I'm not robot

Abb 800xa training manuals pdf

Abb 800xa training manual pdf.

Introduction ---------- The System 800xA Multisystem Integration System Version 5.1 is designed for enhanced productivity and power in various industrial settings. Despite ABB's efforts to ensure the accuracy of this document, they disclaim liability for any damages resulting from its use or from using software and hardware described within. Installation and Configuration ---------- The system installation process involves several steps: * Recommended Hardware Configurations * Small, Medium/Large Configuration Options * Remote Access Server Setup Configuration Options ---------- Configuration options include: * Read-only System setup * User Mapping and Password Configuration * Remote Access Server Advanced Configuration Upgrade Procedure ---------- The upgrade procedure for the system involves several steps to ensure a seamless transition from an older version. Appendix A: Error Messages ---------- Error messages related to the 800xA Multisystem Integration System are listed in Appendix A. Appendix B: Fault Tracing ---------- Physical Connection and Network Configuration are crucial aspects of the system's setup, including protocols and versions used. Revision History ---------- The revision history for the System 800xA Multisystem Integration System Version 5.1 includes updates to various indices and a warning about security measures that users may want to consider based on their specific application and installation. This User Manual includes cautionary notes to highlight important safety information and other key details. You can find a comprehensive list of terms in the System 800xA System Guide Functional Description (3BSE03*). If you need further clarification on specific terminology, refer to Webster’s Dictionary of Computer Terms or standard industry dictionaries. Released User Manuals and Release Notes You can access all applicable User Manuals and Release Notes for System 800xA through the System 800xA Released User Manuals and Release Notes (3BUA000263*). Introduction and Product Overview System 800xA Multisystem Integration allows you to control and monitor multiple systems from a central operating room. This feature enables subscriber and provider systems to communicate with each other, regardless of whether they're in the same or different Windows domains, workgroups, or networks. The connection between these systems can be secured using passwords and encryption. Network Configuration The network configuration options for 800xA Multisystem Integration include high-speed LAN connections (100 MBit/s) and slower modem connections (128 kBit/s). For more information on network configurations, refer to System 800xA, Network, Configuration (3BSE034463*). Control and Point of Control With Multisystem Integration, you can take control locally on the provider system or remotely on the subscriber system. To learn more about the Point of Control function, refer to the Point of Control section in System 800xA Administration and Security (3BSE037410*). Prerequisites and Requirements To use 800xA Multisystem Integration, you'll need a separate license. The version of this integration must match the system version of Process Portal A and other used system extensions. Installation To install 800xA Multisystem Integration, follow these steps: 1. Select Installation media. 2. Double-click on the Setup.exe program. 3. Select 800xA Multisystem Integration product, then click Install. Note: This is a paraphrased version of the original text, condensed and reorganized for easier reading. Page 20: After displaying the dialog, continue with the installation and provide requested information. You can change the installation directory path by clicking Browse (see Fig. 3). Page 21: Following the installation of 800xA Multisystem Integration, load the system extension using the Configuration Wizard. Select System Administration > System Extensions (see Fig. 4). Page 22: After loading the system extension, reboot the machine to ensure Remote Access Server and Client functionality. This chapter covers various configurations for small and medium/large systems. There are no specific hardware requirements for 800xA Multisystem Integration, except those for the 800xA Core system software. The time difference between the Remote Access Client and Server should be reasonable, typically under a minute. For small configurations with few hundred I/O signals, the Remote Access Server can run on the same node as Connectivity and Aspect Directory servers. However, it's not recommended to run this on an operational workplace. For larger systems, consider using a separate node for the Remote Access Server and Client to minimize impact (see Fig. 5). For medium/large configurations, mandatory Windows domain users or user mapping are required. The Remote Access Server provides data to the supervisor system (the Provider), while the subscriber system subscribes to values from the Provider (see Fig. 6). Page 29: To create a Remote Access Server, follow these steps: 1. Select System Administration > Next (see Fig. 9). 2. Select Remote Access Server > Next (see Fig. 10). 3. Create the Remote Access Server. Section 3: Configuring Remote Access Server and Client ---------- Configuring a Remote Access Server (RAS) requires selecting the node to run the service provider, as shown in Figure 11. This choice depends on system size, with recommendations found on page 23. Password Configuration ---------- When mapping subscribers to providers, using the wildcard character '*' can simplify authentication. However, this method should only be used for read-only or Guest users, as it allows write access from all subscriber accounts. Encrypting traffic between RAS and Remote Access Client is recommended but doesn't significantly impact performance. Remote Access Server Advanced Configuration ---------- Configuring advanced settings includes specifying a port number and encryption usage. This is done by selecting Service Structure and Services/Remote Access Server/Basic, Service Group. Using encryption ensures secure communication, even if unauthorized users gain physical network access. Remote Access Client Overview ---------- The Remote Access Client service communicates with the RAS but resides on the subscriber system. There's always a one-to-one relationship between clients and servers. Creating a Remote Access Client ---------- To create a client, enter its name in the New Object Dialog Box (Figure 15) and click Next. The Additional Arguments dialog (Figure 16) will then be displayed. It's essential to set the Connect Account with a valid local or domain user. For encryption, a password must be set using Figure 18, ensuring secure communication between the client and server. To configure the Remote Access Client, follow these steps: 1. Configure the Connect account on the node that executes the Remote Access Client (AfwRAC.exe). 2. Specify the Account used to connect to the Remote Access Server (Provider) and click OK. 3. Before any objects in the provider system can be used in the subscriber system, proxy objects for the remote objects must be created in the subscriber system through an upload operation. Refer to the System 800xA, Tools (2PAA101888*) instruction for details on this process. 4. Select the desired structure/object from the provider system in the left structure selector (Remote object path). 5. To include or remove child objects of a selected object, select or deselect the Include children check box appropriately. The Follow references check box controls if objects needed by an uploaded aspect should be included in the upload as well. 6. The remote system will be uploaded below the Remote System/Inventory object in the Control Structure, in addition to the selected structure. 7. There are three ways to treat an aspect category when it is uploaded by 800xA Multisystem Integration. Refer to Figure 24 for the Inventory Object configuration. 8. The aspect system for the copied aspect must be installed on both the provider and subscriber systems and support the 800xA Multisystem Integration System Extension. If structures are added and uploaded but later removed from the upload configuration, in some cases, objects will be left in the subscriber system. 9. Running Upload Section 3 Configuration Navigate to the Node Administration structure in the upload browser and select the node group “All” Running Upload Configuration: Understanding the Process Configuring an upload from the Upload Execution tab on the System Connection aspect of the Remote System object is a crucial step. Once started, it cannot be aborted. To configure an upload, follow these steps: - Uncheck the aspect category to exclude specific aspects from being uploaded. - All OPC properties, log configurations, and templates will be uploaded unless "Ignore at upload" is checked on the aspect category. The Remote Access Client will continue running even if the Plant Explorer is closed. Rates (1s, 3s, or 9s) should be freely selected as subscription values, but be cautious of a potential higher load on the controller. For more information on Advant Master configuration, refer to System 800xA, Configuration (3BSE030340*). In some applications, it's useful to display process values from multiple providers. With 800xA Multisystem Integration, this is easily achieved through the uploaded proxy aspect, which works identically with all other aspects and OPC data. Subscriber Requirements If users opt for custom groups instead of the default ones, these groups must be exported from the provider and then imported into the subscriber. Node Configuration All nodes in the subscriber system should be configured as nodes in the provider system to assume responsibility within the system. Asset Optimization This section applies only to the System 800xA 5.1 Feature Pack release. Asset Optimization enables a single window interface for all asset management operations, providing maintenance management to the operator environment. Configuration Table The Web View aspects communicate with the AOWebServerNode in the provider system using HTTPS or HTTP protocols. Configuration Figure Default communication protocol is HTTPS; however, it can also be set to HTTP, which does not encrypt data passed between the subscriber and provider. HTTPS Communication Protocol The default configuration uses the AOWebServerNode host name for communicating with the Provider Asset Optimization Server. Instead of a host name, an IP address of AOWebServerNode can be used for communication. HTTPS Communication Protocol A recommended RSA Key Size is 1024 bits. For certificate generation, installation, and renewal information, refer to Microsoft Internet Information Server documentation. IIS Site Bindings After installing the SSL certificate, HTTPS binding must be added to the Internet Information Server running on AOWebServerNode to allow HTTPS communication in the provider system. HTTPS Communication Protocol Certificate of issuing Certificate Authority should be added to Trusted Root Certification Authorities store on Asset Optimization Client and Server Nodes in the Subscriber system. Page 71: Configuration HTTPS Communication Protocol Select an account and click Finish to add or remove snap-ins. Right-click Trusted Root Certification Authorities and select All Tasks > Import from the context menu to import trusted root certification authorities. Confirmed write is used to write SIL-data to High Integrity (HI) controllers, and object lock policies are supported for systems with mixed AC800M controller and 800xA for Advant Master controllers. The only lock policy supported is Lock Optional for Operation. Page 73: Configuration Limitations Object lock policies must be the same for all providers and subscribers. It is not possible to have different lock policies on different systems. Power Plant libraries for PI and PT cannot be used together. Page 74: Limitations MBit/s or higher, and the delay will be hardly noticeable. This section shows additions and deviations in operation for Multisystem Integration compared to ordinary operation. See System 800xA, Operations (3BSE036904*). Process Displays Process displays with process provider system work the same way as local process displays, with the addition that the name and tool-tip for objects include the system name. Faceplates Faceplates for a remote provider system work in the same way as a faceplate for a local object. In order to show System Alarms from Advant Master Controllers, an additional upload of AC 400 System Event Names and descendant objects in the Control Structure needs to be performed. Feature Pack Functionality Operating the Point of Control This section applies to the System 800xA 5.1 Feature Pack release only. This section describes the procedure to use the Point of Control feature for Multisystem Integration, and points users to the Point of Control section in System 800xA, Operations (3BSE036904*) for more information. Point of Control Summary Aspect The Point of Control Summary aspect displays the responsibility status of all configured sections. It includes Grab Responsibility and Release Responsibility options. For more information, refer to Transfer of Responsibility section in System 800xA, Operations (3BSE036904*). Request Responsibility The responsibility of a section can be requested using the object context menu. When a user requests the responsibility of a section, a tree structure including the section with subsections is displayed. Page 80: Transfer of Responsibility Section 4 Operation Figure 51. Request Responsibility Dialog Type the message in the Message box and click OK to request responsibility. The responsibility request process involves several steps. Once sent, the message will be displayed to the responsible user and stored in the audit list. The current responsible user can accept or deny all sections, or select specific ones to transfer responsibility. If accepted, the responsibility is transferred immediately, and a confirmation is sent to the new responsible user. The Asset Optimization section applies only to the System 800xA 5.1 Feature Pack release. It describes the usage of Asset Optimization with Multisystem Integration for Condition Reporting and Monitoring, Work Order Management, and CMMS Views (Maximo, SAP/PM). In this section, users can configure Remote Access Server settings, including Read-only connection check boxes. These settings restrict access to certain Web View aspects, such as Dismissing fault reports or submitting work orders. The Authentication section discusses the use of Windows Integrated Authentication on the Provider system, which secures access to the Web View aspects. Additionally, backup and restore configuration data for proxy objects is crucial, and a recommendation is to include the remote system name and current date in its name. The provider system must be re-uploaded from the subscriber system without a valid backup of the Remote Access Client. System Alarms and Events 800xA generates alarms and events under specific conditions, as shown in Table 5. Audit Events occur both in the subscriber and provider systems, but for different activities. The system status function is extended to aid in fault tracing of remote system connections. The system status overview is similar to a regular 800xA system, with additional details provided about the connection between the Remote Access Server and Remote Access Client. The Remote Access Server and Remote Access Client appear as services in the system status viewer, using the same color scheme to indicate any issues. However, if one part of the service (the subscriber/provider) is not functioning correctly, the entire service can still fail to perform its duties. System status details for the Remote Access Server show incoming connections, OPC data access clients, alarm and event clients, and OPC history data access clients. Similar information can be viewed on the Remote Access Client. Table 7 describes each field in the Connection Tab of the Remote Access Client. The table includes fields such as IP-Address, System Name, Error code, Connect time, and Time difference. More information is available in the Protocol tab of the Remote Access Client, which provides details about the different protocols used between the client and server. When upgrading the Multisystem Integration, it's essential to ensure that Process Portal A and all used system extensions are upgraded to the same service pack or release. The 800xA Multisystem Integration enhances error messages received from the system, including those shown in upload logs or as message boxes. Error messages and their causes are listed below: - BAD_VERSION: The version of the Remote Access Server and Client is different, requiring the installation of the same version on both the provider and subscriber to resolve. - CONSYS_INVALIDACCOUNT: An incorrect account name or password for the connect account needs to be corrected. - FILE_FORMAT: A file format error in the Remote Access Client service data may occur if a newer version of the Multisystem Integration function is installed, requiring a full new upload to correct. Other error messages and their causes include: - NO_LICENSE: Insufficient licenses for Multisystem Integration - NO_LOCAL_INSERT_POSITION: The object configured as parent to uploaded objects does not exist - NOHOST: No valid host definition for the Remote Access Client - NOT_INITED: An internal error caused by using an object without initialization If the suggested action doesn't solve the problem or if the error is internal without a suggestion for correction, collect the error information and contact the ABB support organization. Troubleshooting subscriber system: In a Windows command prompt, check the connection status by running "ping ". Ensure the protocol status and versions are up-to-date in the Service Structure, under the Protocols tab. For remote connections, synchronize time between the subscriber and provider systems. If there's no alarm or event from the provider system on the subscriber side, verify: - The connection to the provider is stable. - The object generating the alarm is uploaded to the subscriber system. If not, upload it to display alarms correctly. In the Library Structure, select System Messages, then Default System Config under Aspects of 'System Messages'. Select Disconnected from Messages and include it in the list that generates System Alarms. Finally, choose "Inactive At Acknowledge" and apply changes. Manual Updates Revision Index A Updates for 800xA 5.1 Rev A: | Section | Sub-section | Description | | --- | --- | --- | | New in This Release | Connect Method for Multisystem Integration | New subsection added | Manual Updates Revision Index C Updates for 800xA 5.1 Feature Pack 3: | Section | Sub-section | Description | | --- | --- | --- | | New in This Release | Asset Optimization with Multisystem Integration | New subsection added | Page 120 Manual Updates Revision Index D ... (truncated) Page 122 Mannheim, Germany Phone: +86 (0) 10 84566688-2193 Phone: +49 18 05 26 67 76 www.abb.com/controlsystems e-mail: marketing.control-products@de.abb.com www.abb.de/controlsystems Copyright © 2003-2016 by ABB. ABB S.P.A. All rights reserved. Control Technologies, Sesto San Giovanni (MI), Italy Phone: +39 02 24 14 75 55 e-mail: controlsystems@it.abb.com www.abb.it/controlsystems Page 1 System 800xA Operations Safety Operator Warnings System Version 6.0 Power and productivity for a better world... Page 3 System 800xA Operations Safety Operator Warnings System Version 6.0... Page 4 This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. User Manual Conventions .....7 Related Documentation .....8 Section 1 - Safety Operator Warnings System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP00 4865-600 RevA9 System 800xA Network Configuration, 3BSE034463*.....22 System 800xA Administration and Security, 3BSE037410* .....22 System 800xA Technical Data and Configuration, 3BSE041434* .....22 System 800xA Operator Manual, 2PAA11 1131* .....22 Page 6 Table of Contents Revision History Introduction .....33 Revision History.....33 2PAA110888-600... 800xA System. This user manual lists the safety operator warnings and electrical warnings as described in the System 800xA Safety AC 800M High Integrity Safety Manual (3BNP00 4865-600 RevA) and the various user manuals referenced in the Safety Manual. Therefore, fully comply with all Warning and Caution notices. Related Documentation A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in System 800xA Released User Manuals and Release Notes (3BUA000263*). Section 1 - Safety Operator Warnings This section provides a list of all the safety warnings. The user manual provides warnings and guidelines for System 800xA, emphasizing the importance of following safety protocols and adhering to applicable standards. The document outlines various mechanisms to ensure safe operation and behavior of certain systems. It highlights the importance of configuring settings correctly, such as I/O module settings, to prevent damage or errors. The guidelines emphasize the user's responsibility in handling warnings related to under-range values. The manual also stresses the need for proper installation, commissioning, and maintenance procedures to avoid potential risks. For instance, interim measures should be taken during operation if required environmental conditions are not yet established. Redundant DO880 configurations require faulty modules to be removed within 72 hours to prevent channel errors. Additionally, the document discusses remote operation procedures, including VPN connection configuration. It also provides guidance on modifying and testing I/O connections in the running AC 800M HI controller. For PM861/PM864/PM865/PM866/PM867 operating in single configuration, ensure that RCU Link Termination plug TB852 is inserted at the RCU Link connector. This termination plug must always be used when running in single config. If TB852 is not available, use RCU Link Cable TK851 for a redundant processor running in single config. When handling devices labeled with an electrostatic sensitive device symbol, take special precautions as described in the installation section to prevent damage. Be cautious when applying supply voltage in the system, as it can cause serious injury or death. Similarly, exercise care during shutdown procedures to avoid electrical hazards. In System 800xA Control 6.0 AC 800M Configuration, be aware that reservations do not protect runtime data or prevent download of modified apps to a controller. When debugging functions based on the real-time clock in Debug mode, note that timer functions will operate according to actual time elapsed since started, regardless of whether the task is halted. To ensure proper supervision of network and PPP connections in System 800xA, configure RNRP at all times. Additionally, be aware that process dump files are large and may require special consideration. For formal safety certification status of an 800xA Safety product, refer to the latest TÜV Certification Report, ABB SolutionsBank or ABB Library (3BSE074100). The report, Annex A, discusses safety operator warnings in relation to bank or library access (3BSE074100). Specifically, Page 32 highlights the Warnings Section 1. The 2PAA110888-600 standard provides guidelines for operators on page 33. This User Manual's revision history is detailed on pages 34 and 36. The revision index is separate from the 800xA 6.0 System Revision. The table on page 34 outlines the revision description, date, and any relevant changes. For inquiries or concerns regarding this manual, contact ABB. The copyright information is as follows: 2015 ABB. www.abb.com/800xA All rights reserved. www.abb.com/controlsystems