XS/SC26-2 Safety Controllers Secure Deployment Guide

Contents

Chapter Contents

Chapter 1   About this Guide

This document provides information to help improve the cyber security of systems that include XS/SC26-2 Safety Controllers.

It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring XS/SC26-2 Safety Controllers.

Blank page

Chapter Contents

Chapter 2 Introduction

This section introduces the fundamentals of security and secure deployment.

2.1 What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system

- Confidentiality: Ensure only the people you want to see information can see it
- Integrity: Ensure the data is what it is supposed to be
- Availability: Ensure the system or data is available for use

Banner recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take the appropriate care in securing their Banner Safety products and solutions.

> **NOTE:** As Banner Safety product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in a particular product version, as well as the version in which the vulnerability was fixed. Banner Safety product security advisories are available at: bannerengineering.com/support/tech-help/PSIRT.

2.2 I have a Firewall. Isn't that Enough?

Firewalls and other network security products, including data diodes and Intrusion Prevention Systems (IPS), can be an important component of any security strategy. However, a strategy based solely on any single security mechanism is not as resilient as one that includes multiple, independent layers of security.

Therefore, Banner Safety recommends taking a "Defense in Depth" approach to security.

2.3 What is Defense in Depth?

Defense in depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, such as a username/password authentication requirement, the attacker needs to find a way to circumvent both the firewall and the username/password authentication.

2.4 General Recommendations

Use the following security practices when using Banner Safety products and solutions.

- The safety controllers covered in this document were not designed for or intended to be connected directly to any wide area network, including, but not limited to, a corporate network or the internet at large. Additional routers and firewalls (such as those illustrated in "Reference Architecture" on page 18) that have been configured with access

rules customized to the site's specific needs must be used to access devices described in this document from outside the local control networks. If a control system requires external connectivity, take care to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.

- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all the latest Banner Safety product security updates, Security Information Management (SIM), and other recommendations.
- Apply all the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up-to-date.
- Use whitelisting software on control systems PCs and keep the whitelist up-to-date.

2.5   Checklist

This section provides a sample checklist to help guide the process of securely deploying XS/SC26-2 Safety Controllers.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node. (See "Communication Requirements" on page 7.)
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls, or other network security devices as appropriate. Update the network diagram. (See "Network Architecture and Secure Deployment" on page 18.)
5. Configure firewalls and other network security devices. (See "Ethernet Firewall Configuration" on page 9 and "Network Architecture and Secure Deployment" on page 18.)
6. Enable and/or configure the appropriate security features on each XS/SC26-2 Safety Controller. (See "Security Capabilities" on page 11.)
7. On each XS/SC26-2 safety controller, set every supported password to a strong value. (See "Password/PIN Management" on page 13.)
8. Harden the configuration of each XS/SC26-2 safety controller, disabling unneeded features, protocols, and ports. (See "Configuration Hardening" on page 15.)
9. Test / qualify the system.
10. Create an update/maintenance plan.

> **NOTE:** Secure deployment is only one part of a robust security program. This document, including this checklist, is limited to providing secure deployment guidance only. For more information about security programs in general, see "Additional Guidance" on page 21.

Chapter Contents

Chapter 3   Communication Requirements

Communication between different parts of a control system is, and must be, supported. However, the security of a control system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed, to only what is needed.

This can be accomplished by disabling every communication protocol that isn't needed on a particular device, and by using appropriately configured and deployed network security devices (for example, firewalls and routers) to block every protocol (whether disabled or not) that doesn't need to pass from one network/segment to another.

Banner Safety recommends limiting the protocols allowed by the network infrastructure to the minimum set required for the intended application. Successfully doing this requires knowing which protocol is needed for each system-level interaction.

This section describes how the supported serial and Ethernet application protocols are used by Banner Safety Controllers and indicates the role of each participant in the communication. Lower-level Ethernet protocols are not discussed here but are instead assumed to be supported when needed by the application protocol.

Use this information is intended to guide the specification of the network architecture and to help configure firewalls internal to that network, to support only the required communications paths for any particular installation.

3.1   Supported Protocols

3.1.1   Ethernet Protocols

The following table indicates which Ethernet protocols are supported Banner XS/SC26-2 Safety Controllers. Note that some of the supported protocols may not be required in a given system, because the installation may only be using a subset of the available protocols.

Table 1. Supported Ethernet Protocols

	Protocol	XS/SC26-2
Link	ARP	x
Internet	IPv4	x
	IGMP	x
	ICMP	x
Transport	TCP	x
	UDP	x
Application	Modbus TCP®[1]	x
	Ethernet/IP™[2]	x

---

[1]
Modbus® is a registered trademark of Schneider Electric USA, Inc.

[2] EtherNet/IP™ is a trademark of ODVA, Inc.

Protocol	XS/SC26-2
PROFINET®[1]	x
TLS 1.2	x

3.1.2   USB Protocols

In addition to Ethernet communication, XS/SC26-2 Safety Controllers support communication over a direct USB connection.

Table 2. Supported USB Protocols

	Protocol	XS/SC26-2
Application	USB Communications Device Class (CDC) with Application-Specific Driver	x

3.2   XS/SC26-2 Application Protocol

The XS/SC26-2 Application protocol is a proprietary protocol that provides access to services supported by the XS/SC26-2 Safety Controllers. This is the only protocol used by the Banner Safety Controller Software when communicating with an XS/SC26-2 Safety Controller.

XS/SC26-2 Application protocol supports many different operations, including the following:
• Upload / download a confirmed configuration
• Confirm a new configuration
• Reset the safety controller to factory defaults
• Enable and configure network interface
• Monitor the live application
• Configure the safety controller user access and passwords
• View and clear (optional) a log of any faults that have occurred in the controller
• Reset the safety controller to factory defaults
• View the Configuration log

The XS/SC26-2 Application Protocol is transported over a direct USB 2.0 CDC connection using a standard USB 2.0-compliant cable or over an Ethernet TLS 1.2 connection.

3.3   XS/SC26-2 Discovery Protocol

The XS/SC26-2 Discovery protocol is a proprietary protocol that allows the Banner Safety Controller Software to locate XS/SC26-2 Safety Controllers on the Local Area Network within a Security Zone.

XS/SC26-2 Discovery Protocol is based on UDP Broadcasts. Because the Discovery Protocol is based on UDP broadcasts, it will not be available outside of a Security Zone or a LAN to which the Controller is connected. Discovery protocol is also not available across VLANs.

3.4   Ethernet Servers

This section summarizes the available Ethernet communication-centric functionality, where the communication is initiated by some other device or PC.

Table 3. XS/SC26-2 Server Capabilities

	Functionality	Required Application Protocols	Example Clients
Ethernet	PROFINET	PROFINET	Other controllers

---

[1] PROFINET® is a registered trademark of PROFIBUS Nutzerorganisation e.V.

Functionality	Required Application Protocols	Example Clients
Modbus TCP Server	Modbus TCP	Other controllers
Ethernet/IP	Ethernet/IP	Other controllers
Live Mode and Remote Configuration Server	XS/SC26-2 Application Protocol	Banner Safety Controller Software (PCI)
Discovery Server	XS/SC26-2 Discovery Protocol	Banner Safety Controller Software (PCI)

3.5 Ethernet Firewall Configuration

Configure network-based and host-based firewalls to allow only expected and required network traffic.

This section identifies the EtherTypes and the TCP/UDP ports used by the protocols supported on XS/SC26-2 Safety Controllers.

Use this information to help configure network firewalls to support only the required communications paths for any particular installation.

3.5.1 Lower-Level Protocols

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application layer are the Transport, Internet, and Link layers.

Information on the supported protocols from these three lower layers is summarized in the following tables.

Table 4. Link Layer Protocols

Protocol	EtherType
Address Resolution Protocol (ARP)	0 × 0806
PROFINET	0 × 8892

Table 5. Internet Layer Protocols

Protocol	EtherType	IP Protocol #
Internet Protocol Version 4 (IPv4)	0 × 0800	(n/a)
Internet Control Message Protocol (ICMP)	0 × 0800	1
Internet Group Management Protocol (IGMP)	0 × 0800	2

Table 6. Transport Layer Protocols

Protocol	EtherType	IP Protocol #
Transmission Control Protocol (TCP)	0 × 0800	6
User Datagram Protocol (UDP)	0 × 0800	17

Each of these lower-level protocols is required by one or more of the Application protocols supported on XS/SC26-2 Safety Controllers.

3.5.2   Application Layer Protocols

The following table lists the TCP and UDP port numbers for the Application layer protocols supported by XS/SC26-2 Safety Controllers.

Table 7. Application Layer Protocols

Protocol	TCP Port	UDP Port	XS/SC26-2
Modbus TCP	502		x
PROFINET		34964 49152	x
ETHERNET/IP	44818	2222 44818	x
XS/SC26-2 Application Protocol	63753		x
XS/SC26-2 Discovery Protocol		63754	x

Chapter Contents

Chapter 4   Security Capabilities

This section describes the capabilities and security features of the XS/SC26-2 Safety Controller. Use the capabilities and security features as part of a defense-in-depth strategy to secure your control system.

4.1   Capabilities by Product

This section provides a summary view of the supported security capabilities.

Table 8. Security Capabilities

Security Capabilities	XS/SC26-2
Predefined set of Subjects and Access Rights	x
Access Control List	x

4.2   Access Control and Authorization

This section describes the Access Control capabilities supported by XS/SC26-2 Safety Controllers, which includes its Authorization capabilities.

The Access Control process can be divided into two phases:
1. Definition – Specifying the access rights for each subject (referred to as Authorization)
2. Enforcement – Approving or rejecting access request

4.2.1   Authorization Framework

Defining the access rights for each subject implies that the system must have some means to identify each subject. The most familiar way this is achieved is by assigning a unique User ID to each person who will access the system.

XS/SC26-2 Safety Controllers, however, do not provide such a facility – there is no support for creating additional User IDs. A User ID does not even have to be specified to authenticate. In this case, authorization is based on the functionality being used and the password that is provided for authentication. However, the authentication features supported on XS/SC26-2 Safety Controllers implicitly define a fixed set of subjects, which are identified here.

The subjects defined and supported by XS/SC26-2 Safety Controllers server protocol are indicated in the following table.

Table 9. Subjects Available on XS/SC26-2 Safety Controllers

	Functionality	Application Protocol	Subjects Available
USB	Configuration and Live Monitoring Requests	USB Application	Anonymous User 1 User 2 User 3

    © Banner Engineering Corp.

	Functionality	Application Protocol	Subjects Available
Ethernet	Live Monitoring Requests	XS/SC26-2 Application Protocol	Anonymous User 1 User 2 User 3
	Configuration Requests	XS/SC26-2 Application Protocol	User 1 User 2 User 3

Table 10. Subjects Available on XS/SC26-2 Safety Controllers

	Functionality	Application Protocol	Subjects Available
Ethernet	PROFINET Server	PROFINET	Anonymous
	Modbus TCP Server	Modbus TCP	Anonymous
	ETHERNET/IP Server	Ethernet/IP	Anonymous

4.2.2   Specifying Access Rights

For each subject, XS/SC26-2 Safety Controllers provide predefined access rights. In some cases, those access rights can be partially restricted, while in other cases they either cannot be changed at all or can only be revoked by disabling the associated server/protocol.

Table 11. Access Rights on XS/SC26-2 Safety Controllers

Subject	Application Configuration	Live Monitoring	Network Configuration	Configuration Log	Fault Log	User Passwords	Reset to Factory Defaults
User 1	RW	R	RW	R	RD	RWD	A
User 2	RW	R	RW	R	RD	-	-
User 3	RW	R	RW	R	RD	-	-

Key:
    A = Access control
    R = Read
    W = Write
    D = Delete/clear

The User 1 has the ability to prohibit any subject from reading or writing the Application configuration and/or Network Configuration. Only User 1 can reset controller to Factory Defaults.

4.2.3   Enforcement

The XS/SC26-2 Safety Controller enforces the access rights for the data and services that it provides. The XS/SC26-2 Safety Controller ensures that the Application and Network Configuration can only be updated by a user with the access rights to write the Application Configuration.

Physical Access: The XS/SC26-2 Safety Controller requires physical or network access to the controller to change the application configuration, application logic, and/or overrides/forces of application data. To secure the safety controller, restrict physical access to it by placing the controller in a secure physical environment, such as a locked cabinet.

4.3 Password/PIN Management

The XS/SC26-2 Safety Controller has a set of predefined subjects. The passwords for each subject must be explicitly managed. The Banner Safety Controller Software enforces unique passwords for each subject.

The XS/SC26-2 Safety Controller requires a PIN that is 4 numeric characters for USB access.

For Ethernet access, XS/SC26-2 Safety Controller requires a password that is between 8 and 31 characters long. The password must contain a mix of the following:
- Upper case letters
- Lower case letters
- At least one number
- At least one special character

In addition, all passwords within a single safety controller must be unique for User 1, User 2, and User 3 .

All of these restrictions are enforced by the controller and the Banner Safety Controller Software when used over Ethernet.

Banner Safety strongly recommends the use of complex passwords wherever passwords are used for authentication.

Table 12. Authentication Supported by the XS/SC26-2 Safety Controller

Functionality	Authenticated Subjects	How Passwords are assigned
Configuration Requests	User 1 User 2 User 3	User 1 controls these passwords.

For more detailed information on assigning these passwords, refer to the XS/SC26-2 User Manual (p/n 174868).

4.3.1 Communication Protocols

Some communications protocols provide features that help protect data while it is "in flight" – actively moving through a network.

The most common of these features include:
- Encryption – Protects the confidentiality of the data being transmitted.
- Message Authentication Codes – Ensures message authenticity and integrity by cryptographically detecting message tampering or forgery. This ensures the data originated from the expected source and was not altered since it was transmitted, regardless of whether or not it was malicious.

Currently, only the XS/SC26-2 Application Protocol provides both of these features when used over Ethernet. Other communications protocols supported by XS/SC26-2 Safety Controllers do not provide either of these features, as detailed in the following tables. Therefore, compensating controls may be required to meet an installation's security requirements for protecting data in-flight.

Table 13. Protocol-provided Security Capabilities on XS/SC26-2 Safety Controllers

	Protocol	Data Encryption	Message Authentication Codes
USB	XS/SC26-2 Application Protocol	N	N
Ethernet	XS/SC26-2 Application Protocol	Y	Y
	XS/SC26-2 Discovery Protocol	N	N

Table 14. Protocol-provided Security Capabilities on XS/SC26-2 Ethernet-based Industrial Protocols

	Protocol	Data Encryption	Message Authentication Codes
Ethernet	PROFINET	N	N
	Modbus TCP	N	N
	EtherNet/IP	N	N

4.4   Logging and Auditing

The XS/SC26-2 Safety Controllers do not provide a dedicated security log embedded within the controller.

However, the XS/SC26-2 Safety Controller does log configuration update events in a small (10 entry) configuration log table. Each entry includes the time and date that the configuration was confirmed, using the date and time of the configuration change as maintained on the PC. Also included are the configuration name and the confirmation Cyclic Redundancy Check (CRC).

View this configuration log using the Banner Safety Controller Software. The log is read-only and cannot be reset or exported from the controller. Resetting the controller to factory defaults also generates an entry in the log table.

The XS/SC26-2 Safety Controller also has a fault log. Most of the events that are logged in the XS/SC26-2 Safety Controller fault log represent functional issues, such as hardware failures and unexpected firmware operations. While those are not specific to security, they may provide information that is useful during a security audit. Fault logs are not retained after the power is removed from the safety controller. View the fault log either through the Banner Safety Controller Software or on the onboard display.

Chapter Contents

Chapter 5   Configuration Hardening

To assist in reducing the potential attack surface, this section provides information that can be used to harden the configuration of the XS/SC26-2 products that are present in a particular installation.

Consider configuration Hardening in addition to enabling and using security features such as Authentication, Access Control, and Authorization.

Banner Safety recommends disabling all ports, services, and protocols that aren't required for the intended application. Do this on each XS/SC26-2 product.

5.1   Safety Controller

Use the information in this section when hardening the configuration of a XS/SC26-2 Safety Controller. Consider these options when configuring any XS/SC26-2 Safety Controller that supports them.

These settings are specified within the hardware configuration that is downloaded to the XS/SC26-2Safety Controller.

5.1.1   USB Port, Onboard Interface, and Physical Access

To reduce the potential attack surface, limit the physical access to the USB Port and the onboard interface by limiting the physical access to the safety controller.

This can be done by placing the safety controller in a physically secure environment, such as a locked cabinet.

5.2   Ethernet Interface

Use the information in this section when hardening the configuration of the XS/SC26-2 Safety Controller's Ethernet Interface. Consider these settings when configuring any XS/SC26-2 Ethernet Interface.

If your deployment does not need to access devices that are not on the Process Control Network, routing should be disabled by setting the Gateway IP Address to all zeros:

Table 15. Disabling IP Routing

Service	Parameter Name	Value
IP Routing	Gateway IP Address	0.0.0.0

These settings are specified within the hardware configuration that is downloaded to the XS/SC26-2 Safety Controller.

Ethernet interface can also be completely disabled using the Banner Safety Controller Software.

For more information on these parameters, refer to the XS/SC26-2Safety Controller User Manual (p/n 174868).

Blank page

Chapter Contents

© Banner Engineering Corp.

Chapter 6 Network Architecture and Secure Deployment

This section provides security recommendations for deploying a XS/SC26-2 Safety Controller in the context of a larger network.

6.1 Reference Architecture

The following figure illustrates a reference deployment of XS/SC26-2 Safety Controllers.

Figure 1. Reference Network Architecture

© Banner Engineering Corp.

July 12, 2023
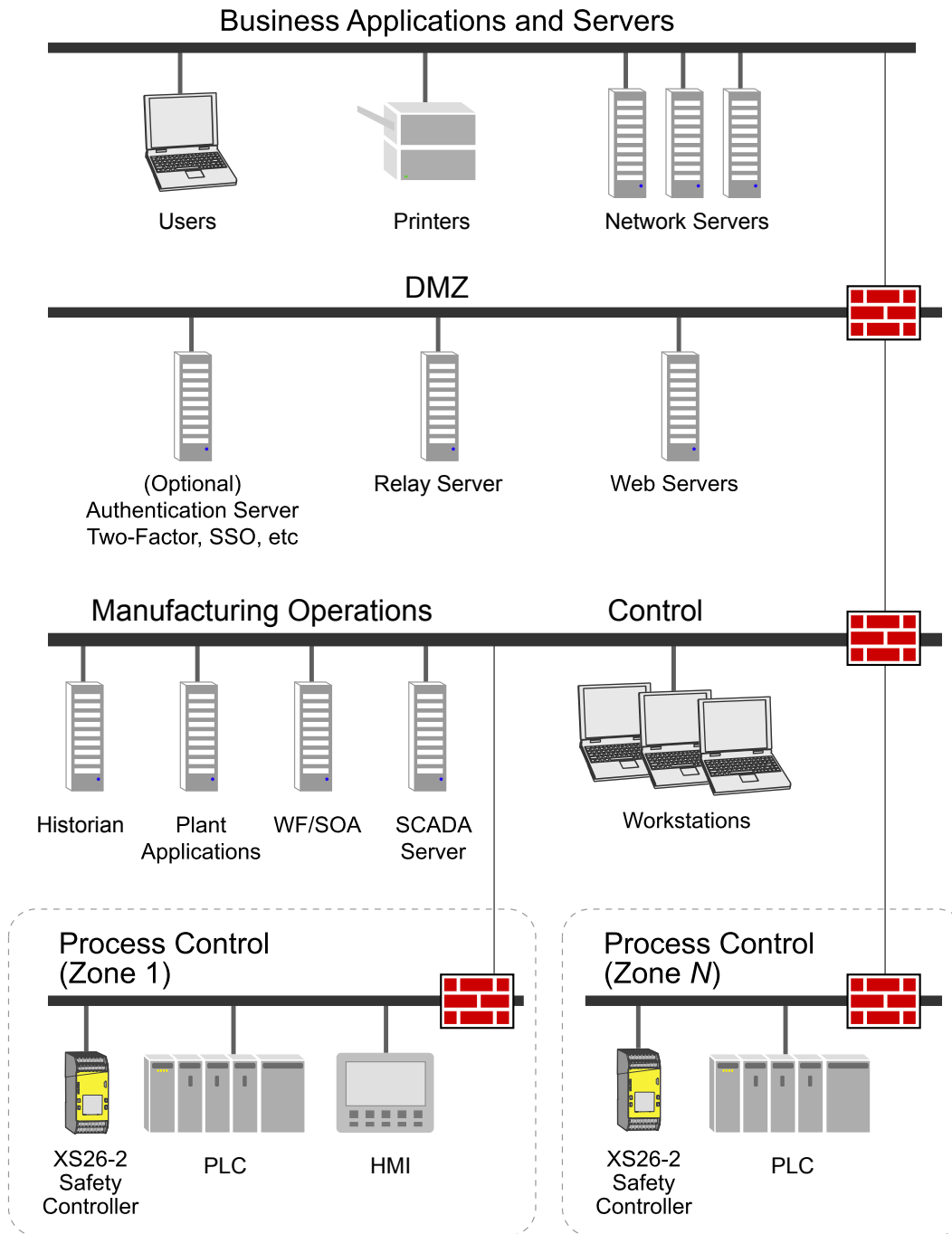
The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet using Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks.

6.2 Remote Access and Demilitarized Zones (DMZ)

DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed so that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. Ideally, the business network and the control network should not communicate directly with each other.

If direct communication to a control network is required from the business network or from the internet, carefully control, limit, and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN) and even then, restrict the allowed protocols/ports to the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

6.3 Access to Process Control Networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required.

However, if a particular protocol (such as Modbus TCP) does not need to be used between those regions, configure the firewall to block that protocol. In addition to blocking the firewall, if a controller does not have another reason it needs to use that protocol, configure the controller itself to disable support for the protocol.

> **NOTE:** Network Address Translation (NAT) firewalls typically do not expose all of the devices on the "trusted" side of the firewall to devices on the "untrusted" side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the "trusted" side of the firewall to a different IP address/port on the "untrusted" side of the firewall. Since communication to the XS/SC26-2 Safety Controller will typically be initiated from a PC on the "untrusted" side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.

Blank page

Chapter Contents

Chapter 7   Other Considerations

7.1   Configuration Management

A strategy for applying security fixes, including configuration changes, should be included in a facility's security plan. Applying these updates often requires that an affected XS/SC26-2 Safety Controller be temporarily taken out of service.

Some installations require extensive qualification and/or commissioning before changes are deployed to the production environment. While this requirement is independent of security, ensuring the ability to promptly apply security fixes, while minimizing downtime, may drive the need for additional infrastructure to help with this qualification.

7.2   Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them.

As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

7.3   Additional Guidance

7.3.1   Protocol-specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document.

7.3.2   Government Agencies and Standards Organizations

Government agencies and international standards organizations may provide guidance on creating and maintaining a robust security program, including how to securely deploy and use Control Systems.

For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and on Recommended Practices for cyber-security with Control Systems. Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

Blank page

Chapter Contents

Chapter 8   Contact Us

Banner Engineering Corp. headquarters is located at: 9714 Tenth Avenue North | Minneapolis, MN 55441, USA | Phone: + 1 888 373 6767

For worldwide locations and local representatives, visit www.bannerengineering.com.