

Frequently Asked Question System 800xA Digital Security Questions and Answers

1. General

1.1 What is the security policy for System 800xA?

The underlying philosophy for network security is based on physically protecting the system, including all nodes, network equipment and network cables, from access by any unauthorized personnel, and further on isolating the system from other networks, allowing access only through properly configured and sufficiently hardened firewalls. This philosophy is described in the white paper "IS Security Considerations for Automation Systems" (3BSE032547).

The System 800xA Administration and Security Guide describes the system's security features and how to use them. Implemented as extensions to Windows security, these features are designed to support validation according to regulatory standards such as FDA 21 CFR Part 11. This includes configurable security functions for user authentication, access control, re- and double authentication on critical operations, audit trail, and digital signatures. Access evaluation includes user authentication and location (node ID), requested operation, and required permissions. Permissions can be set with any granularity: grant or deny for groups and individual users, on individual objects, on structures or substructures of objects, or on the entire system.

The security measures described in the documents mentioned above represent possible steps that a user of System 800xA should consider based on functional requirements and a risk assessment for each particular application and installation. This risk assessment, and the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the System 800xA installation.

1.2 What is your approach to the security of your control system products?

See "IS Security Considerations for Automation Systems" (3BSE032547) and the System 800xA Administration and Security Guide

1.3 Have you undertaken any security assessment/testing of your products?

ABB applies strict quality management procedures in the development of System 800xA. This includes a standardized project model governed by a comprehensive gate review model with checklists for all gates. Design and coding practices include threat modeling, and guidelines and procedures for secure product development. Verification of all project

deliverables is guided by checklists, and the results are subjected to comprehensive testing, including component tests, integration tests, system tests, and release acceptance tests. All testing is done in accordance with written test specifications, and the results are recorded in written test records. The tests include verifying that attempted security breaches are detected and recorded by the system.

1.4 What security vulnerabilities/issues have been identified in any of your products?

There are currently no known security vulnerabilities in the 800xA system software.

1.5 Are there any user groups/forums that you run or are involved in relating to process control security?

ABB is currently represented in ISA SP99, PCSRF, IAONA, IEC TC65A (MT12), CIGRE D2.02 and CIDX.

1.6 What guidance/advice/standards do you provide for the secure use of your products?

1.6.1 General

Guidance and advice for the secure use of System 800xA is given in various documents and instruction manuals, such as

- "IS Security Considerations for Automation Systems" (3BSE032547), is a white paper that provides background information and a general overview of different elements of network security, and presents an overview of security measures and practices that a user of System 800xA may want to consider.
- System 800xA Introduction and Installation provides instructions for how to set up a System 800xA installation, including installation and recommended configuration of Windows and other required 3rd party SW.
- System 800xA Administration and Security Guide describes the system's security features and how to use them, and also provides recommendations for how to secure servers, and how to use Windows Security and Group Policy.
- System 800xA Automation System Network Design and Configuration provides instructions for how to design and configure a System 800xA network, including supported network topologies, network redundancy, Domain Controller and DNS configuration, and clock synchronization.
- System 800xA Configuration provides instructions for application engineering and configuration, including an overview of how to use the FDA 21 CFR Part 11 support.

To facilitate correct and secure installation and configuration, a System Installation Shell is provided. This utility guides you through and partly automates the installation and configuration of Windows and other required 3rd party software, as well as of the System 800xA software. This is done in two main phases:

1. System planning, resulting in a file describing the setup of each node
2. For each node, using the setup files created in phase 1:

- Installation and configuration of Windows, including “hardening”
- Installation and configuration of other required 3rd party SW
- System check, verifying that the correct versions are installed
- Installation and configuration of System 800xA software
- Report generation, creating a report of the installed software per node

System installation using the System Installation Shell is described in documents delivered with the Software media.

1.6.2 Network architecture (segregation etc.)

See “IS Security Considerations for Automation Systems” (3BSE032547), and “System 800xA Automation System Network Design and Configuration” (3BSE034463R4001).

1.6.3 Antivirus

Like any computer system, an automation system should be scanned for viruses at regular intervals. However, if and when a virus is found, the damage has probably already been done. For a mission critical system it is therefore more important to effectively prevent viruses from being introduced to the system than to run frequent virus checks.

A virus checker of good reputation should be used and it should be updated regularly. ABB does not prescribe or recommend any particular brand, however, in our system tests we verify that McAfee does not interfere with system operation.

Virus checking has a significant impact on performance and response times on any computer system. For computer systems that are used for real-time applications, such as process control systems, virus scanning should therefore be done at times when normal system activity is low.

1.6.4 System hardening

The 800xA System Installation Shell (see section 1.6 above) hardens Windows by disabling and/or removing unused functionality to the maximum extent that the system has been verified to work with.

1.6.5 Encryption

Based on the assumption that System 800xA is installed in a physically protected zone with access limited to authorized personnel, and that the 800xA system network is isolated from other networks by means of a properly configured firewall system, internal communication is by default not encrypted. While it is possible to configure the system to use encryption, this has a negative impact on system performance.

All handling of passwords is done by Windows security functions. Authentication is done through SSPI.

For any connection that extends outside the trusted network zone, ABB recommends the use of secure connections. This includes remote workplace configurations as well as connections for remote diagnostics. Note that a remote workplace becomes a member of

the trusted 800xA system network, and therefore requires the same level of physical protection, access control, and isolation from other networks as a local workplace.

- 1.7 Do you provide web-based (or other) reference or resource centers covering process control security?

Yes, at www.abb.com

2. Component Technologies

- 2.1 Which operating systems are your products based upon?

System 800xA servers use Microsoft Windows server 2003 (Windows 2000 Server for certain versions). Workplaces use Microsoft Windows XP Professional. For small systems, Windows XP can be used also for the servers.

AC800M process controllers use the Windriver VxWorks real-time operating system.

- 2.2 What networking technologies are used in your products?

The 800xA system network is based on TCP/IP over Ethernet. Communication between servers and workplaces is by socket communication. Communication between servers and AC800M controllers is according to MMS.

System 800xA uses a routing protocol that is called RNRP (Redundant Network Routing Protocol). This protocol supports redundant network configurations based on standard network components. Detection of a network failure and switch over to the redundant network takes less than one second, with no loss or duplication of data.

The 800xA system network is a private IP network. IP addresses are static, and must be selected according to a scheme defined by RNRP. Each node has two IP addresses, one on the primary network, and one on the backup network.

For performance and integrity reasons, direct connection to the 800xA system network of systems not based on 800xA should be avoided.

It is strongly recommended that the automation system network is defined as a separate Windows domain, i.e. it should not be part of a larger domain, such as a corporate network domain.

System 800xA also supports the following standard fieldbus protocols: HART, PROFIBUS, and Foundation Fieldbus H1 and HSE.

There is also support for a number of ABB proprietary protocols to interface motors, drives, switchgear equipment, etc.

- 2.3 Which of your products use wireless networking technologies?

System 800xA as such does not make use of wireless technologies. However, although this is not generally recommended, a user of a System 800xA installation may obviously elect to use e.g. 802.11 as media for a smaller or greater part of a network installation.

The white paper "IS Security Considerations for Automation Systems" (3BSE032547) describes issues that should be considered when using wireless networks.

Previous versions of Industrial IT include a hand-held product Pocket Portal, which uses Bluetooth or 802.11. This product will be supported in future versions of System 800xA. Note that it is the responsibility of the user of a System 800xA installation to determine whether it is appropriate to use this product or not for his/her particular installation and application.

2.4 Which of your products use web servers?

System 800xA uses Microsoft Internet Information Server (IIS) for some internal functions. IIS should be locked down to accept requests only from nodes within the automation system (private and static IP addresses). This is described in relevant installation guides.

2.5 Are systems/servers hardened when they are installed?

The 800xA System Installation Shell (see section 1.6 above) hardens Windows by disabling and/or removing unused functionality to the maximum extent that the system has been verified to work with.

For most situations adequate hardening is achieved provided that the recommended installation and configuration procedures are followed, see

- "System 800xA Installation" (3BSE034678R4001)
- "System 800xA Administration and Security" (3BSE037410R4001).

Further hardening can be handled according to customers' requirements on a case-by-case basis.

2.6 Do you provide any historian products (or similar applications that provide access to process control data to other users).

Yes, System 800xA Information Management provides this functionality. The instruction manual "System 800xA Information Management, Configuration" describes how to configure this in a secure way.

2.7 Are there any methods for remote applications to write data to the control system?

Yes, there are several ways to do this, all controlled by the system's security functions. Remote accessibility can also be controlled through firewall configuration.

- OPC, OLE-DB, and ODBC client connections
- OLE-DB client connection
- ODBC client connection

- 2.8 What 3rd party components are used in your systems? What testing is done on these and what is the approach to security patching and updates?

A list of required 3rd party software components is provided in the instruction manual "System 800xA Installation" (3BSE034678R4001). These components are tested as part of System 800xA component, integration system and release acceptance tests.

Regarding security updates, see 3.4.

3. Anti Virus Protection

- 3.1 What are your recommendations for anti virus protection?

ABB's philosophy regarding anti virus protection is described in "IS Security Considerations for Automation Systems" (3BSE032547).

Like any computer system, an automation system should be scanned for viruses at regular intervals. However, if and when a virus is found, the damage has probably already been done. For a mission critical system it is therefore more important to effectively prevent viruses from being introduced to the system than to run frequent virus checks.

Virus checking has a significant impact on performance and response times on any computer system. For computer systems that are used for real-time applications, such as process control systems, virus scanning should therefore be done at times when normal system activity is low.

- 3.2 Which anti virus products do you recommend for use with your control system applications?

ABB does not prescribe or recommend any particular brand of AV software, however, in system and release acceptance tests we verify that McAfee and Norton do not interfere with system operation.

- 3.3 What is your policy for ensuring that there is up-to-date accredited AV protection software available for your products?

The update services provided by the AV software vendor should be used. The document "IS Security Considerations for Automation Systems" (3BSE032547) describes possible procedures for performing the updates.

- 3.4 Outline your process for the assessment of patches/updates from other vendors (e.g. operating system providers) and informing current installations?

ABB validates security updates from Microsoft with respect to relevance to and compatibility with the IndustrialIT System 800xA. For updates that Microsoft classifies as "critical", the goal is to communicate to customers within 24 hours the plan for validating each update and within 7 days the result of the validation. For this communication we use the ABB Solutions Bank, which also has possibilities for customers to subscribe for e-mail notification on updates.

4. System Integrity

4.1 Do you have a defined and approved system configuration baseline?

Using the System 800xA Installation Shell will result in configuration settings that are approved and verified in our system tests. The Installation Shell produces a report that describes these settings.

4.2 Do you have any recommended products or assurance tools for assessing whether an installed system is up to date with the current approved system baseline?

The System 800xA Installation Shell produces for each node a list of installed ABB and 3rd party software components, including version numbers.

The System 800xA “about box” lists the version numbers of all installed 800xA software.

Using the System 800xA Installation Shell will result in configuration settings that are approved and verified in our system tests. The Installation Shell produces a report that describes these settings.

Further, the system includes a Security Report feature, which produces a comprehensive report of all security settings, including users and user groups, required and granted permissions, etc.

5. Training and Support Services

5.1 Do you provide any training courses/materials covering the security of your products?

Standard training courses and instruction manuals for System 800xA include system administration, engineering, and operational aspect of the system’s security functions. In addition, specific training and consultancy services addressing security are offered through ABB’s Consult^{IT} Process Automation Product Services.

5.2 Are there any special security services or products that you provide?

ABB offers configuration of System 800xA security functions as part of its regular project engineering activities.

Through Consult^{IT} Process Automation Product Services, ABB also offers consulting services related to IT security, in cooperation with IBM.

5.3 Who should be the main contact for any security questions?

Customers should contact their primary ABB contact on questions regarding security as well as on any other support questions.

6. ESD Systems

6.1 Do you provide your own ESD systems?

A SIL 2 certified safety control version of AC800M was released with system version SV4.0.

6.2 System 800xA also includes integration with SafeGuard ASG410, which is SIL3 certified. Are there any links between the ESD systems and the main control systems?

The ESD system can be set up either as a separate system in parallel to a processes control system, or integrated with the processes control system, depending on user preferences.

6.3 Will your control systems link to ESD systems provided by other vendors? If so how?

There is currently no ready-made integration with any particular ESD system form other vendors. However, System 800xA provides very efficient mechanisms for easy integration of other systems and devices.

© Copyright 2005 ABB. All rights reserved.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document or the information contained therein, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described or referred to in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Trademarks:

Registrations and trademarks used in this document include:

The IndustrialIT wordmark and all product names in the form XXXXXXIT mentioned herein are registered or pending trademarks of ABB.

| | |
|-----------------------------|---|
| Microsoft | Registered trademark of Microsoft Corporation. |
| Windows | Registered trademark of Microsoft Corporation. |
| Windows 2000 and Windows XP | Registered trademarks of Microsoft Corporation. |
| ActiveX and Visual Basic | Registered trademarks of Microsoft Corporation. |
| Aspect Studio | Trademark of ABB Ltd., Switzerland. |
| Aspect Express | Trademark of ABB Ltd., Switzerland. |
| Process Portal | Trademark of ABB Ltd., Switzerland. |



Doc. no. 3BSE037783 en

Rev. ind. A

Date 2005-04-13

REVISION

| Rev. ind. | Page (P) Chapt. (C) | Description | Date Dept./Init. |
|------------------|--------------------------------|--|------------------------------------|
| - A | All | First version for SV3.1. Adjustments for SV4. | 2005-04-13 SE-ATPA/XA Erik D |