is not acceptable to place Human Machine Interface (HMI) (with control capabilities) in the DMZ. If control is required from outside of the OT network, appropriate secured remote connections should be established (VPN).



Control clients (HMI) should never be placed in the DMZ Read-only display clients are acceptable in the DMZ.

Designing the Network for Security

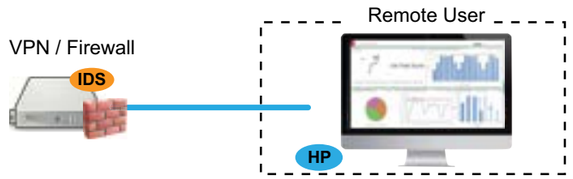
Virtual Private Network (VPN)

If control operations are necessary outside of the secure network, there must be a secure mechanism to provide access (such as a VPN with 2-factor authentication and host management capabilities).

Remote control operations (outside of the secure network) must be secured with an enterprise-grade VPN solution supporting 2-factor authentication and host management.

Two factor authentication requires a user to login with a password (something secret that they know) and something they have (the second factor). Often this second factor is a code sent by text message or a physical item such as a USB token. There is more information on two-factor authentication in subsequent sections.

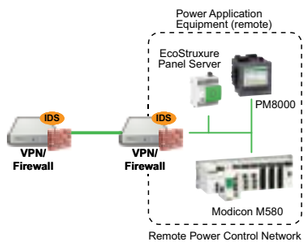
Host Access Control, or sometimes termed host management, involves the VPN client application running security checks on the computer used to connect to the VPN. If the security checks fail (for instance, out date antivirus), the VPN will refuse the connection.



Securing Remote Access with Vericlave

Vericlave is an alternative to a traditional VPN approach and offers considerable advantages including performance and simplicity (both in footprint and simplicity of usage). Vericlave is offered by Schneider Electric Cybersecurity Services and can be deployed in a plug-n-play configuration. This solution can provide secure communications between nodes in transit across any communication medium (including satellite, microwave and GSM). This solution is particularly attractive where the end user may have limited knowledge of security protocols and mechanisms (due to the ease of use).

Due to its ease of use, Vericlave is particularly attractive where the end user may have limited knowledge of security protocols and mechanisms. For more information on Vericlave, visit: www.vericlave.com.



Secure Network Integration

Some installations require multiple secure networks to be bonded or connected. Consider a deployment of a power system in a multi-building data center. Each building has a separate network and these networks must be connected. The networks may be bonded by Ethernet (twisted pair in conduit), fiber-optic (in conduit) or wireless (802.11 with WPA-2).

Regardless of the medium chosen, consider bonding these networks inside a VPN tunnel for added security. This is especially recommended for wireless communications.

Designing the Network for Security

Virtual Local Area Networks (VLANs)

VLANs are commonly used to segment a network logically (not necessarily grouped by physical location or network switch connection). VLANs are particularly helpful when you have a common network that is being used for multiple purposes. For instance, a single OT network may support a power monitoring and control system while simultaneously supporting a building management system.

To address data contamination issues (limiting the scope of broadcast messaging in specific protocols like IEC 61850) and manage bandwidth, it is appropriate to use VLANs. However, VLANs should never be used for security reasons (at least not by themselves). Techniques exist that allow for "VLAN-hopping", reducing the security of VLANs. Great care must be taken when designing and configuring VLANs to ensure that security is not compromised. For more information, SANS has a very informative article on this topic at: https://www.sans.org/white-papers/1090/.

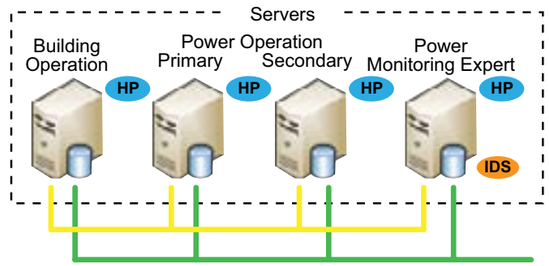
Consult with your Schneider Electric representative to obtain support on proper VLAN configurations and maintenance to implement countermeasures to layer 2 attacks.

Server Network Backplanes

Most deployments contain some element of server redundancy. For instance, EcoStruxure™ Power Operation is generally deployed on a primary and secondary server. These servers frequently communicate with one another to offer heartbeats and backfill data. It is suggested that a separate network is connected between the software servers to remove this overhead from the standard OT network. This simple technique involves two network interface cards (NICs) with one connected to the OT network and the second connected to a smaller network (backplane) that is specifically for interconnecting the servers. Note that **this is not a security requirement**; it is mentioned as it will offer additional bandwidth on the OT network.

Server network backplanes are generally confined to a server cabinet or server room and should be protected by physical security. If the server backplane must span physical locations, appropriate security measures should be placed (the server backplane should be treated as an OT network).

Additionally, security configuration on the servers should prevent routing between NICs and any changes to the configuration should be monitored to prevent unauthorized modification.



Note that some environments restrict the use of dual-homed or multiple NICs on a single server. Ensure that the use of a dedicated server backplane is compliant with applicable policies.

Designing the Network for Security

Firewalls

Considered the traditional protection against network breaches, firewalls are only one (albeit critical) component of a cybersecure network deployment. Firewalls offer the most visible element for use in defense in depth designs. A proper design includes many firewalls at different levels, including IT (perimeter) firewalls and OT firewalls (sectioning off a portion of the power monitoring and control network). Based on the situation a firewall such as the Palo Alto Networks PA-220 or PA-220R may be used.

Perimeter Firewalls

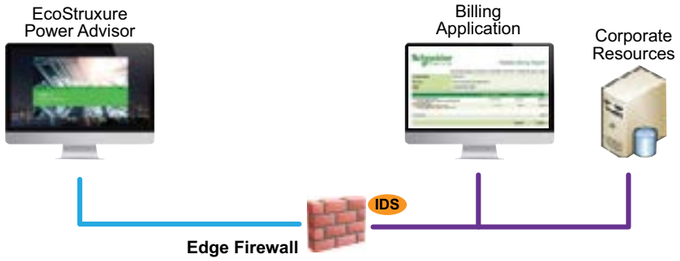
Perimeter firewalls include any firewalls that interact at the application layer and allow (or deny) access to applications (or users). These firewalls are used commonly in the DMZ and in any other situation where network security segmentation is desired. For instance, two networks with the same security posture (such as two data center networks in different buildings on the same campus) may be connected via firewall to provide further isolation. These firewalls can be configured to respond to Intrusion Detection Systems (IDS) and isolate areas of the network in the event of an attack. There is more detailed information on IDS provided in subsequent sections.

Perimeter firewalls must be used when connecting a secure network to a less-secure network.

Perimeter firewalls may be used when connecting two secure networks.

Traditional IT-centric firewalls are typically used as a perimeter firewalls in OT systems. These firewalls are usually capable of understanding application-specific protocols and features as well as integrate well within an existing enterprise installation. Many customers will have a brand of firewall that is familiar to their IT and may require that the firewall meets their guidelines for consistency.

Firewall configuration recommendations and requirements are covered in a later section.



Designing the Network for Security

OT Firewalls

OT firewalls are specific to the Industrial Control System (ICS) space and understand low-level protocols that are exchanged on the OT network. Examples of the protocols include Modbus, IEC-61850 and DNP3. OT firewalls should be placed inside of the enclosures that include the connected downstream devices (for instance, an OT firewall should be placed in the switchgear that contains ethernet-connected relays and gateways). These firewalls offer Deep Packet Inspection (DPI) for the OT protocols and this allows for a much more restrictive filter to be placed on allowable traffic.

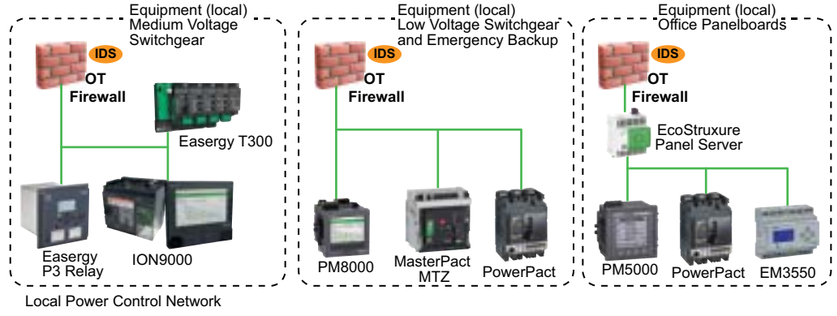
For instance, in addition to standard IP and port-based filtering, these firewalls can restrict Modbus "write" operations to a specific range of registers.

OT firewalls **must** be used when connecting to a secure network outside of a locked enclosure. This typically means one firewall per switchboard.

Make sure that the OT firewall selected meets the DPI criteria for the protocols used in the network. Inspect the DPI feature set carefully as this functionality varies widely from one manufacturer to another.

Like the perimeter firewall, the OT firewall can also be configured to respond to IDS alerts (as shown in the previous image). Note that careful consideration must be taken when configuring firewall rules (and actions in response to an IDS event). Misconfigured firewall rules and actions on an OT firewall can result in the loss of control and monitoring of critical systems.

Palo Alto Networks is one common provider of OT firewalls that meet ICS / OT network criteria. https://www.paloaltonetworks.com/.



Designing the Network for Security

Wireless Networks

Additional care must be taken when using wireless networking in critical infrastructure.

Configuration, naming conventions and segmentation of wireless access points are some countermeasures defined, configured and verified following the IEC 62443-2-4 standard.

There are three different categories of wireless networking to be considered:

- Application-level usage
- Device communications
- Network binding

Application-level usage

The most common type of wireless usage in critical infrastructure is for human interaction with the control system. This may include using a notebook computer to interact with an HMI display or for wireless phone or tablet access to a monitoring system.

Wireless Networks are a balance of security and convenience. By allowing wireless connections to access the control system, a multitude of defenses are "jumped over". For example, if the wireless network is on the internal "secure" network, then the upper-level firewalls are completely bypassed.

For this reason, it is a common approach to have multiple levels of protection on the wireless network. This may include a directory server for wireless connections (including two-factor authentication) and a secondary VPN (or Vericlave) connection (with another layer of two-factor authentication). At a minimum, wireless networks should have WPA2-Enterprise level security with a RADIUS server.

Wireless network configuration is a very complex topic and is beyond the scope of this document, but make sure to consider interest in this attack vector as it is a common method of penetration.

www.se.com
SECTION 2 | Designing the Network for Security
Designing the Network for Security

Device Communications (Low-Level Protocols)

In some situations, it may be necessary to communicate with devices with wireless protocols such as WiFi (802.11), ZigBee, or Bluetooth. It is imperative that these devices are secured (running in a secure mode such as WPA-2 for 802.11). Further, it is a common misconception that low-power devices are not susceptible to attack because their transmissions will not "get out" of the facility. This is not the case as there are high-gain receivers that specialize in observing this traffic from in some cases miles away.

Wireless device connections **must** be secured.

ZigBee-Specific Security Measures

Security of ZigBee-based connections is almost entirely dependent on the secure storage and transmission of the keys that are used to encrypt the communications.
The following concepts should be understood and practiced when deploying, maintaining and administering systems with ZigBee based devices:

- Key isolation and Anti-tampering – devices must protect symmetric keys from exposure or modification. This may include the use of a Trusted Platform Module (TPM) or Physical Unclonable Function (PUF).
- Key Transport – devices must not use a default key from the manufacturer.
- Key Establishment – out-of-band channels must be used to initially distribute the key (for example: serial port, NFC). This key distribution should only work if the target device is in pairing mode.
- Key Rotation – keys should be rotated (changed) after a pre-defined period or number of messages.

For more information on ZigBee security, review the document titled Wireless Personal Area Network Security Recommendations.

Network Binding

The final usage of wireless networks discussed here involves the interconnection of two networks. This typically involves the use of a rotating key service (or the less-secure pre-shared key). In addition to normal wireless security recommendations mentioned previously, a network binding connection should be dedicated (for example: not shared with application level usage or client computers).

Wireless connections for networking binding should **never** be used for other uses.

It is strongly recommended to use a VPN or Vericlave implementation on all wireless networks used for binding.

Designing the Network for Security

IPv4 and IPv6 Considerations

Most OT networks rely on IPv4 and many include Network Address Translation (NAT). By using NAT and IPv4, the OT network uses non-public IP addresses (usually of the 192.168.x.x or 10.x.x.x variety) to communicate. This offers and advantage of isolating internal addresses from the outside world (a router "converts" requests and responses from external addresses to these internal, private addresses). NAT is not generally considered a security mechanism but isolating (masking) the IP addresses of internal networking devices makes attack surface discovery substantially more difficult.

A description of NAT can be found at: https://en.wikipedia.org/wiki/Network_address_translation.

Unlike IPv4 with NAT, IPv6 allows each address to be publicly routable (if allowed by the perimeter firewall). As a result, extra precaution must be taken with IPv6 addressing to make sure that devices are not accessible on less secure networks. If IPv6 is chosen for deployment it is necessary to make sure that all software (including drivers) and hardware support the IPv6 standard (as many do not).

When configuring IPv4 addresses for devices on the OT network, ensure that all internal addresses are part of the official internal address ranges of 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 or 192.168.0.0-192.168.255.255. Using and IP address outside of this range may cause routing problems and false positives with IDS and other scanning systems.

OT Network Protocols

Many devices on the OT network operate with unsecured protocols. These protocols include, but are not limited to, Modbus, DNP3, BACNET, FTP, SNMP and IEC 61850.

If a device requires connectivity on an unsecured protocol, countermeasures should be taken to protect the device and the communication path. These countermeasures may include physical security, firewalls, VPN tunnels and intrusion detection mechanisms.

The usage of insecure protocols, even with countermeasures, carries and amount of residual risk that must be disclosed to and accepted. More information on this is available at: https://www.se.com/ww/en/work/services/cybersecurity-services/

Intrusion Detection System

An Intrusion Detection System (IDS), also referred to as Anomaly Detection, is a critical part of the defense network. This system actively monitors traffic on the network and can provide alerts when unusual traffic patterns are observed. These alerts can be pushed to HMI displays and other devices that are used to notify personnel. It is also possible to react to these alerts by actively re-configuring firewalls on demand (to reduce allowable traffic during a possible attack).

Like most cybersecurity solutions, IDS originated in the IT network space and has gained traction in the OT network. Recently, IDS implementations have been designed to specifically support ICS networks, making it much easier to detect and respond to anomalies on the OT network.

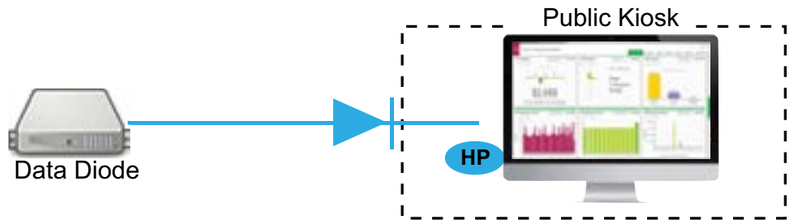
www.se.com

Designing the Network for Security

Unidirectional Gateways (Option)

Unidirectional Gateways, also referred to as Data Diodes, provide a secure means to egress (push) data out of a secure network to a less-secure network. A common example involves a campus where kiosks show energy saving as a result of an energy management plan.

Unidirectional gateways guarantee that data can only flow in one direction (from a secure network to the less secure network) by using hardware components and not relying solely on software configurations that could be vulnerable to attack.



SECTION 3

Configuration of Devices

Introduction

Why Read this Section?

This section focuses on power monitoring and control devices such as breakers, relays, power meters and bay controllers.

Contents of this Section

First, we explain the importance of updating all devices.

Then, to facilitate understanding, we define the configuration of all devices and network.

Finally, we explain the configuration of all devices and how to configurate a wireless networking.

Configure Hardware Devices

Update to Latest Firmware

All devices should be updated to the latest firmware prior to configuration. It is possible that device configuration will be lost during a firmware update. The firmware updates should be retrieved directly from the manufacturer's website. If available, verify signatures of the firmware to verify authenticity.

Always obtain firmware from official sources.

It is necessary to make sure that the security posture of the system is preserved after the update. This can be accomplished by having a documented process during commissioning or maintenance to restore security configurations.

If using compatible devices, it may be useful to use the EcoStruxure™ Power Commission tool to setup and maintain hardware devices. In order to setup and maintain hardware devices use the appropriate setup software such as EcoStruxure™ Power Commission. More information on this software is available at: https://www.se.com/ww/en/product-range/62980-ecostruxure-power-commission/#overview.

User Accounts / Set Passwords

All devices should be configured with a new administrative password. Administrative passwords should meet complexity rules as defined by the organization (per regulatory requirements).

Passwords should **never** be left in their default state.

Passwords must be securely delivered and exchanged with the customer (never written down or stored in plain text). One recommendation is a text file inside of an encrypted ZIP file. For instance, send the encrypted ZIP file via email to the customer and then send the password to the zip file via text message. Another option is to use password management software such as KeePass to manage credentials. More information about KeePass is available at https://keepass.info.

Passwords **must** be exchanged and delivered in a secure manner.

Make sure that any unused user account is disabled. This includes guest accounts. A process must also be in place to notify the customer of changes in service provider (including any personnel or entity with access to system credentials).

Note that systems targeting protections against unintentional or coincidental Cybersecurity events (referred to Security Level 1 in IEC 62443), however for systems targeting protections against intentional, but low sophistication security events (referred to as Security Level 2 in IEC 62443) and above requires unique passwords (each device or user has their own password).

www.se.com
SECTION 3 | Configuration of Devices
Configure Hardware Devices

Network Configuration

The network configuration should be set in accordance with the deployment plan. While not a security issue, it is recommended to use static IP addresses for power monitoring and control devices. A record should be kept of all device IP addresses, MAC addresses, TCP/UDP ports, device names and locations. This information is useful when configuring firewalls and intrusion detection systems.

Note that the IEC 62443-2-4 standard requires accurate records and drawings of the logical and physical infrastructure. The documentation must be kept current and must include all network devices, internal interfaces and external interfaces.

Disabling Unused Functions

All devices should be configured to turn off all unused services and "ports". This includes disabling unused Ethernet, wireless, field bus, NFC, USB and infrared ports. In some cases, it may be necessary to use a physical barrier, especially with USB ports. USB ports that cannot be disabled in the device should be disabled using super glue or similar. If there is reason to use the port in the future, tamper-proof USB locking covers are available for this purpose. While not as effective as permanent disablement, these locking covers can indicate tampering.

It is also necessary to disable certain unused features. Many devices include a web server, FTP server, NTP server, SMTP server and/or DHCP server. Disable any servers that will not be actively used in this deployment. Not only will this reduce the sustaining of the system, but it will also greatly reduce the attack surface of these devices.

If the device requires the use of insecure protocols (as detailed earlier in this document), perform a gap assessment and identify the appropriate countermeasures necessary to accommodate the customer's risk tolerance. For assistance, contact your local Schneider Electric representative.

This process should be done in accordance with a threat map (an activity required by IEC 62443-4-1) and the acceptable risk tolerance of the customer.

Wireless Networking

Wireless networking (ZigBee) should be configured to operate as securely as the device supports. If no security is offered on the wireless interface, the wireless transceiver should be disabled entirely when operating in critical infrastructure. Contact the device manufacturer for possible alternative connection methods.

Never enable an unsecured wireless connection.

SECTION 4

Configuration of Servers

Introduction

Why Read this Section?

This section focuses on the preparation and maintenance procedures of PC hardware (server) prior to installation of application software. Continued configuration of the server will be discussed in "Section 6" Integration and Hardening.

Contents of this Section

For each procedure of PC hardware (server) prior to installation, the related parameters are presented as follows:

- Update BIOS
- Update Operating System
- Uninstall Unnecessary Applications

Configure Servers

Hardware and Operating System

Update BIOS

Due to the recent hardware related vulnerabilities (for example: Spectre, Meltdown), it is crucial that all servers and workstations have the most recent BIOS installed. These BIOS updates should be downloaded directly from the PC manufacturer's website (do not apply BIOS updates form and unknown origin).

Never apply BIOS updates from and unknown origin (such as a Google search result).

Update Operating System

All servers and workstations should be updated using the Windows Update function of the operating system. Application software should not be deployed until all Windows updates have been applied. It is also recommended to make sure all drivers are updated to the most recent versions available. Driver updates should be downloaded directly from the manufacturer's website.

It is highly recommended to have a "testbed environment" to update and validate before applying updates to a live production system. This applies to operating system and application updates.

Never apply Windows or driver updates from an unknown origin (such as Google search result).

Uninstall Unnecessary Applications

Most servers and workstations come pre-loaded from the manufacturer with "bundled" applications. Some of the applications are used for supporting the system and others are simply productivity applications. It is strong recommended to uninstall any unused applications. Be especially cautious with preloaded applications that provide remote support assistance (these should be uninstalled.

Uninstall any preloaded applications that provide remote assistance.

It may be desirable to format or wipe the hard drive and install a fresh copy of the operating system (only). This provides a clean slate without the preloaded applications.

Unused services should also be disabled on servers and workstations. This includes unused DHCP, TELNET, DNS, FTP and web servers.

Always disable any unused services on servers and workstations.

SECTION 5

Configuration of Software Products

Introduction

Why Read this Section?

This section focuses on software application deployment on servers and workstations.

Contents of this Section

We explain how to configure Power Operation and Power Monitoring Expert (PME).
We also mention the Cybersecurity Admin Expert (CAE) application.

Configure Software Products

EcoStruxure™ Power Operation

Install Application and Product Updates

Following the Power Operation System Guide, ensure that the product is installed and all available updates have been applied. Pay attention to the Cybersecurity related directions in the guide (located under Configuration → Cybersecurity).

Active Directory Integration

Power Operation supports Windows integrated users (which provides connection to Windows Active Directory). Follow the directions in the Power Operation System Guide to enable integrated user support.

Roles, permissions, and privileges should also be configured at this time.

Two Factor Authentication

Power Operation supports two-factor authentication via YubiKey. This solution does not require Internet connectivity and is required for upper levels of IEC 62443 compliance. Follow the directions in the Power Operation System Guide to enable two-factor authentication.

Visit https://www.yubico.com for more information on YubiKey devices.

Notification (SSL) / Prefer GSM

Power Operation supports notification of alarms and events via email and text message (SMS via GSM modem). If using email (SMTP), make sure that the configuration specifies SSL for the SMTP connection. For additional security (with no need for a connection to the Internet / SMTP server), it is recommended to use a GSM modem with SMS. This solution uses a local GSM modem that is configured to send outbound SMS only (no data connection).

HTTPS

Power Operation supports HTTPS (TLS v1.2) via the use of an optional module called Power Operation Anywhere with Secure Gateway. This is required if there will be workstations of clients that are accessible outside of the OT (secure) network. Deployment of this module relies on the use of Active Directory with a domain controller (it will not work with local windows user accounts).

Domain integration across OT and IT networks must be analyzed and trust relationships must be clearly defined to prevent unauthorized access.

Operating System Firewall

The Windows Defender Firewall should be adjusted to allow appropriate traffic to and from the server and workstation. For servers and workstations, refer to the Power Operation System Guide for ports that should be allowed (Configuring → Cybersecurity → Configuring Power Operation for Network Segmentation).

Configure Software Products

EcoStruxure™ Power Monitoring Expert (PME)

Install Application and Product Updates

Following the PME System Guide, make sure that the product is installed and all available updates are applied. Pay attention to the Cybersecurity related directions in the guide (located under Configuration → Cybersecurity).

Active Directory Integration

PME supports Windows Active Directory. Follow the directions in the PME System Guide to enable Active Directory support (Configuring → User Manager).

Operating System Firewall

The Windows firewall should be adjusted to allow appropriate traffic to and from the server and workstation. For servers and workstations, refer to the PME System Guide for ports that should be allowed (Planning → IT Requirement → Network Connectivity).

HTTPS

PME Supports HTTPS and is installed with a self-signed certificate. It is recommended that this is replaced with a certificate from a server acting as a Certificate Authority (CA). Refer to the PME System Guide for more information (Planning → System Installation and Upgrades → Install Planning).

If self-signed certificates are used, public key certificates should be deployed to all peers that require access.

Cybersecurity Admin Expert (CAE)

Cybersecurity Admin Expert (CAE) is an application that is used to configure various security parameters on software and hardware devices in a system. This application is also used for certificate management. This application is usually used on an engineering laptop connected to the ICS network or it may be installed on a server on premise.

CAE operates on a concept known as a Role Based Access Control (RBAC) and security policy. For more information on CAE, review the CAE User Guide.

More information on CAE is available here: https://www.se.com/ww/en/product-range/63515-ecostruxure%E2%84%A2-cybersecurity-admin-expert.

SECTION 6

Integration and Hardening

Introduction

Why Read this Section?

The objective of this section is to concentrate on integration topics and server/workstation hardening the servers and workstations.

Contents of this Section

This section will follow the security architecture methodology as follows:

- Software Integration (Power Operation and PME)
- Time Synchronization
- Patch Management
- Backup Solution
- UPS Software
- McAfee Application Control
- Antivirus
- Cloud Connectivity
- Password Configuration
- Logging Configuration
- Disable Unused Ports
- OT Firewall Configuration
- Deep Packet Inspection
- IDS Integration

Integration and Hardening

Software Integration (Power Operation and PME)

Many large and critical facilities employ a combination of software products that must be integrated together, specifically Power Operation and PME. Following the appropriate system guides, perform the integration steps listed. Make sure that a server backplane network is used for these communications (and firewalled appropriately). Further, enable encryption where available on the interfaces used in the integration.

Time Synchronization

Time synchronization is a typical feature of power systems in critical infrastructure. This synchronization is achieved by several methods, including Precision Time Protocol (PTP), Network Time Protocol (NTP) and other legacy interfaces such as IRIG and DCF77. In addition to providing accurate time stamps for power related events, this accurate timestamping is crucial for correlating security events across multiple network devices and other infrastructure. Selection of a time synchronization service depends on the unique requirements of the deployment, but PTP is the recommended solution for most deployments. Note that PTP support is generally focused on hardware devices (such as power meters and PLCs).

Patch Management

Operating system and product patches and updates must be carefully managed in a critical installation. This can be made easier by using services that offer automated patching and device reboot control. Additionally, some services providers make available reports that are necessary for IEC 62443-2-4 compliance.

Backup Solution

Disaster Recovery is a necessary component of any critical installation. In addition to help protect against hardware failure, this is an absolute necessity to protect against ransomware and similar attacks. The customer may have an adopted approach for disaster recovery and it is possible to integrate both Power Operation and PME with most IT-centric disaster recovery mechanisms. Refer to the appropriate system guide for details.

UPS Software

Uninterruptable Power Supplies (UPS) are used to provide power conditioning and ride-through capabilities. If supported, ensure that proper integration is achieved with the UPS infrastructure.

In critical infrastructure, suggested UPS implementations include the Galaxy and Gutor ranges of devices. More information on these products available here: https://www.se.com/us/en/product-subcategory/55615-data-center-and-facility-3-phase-ups.

Server and Workstation Hardening

This is not fully inclusive and additional measures may need to be taken for a specific environment. For instance, a workstation may need a specific configuration to disable the Start Menu, task manager or screensavers. Refer to documentation for the specific operating systems for guidance.

McAfee Application Control

McAfee Application Control is a allow-listing application that should be deployed on servers and workstations in critical installations. This is highly recommended as a software allow-list will prevent execution and file access to anything that is not trusted. This is available as an option for both Power Operation and PME (only one license is needed per physical server) and is deployed similar to an installation of antivirus. Application allow-listing does not require Internet access as it does not require definition updates. Application allow-listing is considered a higher level of security when compared to antivirus.

Always use application allow-listing on servers in critical infrastructure.

Application allow-listing is not recommended for workstations where applications may be installed and/or uninstalled frequently or where files are exchanged. An antivirus solution is more appropriate in this situation.

Antivirus

Antivirus should be deployed on workstations that are not running application allow-listing. It is imperative that antivirus receive frequent definition updates. If Internet connectivity is not available preventing definition updates, application allow-listing must be used.

A malware protection strategy should be defined for components that cannot support application allow-listing or antivirus.

Cloud Connectivity

If cloud connectivity is desired, it is recommended that the cloud connected device resides in the Demilitarized Zone and is configured for encrypted communication with the cloud service. Application security may be required depending on the acceptable risk tolerance for the vertical or the specific costumer.

www.se.com

www.se.com

SECTION 6 | Integration and Hardening

Configure Network Devices

Password Configuration

Most network devices have a web portal that can be accessed by commonly known default passwords. All network devices should have the default passwords changed. Make sure that passwords (and other sensitive information) is encrypted (this includes enabling HTTPS, for instance).

Always change the default passwords for networking equipment.

Logging Configuration

Many network devices support forwarding logs to a SYSLOG or SIEM server. If available configure network devices to forward logs.

Note that this is a requirement for IEC 62443-2-4 and must be configured, validated and tested during FAT/SAT and maintenance sessions.

Disable Unused Ports

Network devices should be configured to disable any unused ports. A port is considered unused if a device is not actively connected. For instance, a port that is connected to a wall outlet with no device connected is considered unused (connectivity to a wall outlet does not justify the port being in use).

OT Firewall Configuration

Analyze each layer of the network to determine the protocols and ports that should be allowed. For instance, a firewall embedded in switchgear may only need to pass Modbus traffic on TCP port 502. In addition to port rules, consider adding source IP addresses to the rules (for instance allow port 502 to be accessed only from the source IP that belongs to the Power Operation server). This helps prevent simple packet injection (but does not completely mitigate it due to the ability to spoof IP addresses). Full mitigation will require transport encryption such as VPN connection.

Deep Packet Inspection

Many OT firewalls support Deep Packet Inspection (DPI) for popular ICS protocols (such as Modbus, DNP3 and IEC 61850). For heightened security, consider adding rules to the switchgear firewall that filter bases on Modbus address range and function code (in addition to source IP and port). A rule, for instance, could allow traffic from a specific IP address on port 502 with a Modbus Read command on registers 4001-4002. Refer to the firewall documentation for information on specific DPI features and configuration.

IDS Integration

Some OT firewalls support the ability to react to alerts from an intrusion detection system. If available, follow the firewall and IDS documentation to configure the firewall to react to an event by appropriately tightening the rules.

Bibliography

Useful Documentation

Design Guide

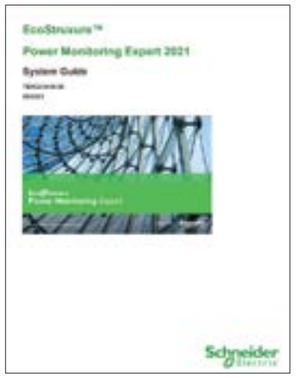
Digital Applications for Large Buildings and Critical Facilities

The Digital Applications Design Guide provides comprehensive details on the building blocks of EcoStruxure™ Power: the IoT applications are driven by a software layer to control the traditional electrical distribution infrastructure. Developed to help engineering consultants and designers, this guide is an invaluable resource for specifying, designing and prescribing EcoStruxure™ Power architectures capable of performing one or more of the business-driven applications described within.

EcoStruxure™ Power Design Guide for North America
Ref: 0100DB1802R11/20
11/2020

https://download.schneider-electric.com/files?p_Doc_Ref=0100DB1802

System Guides



EcoStruxure™ Power Monitoring Expert 2021

Power Monitoring Expert system design, deployment and usage.

System Guide
Ref: 7EN02-0445
PowerMonitoringExpertSysGuide
05/2021

https://www.se.com/ww/en/download/document/7EN02-0445//

EcoStruxure™ Power Operation 2021 with Advanced Reporting and Dashboards

Power Operation system design, deployment and usage.

System Guide
Ref: 7EN02-0462-00
PowerOperationSystemGuide
07/2021

https://www.se.com/ww/en/download/document/7EN02-0440/

Useful Documentation

Certificates

EcoStruxure™ Power Monitoring Expert

PME Cybersecurity IEC 62443 Certificate

Certificate
01/2019

https://www.se.com/us/en/download/document/cybersecurity/

EcoStruxure™ Power System for Large & Critical Facilities

ESXP Certificate - IEC 62443-3-3 Large & Critical Architecture

Certificate
07/2021

https://www.se.com/us/en/download/document/EcoStruxure/

EcoStruxure™ Power Operation

Power Operation 2021 IEC 62443 SL2 Certificate

Certificate
08/2021

https://www.se.com/us/en/download/document/IEC62443/

Green Premium™

An industry leading portfolio of offers delivering sustainable value

More than 75% of our product sales offer superior transparency on the material content, regulatory information and environmental impact of our products:

- RoHS compliance
- REACh substance information
- Industry leading # of PEP's*
- Circularity instructions

Discover what we mean by green
Check your products!

The Green Premium program stands for our commitment to deliver customer valued sustainable performance. It has been upgraded with recognized environmental claims and extended to cover all offers including Products, Services and Solutions.

CO_2 and P&L impact through… Resource Performance

Green Premium brings improved resource efficiency throughout an asset's lifecycle. This includes efficient use of energy and natural resources, along with the minimization of CO_2 emissions.

Cost of ownership optimization through… Circular Performance

We're helping our customers optimize the total cost of ownership of their assets. To do this, we provide IoT-enabled solutions, as well as upgrade, repair, retrofit, and remanufacture services.

Peace of mind through… Well-being Performance

Green Premium products are RoHS and REACh compliant. We're going beyond regulatory compliance with step-by-step substitution of certain materials and substances from our products.

Improved sales through… Differentiation

Green Premium delivers strong value propositions through third-party labels and services. By collaborating with third-party organizations we can support our customers in meeting their sustainability goals such as green building certifications.

*PEP: Product Environmental Profile (i.e. Environmental Product Declaration)

Legal information

www.se.com

Notes

Notes

Schneider Electric USA, Inc.

800 Federal Street
Andover, MA 01810 USA
888-778-2733

www.se.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

10/2021
ESXP2TG003EN

Life Is On Schneider Electric