A practical guide to maximizing the resilience of your EcoStruxure Triconex Safety Systems against cyber threats.

by Steve J Elliott, Senior Marketing Director – EcoStruxure Triconex Safety Systems

Executive summary

Safety Instrumented Systems are a vital layer of protection and often form the last line of defense between you and a potential incident.

Typically these systems are designed to mitigate process risks within the boundary of the operating asset. However the threats are no longer contained within the walls of the operating asset and are now subject to “digital” threats caused by malicious attacks from outside of the boundary.

This paper looks at the some of the practical means and mechanisms available to maximize the resilience and minimize the vulnerabilities of your EcoStruxure Triconex Safety Systems.

Introduction

The exponential increase in cyber-threat levels

Over the last decade, the rise in cyber-attacks on critical infrastructure has resulted in cybersecurity becoming a central concern amongst industrial automation and control system users and vendors. These strategic attacks are aimed at disrupting industrial activity for monetary, competitive, political or social gain, or even as a result of a personal grievance.

Many industrial operations rely on electrical/electronic/programmable electronic (E/E/PE) Safety Instrumented Systems as a layer of protection to keep them safe from harm or damage to people, production and profits.

The days of a safety system being an island no longer exist, as systems require patching and updates on a regular basis. There is a growing demand to integrate SIS with control systems to facilitate one consistent methodology for updating systems. As these systems are electronic, often connected to other equipment such as engineering workstations, Distributed Control Systems (DCS) and plant historians, they should now be considered in any cybersecurity program(s). However, every added connection results in increased risk.

Reduce the threats of a cyber-attack on your operations

When implementing any cybersecurity solution a defense-in-depth approach should always be considered. In this paper we will take a practical look at a multi-layered approach and some of the practical methods that can be implemented to make EcoStruxure Triconex Safety Systems more robust and minimize the likelihood of cyber related incidents.

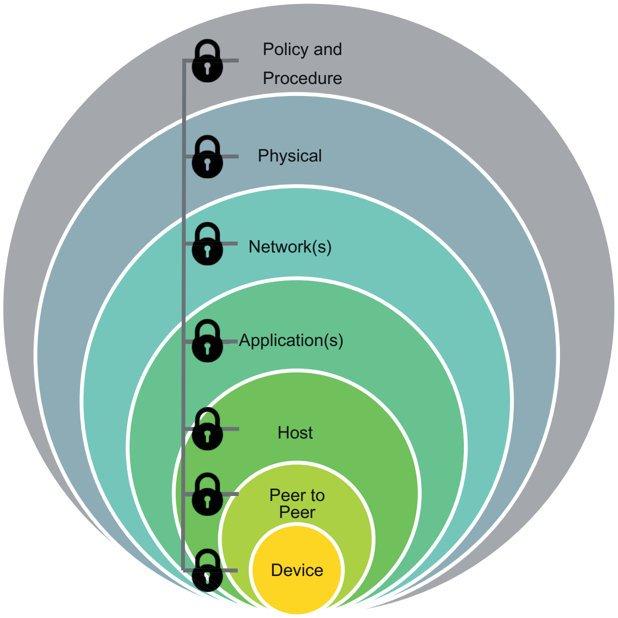


Figure 1

Apply a defence in depth approach to help secure your EcoStruxure Triconex Safety Systems.

Topics in this paper include:

- Know and understand the cybersecurity risks
- Get help from the safety (IEC61511) and security (IEC62443) standards
- Implement a secure architecture
- Apply zones and conduits
- Develop a sustainable cybersecurity program

5 key security consideration

Organizations should apply the following steps toward a more robust security environment and significantly reduce the risk to operational safety systems.

1. Identify, minimize, and secure all network connections to the safety system.
2. Harden the safety system and supporting systems by disabling unnecessary services, ports, and protocols: enable available security features: and implement robust configuration management practices.
3. Continually monitor and assess the security of the safety system, networks, and interconnections.
4. Implement a risk-based defense-in-depth approach to securing safety system systems and networks.
5. Manage the human – clearly identify requirements for the safety system: establish expectations for performance: hold individuals accountable for their performance: establish policies: and provide safety system security training for all operators and administrators.

TIP 1

Establish a common vocabulary that everyone understands and use it consistently

Phrases, expressions, acronyms can mean different things to different people, in this paper we will use the following definitions:

- **Vulnerability:** weakness in an Industrial Control Systems (ICS) function, procedure, internal control or implementation that could be exploited or triggered by a threat source.
- **Threat:** any circumstance or event with the potential to adversely affect organizational operations, assets, industrial Control Systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service.

It is extremely important to establish a common vocabulary that everyone understands and then use it consistently. Make sure that everyone knows and understands the threats, the vulnerabilities and the potential impact on the business.

Get help from the standards

Cybersecurity is evolving in a similar trend to that of functional safety. Just as safety standards have been evolving for the last 20+ years, cybersecurity standards are being developed that provide a consistent framework, good engineering practice and a systematic method for implementing cybersecurity protection methods.

In this paper we will reference two standards:

- IEC61511-1:2016 – Functional safety – Safety instrumented systems for the process industry sector
- IEC62443-3-3:201 3 – Industrial communication networks – Network and system security

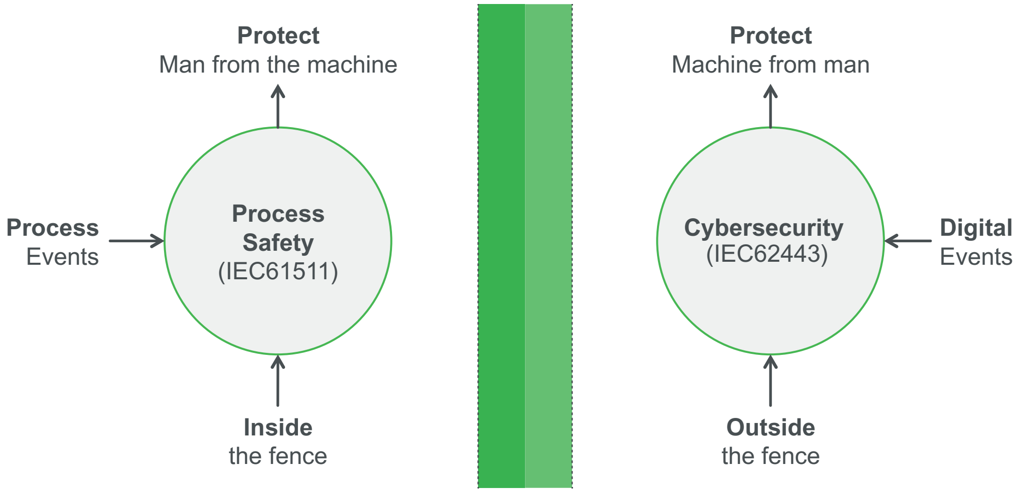


Figure 2

Functional Safety and Cybersecurity standards have much in common.

Take a lifecycle approach

The approach to cybersecurity is very similar to that of functional safety i.e. it follows a lifecycle:

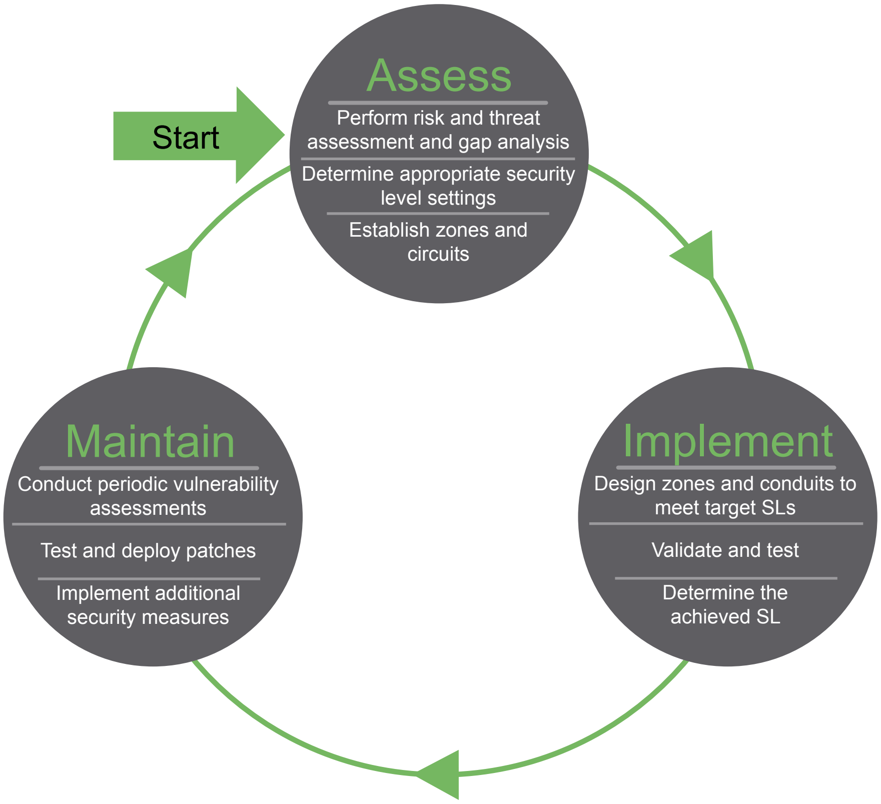

Start
Assess
Perform risk and threat assessment and gap analysis
Determine appropriate security level settings
Establish zones and circuits
Implement
Design zones and conduits to meet target SLs
Validate and test
Determine the achieved SL
Maintain
Conduct periodic vulnerability assessments
Test and deploy patches
Implement additional security measures

Figure 3

Example cybersecurity lifecycle.

The overall objective is to ensure that cybersecurity protection methods are addressed across the entire lifecycle and not as an "add-on" when the system is delivered.

This approach is re-enforced by IEC61511-1:2016 which includes requirements for cybersecurity threats to be addressed during the various safety lifecycle stages and activities:

8. Process Hazard and Risk Assessment (H&RA)

8.24 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- a description of the devices covered by this risk assessment (e.g. SIS, BPCS or any other device connected to the SIS);
- a description of identified threats that could exploit vulnerabilities and result in security events (including Intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);
- a description of the potential consequences resulting from the security events and the likelihood of these events occurring:
- consideration of various phases such as design, implementation, commissioning, operation and maintenance.
- the determination of requirements for additional risk reduction:
- a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1 Guidance related to SIS security is provided is IS TR84.00.09, IO/IE 27001:2013, and IEC 62443-2-1-2010

Figure 4

IEC61511 Edition 2. Section 8 process Hazard and Risk Assessment (H&RA).

11. SIS design and engineering

11.2.12 The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).

11.7.3.2 The maintenance/engineering Interface shall provide the following functions with access security protection to each

- SIS mode of operation, program, data, means of disabling alarm communication, test bypass, maintenance;
- SIS diagnostic. voting and fault handling services;
- add, delete, or modify application program;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

11.7.3.4 Enabling and disabling the read-write access shall be carried out only by a configuration management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

11.8.6 Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).

Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.

Figure 5

IEC61511 Edition 2, section 11 SIS design and engineering.

12. SIS application program development

12.4.2 The following information shall be contained in the application program or related documentation:

a) the application program originator;

b) a description of the purpose of the application program;

c) the versions of the safety manuals that were used;

d) identification of the dependency of each SIF on the parts (modules) of the application program;

e) traceability to the application program safety requirements specification;

f) identification of each SIF and its SIL;

g) identification and description of the symbols used, including logic conventions, standard library functions, application library functions;

h) identification of the SIS logic solver input and output signals;

i) where the overall SIS utilizes communications, a description of the communications information flow;

NOTE: An example would be where a SIF uses several logic solvers.

j) a description of the program structure, including a description of the order of the logical processing of data with respect to the input/output sub-systems and any limitations imposed by scan times;

k) if required by the SRS, the means by which:

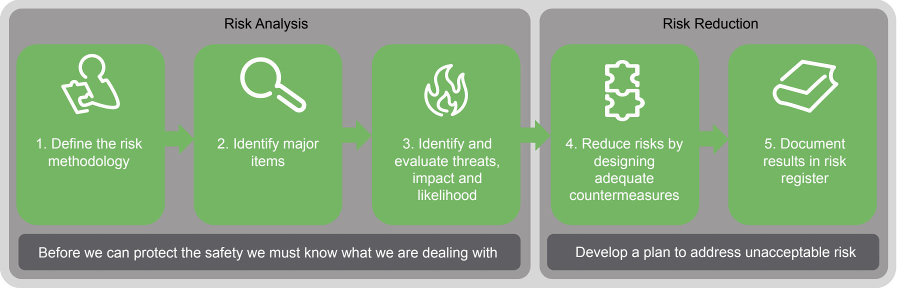
- the correctness of the field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);
- the correctness of data sent over a communication link is ensured (e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted);
- communications are made secure (e.g., cybersecurity measures).

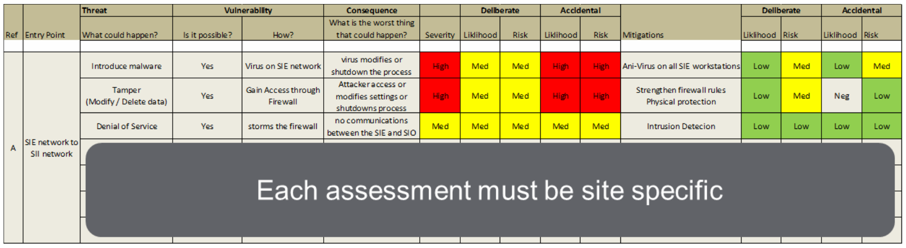
l) version identification and a history of changes.

Figure 6

IEC61511 Edition 2, section 12 SIS application program development.

A cybersecurity risk assessment should be performed at an early stage of any project be it a new project or after a modification. A typical 5 step approach, as shown below, should be viewed as an iterative and continuous process:


Risk Analysis
Risk Reduction
1. Define the risk methodology
2. Identify major items
3. Identify and evaluate threats, impact and likelihood
4. Reduce risks by designing adequate countermeasures
5. Document results in risk register
Before we can protect the safety we must know what we are dealing with
Develop a plan to address unacceptable risk



		Threat	Vulnerability		Consequence		Deliberate		Accidental			Deliberate		Accidental	
Ref	Entry Point	What could happen?	Is it possible?	How?	What is the worst thing that could happen?	Severity	Liklihood	Risk	Liklihood	Risk	Mitigations	Liklihood	Risk	Liklihood	Risk
A	SIE network to SII network	Introduce malware	Yes	Virus on SIE network	virus modifies or shutdown the process	High	Med	Med	High	High	Ani-Virus on all SIE workstations	Low	Med	Low	Med
		Tamper (Modify / Delete data)	Yes	Gain Access through Firewall	Attacker access or modifies settings or shutdowns process	High	Med	Med	High	High	Strengthen firewall rules Physical protection	Low	Med	Neg	Low
		Denial of Service	Yes	storms the firewall	no communications between the SIE and SIO	Med	Med	Med	Med	Med	Intrusion Detecion	Low	Low	Low	Low

Each assessment must be site specific

Figure 7

5 step cybersecurity risk assessment.

Based on the risk assessment and the potential consequence, the systems should be assigned a security profile or security level which determines the minimum level of cybersecurity protection method. As the safety systems are often the last line of defense between an initiating cause and a hazardous event, these should always be treated with the most stringent protection.

Implement a secure architecture

In the fast changing world of cybersecurity it is important to stay current with the latest manufacturer's recommendations and guidelines. Much of the information in this white paper has been extracted from the EcoStruxure Triconex product literature.

- Tricon Planning and installation guide (Assembly Number 9700077-022)
- Trident Planning and installation guide (Assembly Number 9700110-010)
- Tri-GP Planning and installation guide (Assembly Number 9700122-007)
- TriStation 1131 Developer Guide (Assembly Number 9700100-09)

TIP 2

Always check the manufactures published data for the latest information.

Important Note: for product manuals and information please refer to the Global Customer Support website https://pasupport.schneider-electric.com

When we look at a typical EcoStruxure Triconex safety solution architecture it encompasses many different elements that combine to make the system.

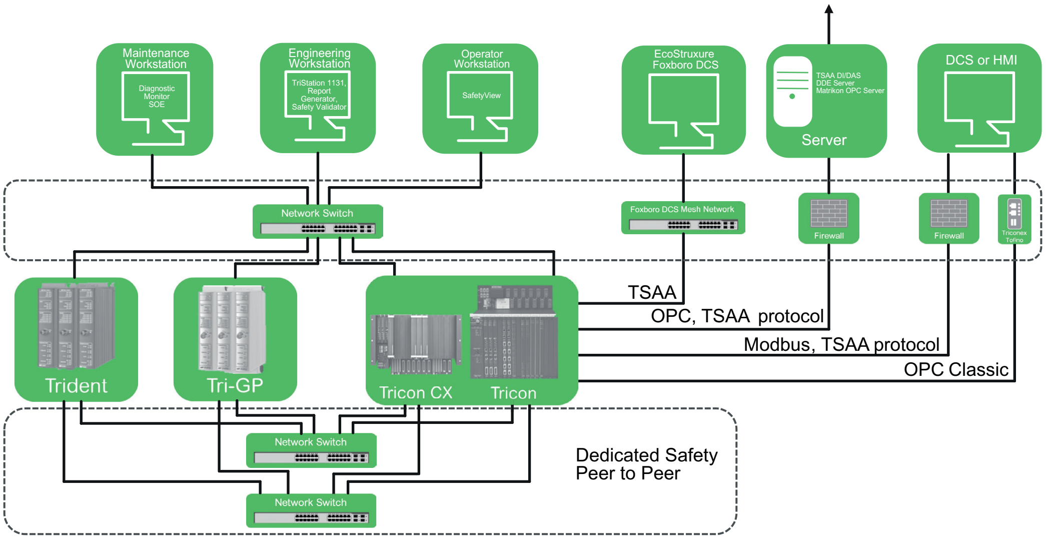


Figure 8

Typical elements that make up an EcoStruxure Triconex Safety Systems architecture.

You should always assess the security threats to your system within the context of the overall plant hierarchy and architecture, any applicable standards, industry best practices, including your corporate practices, policies and procedures.

Step 1- Secure the device

Secure the Device

The first step in securing any EcoStruxure Triconex Safety System should be to secure the device itself (device = the Tricon, Tricon CX, Trident or Tri-GP Logic Solver). To reduce the security risk associated with the controller, you should:

- Use the Access Control List in the TriStation 1131 software to control access to TCM or UCM resources. For more information, see the TriStation 1131 Developer's Guide.
- Design your control application so that it reads and reports the position of the key switch to the operator.
- Keep the controller in Run mode or Remote mode.
- If you want to remotely access the Tricon controller, you should take care to evaluate and mitigate all security threats to the necessary level per your organization's security policy, following industry best practices and applicable standards.
- Use physical means, such as a locked cabinet, to protect the Main Chassis and Expansion Chassis, including debug ports on modules.

- Implement organizational procedures to control access to the key that unlocks the cabinet/enclosure that contains the controller. Consider keeping a log of the personnel who are granted physical access to the controller.

There are a number of inherent cybersecurity features in each of the EcoStruxure Triconex controllers and associated versions:

Table 1

Tricon/Tricon CX system cybersecurity features.

Tricon Version	Feature
Version 11.0 and earlier	Integrated physical Key switch to prevent unauthorized writes IP White List; Modbus, TSAA protocol, network write enable configuration EcoStruxure Triconex - Tofino device for OPC Classic/additional security layer (firewall) Achilles Level 1 Certified
Version 11.1	Certified by TUV Rheinland for Safety & Security per IEC 62443-4-1 and IEC 62443-4-2 for Security Level 1 Achilles Level 2 Certified Security Considerations for end users added to the user manuals

Table 2

Trident and Triconex General Purpose system cybersecurity features

Trident / Tri-GP Version	Feature
Version 2.x and earlier	User implemented Key switch using function blocks to prevent unauthorized writes IP White List; Modbus, TSAA protocol, network write enable configuration Achilles Level 1 certified
Version 3.0	Strong authentication and encryption of HMI communications via OPC UA security profile using self-signed X509 certificates Strong authentication and encryption of Trident to TriStation communications using self-signed X509 Certificates Configure system to generate alert/alarm prior to certificate expiration Achilles Level 1 certified

Step 2 – secure device peer to peer communication

To reduce the security risks associated with a safety peer-to-peer network, follow these guidelines:

- Confine the network to use of peer to peer communications between devices only.
- Configure network switches and routers in a manner that limits the addition of unauthorized network nodes.
- Use external firewalls to limit the network traffic to only safety peer-to-peer network traffic.
- Use TCMs that are dedicated to the safety peer-to-peer network.
- Use redundant TCMs/UCMs with network redundancy to other Tricon controllers.

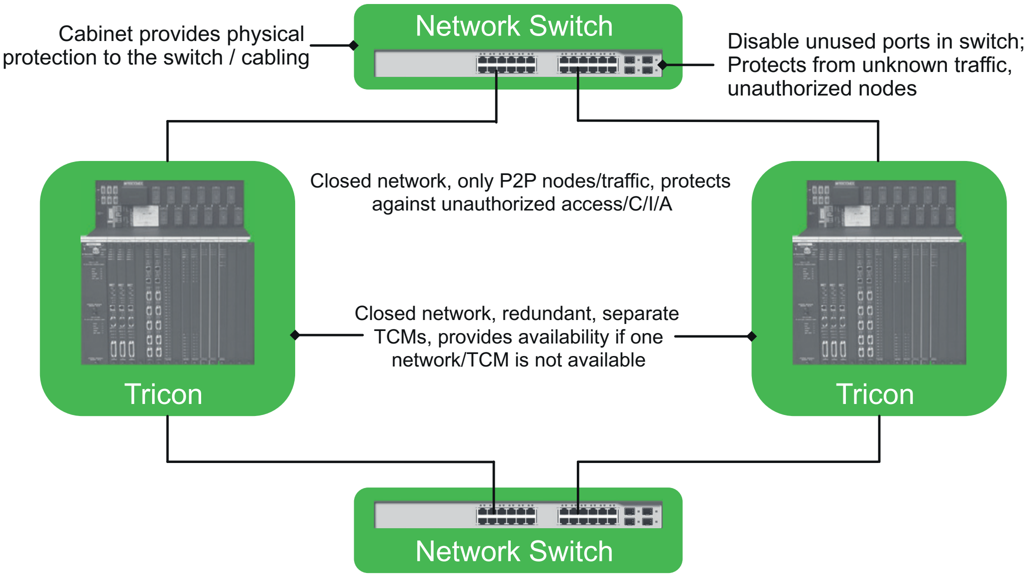

Cabinet provides physical protection to the switch / cabling
Network Switch
Disable unused ports in switch; Protects from unknown traffic, unauthorized nodes
Closed network, only P2P nodes/traffic, protects against unauthorized access/C/I/A
Closed network, redundant, separate TCMs, provides availability if one network/TCM is not available
Tricon
Tricon
Network Switch

Figure 9

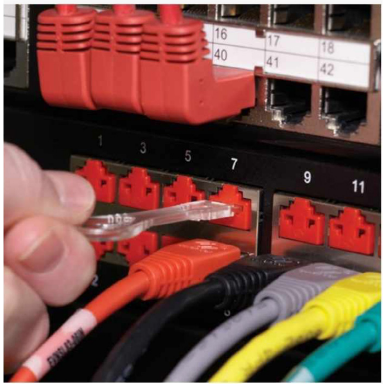
Safety peer to peer communications.

TIP 3

Lock up unused network ports

Disable unused network ports from unauthorized access

- Secure open RJ-45 jacks.
- Prevent unauthorized network access via unused ports.
- Removal only with approval – and a special Removal Key.



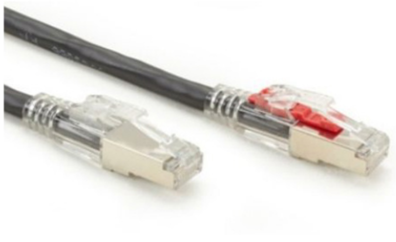


Figure 10

Example secure port plugs and lockable cables.

Step 3 – secure non safety networks

Non safety networks are often used for the connection of engineering workstations, maintenance workstations, communications gateways, connection to host DCS systems and third part systems such as HMI or DCS systems.

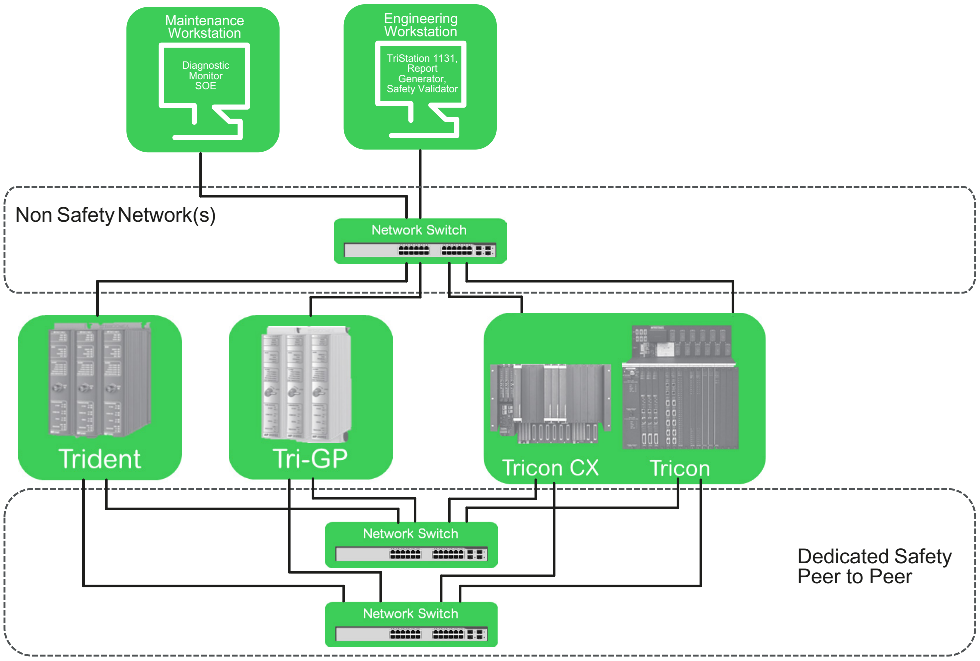


Figure 11

Secure non safety networks.

When using network switches, the same security measures should be used as those for a closed network:

- Configure network switches and routers in a manner that limits the addition of unauthorized network nodes.
- Restrict communications to the expected ports as per your network configuration. Only open those ports that are necessary for network communication
- Close or disable unused ports to prevent unauthorized connection of network nodes, PCs, PLCs or other devices
- Periodically inspect/monitor switches to ensure the configuration has not changed, and that the switch status does not indicate communication has occurred on unexpected ports.

Step 4 – secure host workstations

When using a PC as the engineering or maintenance workstation, to reduce the security risks associated with the PC, you should follow these guidelines:

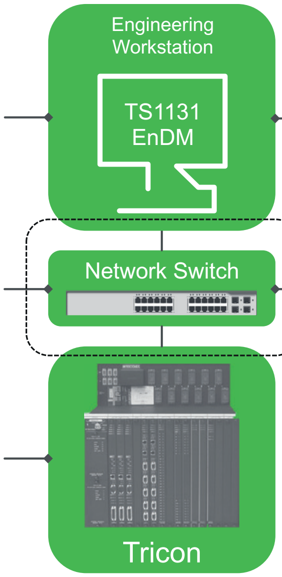
- If you use a domain controller/Active Directory, follow Microsoft's recommended practices for security.
- Create separate Windows accounts for each user
- Manage user accounts per your organization's corporate policy
- Implement strong user authentication practices, including password strength and periodic password change requirements
- Periodically monitor the Windows accounts available on the workstation to ensure that only the necessary personnel can log on to the workstation, with the appropriate level of access. Inactive or unnecessary user accounts should be removed.
- Review the Windows System Events Log to monitor log-on and log-off activity on all workstations, and to detect attempted unauthorized activity.
- Disable unused USB ports.
- Use firewalls and other security devices or settings to limit access to the host network, based on your security risk assessment.
- When using a firewall:
  - restrict communication to the expected ports and protocols, as per your network configuration. Only open those ports that are necessary for the required network communication;
  - periodically inspect/monitor the firewall to ensure the configuration has not been changed, and that the firewall status does not indicate communication has occurred on unexpected pods.
- When using network switches:
  - close or disable unused network ports to prevent unauthorized connection of network nodes or PLCs;
  - periodically inspect/monitor the switch to ensure the configuration has not been changed, and that the switch status does not indicate communication has occurred on unexpected ports.
- Install operating system patches and anti-virus software updates, as they are released, on the workstation.

If you want to remotely access the workstation(s) TriStation 1131 is installed on. You should take care to evaluate and mitigate all security threats to the necessary level per your organization's security policy, following industry best practices and applicable standards.

Step 5 – secure the application(s)

To reduce the security risks associated with the TriStation 1131 PC and project file, follow these guidelines:

- Enable Enhanced Security, which authenticates the user against the Windows®-based PC or domain. If you use a domain controller/Active Directory, follow Microsoft's recommended practices for security.
- Create a user account for each person who will be working with the TriStation 1131 project and do not allow sharing of user accounts. Periodically review user accounts and their roles and privileges to ensure compliance with your organization's policy.
- Configure the security banner that appears when logging on to a TriStation 1131 project file to remind users of your organization's corporate security policy.
- Implement strong user authentication practices, including password strength and periodic password change requirements.
- Periodically review the Windows accounts available on the workstation to ensure that only the necessary personnel can log on to the workstation, with the appropriate level of access. Inactive or unnecessary user accounts should be removed.
- Review the Windows System Events Log to monitor log-on and log-off activity on all workstations, and to detect attempted unauthorized or anomalous activity.
- When logging on to a TriStation 1131 project, review the information in the Log On dialog box about the last time the project was opened. Ensure that this information is correct; incorrect or suspicious information could indicate unauthorized access to the project and/or controller.
- Back up the project file (.pt2) regularly and store it in a secure, separate, non-shared location.
- Store original and backup copies of certificates and private keys in a secure, separate, non-shared location.
- Install OS patches and anti-virus software updates on the TriStation PC as they are released.
- Periodically collect and review the following items for unusual activity related to the controller or the TriStation 1131 PC:
  - individual project file's audit trail/project history;
  - logs in the Enhanced Diagnostic Monitor;
  - enhanced Security Mode logs in the Event Viewer on the TriStation 1131 PC.
- Disable unused USB ports.



Secure Host
Windows Patches,
Anti Virus to protect against
malicious code

Secure Application(s)
Enhanced security mode to protect
against unauthorized access/A/I/C, via
Strong passwords, TS1131 access
rights, Windows Logs

Closed Network, protects against unauthorized access/A/I/C

Cabinet provides physical
protection to the switch / cabling

Disable Unused Ports in switch
Protects from unknown traffic,
unauthorized nodes

Key switch, access list, protects
against unauthorized
programing changes

Figure 12

Secure all host workstations and associated applications.

TriStation TS1131 Security

When configuring and using TriStation 1131, be sure to follow these guidelines:

- Enable Enhanced Security, which authenticates the user against the Windows-based PC or domain.
- Create a TriStation 1131 user account for each person who will be working with the TriStation 1131 project, and do not allow sharing of user accounts, periodically review user accounts, and their roles and privileges, to ensure compliance with your organization’s security policy.
- Use the Windows Access Control List (ACL) to define the file and folder access permissions available to each Windows user account or group account. You can prevent unauthorized access to TriStation 1131 configuration or project files by configuring the ACL on the Security tab of each file’s ‘File Properties’ dialog box. You can also manage user accounts, and set their file and folder access permissions at a workstation-level via the Windows Control Panel.
- Configure the security banner that appears when logging on to a TriStation 1131 project file to remind users of your organization’s corporate security policy.
- When logging onto a TriStation 1131 project, review the information in the Log On dialog box about the last time the project was opened. Ensure that this information is correct; incorrect or suspicious information could indicate unauthorized access to the project and/or controller.
- Back up the project file (.pt2) regularly, and store it in a secure, separate, non-shared location
- Care should be taken to ensure the network is a closed network or a direct connection when downloading the control program to the controller – the key switch in this case is in the program mode; and the control program behaviour should be validated in keeping with requirements of applicable safety standards.
- If applicable, store original and backup copies of certificates and private keys in a secure, separate. non-shared location.

- Periodically collect and review the following for unusual activity related to the controller or TriStation 1131 PC:
  - individual project file's audit trail/project history (see View Project History Command);
  - logs in the Enhanced Diagnostic Monitor (see the Enhanced Diagnostic Monitor Users Guide for more information);
  - enhanced Security Mode logs in the Windows Event Viewer on the TriStation PC (see Viewing the User Access Log in Windows Event Viewer).

Table 3

TriStation cybersecurity features.

TriStation Version	Feature
TriStation 4.7.0	Enhanced security mode for user authentication via window Enhanced security events written into Windows System log
TriStation 4.9.1	Allow user to remove customer support account
TriStation 4.11.0	Application digitally signed by Schneider Electric Certificate
TriStation 4.13.0	Security Considerations for end users added to the user manuals
TriStation 4.14.0	Prevent third party access to some DLLs via friend assemblies
2015+	Monthly OS Security Patch testing for Win 7, Win 2008, Win 2012.

Step 6 – secure EcoStruxure Foxboro DCS communications

There are two commonly used methods of connecting a EcoStruxure Triconex controller to the EcoStruxure Foxboro DCS:

1. Direct integration on to the Foxboro DCS control network
2. Interface to the Foxboro DCS via gateways such as the Field Device Serial Interface (FOSI) and associated Control Processors (CP)

In both cases, securing the communications requires a combination of Foxboro DCS cybersecurity measures and Triconex cybersecurity measures:

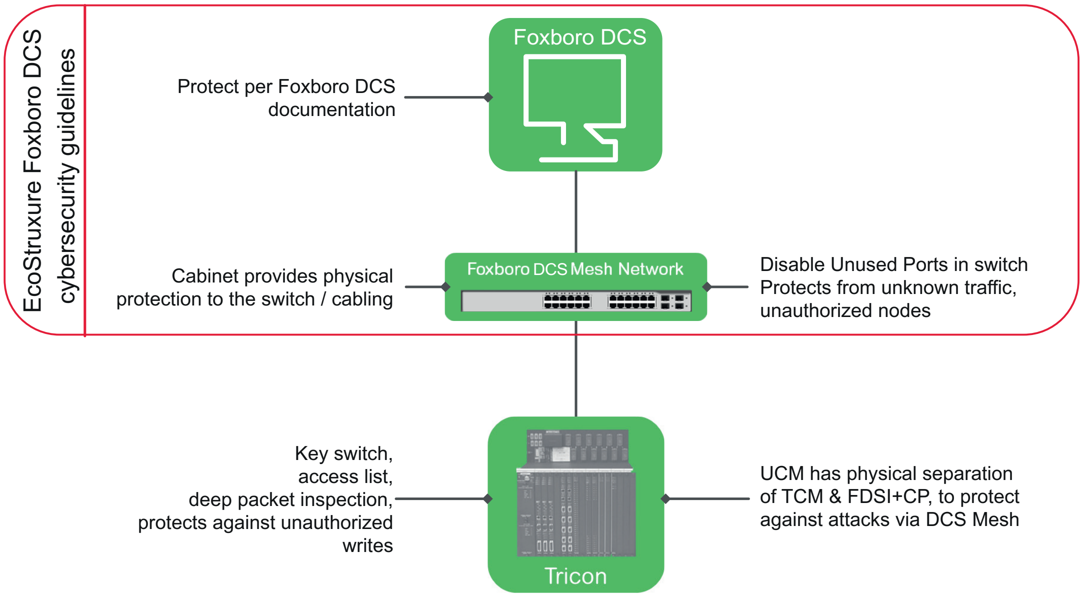
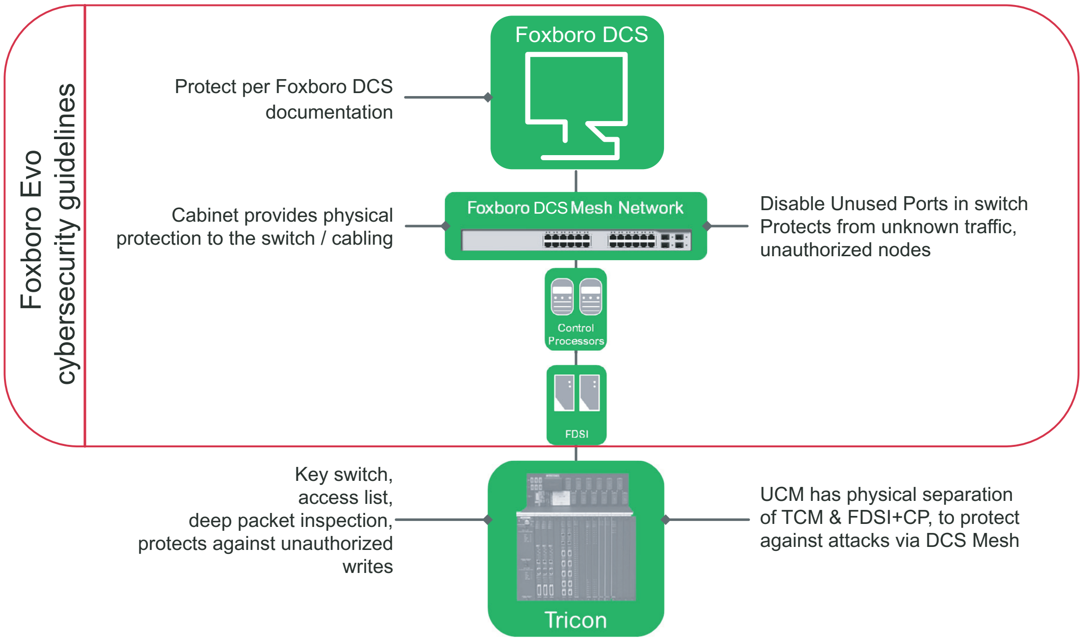

EcoStruxure Foxboro DCS cybersecurity guidelines
Foxboro DCS
Protect per Foxboro DCS documentation
Foxboro DCS Mesh Network
Cabinet provides physical protection to the switch / cabling
Disable Unused Ports in switch Protects from unknown traffic, unauthorized nodes
Key switch, access list, deep packet inspection, protects against unauthorized writes
Tricon
UCM has physical separation of TCM & FDSI+CP, to protect against attacks via DCS Mesh

Figure 13

Direct EcoStruxure Triconex integration with EcoStruxure Foxboro DCS mesh network



Protect per Foxboro DCS documentation

Cabinet provides physical protection to the switch / cabling

Disable Unused Ports in switch Protects from unknown traffic, unauthorized nodes

Key switch, access list, deep packet inspection, protects against unauthorized writes

UCM has physical separation of TCM & FDSI+CP, to protect against attacks via DCS Mesh

Figure 14

EcoStruxure Triconex interface with Foxboro DCS mesh network.

Step 7 – secure communications with 3rd party devices

This section includes guidelines for securing open networks to 3rd party devices and applications that should follow these guidelines:

- Secure the host PCs (that run Modbus. TSAA, or OPC clients to communicate with the Tricon controller) by keeping the user authentication strong and the anti-virus software and OS patches up-to-date.
- Limit writes to the Tricon controller by using organizationally defined policies and by controlling access to the keyswitch.
- Physically isolate (sometimes referred to as an air gap) the Tricon controller and its networks from the rest of the networks in your plant or facility.
- Limit network traffic by using external firewalls.
- Use redundant TCMs/UCMs with network redundancy to external clients.
- Use firewalls and other security devices or settings to limit access to the host network, based on your security risk assessment.
- When using a firewall:
  - restrict communication to the expected ports, as per your network configuration. Only open those ports that are necessary for network communication;
  - periodically inspect/monitor the firewall to ensure the configuration has not been changed, and that the firewall status does not indicate communication has occurred on unexpected ports.
- When using network switches:
  - close or disable unused network ports to prevent unauthorized connection of network nodes or PLCs;
  - periodically inspect/monitor the switch to ensure the configuration has not been changed, and that the switch status does not indicate communication has occurred on unexpected ports.

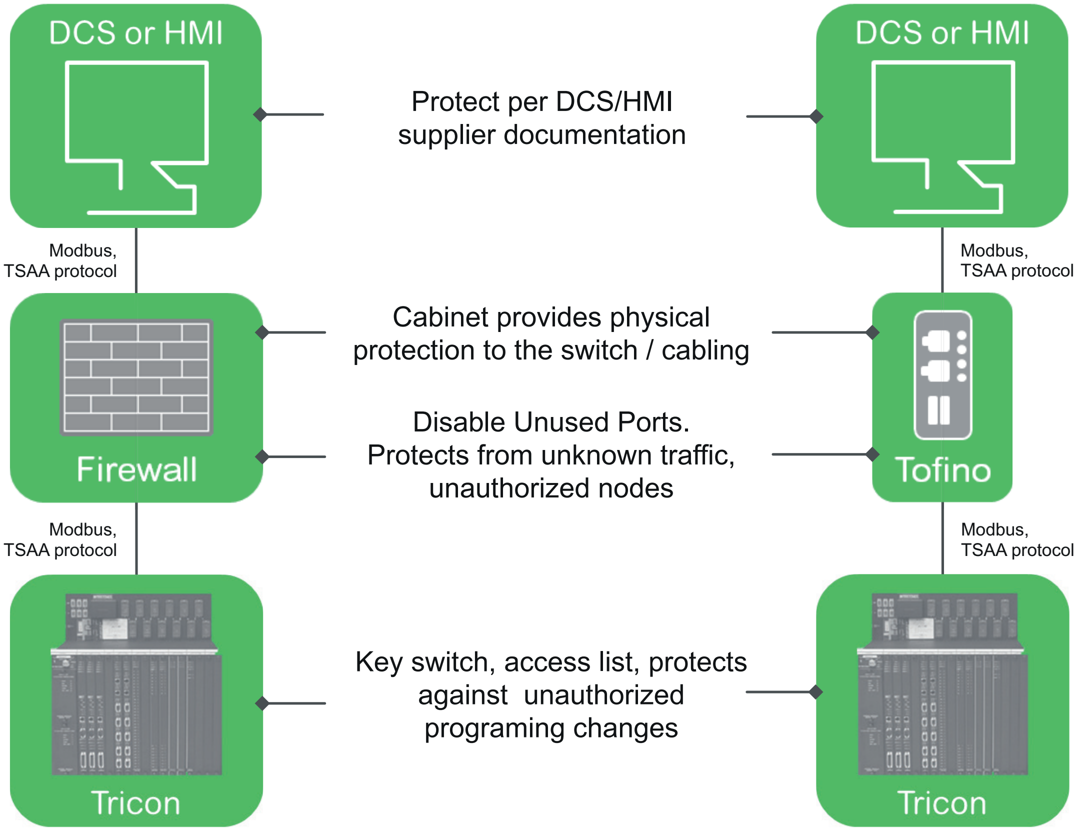

DCS or HMI
Protect per DCS/HMI supplier documentation
DCS or HMI
Modbus, TSAA protocol
Modbus, TSAA protocol
Firewall
Cabinet provides physical protection to the switch / cabling
Disable Unused Ports. Protects from unknown traffic, unauthorized nodes
Tofino
Modbus, TSAA protocol
Modbus, TSAA protocol
Tricon
Key switch, access list, protects against unauthorized programing changes
Tricon

Figure 15

Secure Modbus, TSAA protocol communications.

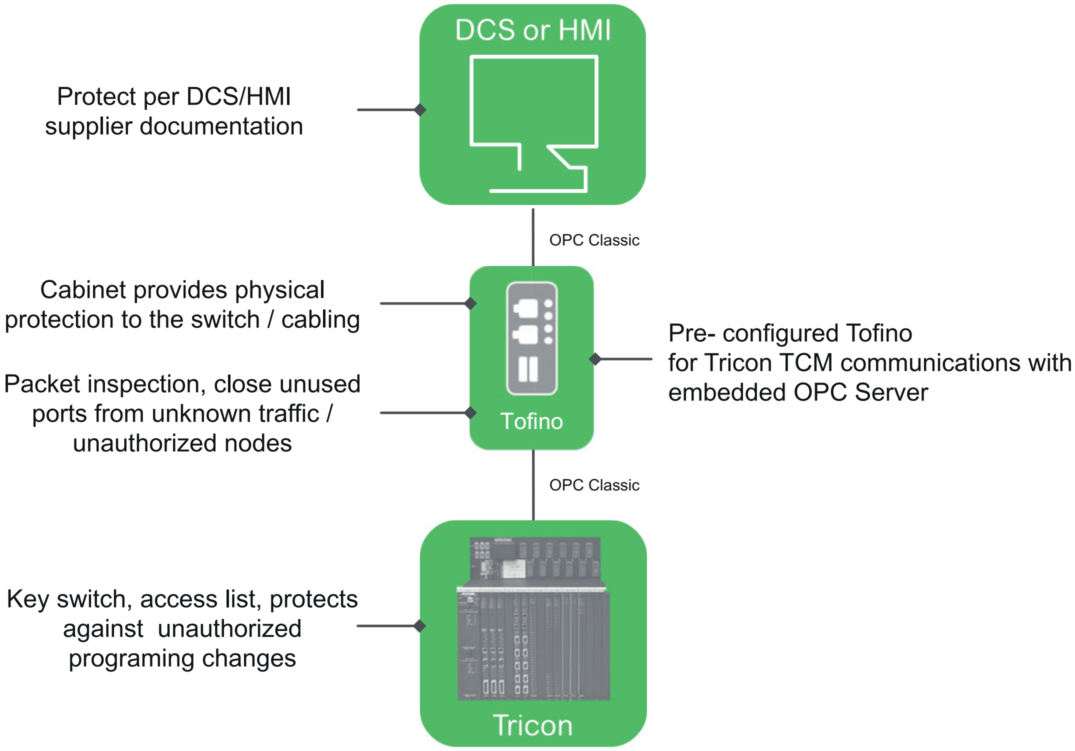

DCS or HMI
Protect per DCS/HMI supplier documentation
OPC Classic
Cabinet provides physical protection to the switch / cabling
Packet inspection, close unused ports from unknown traffic / unauthorized nodes
Tofino
Pre- configured Tofino for Tricon TCM communications with embedded OPC Server
OPC Classic
Key switch, access list, protects against unauthorized programing changes
Tricon

Figure 16

Secure OPC Classic communications.

Step 8 – create architectural zones and demilitarized zones (DMZ)

In accordance with best recommendations by both ISA99 & IEC62443 segregating your system into zones and conduits will help mitigate risk.

For example, if a zone was to be created encompassing machines running a legacy OS, they can be protected by employing mitigation against known vulnerabilities at the conduit(s) of that zone.

Using the zones & conduits approach heightens awareness of system component parts, the risk posed by OSs. Anti-Virus Patch status as well as segregates the network to prevent propagation should a system be compromised.

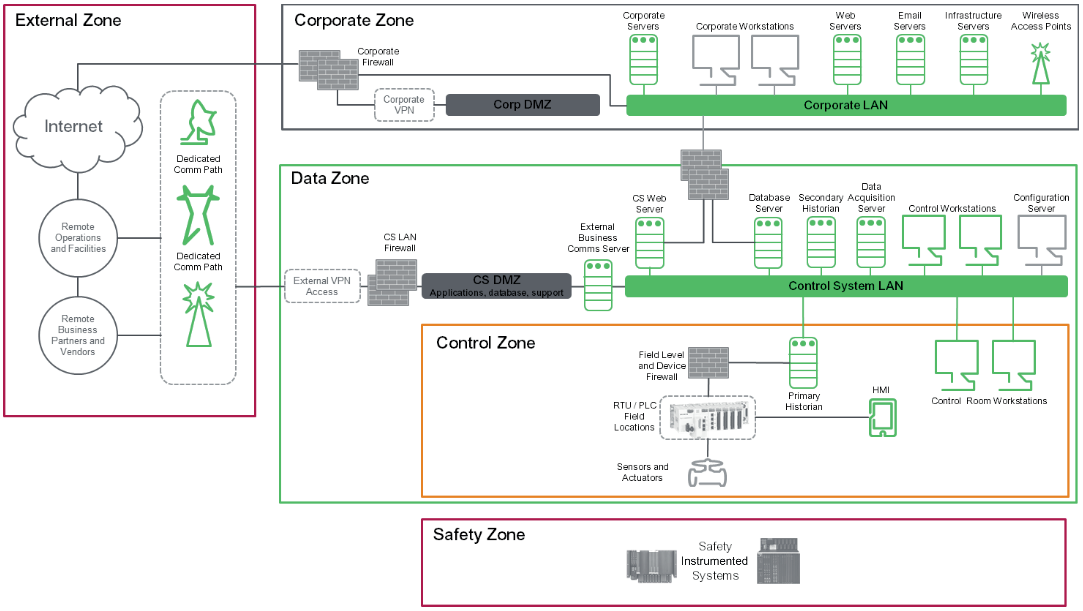


Figure 17

Recommended Practices: Improving Industrial Control System Cybersecurity with Defence in Depth Strategies from Department of Homeland Security.

Step 9 – identify network assets and protect the conduit

IEC62443 introduces the concepts of 'zones' and conduits' as a way to segment and isolate the various sub-systems in a control system.

Zones and conduits are a fundamental concept of industrial network cybersecurity. By grouping similar devices or systems into "zones" according to security levels, and controlling communications between zones, a strong foundation of security will be realized.

A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken.

Any communications between zones must be via a defined conduit. Conduits control access to zones, resist Denial of Service (DoS) attacks or the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic.

Each conduit should be defined in terms of the zones it connects, the technologies it utilizes, the protocols it transports and any security features it needs to offer its connected zones.

Typically, determining the information transfer requirements between zones over the network is straight forward. Tools like traffic flow analyzers or even simple protocol analyzers can show which systems are exchanging data and the services they are using.

It is also wise to look beyond the network, to determine the hidden traffic flows. For example, are files ever moved via USB drive between the lab and the primary control systems?

Once the conduits and their security requirements are defined, the final phase is to implement the appropriate security technologies.

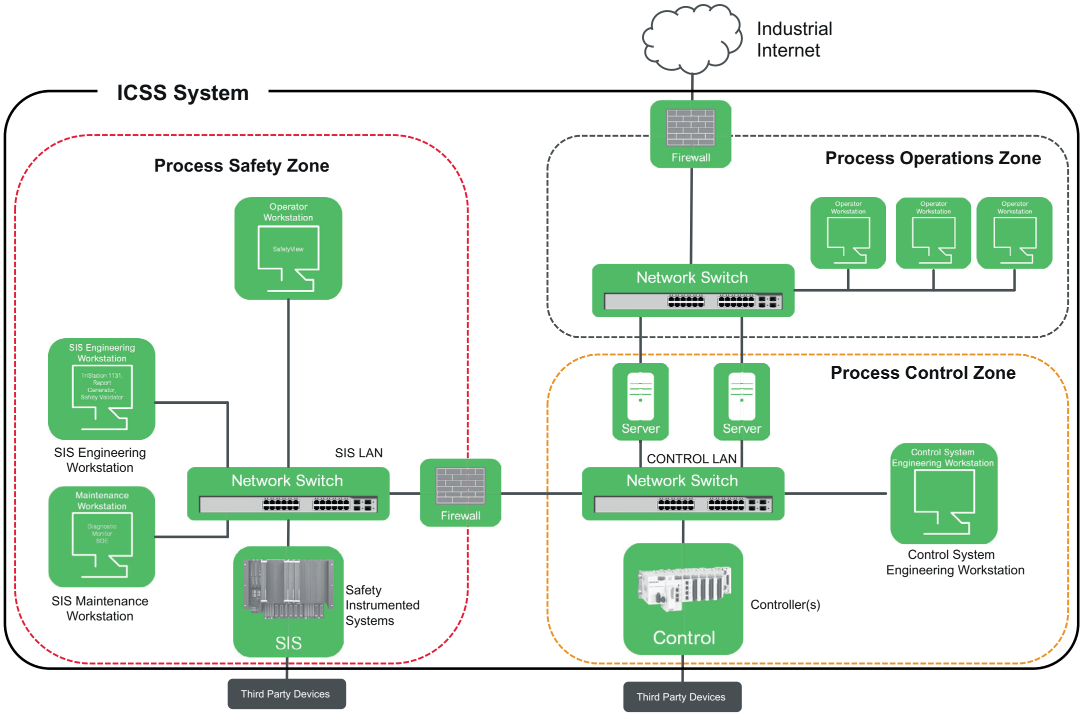


Figure 18

Create zones and protect conduits.

Be secure by design

From a product perspective, there are a number of standards and certificates a vendor aspires to. Schneider Electric subscribes to both Wurldtech Achilles and ISASecure/ IEC62443 testing and compliance.

Achilles testing is commonly a Communication Robustness Test (CRT) of any interface that has an Internet Protocol (IP) stack. The objective of developing any product is to ensure that any interfaces are resilient to attack. The Wurldtech Achilles CRT testing and certificate is one methodology of ensuring this is achieved.

ISASecure/IEC62443 Embedded Device Security Assurance (EDSA) has a greater amount of criteria that has to be met before a compliance certificate is issued. CRT is about 30% of the criteria. EDSA tests development practices, documentation, robustness, best practices, policies and procedures as well as the technical element.

Furthermore, in its efforts to comply with IEC62443, Schneider Electric was the first automation vendor to have development centers certified as Secure Development Lifecycle Assurance (SDLA) compliant. The SDLA criteria covers all aspects of a Development department, ensuring that the development of all projects/products meet a particular level of competency. This includes cybersecurity from concept to delivery, best practices, policies, procedures and ensures that due diligence is exercised throughout the whole product development cycle. This further includes training of personnel, static code analysis as well as Incident response and report procedures.

Put a sustainable cybersecurity program in place

While every effort should be made to protect the technology against cyber-threats, any cybersecurity schema is only as secure as the weakest link. For cybersecurity to be effective it is extremely important to consider the operational aspects such as policies and procedures and the personnel aspects such as skills and competencies to provide further defence in depth.

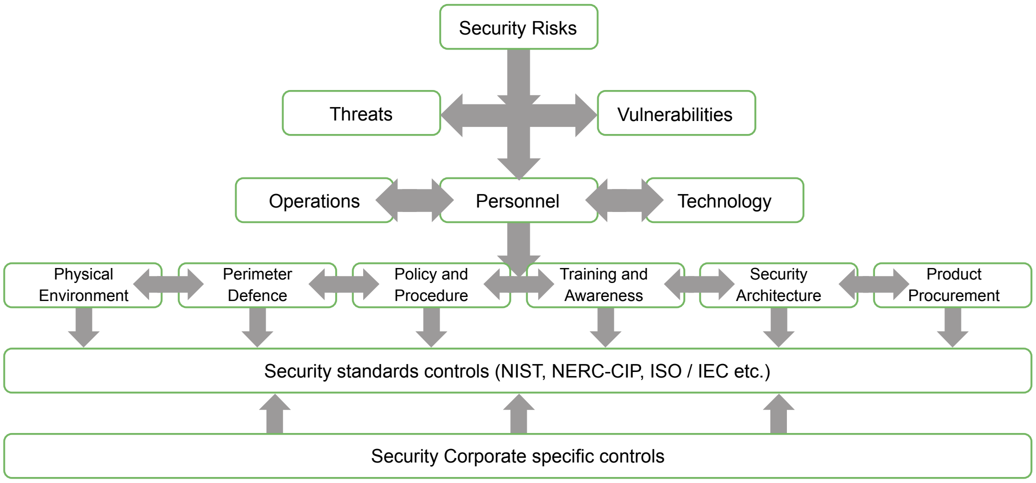


Figure 19

Recommended practices: improving industrial control system cybersecurity with Defence in Depth strategies from Department of Homeland Security.

The human element

Large and complex systems are susceptible to mistakes made by inexperienced or untrained personnel, as well as the activities of malicious insider threats. Many organizations often overlook security training and awareness activities more often than many other areas in control and safety operations. As control and safety systems become more interconnected and cyber-threats and vulnerabilities rise, it is critically important for organizations to ensure that they require and support control and safety security-specific training.

Policies

Clear, actionable policies are necessary to secure control and safety technologies and also provide the governance needed to manage human factors. Policies lay the framework for detailed procedures and set the expectations of the organization with regard to the functions performed. Policies outline the rules with regard to securing the control and safety systems and should clearly state the expected rules of behavior and also required controls.

TIP 4

Implement a sustainable cybersecurity program.

Procedures

Historically, security management was the responsibility of the corporate IT security organization, usually governed by operating plans and procedures that protect vital corporate information assets, as control and safety systems become part of larger conjoined network architectures, organizations should update security procedures to cover the control and safety system domain as well.

Organizations should design procedures to state how personnel should conduct a particular process, or configure a particular system, to ensure secure functioning and provide a standard, repeatable means to accomplish a task in a safe manner.

Security procedures should instruct operators on the steps to take in order to protect the system from cyber-based intrusion(s). Network-based security procedures are especially important for the control and safety domain, because the use of unique vendor specific protocols and legacy systems may hamper efforts to protect mission critical systems

Stay current

Continuous Monitoring and Improvement

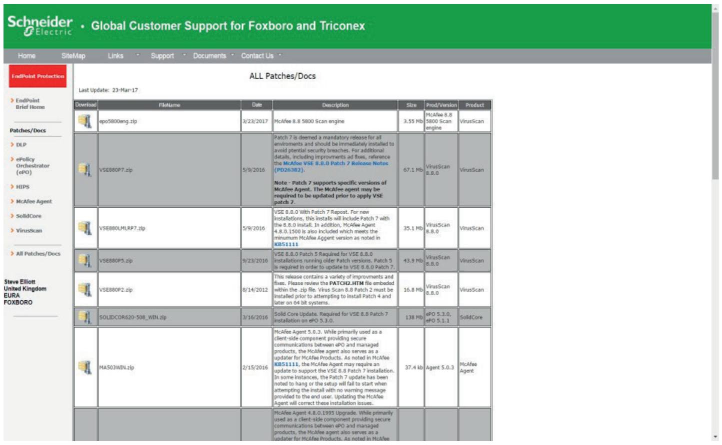
Since ease of exploitation of vulnerabilities changes, sometimes rapidly, and new vulnerabilities /threats are discovered continuously, organizations should put a program in place to reassess their threat models & mitigations on a periodic basis. This includes working to close any gaps between the target system security levels and the actual security levels.

The system, procedures and personnel (training) should be regularly reviewed and updated to address new findings.

Patch Management

As new threats emerge, software patches (incremental software changes) may be required to address potential security vulnerabilities to the operating systems or software applications.

Patches are tested and validated prior to release. Notification and availability of the latest software patches are available via the Global Customer Support (GCS) website at https://pasupport.schneider-electric.com



ALL Patches/Docs

Last Update: 23-Mar-17

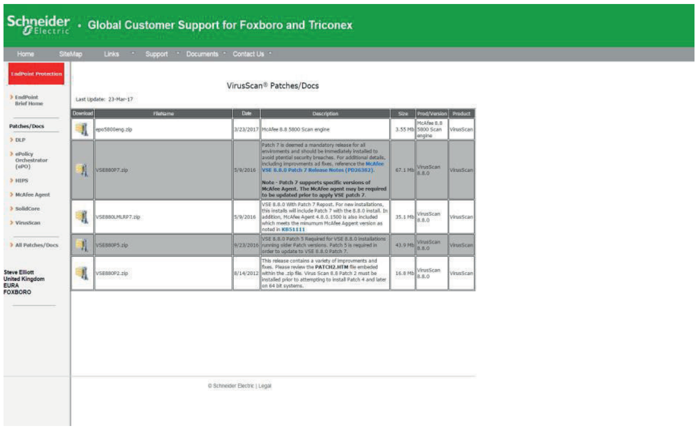
Download	FileName	Date	Description	Size	Prod/Version	Product
	epo5800eng.zip	3/23/2017	McAfee 8.8 5800 Scan engine	3.55 Mb	McAfee 8.8 5800 Scan engine	VirusScan
	VSE880P7.zip	5/9/2016	Patch 7 is deemed a mandatory release for all enviroments and should be immediately installed to avoid ptential security breaches. For additional details, including improvments ad fixes, reference the McAfee VSE 8.8.0 Patch 7 Release Notes (PD26382). **Note - Patch 7 supports specific versions of McAfee Agent. The McAfee agent may be required to be updated prior to apply VSE patch 7.**	67.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880LMLRP7.zip	5/9/2016	VSE 8.8.0 With Patch 7 Repost. For new installations, this installs will include Patch 7 with the 8.8.0 install. In addition, McAfee Agent 4.8.0.1500 is also included which meets the minumum McAfee Aggent version as noted in KB51111	35.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880P5.zip	9/23/2016	VSE 8.8.0 Patch 5 Required for VSE 8.8.0 installations running older Patch versions. Patch 5 is required in order to update to VSE 8.8.0 Patch 7.	43.9 Mb	VirusScan 8.8.0	VirusScan
	VSE880P2.zip	8/14/2012	This release contains a variety of improvments and fixes. Please review the **PATCH2.HTM** file embeded within the .zip file. Virus Scan 8.8 Patch 2 must be installed prior to attempting to install Patch 4 and later on 64 bit systems.	16.8 Mb	VirusScan 8.8.0	VirusScan
	SOLIDCOR620-508_WIN.zip	3/16/2016	Solid Core Update. Required for VSE 8.8 Patch 7 installation on ePO 5.3.0.	138 Mb	ePO 5.3.0, ePO 5.1.1	SolidCore
	MA503WIN.zip	2/15/2016	McAfee Agent 5.0.3. While primarily used as a client-side component providing secure communications between ePO and managed products, the McAfee agent also serves as a updater for McAfee Products. As noted in McAfee KB51111, the McAfee Agent may require an update to support the VSE 8.8 Patch 7 installation. In some instances, the Patch 7 update has been noted to hang or the setup will fail to start when attempting the install with no warning message provided to the end user. Updating the McAfee Agent will correct these installation issues.	37.4 kb	Agent 5.0.3	McAfee Agent
			McAfee Agent 4.8.0.1995 Upgrade. While primarily used as a client-side component providing secure communications between ePO and managed products, the McAfee agent also serves as a updater for McAfee Products. As noted in McAfee			

Figure 20

Available patches from the Global Customer Support website.

AntiVirus Management

Antivirus software patches are tested and validated prior to release. Notification and availability of the latest software patches are available via the Global Customer Support (GCS) website at https://pasupport.schneider-electric.com



VirusScan® Patches/Docs

Last Update: 23-Mar-17

Download	FileName	Date	Description	Size	Prod/Version	Product
	epo5800eng.zip	3/23/2017	McAfee 8.8 5800 Scan engine	3.55 Mb	McAfee 8.8 5800 Scan engine	VirusScan
	VSE880P7.zip	5/9/2016	Patch 7 is deemed a mandatory release for all enviroments and should be immediately installed to avoid ptential security breaches. For additional details, including improvments ad fixes, reference the McAfee VSE 8.8.0 Patch 7 Release Notes (PD26382). **Note - Patch 7 supports specific versions of McAfee Agent. The McAfee agent may be required to be updated prior to apply VSE patch 7.**	67.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880LMLRP7.zip	5/9/2016	VSE 8.8.0 With Patch 7 Repost. For new installations, this installs will include Patch 7 with the 8.8.0 install. In addition, McAfee Agent 4.8.0.1500 is also included which meets the minumum McAfee Aggent version as noted in KB51111	35.1 Mb	VirusScan 8.8.0	VirusScan
	VSE880P5.zip	9/23/2016	VSE 8.8.0 Patch 5 Required for VSE 8.8.0 installations running older Patch versions. Patch 5 is required in order to update to VSE 8.8.0 Patch 7.	43.9 Mb	VirusScan 8.8.0	VirusScan
	VSE880P2.zip	8/14/2012	This release contains a variety of improvments and fixes. Please review the **PATCH2.HTM** file embeded within the .zip file. Virus Scan 8.8 Patch 2 must be installed prior to attempting to install Patch 4 and later on 64 bit systems.	16.8 Mb	VirusScan 8.8.0	VirusScan

Figure 21

Available virus scan patches and documents from the Global Customer Support website.

Summary

Schneider Electric recommends the following defence in depth methods to protect your safety systems:

Table 4

Recommendation Checklist.

Security Program	Security Feature
Policies and Procedures	● Yearly Review ● Log & Event Management ● Security Policies (e.g. NERC) – Baseline configuration management – Account/role management – Backup management ● Patch Management Planning & Procedures ● Security Training Programs ● Incident Response & Forensics
Intrusion Detection System	● Tools & procedures ● Allows network administrator to understand how network is being used ● Watch traffic & ingress /egress ● Passive
System Architecture	● Standalone safety workstation ● Separate safety peer to peer network
Prevent unauthorised writes	● Using inherent technical features ● Key switch in run/remote, gate enable, access security list, protocol access ● Remove key from Tricon arid store in a secure location ● Monitor key switch position in external/HMI ● In Trident, implement key switch m application ● Create operational procedures to authorize access to cabinet key and Tricon key
Account management	● Manage individual accounts ● Review roles and permissions periodically
Backups	● Periodically perform backups
Audit trails periodic reviews	● Log from account login/audit waits ● TriStation TS1131 ● PC/Windows logon ● TriStation Enhanced Diagnostic Monitor (EnDM)
Restrict access to PT2 file	● Do not put it in a public folder
Host intrusion protection	● Antivirus ● “White listing” application control ● Implement device control (USB)
Patch management	● Keeping Windows and antivirus up to date
Verify TriStation application integrity	● Run TriStation install check periodically
Stay current	● Review EcoStruxure Triconex cybersecurity recommendations in user manuals

Conclusion

As control and safety systems grow in complexity and connectivity, the number of potential security issues and associated risks grows as well. Protecting your safety instrumented systems is a journey, even with the best will in the world, vulnerabilities can appear in cybersecurity measures so owners/operators should not depend on a single countermeasure.

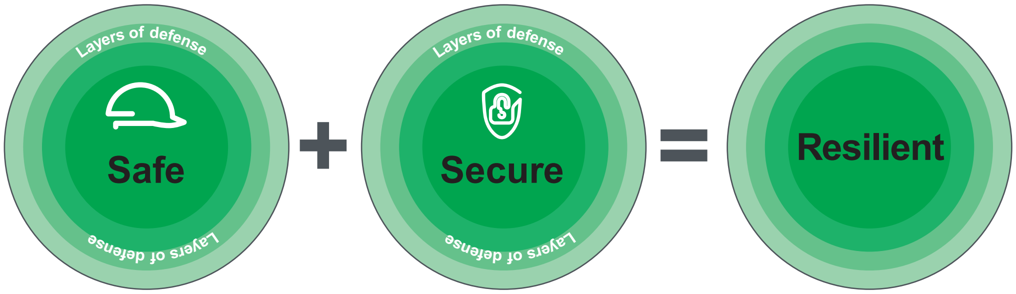
"Don't leave yourself open and vulnerable to attack. Use all of the tools available to you to build a strong defence."

Multiple countermeasures should be applied to protect your safety systems, thus reducing risk using defense-in-depth techniques. Don't just look to technology to keep you secure – never underestimate the importance of your people, effective policies and meaningful procedures, After all, any cybersecurity protection schema is only as strong as the weakest link.

Make sure that you:

1. Know the security risks that an organization faces
2. Quantify and qualify risks
3. Use key resources to mitigate security risks
4. Define each resource's core competency and identify any overlapping areas
5. Abide by existing or emerging security standards for specific controls
6. Create and customize specific controls that are unique to an organization
7. Create and Incident Response (IR) procedure and practice it
8. Conduct cybersecurity review on a quarterly or bi-annual basis

Defense-in-depth measures do not and cannot protect all vulnerabilities and weaknesses. When applied, they primarily slow down an attacker enough to allow the relevant personnel to detect and respond to ongoing threats, or to make the effort on the attacker's side so cumbersome, that they'll decide to put their effort toward easier prey!



About the author

Steve J Elliott is a Senior Marketing Director for EcoStruxure Triconex Safety Systems and Solutions. He is a TÜV certified functional safety engineer with over 20 years of experience in distributed control systems. SCADA systems. PLC and safety systems. He holds a Process Safety patent and has published multiple articles in global journals focused on functional and process safety and has authored several while papers. Steve regularly blogs on process safety related topics: https://blog.schneider-electric.com/author/selliott/

Acknowledgements

Special thanks to **Gary Williams** the Senior Director for Schneider Electric Industry Business Cybersecurity and Communications. Gary has more than 30 years' experience in networks, communications, innovation, design and implementation of secure network solutions. He has an MSc in IT Security; is a certified ISO27000 Lead Auditor, was a qualified Computer Hacker Forensic Investigator and has been trained to conduct risk and threat assessments, write policy and compliancy document. Gary sits on a number of standards bodies including SCI, ISASecure, IEC, IET

Special thanks to **Ajay Mishra**. Ajay is the R&D Program Director for EcoStruxure Triconex Safety Systems and helps define the detailed features and technology roadmaps for the EcoStruxure Triconex safety and critical control products. Ajay is a TÜV certified Functional Safety Engineer for hardware/software design (IEC 61508) and Safety Instrumented Systems (IEC 61511), he has 25+ years of experience in safety and critical control systems in process control SIS, railways systems and medical devices, including product development, project engineering, project management and technical product management.

Contact us

If you are a Schneider Electric client and have questions specific to your automation system cybersecurity requirements:

Contact your representative at

https://www.schneider-electric.com/en/work/support/contacts.jsp

For information on EcoStruxure Triconex Safety Systems visit
www.schneider-electric.com

Appendix A: References

IEC61511: Edition 2.0 Functional safety – Safety instrumented systems for the process industry sector

IEC62443-3-1:2010 Information technology – security techniques – information security management systems – requirements

ISA TR 84.00.09:2013 Security countermeasures related to safety instrumented systems (SIS)

ISO/IEC27001:2013 Information technology – Security techniques – information security management systems – Requirements

Homeland Security- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies – September 2016

Tricon planning and installation guide (Assembly Number 9700077-022)

TriStation 1131 Developers Guide (Assembly Number 9700100-019)

Schneider Electric
70 Mechanic Street, Foxborough, MA 02035 USA Telephone: +1 877 342 5173 schneider-electric.com/triconex

PN SE-998-20241664_GMA-US Rel. 03/18

Maximize the resiliance of your
EcoStruxure Triconex Safety Systems