Schneider Electric
Security Features
For 21 CFR Part 11 Compliance
User Guide

Version 1.0

31004553 00

a brand of Schneider Electric

Telemecanique

This page is intentionally blank.

Table of Contents

Safety Information 5

About the Book 7

Chapter 1 Overview of 21 CFR Part 11 Compliance 11

At a Glance 11
About 21 CFR Part 11 Compliance 12
Requirements of a Part 11 Compliance System 13
Resources about 21 CFR Part 11 14

Chapter 2 Implementing Part 11 15

At a Glance 15
Implementing Part 11 Compliance Solutions 16
Schneider Electric Features Supporting Part 11 Compliance Solutions 18
Access Protection 19
Audit Trail 29
Secure Application 34
Protection of Information 37

Chapter 3 Integration Issues 43

At a Glance 43
Exemptions to Write Restrictions 44
Potential Error Messages Using Communication Services 45
Preventing Inadvertent Writes Using a Modbus Plus Network 46
Connecting a Concept Personal Computer to a Write-restricted Quantum PLC through a Bridge 51

Appendices **55**
At a Glance 55
Appendix A **NOEs/NOMs Supporting Write Blocking 57**
NOEs/NOMs Supporting Write Blocking 57
Appendix B **Schneider Electric 21 CFR Part 11 Product Compatibility . . . 59**
Schneider Electric Product Compatibility Chart 59
Glossary **65**
Index **67**

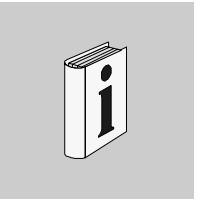
PLEASE NOTE

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When controllers are used for applications with technical safety requirements, please follow the relevant instructions.

No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. This document is not intended as an instruction manual for untrained persons.

About the Book



At a Glance

Document Scope

This user guide presents an overview of the U.S. Food and Drug Administration (FDA)'s Final Rule, 21 CFR Part 11 ("Part 11"), maps the FDA requirements to Schneider Electric equipment, describes Schneider Electric equipment that assists in implementing Part 11 compliance solutions, and offers Schneider Electric's suggestions for integrating Schneider Electric equipment into a system that will become a Part 11 compliance solution.

Part 11 compliance concerns a uniform approach to paperless systems, specifically electronic records and electronic signatures, and Part 11 compliance applies to organizations that are regulated by the FDA.

A Part 11 compliance solution for a secure system must include:

- FDA requirements
- Appropriate equipment
- On-site procedures and controls

Note: Schneider Electric Involvement:
Schneider Electric sells products, Concept 2.6 and Quantum PLCs, that assist you in implementing compliance solutions for organizations. Schneider Electric has mapped some FDA requirements to the Concept/Quantum equipment, but Schneider Electric CANNOT establish the procedures and controls inside the facility of an FDA regulated industry. Responsibility for implementing the procedures and controls lies with the management of the respective industry.
If, in moving towards Part 11 compliance, you choose to implement Schneider Electric equipment, you will NOT implement a fully Part 11 compliance solution. You are responsible for implementing procedures and controls, which, when combined with the equipment and software, enable you to implement a Part 11 compliance solution.

Please Note

Electrical equipment should be serviced only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material. This document is not intended as instruction manual for untrained persons.

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Related Documents

Title of Documentation	Reference Number
Quantum Hardware Reference Guide	840 USE 100 00
Concept User Manual	840 USE 503 00
Modicon Modbus Plus Network Planning and Installation Guide	890 USE 100 00

Product Related Warnings

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When controllers are used for applications with technical safety requirements, please follow the relevant instructions.

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

Failure to observe this product related warning can result in injury or equipment damage.

User Comments

We welcome your comments about this document. You can reach us by e-mail at TECHCOMM@modicon.com

This page is intentionally blank.

1. Overview of 21 CFR Part 11 Compliance

1

At a Glance

Purpose

This material presents an overview of Final Rule, 21 CFR Part 11 ("Part 11") compliance regulations issued by the U.S. Food and Drug Administration (FDA), an agency of the U.S. Department of Health and Human Services.

For a complete discussion of the requirements for Part 11 compliance, see:

- Department of Health and Human Services, Food and Drug Administration. "21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice, Rules and Regulations." Washington, D.C.: *Federal Register* 62, no. 54 (20 March 1997): 13429. `http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf`

What's in this Chapter?

This chapter contains the following topics:

Topic	Page
About 21 CFR Part 11 Compliance	12
Requirements of a Part 11 Compliance System	13
Resources about 21 CFR Part 11	14

1.1. About 21 CFR Part 11 Compliance

1.1.1. Overview

1.1.1.1. This unit presents a general understanding of Part 11 compliance solutions for electronic records and electronic signatures. For an in depth understanding, Schneider Electric recommends that you read documents not written by Schneider Electric.

1.1.1.2. As used in this guide, the phrase "Part 11" refers to regulations issued by the U.S. Food and Drug Administration (FDA), an agency of the U.S. Department of Health and Human Services, specifically Final Rule *Title 21 Code of Federal Regulations* (*21 CFR Part 11*), published in the *Federal Register* (Mar. 20, 1997, pages 13464-13466; effective: Aug. 20, 1997).

`http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf`

1.1.2. Summarizing 21 CFR Part 11

1.1.2.1. Industries concerned with Part 11 compliance are FDA regulated industries, which asked the FDA to establish uniform approaches to the authenticity, integrity, and confidentiality of electronic records and electronic signatures.

1.1.2.2. Part 11 establishes the criteria under which electronic records and electronic signatures are considered equivalent to records and handwritten signatures executed on paper. Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations, as well as documents submitted to the FDA that are not required by the agency. Currently, the FDA accepts the electronic submission of documents (in whole or part) as identified in Public Docket 92S-0251, including:

1. Biologics License Applications (BLA)
2. Product License Applications (PLA)
3. Establishment License Applications (ELA)
4. New Drug Applications (NDA)
5. Biologics Market
6. Basic Information re Submission of Notices of Claimed Investigational Exemption to Center for Veterinary Medicine (CVM)

1.1.2.3. Part 11 does not apply to paper records transmitted by electronic means.

1.2. Requirements of a Part 11 Compliance System

1.2.1. Requirements

1.2.1.1. A Part 11 compliance solution must contain mechanisms to:

1. **Validate electronic records and electronic signatures**
   The FDA defines validation as "the process of establishing documented evidence which provides a high degree of assurance that a system will consistently perform in accordance with its predefined specifications and quality attributes" (Ref: FDA, Glossary of Computerized System and Software Development Terminology). The system must be able to generate copies of documents in human readable (i.e., in plain text) and in electronic forms.
2. **Generate built-in checks of closed systems**
   1. System checks that enforce the sequencing of events, where required
   2. Authority checks that determine who has access to the system and at what level
   3. Device checks that determine the validly of sources of data being entered into a system
3. **Create an audit trail**
   An audit trail is a record showing who has accessed a computer system and what operations were performed during a given period. Audit trails:
   1. Must be secure
   2. Must be computer-generated and time-stamped
   3. Cannot obscure previously changed data
   4. Must identify the person responsible for making the change
   5. Must include both the original and changed data
   6. Must be available for review and copying by the FDA

   Audit trail documentation thus generated must be retained for at least as long as the subject electronic records, either pursuant to a predicate rule or to the organization's own records retention policy.
4. **Limit access to systems**
   Organizations using electronic records must also limit system access to authorized individuals. Limiting access requires a policy decision regarding the levels of access, the roster of individuals within each level, the criteria for determining eligibility for that level, and other system safeguards to prevent access by unauthorized individuals.
5. **Require a suitable level of training for personnel**
   As with most FDA regulations, including most predicate rules, Part 11 requires that individuals who develop, maintain, or use electronic records and electronic signatures have the education, training, and experience to perform their assigned tasks.

1.3. Resources about 21 CFR Part 11

1.3.1. Resources

1.3.1.1. The following list offers resources for gaining in depth information about Part 11 regulations:

1. `http://www.fda.gov/ora/`
   (describes the Office of Regulatory Affairs (ORA) including *Compliance References* published by ORA)

2. `http://www.fda.gov/ora/compliance_ref/part11/`
   (information and links about Final Rule, 21 CFR Part 11)

3. `http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf`
   (complete Final Rule as a PDF document viewable with Adobe *Acrobat Reader*)

4. `http://www.21cfrpart11.com/index.html`
   (information on the Final Rule and active discussion of issues and concerns with industry peers and government regulators)

2. Implementing Part 11

2

At a Glance

Purpose

This material presents the Schneider Electric features that support 21 CFR Part 11("Part 11") compliance solutions for FDA-regulated industries.

What's in this Chapter?

This chapter contains the following topics:

Topic	Page
Implementing Part 11 Compliance Solutions	16
Schneider Electric Features Supporting Part 11 Compliance Solutions	18
Access Protection	19
Audit Trail	29
Secure Application	34
Protection of Information	37

2.1. Implementing Part 11 Compliance Solutions

2.1.1. Products Supporting Part 11

2.1.1.1. The following Schneider Electric products are referred to throughout as the "Concept and Quantum package" or "Concept/Quantum package." "Quantum PLC" is a complete Quantum system.

1. Concept 2.6 SR1 (and later). No application conversion is required for Concept when upgrading from version 2.5 SR2 to version 2.6.
2. Quantum 140CPU43412A (Executive (SV) Revision 1.20 or higher)
3. Quantum 140CPU53414A (Executive (SV) Revision 1.20 or higher)
4. Compact: E258, E265, E275, and E285
5. Momentum PLCs

2.1.1.2. Note: Concept/Quantum
Older versions of Concept/Quantum do not support Part 11.

2.1.1.3. Note: Quantum
- If the Part 11 features are not activated, the new PLC Exec will be fully backward compatible with previous Execs.
- To update a CPU to support Part 11, download the latest version of the 434A/534A executive from:
  `http://www.modicon.com`
- Non A versions (434/534) will accept a download of a project with Quantum Security Parameters set, but NO security features will be in effect.
- Schneider Electric recommends disabling the Modbus and Ethernet ports for an optimal secure system.

2.1.1.4. Note: Compact and Momentum
The following features are NOT available in Compacts and Momentums:
- Write restriction
- Auto Logout
- Secure Application

2.1.2. Windows Operating System

2.1.2.1. Schneider Electric cannot guarantee the security of any operating system. Schneider Electric recommends using a Windows NT class security system. At a minimum, Schneider Electric recommends NT 4.0 SP5. Schneider Electric recommends that you perform these steps:

1. Review the security issues in your present organization.

2. Make adjustments so your organization can have a Part 11 compliance solution.

2.1.2.2. Note: Schneider Electric sells products that assist you in implementing Part 11 compliance solutions.
Software and hardware alone DO NOT ensure compliance. **You are responsible** for implementing procedures and controls, combining them with the software and hardware, to ensure compliance.

2.2. Schneider Electric Features Supporting Part 11 Compliance Solutions

2.2.1. Concept/ Quantum Package

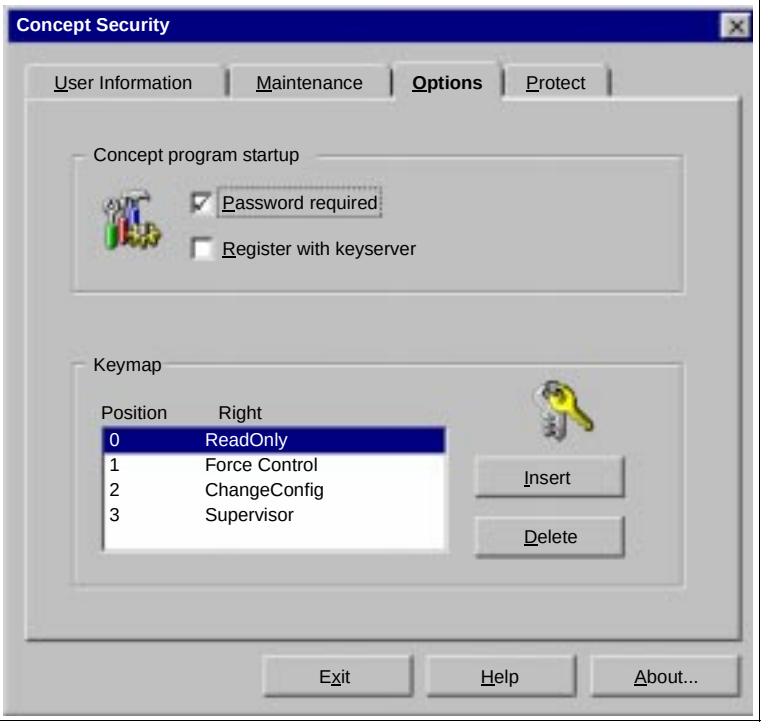
2.2.1.1. The following Final Rule, 21 CFR Part 11 Compliance requirements map to these Schneider Electric features

Item	Part 11 Requirement	Schneider Electric Feature
1	Generate built-in checks of closed systems Limit access to systems	**Access Protection** **1.** Protect the Concept software with a startup password **2.** Protect the hardware by selecting a set of Modbus Plus nodes (addresses) for write access, excluding write access to the CPU from Quantum PLC Ethernet modules (NOEs) and Modbus Plus modules (NOMs), or excluding writes from the Quantum PLC's native Modbus ports **3.** Protect the Quantum PLC hardware with a password **4.** Protect the hardware by logging out users after a specified period of inactivity
2	Validate electronic records and electronic signatures Create an audit trail	**Audit Trail** **1.** Create an encrypted event-log file (with hidden log-file path stored on your personal computer) **2.** Use a consistent format for the time stamp, project ID, and user name **3.** View and print the event-log file using Concept Logfile Viewer on your personal computer
3	Validate electronic records and electronic signatures	**Secure Application** Automatically set **1.** Enable encrypted logging **2.** Universal date format **3.** Enable a log-file path
4	Generate built-in checks of closed systems	**Protection of Information** **1.** Protect projects and Derived Function Blocks (DFB) using Concept's Security Tool **2.** Protect memory using the Quantum CPU's key switch **3.** Protect data stored in the Quantum PLC using the Data Access Protection config extension **4.** Protect against lost changes using Concept's automatic save

2.3. Access Protection

2.3.1. Using Passwords in Concept

2.3.1.1. To require a password for a user

Step	Action
1	Start the Concept Security tool. Log on as a user with Supervisor privileges.
2	On the Options tab, select Password required 
3	On the Maintenance tab, Supervisors establish access levels and assign users, but cannot set user passwords.

2.3.1.2. Note: Passwords (Concept)
Must be at least 6 characters long and are case-sensitive. Schneider Electric recommends using standard alphanumeric characters and avoiding special characters: ! @ # $ % ^ & * ( ) ? / \ [ ]. Users supply a password when they log on for the first time.

2.3.1.3. When Concept security is enabled, users who have set passwords can log on using the Concept Security Logon dialog. Unregistered users (whose names do not appear in the registered users list in the Concept Security dialog) and users without valid passwords no longer have read-only access.

2.3.1.4. Note: To register a user, a Supervisor must enter the user's name into the registered users list.

2.3.1.5. Create and delete additional users with Supervisor privileges using the Concept Security Tool.

2.3.1.6. Note: Even with Supervisor privileges, Concept Security Tool does not allow deletion of all users.

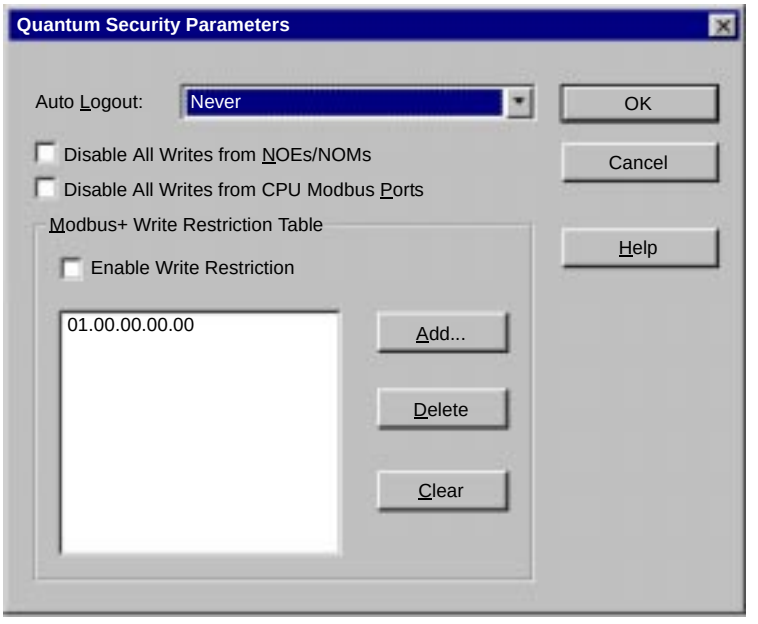
2.3.1.7. To add users in Concept,

Step	Action
1	Select the Maintenance tab.
2	Click Add.
3	Type the user name in the Name field.
4	Select the user permissions from the Access Rights list.
5	Click OK
6	To add additional users, repeat Steps 2-5.
7	If finished, click Exit.

2.3.2. Using Write Restrictions

2.3.2.1. Write restrictions block the write communication function codes listed in the *Communication Function Codes, p. 44* unit.

2.3.2.2. To set a write restriction (ability to modify the project's logic, configuration, and State RAM) to a Quantum PLC:

Step	Action
1	Start Concept program.
2	Select Configure | Security extension. The following dialog appears 

2.3.3. Disabling All Writes

2.3.3.1. Two options exist for disabling all writes:

Option	Action
NOE/ NOM Modules	To exclude all writes through Quantum PLC Ethernet modules (NOE) and Modbus Plus modules (NOM), select Disable All Writes from NOEs/NOMs. This option: **1.** Blocks all writes sent to the Quantum PLC from all NOE and NOM modules, including writes to any user memory location in the Quantum PLC **2.** May require reconfiguring the network to route specific traffic to the native Modbus Plus port that allows selective write access. All other non-write messages are processed normally. **3.** Does not affect native Modbus or Modbus Plus ports. Enabling the exclude all writes through NOE/NOMs allows no NOE/NOM module to write to the Quantum PLC and no NOE I/O scanning.
CPU Modbus Ports	To exclude all writes through the Quantum PLC's native Modbus port, select Disable all Writes from CPU Modbus Ports. This option: **1.** Blocks all writes from the 2 native Modbus ports **2.** Does not affect Quantum NOE or Quantum NOM writes **3.** Does not affect the native Modbus Plus port on the CPU **4.** Allows reads

WARNING

UNINTENDED SYSTEM OPERATION

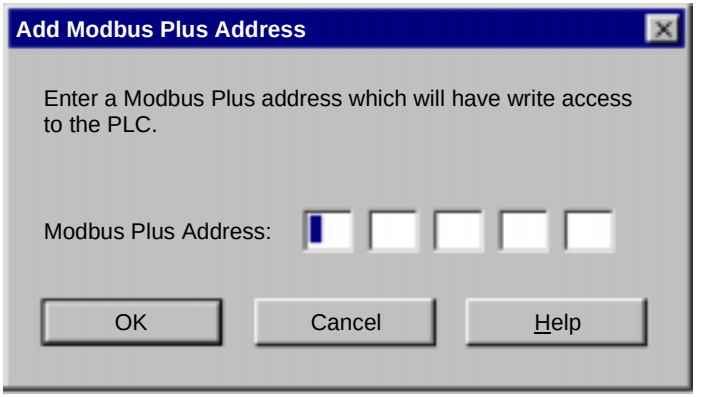
Use of network adapters other than those specified in *NOEs/NOMs Supporting Write Blocking, p. 57* will not prevent write access from that adapter to a write-restricted Quantum PLC.

- Use only those network adapters specified.

Failure to follow this precaution can result in death, serious injury, or equipment damage.

2.3.4. Enabling Write Restriction

2.3.4.1. To give write permission to a set of Modbus Plus network nodes (addresses) and prevent writing to the Quantum PLC from any address not in the list:

Step	Action
1	Select Enable Write Restriction (check box). **Note:** You can only use this feature for nodes communicating to the Quantum PLC through its native Modbus Plus port. The address of the programming panel cannot be deleted. **1.** Delete: removes the selected address **2.** Clear: removes all addresses except the address of the personal computer that is running
2	Click Add. The following dialog appears  **Note:** Use standard Modbus Plus addresses (valid addresses are 1-64). If any entry in a Modbus Plus path is a zero (0), all subsequent entries in that path must be 0.
3	Enter an address: **1.** Addresses must be entered looking from the receiving write-restricted Quantum PLC toward the sender. (Sender and receiver may be on different Modbus Plus network segments, separated by one or more bridges/ gateways). **2.** Begin the address with the first gateway or Quantum PLC encountered. **Note:** Failure to follow these instructions may prevent you from using the Quantum PLC through its Modbus Plus port.
4	Click OK.
5	(Optional) Repeat steps 1-4 for additional addresses (maximum 12).

2.3.4.2. If a Global or Specific input (PEER COP) or other input (DIO) is configured using an address from a Quantum PLC not in the write restriction list box, the configuration is invalid and you cannot start the Quantum PLC, and you will get a Traffic Cop error with Stop Code 4000.

	**WARNING** **UNINTENDED SYSTEM OPERATION** For a bridge/gateway with write access, all nodes on all nonlocal network segments will have the ability to write to the write-restricted Quantum PLC. To prevent this condition, do one of the following: ● Do not use bridges/gateways, or ● Do not allow write access to bridges/gateways, or ● If you must give write access to a bridge/gateway, place only those devices that you want to have write access privileges to the Quantum PLC on the bridged network segments. For an expanded discussion, see *Preventing Inadvertent Writes Using a Modbus Plus Network, p. 46*. **Failure to follow this precaution can result in death, serious injury, or equipment damage.**

2.3.5. Reading Information

2.3.5.1. Reading information from a Quantum PLC is allowed regardless of write restrictions.

2.3.6. Downloading Projects

2.3.6.1. If you select Disable All Writes from NOEs/NOMs, Disable All Writes from CPU Modbus Ports, or Enable Write Restriction while in a write-restricted path:

1. You will be locked out while downloading projects if a project is downloading to a Quantum PLC in Dim Awareness state.
2. You will be unable to load the user logic.

2.3.7. Setting a Logon Password for a Quantum PLC

2.3.7.1. Supervisors set Quantum PLC passwords and provide them to users.

2.3.7.2. To edit passwords, users must have at least download permissions activated in Concept Security (see the Concept Security chapter in the *Concept User Manual*).

2.3.7.3. Note: Passwords (Quantum)
Must be 6-16 characters long and are not case-sensitive. Use standard alphanumeric characters only (no spaces). The default password is an empty field (null string).

2.3.7.4. To set or edit a Quantum PLC password

Step	Action
1	Connect to the Quantum PLC by selecting Online | Connect.
2	If the Quantum PLC has a password, enter now.
3	Select Online | Control Panel.
4	Click Stop PLC and click Set PLC Password.
5	Enter or edit the password, then confirm it.
6	Click OK.

2.3.7.5. The password will take effect the next time you log on.

2.3.7.6. To log on to a password-protected Quantum PLC, enter your Quantum PLC password and click OK.

2.3.8. Lost Password Procedure

2.3.8.1. This procedure:

1. Erases the battery-backed-up RAM without loading the Quantum PLC program from Flash (if the program was saved to Flash).

2. Sets the Quantum PLC into its initial unconfigured state, disabling its logon password protection.

2.3.8.2. If you lose your password:

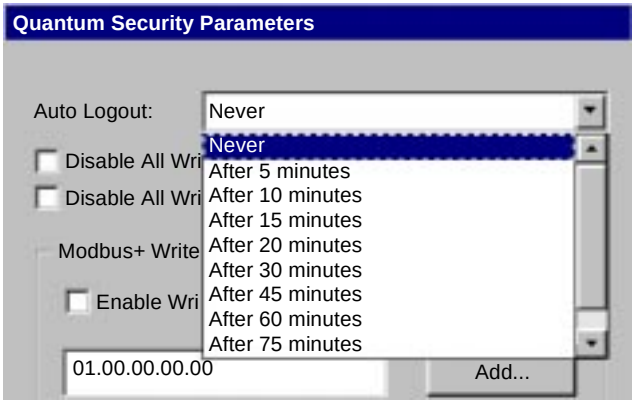
Step	Action
1	Reload the Executive using ExecLoader.
2	Cycle power to the Quantum PLC.
3	Connect to the Quantum PLC using Concept. (No password required.)
4	Download both configuration and program to the Quantum PLC.
5	Select Online | Online Control Panel... .
6	Set new PLC Password.
7	Enter and confirm password.
8	If needed, save program to Flash by selecting Flash program...
9	When finished, start the Quantum PLC.

2.3.9. Using Auto Logout

2.3.9.1. If a personal computer remains connected to a Quantum PLC for long periods of inactivity, unauthorized access to the Quantum PLC is possible. Use the Auto Logout feature to set a logout interval.

2.3.9.2. Note: Auto Logout only logs you out of the Quantum PLC, not out of Concept. If necessary, use your operating system's logout capabilities to shut down Concept.

2.3.9.3. To set an Auto Logout interval

Step	Action
1	Select Configure | Security extension. The following dialog appears. 
2	From the Auto Logout dropdown, select a time interval. If you select **1.** Never: The personal computer is never disconnected from the Quantum PLC. **2.** Auto Logout: The personal computer is connected, but if the personal computer is not performing an operation, it disconnects from the Quantum PLC when the selected time interval expires.
3	Click OK.

2.3.9.4. Note: Programming or animating
If you are actively programming or animating, the personal computer is not disconnected from the Quantum PLC.

2.3.9.5. Note: To use Auto Logout through an NOE, requires one NOE dedicated to the Concept connection, and that NOE must not be used for any other communication purposes.

2.4. Audit Trail

2.4.1. Creating an Audit Trail

2.4.1.1. Creating an audit trail requires logging events in a file on a personal computer. Logs are provided in a consistent format. For each event logged in Concept and Quantum PLCs, you can:

1. Create an encrypted event-log file (*.enc) with a consistent format for the time stamp, project ID, and user name. Encrypting hides the path to the event-log file and makes the file unreadable with external editors.

2. View encrypted event-log files and print event-log files using Concept Logfile Viewer.

2.4.1.2. Event-log files created by Concept contain some or all of these entries:

1. Old value/New value
2. Project name
3. User name
4. Date and time
5. Section name
6. EFB/DFB instance name or instance number
7. EFB type
8. EFB Pin-Name (Variable Name, or Literal, or Address)

2.4.1.3. Naming conventions:
1. <4 digit year><2 digit month><2 digit day>.enc, for example 20021225.enc
2. Unencrypted event-log files have the extension *.log

2.4.1.4. Note: Event-log files are created daily at midnight.

2.4.1.5. When creating an audit trail, consider that:

1. When switching between encrypted and unencrypted logging, a log message indicates the change.

2. On open projects, changes are not allowed to the log-file path (in the Directory for Log-File: field) or the Encrypt Logfile and Universal Date Format check boxes (disabled). Even a Supervisor cannot make changes.

2.4.1.6. Note: External applications may be able to find, then corrupt and destroy event-log files.

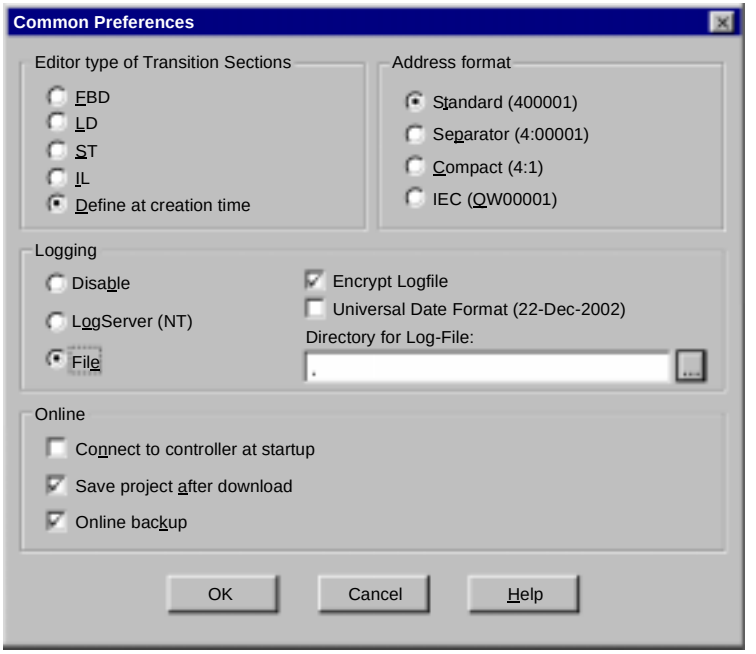
2.4.1.7. If you do not define a log-file path, Concept creates a default path to the Concept install directory (always writable). If no writable disk is found, Concept displays an error message. Correct this condition before opening a project.

2.4.2. Creating Encrypted Event-Log Files

2.4.2.1. Encrypted log file paths are visible only to Supervisors.

2.4.2.2. Note: Only Supervisors may make changes in the Logging area of the Common Preferences dialog.

2.4.2.3. Encrypting Log Files

Step	Action
1	In Concept, select Options | Preferences | Common Preferences.
2	Select Encrypt Logfile in the Logging area 
3	To select a path for storing log files on your personal computer, type a directory name in the Directory for Log-File: field or click the ellipsis button (...) and select a directory.
4	Click OK.

2.4.3. Formats for Event-Log Files

2.4.3.1. To identify changes easily and quickly and create consistently formatted event-log files, select the Universal Date Format in the Logging area of the Common Preferences dialog.

2.4.3.2. Universal Date Format specifications:

1. Format: day-month-year
2. Abbreviated months (Jan, Feb, Mar, etc.)
3. 24-hour clock (no AM/PM)

2.4.3.3. Example: 22-Dec-2002 14:46:24

2.4.3.4. Note: The default date format is the Windows short date format (to view this format, in Windows select Start | Settings | Control Panel | Regional Settings).

2.4.4. Viewing Encrypted Event-Log Files

2.4.4.1. Use the Concept Logfile Viewer to view encrypted event-log files (Supervisors only)

Step	Action
1	Select File | View Logfile.
2	Select the event-log file in the Open dialog.
3	Click OK.
4	The Concept Logfile Viewer appears. **1.** If the file has been altered, corrupted, or damaged, a message appears. **2.** The Concept Logfile Viewer displays both types of event-log files (.enc/.log). **3.** You can search the file, but you cannot edit it.

2.4.4.2. You can view unencrypted event-log files using Concept Logfile Viewer or a text editor.

2.4.4.3. Note: If you use an external text editor to view an event-log file, the data may become corrupted.

2.4.4.4. Considerations for event-log files:

1. To print an event-log file, use the personal computer's standard printing procedure.

2. To avoid possible unauthorized access to event-log files, view or print them only from the personal computer that created them. Only Supervisors can view or print from another personal computer.

3. If you move an event-log file after it is encrypted, the new file path is not recorded.

4. If you delete an event-log file after it is encrypted, the deletion from the directory is not recorded.

2.5. Secure Application

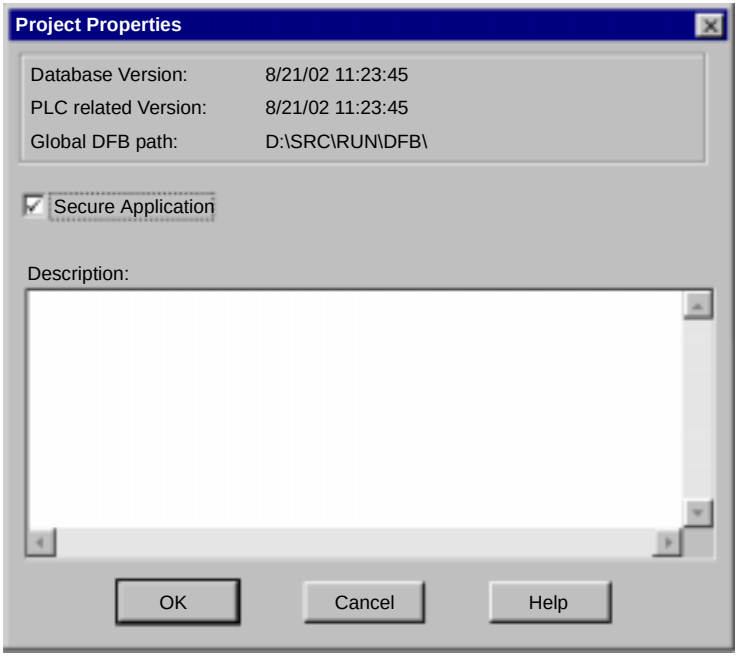
2.5.1. Setting a Secure Application State

2.5.1.1. You are not required to select Secure Application for Part 11 compliance, but if you do not select Secure application, you must encrypt logging by selecting the Encrypt Logfile check box in the Concept Common Preferences dialog.

2.5.1.2. Select Secure Application or define a procedure to set up and verify that logging is operating correctly.

2.5.1.3. Note: You must be a supervisor to perform this procedure and make sure you are disconnected from the PLC.
Your Concept application/project must include at least one IEC section. If you have a 984 only application/project, you must add an IEC section. During downloads, Concept checks for an IEC section; the download fails if no IEC section is found.

2.5.1.4. To set a secure application state

Step	Action
1	In the Concept Project Properties dialog, select Secure Application. 
2	Click OK.

2.5.1.5. The secure application state is part of the Quantum PLC's configuration and is included when you download a project to the Quantum PLC.

2.5.2. Automatically Setting Parameters and Verifying Valid Values

2.5.2.1. By creating, opening, or uploading a project with the Secure Application check box selected, Concept does the following:

1. Automatically sets
    1. Universal Date Format
    2. Encrypt log file
    3. Log file path
2. Verifies log file path parameter contains valid values

    If the log file path does NOT contain valid values, Concept will use default values (Concept install directory).

    Once you select secure application, Concept does not allow changes to the path.

2.6. Protection of Information

2.6.1. Protecting Projects and DFBs

2.6.1.1. Supervisors protect projects, and you can not modify protected projects.

2.6.1.2. To protect projects/DFBs

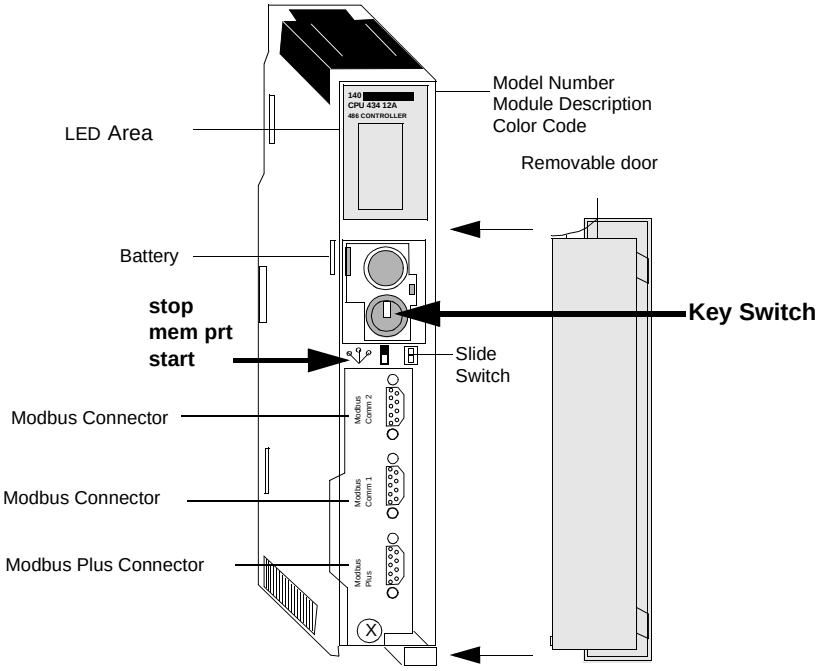
Step	Action
1	Start access management by double clicking Concept Security.
2	Enter password of a user with Supervisor rights and click OK.
3	Select the Protect tab.
4	Click Select.
5	Select a project/DFB and click OK.
6	Highlight the project/DFB and click Protect.
7	Enter and confirm your password. The project/DFB is now protected. The list box symbol (c) appears next to the project name to show that the application/project is protected.
8	Save the list in the Program/DFB list box using the Save List button.

2.6.1.3. To remove protection for projects/DFBs

Step	Action
1	Repeat steps 1-5 of the protect projects/DFbs process.
2	Highlight the project/DFB and click Unprotect.
3	Enter and confirm your password. The project/DFB is now protected. The list box symbol (c) disappears from the project name. The application/project is NOT protected.

2.6.2. Protecting the Quantum PLC Memory

2.6.2.1. To protect information, set the switch to either Memory Protect (mem prt) or Stop and remove the key.

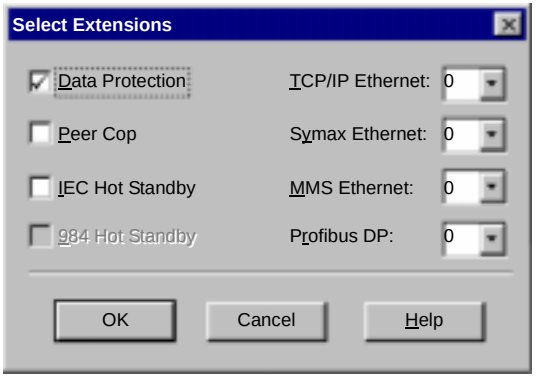


2.6.2.2. To protect the memory, set the key switch to mem prt or Stop and remove the key.

2.6.2.3. Note: In these positions, no program changes are possible. The Quantum PLC also ignores start and stop commands from an external programming panel.

2.6.3. Protecting Data in the Quantum PLC

2.6.3.1. Follow steps.

Step	Action
1	In the Concept menu, select Config | Config Extensions. The Select Extension dialog appears. Ensure the Data Protection check box is checked. 
2	Click OK.
3	Return to the Concept menu, select Config | Data access protection... . The following dialog appears: 
4	Select the Start address and Length (range) of accessible data. **1.** By selecting, you write protects coils (0x) and registers (4x). **2.** All addresses preceding and following the designated range (Length) are write protected.

2.6.3.2. Note: Selecting Data Protection protects data from external changes except when changes come from programming panels.

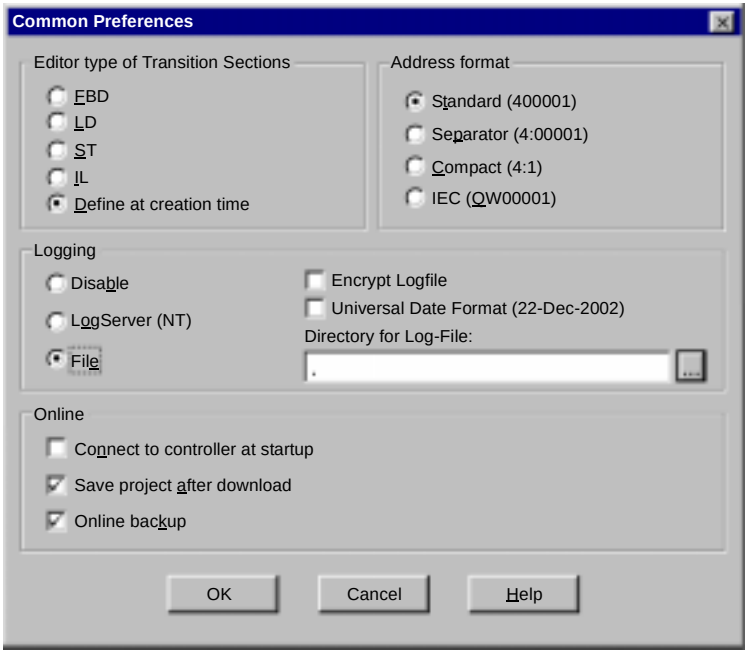
2.6.4. Saving Changes Automatically

2.6.4.1. You can set Concept to save automatically:

1. Every time you make a change to an application/project.

2. After the application/project is downloaded to the Quantum PLC.

2.6.4.2. To save changes automatically

Step	Action
1	Select Options | Preferences | Common Preferences. The following dialog appears 
2	Select Save project after download in the Online area to save the project after every download and every literal change in the animation mode.

Step	Action
3	(Optional) To save a backup of the last successful download of an application/ project, select Online backup. **1.** Online backup is available only if you select Save project after download. **2.** Concept creates a file called "Projectname.BAK" in the project directory. **3.** The project directory contains the subdirectories "DFB" and "DFB.GLB" which contain the backup files for the local and global DFBs and derived data types. **4.** Concept creates a backup every time you perform the commands Online | Download and Online | Download changes. **5.** Online backup overwrites the backup files each time the program downloads. **6.** In case of a program or programming fault, you can reconnect to a running Quantum PLC with the backup project.
4	Click OK.

This page is intentionally blank.

3. Integration Issues

3

At a Glance

Purpose

As you integrate a Part 11 compliance solution into your system, you must account for

- exemptions to write restrictions
- potential error messages using communication services
- preventing inadvertent writes using a Modbus Plus network
- connecting a Concept personal computer to a write-restricted Quantum PLC through a bridge

Note: Using some features may result in exemptions to write restrictions or noncompliance management of event-log files.

What's in this Chapter?

This chapter contains the following topics:

Topic	Page
Exemptions to Write Restrictions	44
Potential Error Messages Using Communication Services	45
Preventing Inadvertent Writes Using a Modbus Plus Network	46
Connecting a Concept Personal Computer to a Write-restricted Quantum PLC through a Bridge	51

3.1. Exemptions to Write Restrictions

3.1.1. Communication Function Codes

3.1.1.1. Write restrictions block certain communication function codes (but not read function codes). To block all the following communication function codes from writing to memory, select the Enable Write Restriction, Disable all Writes from CPU Modbus Ports, and Disable or Writes from NOE/NOMs check boxes.

3.1.1.2. The following function codes are blocked

Function Code	Description
5	Write single coil
6	Write single register
13	Program by host
15	Force multiple coils
16	Force multiple registers
21	Write general reference
22	Mask write register
23	Write/read 4x register
40	IEC communication
42	IEC native services
125	Load executive request
126	Program panel commands

3.2. Potential Error Messages Using Communication Services

3.2.1. Peer Cop/ DIO

3.2.1.1. If a Global or Specific input (PEER COP) or other input (DIO) is configured using an address from a Quantum PLC not in the write restriction list box, or through a NOM and the Disable All Writes from NOE/NOM check box is selected, then

1. the configuration is invalid, and
2. you cannot start the Quantum PLC, and
3. you will get a Traffic Cop error with Stop Code 4000.

3.2.2. NOG

3.2.2.1. If a NOG runs A-Line I/O and the Disable All Writes from NOE/NOM check box is selected,

1. the configuration is invalid, and
2. you cannot start the Quantum PLC, and
3. you will get a Traffic Cop error with Stop Code 4000.

3.2.3. NOE I/O Scanning

3.2.3.1. You cannot use NOE I/O scanning if you select the Disable All Writes from NOE/NOM check box. You will receive an error message during program analysis.

3.2.4. MSTR Block

3.2.4.1. Either (A) reads by MSTR blocks in the restricted Quantum PLC or (B) writes by MSTR blocks to a restricted Quantum PLC, will report an error code (6m14) since both behaviors (A and B) are trying to write data to a restricted Quantum PLC.
3.2.4.2. "m" indicates routing information:

1. 0 = restricted CPU on segment
2. 1 = next network segment
3. 2 = second network segment
4. 3 = third network segment
5. 4 = fourth network segment

3.2.4.3. Writes by MSTR blocks in the restricted Quantum PLC to other Quantum PLCs, and reads by MSTR blocks to a write-restricted Quantum PLC are unaffected and should function normally.

3.3. Preventing Inadvertent Writes Using a Modbus Plus Network

3.3.1. Modbus Plus Network Issues

3.3.1.1. Modbus Plus is an industry-standard network, which supports up to 64 nodes on a segment. For a network larger than 64 nodes, Modbus Plus supports network extension via bridges, bridge/multiplexers, and gateways.

1. A bridge connects 2 Modbus Plus network segments.
2. A bridge/multiplexer allows connecting together 2 or more Modbus serial devices and bridging them into the Modbus Plus network.
3. A gateway connects one Modbus Plus network to an Ethernet network.

3.3.1.2. Due to Modbus Plus network routing rules and the design of the write restriction feature, the Quantum PLC's native Modbus Plus port can only see the address of the last node that handled a particular message.

3.3.1.3. A Modbus Plus routing path may contain up to 4 intermediate addresses of either gateways or bridge/multiplexers. Gateways or bridge/multiplexers have one Modbus Plus address. Bridges have 2 Modbus Plus addresses. If the gateway or bridge/multiplexer address is a valid writing address, a message from the other side of the bridge (from a unit without write permissions) could change data in the Quantum PLC.

WARNING

UNINTENDED SYSTEM OPERATION

For a bridge/gateway with write access, all nodes on all non-local network segments will have the ability to write to the write-restricted Quantum PLC.

To prevent this condition, do one of the following:

- Do not use bridges/gateways, or
- Do not allow write-access to bridges/gateways, or
- If you must give write-access to a bridge/gateway, place only those devices that you want to have write-access privileges to the Quantum PLC on bridged network-segments.

Failure to follow this precaution can result in death, serious injury, or equipment damage.

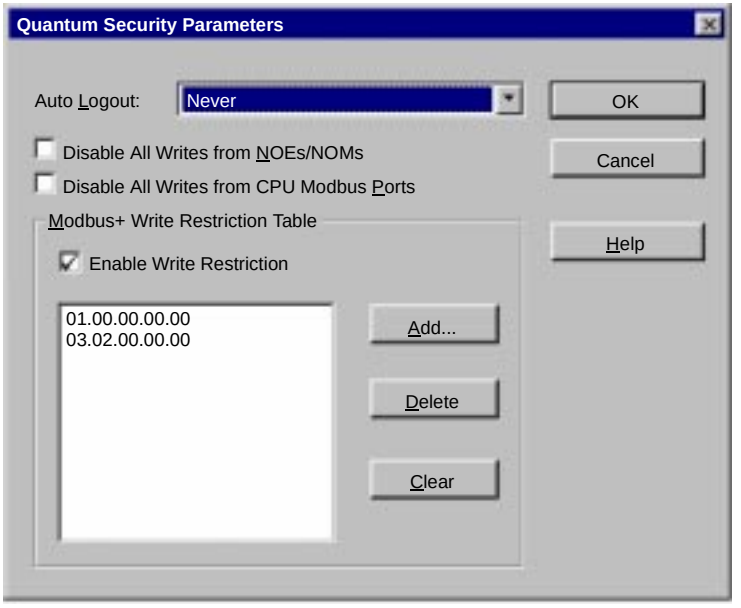
3.3.2. Configuration Examples

3.3.2.1. The following content describes the integration issues involved when bridges are used.

3.3.2.2. A Quantum PLC at address: 6 is a write-restricted Quantum PLC, It will be programmed by a Concept personal computer at address: 1 (01.00.00.00.00) located on the same Modbus Plus network segment, and a

3.3.2.3. Quantum PLC address: 2 (03.02.00.00.00.) located on a bridged Modbus Plus segment will have write access to the write-restricted Quantum PLC at address: 6.

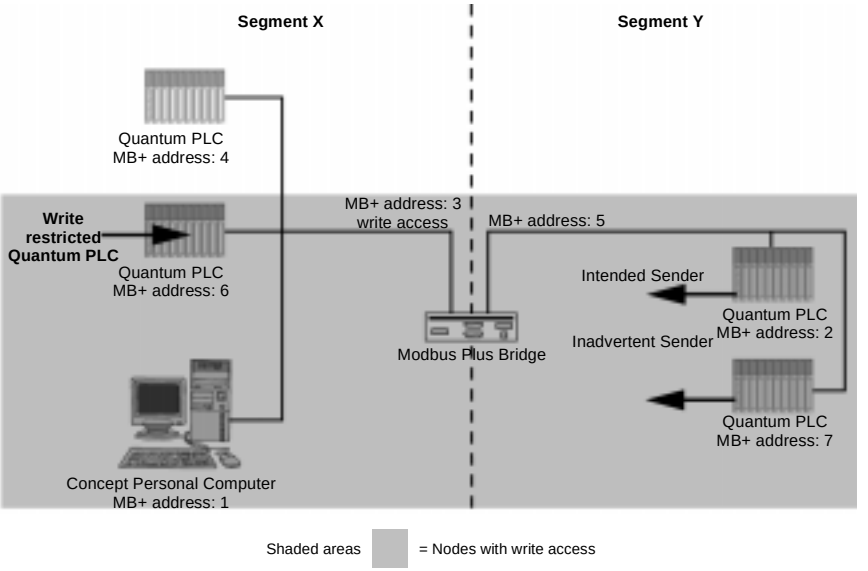
3.3.2.4. The settings in the Quantum Security Parameters dialog



3.3.3. Incorrect Configuration

3.3.3.1. The Quantum PLC at address: 6 is the receiving Quantum PLC and is write-restricted. We want ONLY the Concept personal computer at address: 1 (01.00.00.00.00) and the Quantum PLC at address: 2 (03.02.00.00.00) to have write access to the write-restricted Quantum PLC at address: 6.

3.3.3.2. Incorrect configuration



3.3.3.3. This network configuration is incorrect because it gives write access to

- All Modbus Plus addresses on the bridged segment Y
  (entry 03.02.00.00.00 in the Modbus+ Write Restriction Table).

3.3.3.4. Therefore, both Quantum PLCs (address: 2 and address: 7) in Segment Y, have write access to the write-restricted PLC at address: 6.

3.3.3.5. Note that any additional Modbus Plus nodes added on the Segment Y-side of the bridge will also have write access.

3.3.3.6. The preceding configuration could cause inadvertent writes.

3.3.4. Why Inadvertent Writes

3.3.4.1. Inadvertent writes occur because the write-restricted Quantum PLC at address: 6 knows only that

1. a message was received from address: 3 (Modbus Plus bridge), and

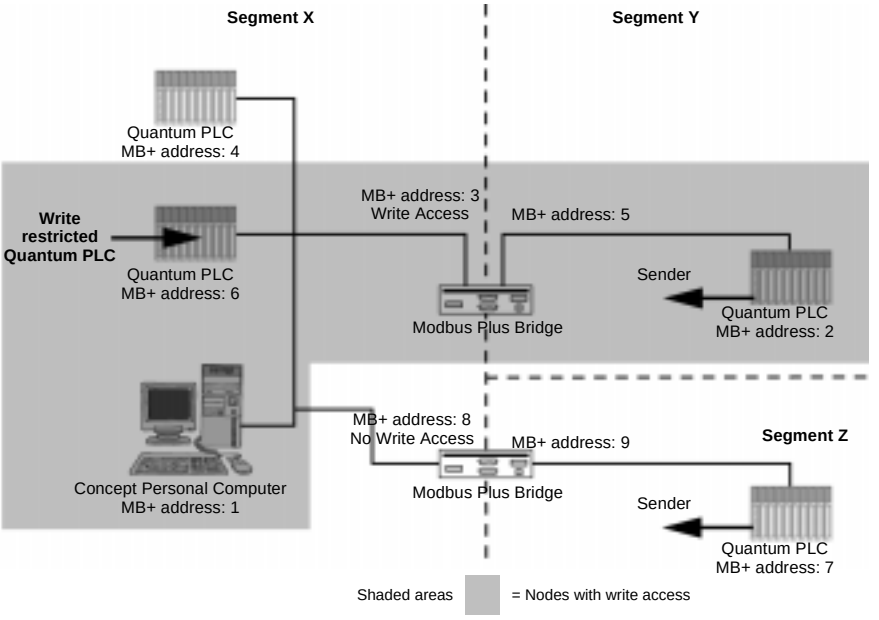
2. address: 3 has write access

3.3.4.2. The Quantum PLC at address: 6 accepts the message causing an inadvertent write in the above incorrect configuration.

3.3.5. Correct Configuration

3.3.5.1. The Quantum PLC at address: 6 is the receiving Quantum PLC and is write-restricted. We want ONLY the Concept personal computer at address: 1 (01.00.00.00.00) and the Quantum PLC at address: 2 (03.02.00.00.00) to have write access to the write-restricted Quantum PLC at address: 6.

3.3.5.2. Correct configuration



3.3.5.3. The correct configuration gives write access to

- Concept personal computer at address: 1
  (entry 01.00.00.00.00 in the Modbus+ Write Restriction Table)

3.3.5.4. and only to

- Quantum PLC at address: 2
  (entry 03.02.00.00.00 is in the Modbus+ Write Restriction Table)

3.3.5.5. Note that any additional Modbus Plus nodes added on the Segment Y-side of the bridge will also have write access.

3.3.5.6. Since the second bridge at address: 8 (08.00.00.00.00) is not in the Write Restriction Table, writes from the PLC at address: 7 (on Segment Z) will be blocked.

3.4. Connecting a Concept Personal Computer to a Write-restricted Quantum PLC through a Bridge

3.4.1. Overview

3.4.1.1. To give the Concept Personal Computer access to the restricted Quantum PLC, please ensure that

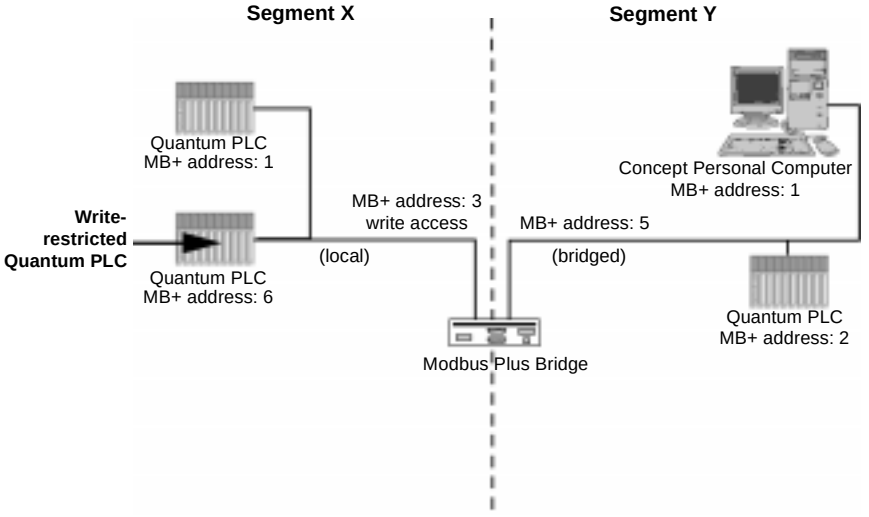
1. bridge's (Segment X in the example) Modbus Plus address is included in Write Restriction Table
2. bridge's (Segment X in the example) Modbus Plus address is the same as Concept personal computer

3.4.1.2. Or, ensure that no Modbus Plus address on the same network segment as the write-restricted Quantum PLC has the same Modbus Plus address number as the Concept personal computer.

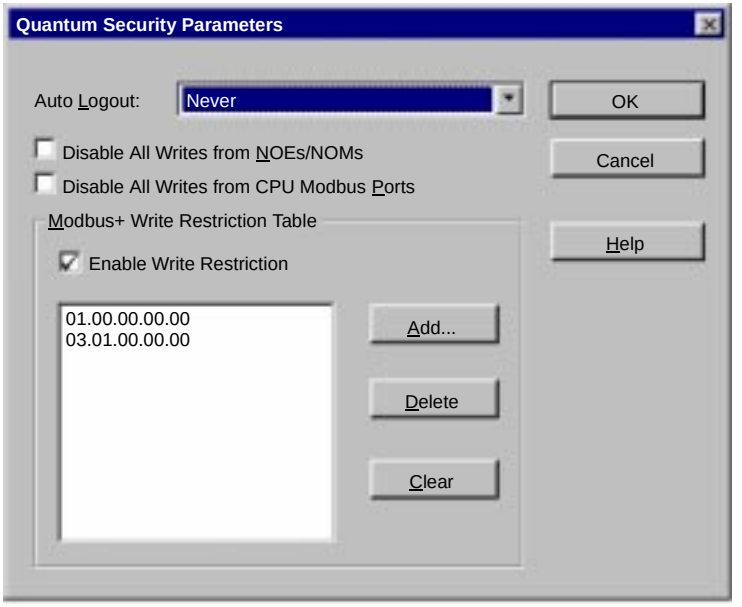
3.4.1.3. Note: The statement above also applies to bridge/muxes with a Concept personal computer connected on the Modbus side and to Modbus Plus/Ethernet gateways with a Concept personal computer connected on the Ethernet side.

3.4.2. Incorrect Configuration

3.4.2.1. Incorrect Configuration



3.4.2.2. The settings in the Quantum Security Parameters dialog



3.4.2.3. In the example above, the Quantum PLC at address: 1 would have write access to the write-restricted Quantum PLC (address: 6) because Concept forces its address (address: 1 (01.00.00.00.00)) into the Modbus Plus Write Restriction Table.

3.4.3. Correct Configuration

3.4.3.1. You should

1. ensure that no addresses on the same network as the write-restricted Quantum PLC have the same address as the Concept personal computer

   In the example below, we change the Modbus Plus address of the Quantum PLC (same side, but nonwrite-restricted) from 1 to 4. The address of the write-restricted Quantum PLC remains as "6".

2. ensure that the address of the Modbus Plus bridge on Segment X is included in the Modbus Plus Write Restriction Table

3.4.3.2. Schneider Electric recommends that you change the Modbus Plus address of the bridge on the side of the write-restricted Quantum PLC (Segment X) to match the address of the Concept personal computer. In our example, both addresses are (01.00.00.00.00).

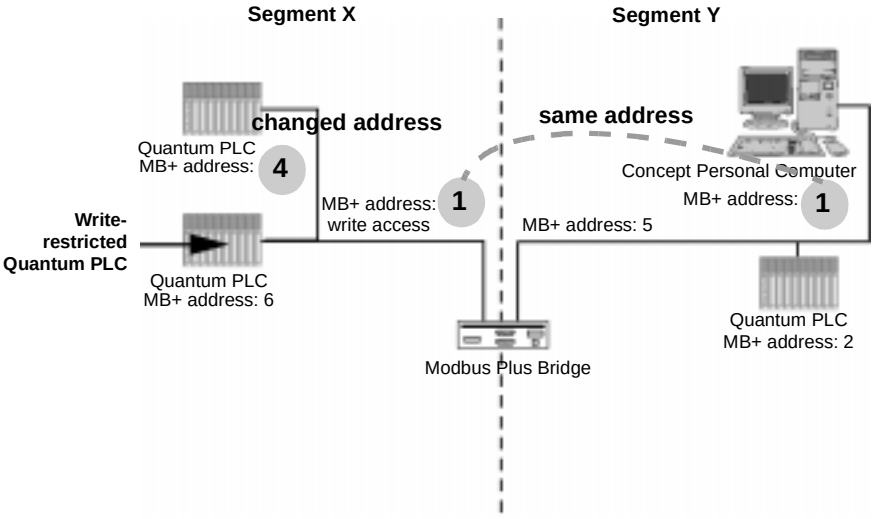
3.4.3.3. Because the bridge's new address is "1" and matches the address of the Concept personal computer, this change

1. requires no specific additions to the Write Restriction Table list, because Concept forces the address (1 (01.00.00.00.00)) to be the first address in the list of the Modbus+ Write Restriction Table

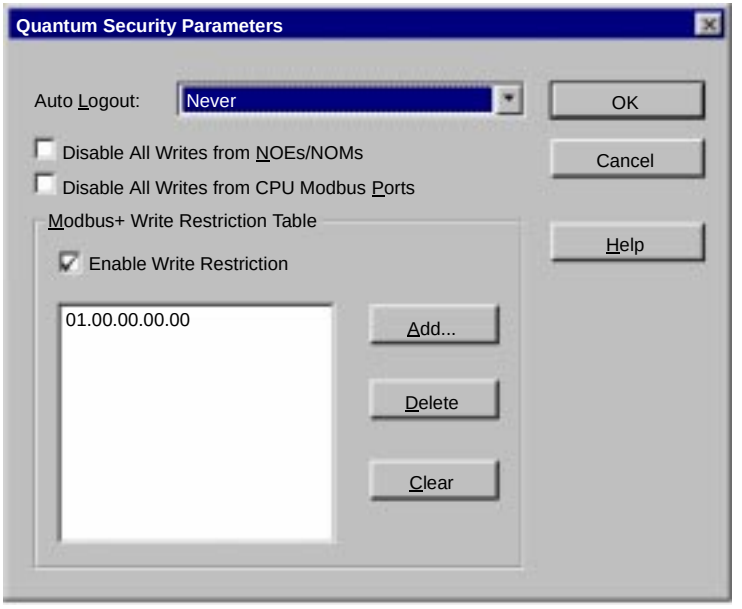
2. allows the Concept personal computer access to the Quantum PLC

3. prevents giving unintended write access to any nodes on the side of the write-restricted Quantum PLC (Segment X)

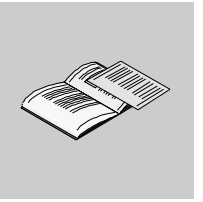
3.4.3.4. Correct Configuration



3.4.3.5. The settings in the Quantum Security Parameters dialog



Appendices



At a Glance

Purpose

Material in the following sections enhance information presented earlier.

What's in this Appendix?

The appendix contains the following chapters:

Chapter	Chapter Name	Page
A	NOEs/NOMs Supporting Write Blocking	57
B	Schneider Electric 21 CFR Part 11 Product Compatibility	59

This page is intentionally blank.

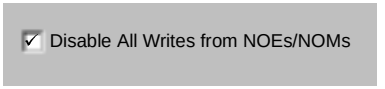
A. NOEs/NOMs Supporting Write Blocking

A

A.1. NOEs/NOMs Supporting Write Blocking

A.1.1. Modules Supporting Write Access

A.1.1.1. Selecting the Disable All Writes from NOES/NOMs check box



A.1.1.2. When the Disable All Writes from NOEs/NOMs check box is selected, only the following model numbers are affected.

- 140 NOM 211 00
- 140 NOM 212 00
- 140 NOM 252 00

- 140 NOE 211 00
- 140 NOE 251 00
- 140 NOE 311 00
- 140 NOE 351 00
- 140 NOE 511 00
- 140 NOE 551 00

- 140 NOE 771 00
- 140 NOE 771 10
- 140 NOE 771 01
- 140 NOE 771 11

A.1.2. Modules Not Supporting Write Access

A.1.2.1. Note: Other Modules

- All other Schneider Electric and 3rd party modules will always have write access to the Quantum PLC.

B. Schneider Electric 21 CFR Part 11 Product Compatibility

B

B.1. Schneider Electric Product Compatibility Chart

B.1.1. Products Enabling 21 CFR Part 11 Compliance

B.1.1.1. Assume 21 CFR Part 11 features are selected

Product/ Feature		Restrictions
NOE	I/O Scanning	If Disable All Writes from NOEs/NOMs is selected, the I/O Scanning will not work for input scanning (writes DATA to the PLC). Output scanning will work.
	Global Data	If Disable All Writes from NOEs/NOMs is selected, Global Data does not work.
	FDR	NO Restrictions
	MSTR messages	If Disable All Writes from NOEs/NOMs is selected, only write message from the PLC will be allowed. All MSTR read messages will not work since they write DATA into the PLC.
	WEB server	If Disable All Writes from NOEs/NOMs is selected, the WEB server will not be able to write DATA to the PLC but will not have any problem with reading DATA and displaying it on a WEB page.
	Communication Responses	If Disable All Writes from NOEs/NOMs is selected, the Quantum PLC will not execute any write requests that gets to it through the NOE. On the other hand, the Quantum PLC will respond to all read requests.

Product/ Feature		Restrictions
NOM	DIO	If Disable All Writes from NOEs/NOMs is selected, the I/O Scanning will not work. Part of this feature could actually try to write DATA to the PLC.
	Peer Cop	If Disable All Writes from NOEs/NOMs is selected, the Peer Cop will not work. Part of this feature could actually try to write DATA to the PLC.
	Global Data	If Disable All Writes from NOEs/NOMs is selected, Global Data will not work.
	MSTR messages	If Disable All Writes from NOEs/NOMs is selected, only write message from the PLC will be allowed, all MSTR read messages will not work since they write DATA into the PLC.
	Communication Responses	If Disable All Writes from NOEs/NOMs is selected, the Quantum PLC will not execute any write requests that get to it through the NOM. On the other hand, the Quantum PLC will respond to all read requests.
Quantum PLC Modbus Plus (MB+) Port	DIO	If Enable Write Restriction is selected and a DIO Modbus Plus node is not listed in the Modbus+ Write Restriction Table, the Quantum PLC will not start, and an error message displays.
	Peer Cop	If Enable Write Restriction is selected and a "Peer Copped" Modbus Plus node is not listed in the Modbus+ Write Restriction Table, the Quantum PLC will not start, and an error message displays.
	Global Data	If Enable Write Restriction is selected, Global Data will not work.
	MSTR messages	If Enable Write Restriction is selected, read messages will only be allowed from Modbus Plus nodes listed in the Modbus+ Write Restriction Table. Write messages are allowed.
	Communication Responses	If Enable Write Restriction is selected, the Quantum PLC will not execute any write requests that gets to it through the Quantum PLC Modbus Plus port if the sender Modbus Plus node is not in the Modbus+ Write Restriction Table. On the other hand, the Quantum PLC will respond to all read requests.
Quantum PLC Modbus port	XMIT block	If Disable All Writes from CPU Modbus Ports is selected, the XMIT block will not be allowed to execute Read instruction, because this instruction writes DATA into the PLC's memory.
	Modbus responses	If Disable All Writes from CPU Modbus Ports is selected, the CPU port will not execute write orders coming through the CPU port. The CPU will respond to all read requests.

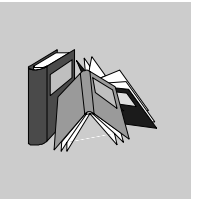
Product/ Feature		Restrictions
Hot Standby		If Disable All Writes from NOEs/NOMs is NOT selected, then no restrictions apply.
		If Disable All Writes from NOEs/NOMs is selected, then all NOE/NOM restrictions apply.
CRP (Profibus DP)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the Profibus scanner does not create unexpected results.
NOG (A-line I/O manager)		If Disable All Writes from NOEs/NOMs is selected, the NOG will not work.
NOA 61110 (Interbus G3)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the Interbus scanner does not create unexpected results.
NOA 62200 (Interbus G4)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the Interbus scanner does not create unexpected results.
EIA (AS-I bus)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the AS-I scanner does not create unexpected results.
NOE (Symax)	MSTR messages	If Disable All Writes from NOE/NOMs is selected, only write message from the PLC will be allow, all MSTR read messages won't work since they write DATA into the PLC.
ESI (ASCII)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the ESI module does not create unexpected results restrictions.
NOL (Lonworks)		**NO restrictions** It is your responsibility to ensure that the DATA coming from the Lonworks scanner does not create unexpected results.
Third party	Comm. Modules	Consult Tech Support at customer.services@modicon.com
	I/O modules	Consult Tech Support at customer.services@modicon.com
	Loadables	Consult Tech Support at customer.services@modicon.com
NW-BP85. MB+ Bridge		You should either: ● Not use bridges, or ● Not allow write access to bridges, or ● If you need to give write access to a bridge, you should place only devices that have write access privileges to the Quantum PLC on the bridges network segments, or ● Install the bridge in a network segment that is attached to a protected NOM.

Product/ Feature	Restrictions
NW-BM85. MB+ to Modbus BMUX	You should either: ● Not use BMUXes, or ● Not allow write access to BMUXes, or ● If need to give write access to a BMUX, you should place only devices that have write access privileges to the Quantum PLC on the Modbus side of the BMUX, or ● Install the bridge in a network segment that is attached to a protected NOM.
174CEV20030 MB+ to Ethernet gateway	You should either: ● Not use the CEV Gateway ● Not allow write access to CEV gateways ● If need to give write access to a CEV Gateway, you should place only devices that have write access privileges to the Quantum PLC on the Ethernet side of the Gateway, or ● Install the Gateway (Ethernet or Modbus Plus) in a network segment that is attached to either a protected NOM or a protected NOE.
174CEV30010 MB to Ethernet bridge	You should either: ● Not use the CEV bridge ● If need to use a CEV bridge, you should install the bridge (Ethernet or Modbus) in a network segment that is attached to either a protected NOE or a protected CPU port.
Connexium offer	NO Restrictions
Sercos	**NO restrictions** It is your responsibility to ensure that the DATA coming from the Sercos scanner does not create unexpected results.
ERT (Sequential event recorder)	**NO restrictions** It is your responsibility to ensure that the Mapping of DATA coming from the ERT module does not create unexpected results.

Product/ Feature		Restrictions
I/O	Quantum Analog I/O	**NO restrictions**
	Quantum Intrinsic Safety I/O	**NO restrictions**
	HLI (High Speed module)	**NO restrictions**
	EHC (High speed counters)	**NO restrictions**
	Motion Modules	**NO restrictions**
	Momentum I/O	Depending on the bus you select to control the Momentum I/O, see below. ● Ethernet: See NOE in this table. ● Modbus Plus: See NOM or Quantum PLC Modbus Plus (MB+) port in this table. ● Profibus: See CRP in this table. ● Interbus: See NOA in this table.
	800 Series	**NO restrictions**
	200 Series	**NO restrictions**
	Symax	**NO restrictions**
Software	ProWORX NxT	Does not support the following 21 CFR Part 11 features: ● Quantum PLC password ● NOE/NOM disable writes ● Modbus CPU port disable writes ● Modbus Plus write restrictions ● Auto Logout ● Log file encryption
	ProWORX 32	Does not support the following 21 CFR Part 11 features: ● Quantum PLC password ● NOE/NOM disable writes ● Modbus CPU port disable writes ● Modbus Plus write restrictions ● Auto Logout ● Log file encryption
	Concept	Version 2.6 or later supports CFR 11 features. Previous versions of Concept do not support CFR11 features.
	OFS	See NOE, NOM, and Quantum PLC Modbus and Modbus Plus ports in this table.
	Factory Cast	See NOE/Web Server in this table.
	OSG	Not covered in this document.

Product/ Feature		Restrictions
Quantum Execs.	Version <1.2	Does not support CFR 11 features
	Version >= 1.2	Supports 21 CFR Part 11 features **Note:** If the features are not selected, the Execs. are fully backward compatible with Concept 2.5 Execs.
Momentum PLCs		Do not support the following 21 CFR Part 11 features: ● Modbus CPU port disable writes ● Modbus Plus write restrictions ● Auto Logout ● Secure Application check box
Compact PLCs		Do not support the following 21 CFR Part 11 features: ● Modbus CPU port disable writes ● Modbus Plus write restrictions ● Auto Logout ● Secure Application check box

Glossary



!

21 CFR Part 11 The phrase used to describe a Final Rule published in the United States' Federal Register by the U.S. Food and Drug Administration (FDA). The phrase also appears as "Part 11" or "the rule". This final rule applies to the authenticity of electronic records and electronic signatures.

C

CFR Code of Federal Regulations

Closed System An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

D

Digital Signature An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

E

Electronic Record — Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature — A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

F

FDA — United States Food and Drug Administration, a regulatory (legal enforcement) agency of the U.S. Department of Health and Human Services.

H

Handwritten Signature — The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form.

V

Validation — As defined by the U.S. Food and Drug Administration (FDA)
"The process of establishing documented evidence which provides a high degree of assurance that a system will consistently perform in accordance with its predefined specifications and quality attributes" (Ref: FDA, Glossary of Computerized System and Software Development Terminology).

Index

Numerics

4x registers, 39
984 projects, 34

A

access
  protecting, 19
  write access, 21, 22, 23
access levels
  setting up, 19
Add Modbus Plus Address dialog, 23
audit trail, 13, 29
Auto Logout, 27
Auto Save, 40

B

bridge/multiplexers, 46
bridges, 46, 48

C

Change PLC Password dialog, 25
characters
  valid (Concept), 20
  valid (Quantum), 25
check boxes
  Enable Write Restriction, 23
  Universal Date Format, 32
coils (0x), 39
Common Preferences dialog (Concept), 31, 35, 40
communication function codes, 44
  blocked, 44
  not blocked, 44
  overriding, 44
Compacts, 16
Concept 2.6 SR1, 16
Concept Security Logon dialog, 19

D

Data Access Protection config extension, 39
Data Protection dialog, 39
Derived Function Blocks (DFBs), 37
dialogs
  Add Modbus Plus Address, 23
  Change PLC Password, 25
  Common Preferences (Concept), 31, 35, 40
  Concept Security Logon, 19
  Data Protection, 39
  Enter PLC Password, 25
  Project Properties (Concept), 35
  Quantum Security Parameters, 21, 22, 23, 27
  Select Extensions, 39
DIO, 45

E

electronic
- forms, 12
- records, 13
- signatures, 13

Enable Write Restriction check box, 23
Enter PLC Password dialog, 25
event-log files
- editing, 32
- entries, 29
- external access, 30
- viewing encrypted, 32

events
- logging, 29
- recording, 29

extensions
- encrypted event-log files, 29
- unencrypted event-log files, 29

F

Federal Register, 11
file extensions, 29
Final Rule, 11

G

gateways, 46

I

IEC sections, 34

K

key switches, 38

L

logging events, 29
lost-password procedure, 26

M

mapping requirements to features, 18
memory protection, 38
Momentums, 16

N

not connected
- see offline, 34

O

offline, 34
offline state
- see offline, 34

output-addresses, 39

P

paper records, 12
parameters
- changing (Concept), 31
- entering, 22, 23
- entering (Quantum), 21
- selecting, 22, 23
- selecting (Quantum), 21

Part 11
- definition, 12
- requirements, 13
- resources, 14

passwords
- case sensitive (Quantum), 25
- changing (Quantum), 25
- default (Quantum), 25
- disabled (Quantum), 26
- entering (Concept), 19
- entering (Quantum), 25
- lost, 26
- not case sensitive (Concept), 19
- rules (Concept), 19
- rules (Quantum), 25
- setting up (Concept), 19
- setting up (Quantum), 25
- spaces (Quantum), 25

paths
- visible, 31

Peer Cop, 45

permissions
Quantum passwords, 25
personnel training, 13
Project Properties dialog (Concept), 35

Q

Quantum 140CPU43412A, 16
Quantum 140CPU53414A, 16
Quantum Security Parameters dialog, 27

R

reads
accessing, 24
allowing, 22
registers (4x), 39
restricted writes, 21, 22, 23

S

secure application
requirements, 34
states, 35
security
operating systems, 17
Select Extensions dialog, 39
software protection, 19
states
secure application, 35
Supervisors
changing parameters (Concept), 31
changing projects, 29
encrypted event-log files, 32
establishing access levels (Concept), 19
log-file paths, 31
setting up (Quantum) passwords, 25
systems
built-in checks, 13
closed, 13
limiting access, 13
validating, 13

T

time intervals, 27

U

Universal Date Format check box, 32
, 19
users
DIO, 45
Peer Cop, 45
registered, 20
setting up, 19

V

validation
definition, 13

W

Windows NT, 17
write access, 21, 22, 23
write restriction list box, 45
writes
enabling, 23
inadvertent, 46
restricted Quantum Security Parameters dialog, 21, 22, 23

This page is intentionally blank.