System 800xA

800xA 4.1 to 5.0 SP2
Upgrade

System Version 6.0

Power and productivity
for a better world™

ABB

System 800xA

800xA 4.1 to 5.0 SP2 Upgrade

System Version 6.0

NOTICE

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. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

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, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described 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.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

Table of Contents

About This User Manual

Section 1 - Introduction

Section 2 - Upgrading SV 4.1 to SV 5.0 SP2

Appendix A - Control Builder M Compatibility Issues

Appendix B - Online Upgrade Controller Level

About This User Manual

Any security measures described in this User Manual, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as 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 800xA System.

This user manual describes how to manually perform upgrade procedures from SV 4.1 to System 800xA 5.0 SP2.

Systems running on SV 4.0 should first upgrade to SV 4.1 before upgrading to System 800xA 5.0 SP 2.

It does not include information on site planning, engineering planning, software configuration, network design, security measures, tools, maintenance, etc. that can be found in other 800xA instructions.

The procedures described in this user manual require Windows® Administrator privileges.

User Manual Conventions

Microsoft Windows conventions as defined in the Microsoft Manual of Style are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, and so on.

Warning, Caution, Information, and Tip Icons

This publication includes **Warning**, **Caution**, and **Information** where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard which could result in *electrical shock.*

Warning icon indicates the presence of a hazard which could result in *personal injury.*

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property.*

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, **fully comply** with all **Warning** and **Caution** notices.

Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018*).* The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard

dictionaries such as Webster's Dictionary of Computer Terms. Terms that uniquely apply to this instruction are listed in the following table.

Term/Acronym	Description
Backup	**800xA Backup:** Backup using the 800xA Backup Definition aspect.
	Functional Area Backup: Backup via defined tools or copy of Functional Area configuration and/or data to a safe media for items not covered by 800xA Backup.
	The specific operations called out for the Functional Area within the Backup/Restore procedure in *System 800xA Maintenance (3BSE046784*) f*or same version to same version backup and restore.
Restore	**800xA Restore:** Restore via Configuration Wizard.
	Functional Area Restore: Restore via defined tools or copy of Functional Area configuration and/or data from a safe media for items not covered by 800xA Backup.
	The specific operations called out for the Functional Area within the Backup/Restore procedure in *System 800xA Maintenance (3BSE046784*)* for same version to same version backup and restore.
Upgrade	Moving from one 800xA release to a later 800xA release, whether it be a major or minor release.
Update	Adding service packs, patches, hot fixes, or rollups to an existing 800xA System.

Section 1 Introduction

Overview

This document reflects 800xA System and Functional Area software at the time of release. All 800xA System and Functional Area Release Notes must be read and understood before performing any automated or manual installation, post installation, or upgrade procedures. The Release Notes contain any last minute changes that must be performed when installing or upgrading the 800xA System. All Release Notes can be found on the CD labeled *System Version 5 Released Documents.*

The upgrade from SV 4.1 to System 800xA 6.0 must be performed in a two-step procedure as follows:

1. The first step will be to upgrade from SV 4.1 to the latest revision of System 800xA 5.0 SP2. This instruction describes how to upgrade to the latest revision of System 800xA 5.0 SP2.

2. The second step will be to upgrade from the latest revision of System 800xA 5.0 SP2 to System 800xA 6.0. Refer to *System 800xA 5.0 SP2 to 6.0 Upgrade (2PAA111695*)* for instructions on upgrading from the latest revision of 800xA 5.0 SP2 to System 800xA 6.0.

The topics in this section briefly describe the prerequisite requirements, procedures, and other considerations depending on the current software version. Review this information before installing SV 5.0 SP2.

If virus checking software is installed on a node, disable it until after the 800xA System is installed and configured (post installation).

Upgrading directly from SV 4.0 to SV 5.0 SP 2 is not supported. If running this version, it is necessary to upgrade to SV 4.1 before upgrading to SV 5.0 SP 2.

Refer to *Industrial IT, 800xA - System, 800xA for Harmony, Release Notes (3BUA000112Rxxxx)* before updating an 800xA SV 5.0 SP1a System or upgrading an 800xA SV 4.1 System if 800xA for Harmony is installed on any node in the system.

Supported Operating Systems

The Microsoft Windows Operating Systems supported in SV 5.0 SP2 are:

- Windows XP Professional with SP2.
- Windows Server 2003 R1 with SP2.
- Windows Server 2003 R2 with SP2.

If using Windows Server 2003 R2 with SP2, unless otherwise specified, do not enable any Windows components that are not enabled in the default installation.

The following rules apply:

- Preconfigured workstations that come from the workstation manufacturer must be preconfigured by the workstation manufacturer to meet 800xA System specifications. If they are not, they must be reconfigured by the user to meet 800xA System specifications.

- Existing nodes that *are running* Windows XP Professional, Windows Server 2003 R1, or Windows Server 2003 R2 but are not at SP2 require an update of the existing Operating System.

- Existing nodes that *are not running* Windows XP Professional, Windows Server 2003 R1, or Windows Server 2003 R2 must be reformatted and the compatible Operating System must be installed.

- All IM (Information Management) Server nodes being upgraded from SV 4.1 to SV 5.0 SP 2 must be reformatted and the Operating System installed, even if the existing Operating System is compatible.

- All 800xA for Harmony and Melody Connectivity and Configuration Server nodes being upgraded from SV 4.1 to SV 5.0 SP 2 must be reformatted and the Operating System installed, even if the existing Operating System is compatible.

Planning for the Upgrade

Planning for the upgrade can save time and resources. The upgrade paths in this instruction are presented in sequential order; however, depending on the plant performing the upgrade, some of the actions can be performed in advance or in parallel. For example, the upgrade flows are written to reflect upgrading and using existing servers and workstations. If new servers and workstations are being used, prepare those before beginning the upgrade (load and configure the Windows Operating System, third party software, etc.), or while performing the pre-upgrade procedures .

For optimal software prerequisites, refer to *Third Party Software System 800xA (3BUA000500Rxxxx)*. The prerequisites depend on the functions installed in the system, or on each node type. This document is accessible from ABB SolutionsBank.

For an upgrade, performance will be determined by the actual hardware of the system. System performance after the upgrade is completed will be determined by the hardware being upgraded. Memory size and processor speed have a direct impact on system performance. Refer to *Third Party Hardware Products Verified for Industrial IT System 800xA (3BSE046579)* for a list of hardware verified for use with the 800xA System. This document is accessible from ABB SolutionsBank.

3. If upgrading from SV 4.1, order new SV 5.0 licenses. New licenses are not required if updating from SV 5.0 SP1a to SV 5.0 SP 2. Contact an ABB sales representative to perform the license upgrade.

4. If new servers and workstations are being used, prepare those before beginning the upgrade (load and configure the Windows Operating System, third party software, etc.).

5. Consider other issues that are important prior to starting the upgrade, such as:

   Concurrent access to the current 800xA System version and the SV 5.0 SP 2 system is recommended until the upgrade has been performed. This makes it possible to easily retrieve any data or files that have been missed. Concurrent access depends upon many different factors, including:

   – Configuration of the existing system.
   – Desired configuration of the SV 5.0 SP 2 system.
   – Server and workstation use strategy.

        –   Configuration of user and user groups.
        –   Use of service accounts.
        –   Domain controllers.
        –   Redundancy.
        –   Logical and physical networks.

One strategy is to leave a minimal part of the existing system intact, such as an Aspect Server, while preparing a major part of the SV 5.0 SP 2 System. Another strategy is to prepare a minimal SV 5.0 SP 2 System.

Retaining an Aspect Server from the existing system minimizes the time it takes to retrieve data or files from it. A disk drive image provides a quick way to recover, but often it requires no hardware upgrade. Try to delay the upgrade of the hardware in one Aspect Server as long as possible.

If it is not necessary to do the complete upgrade in one process, it may be possible to perform the upgrade in steps by stopping selected system functions or by stopping some parts of the plant, or a combination of the two.

6.   Prepare the Device Library (select the set of devices used at the customer site and prepare the files on a transportable media, ready to install).

7.   Refer to System Installer and determine whether or not System Installer can be used to perform the upgrade.

System Installer

Upgrades from SV 4.1 to SV 5.0 SP2 can be executed either semi-automatically using the System Installer as described in *Industrial IT, 800xA - System, Automated Installation (3BSE034679Rxxxx)*, or manually as described in this instruction.

The System Installer is more efficient since it performs many of the time-consuming and difficult tasks, and verifies that the software is installed in the correct order, the desired configurations are supported, etc. However, there are some conditions that prevent System Installer from being used or some special considerations that must be taken into account:

•   Refer to *Industrial IT, 800xA - System, 800xA for Harmony, Release Notes (3BUA000112Rxxxx)* before using System Installer to update or upgrade an 800xA System if 800xA for Harmony is installed on any node in the system.

- Uninstalling 800xA software is not necessary when using System Installer to update from SV 5.0 SP1a to SV 5.0 SP2.

- The System Installer can only be used to upgrade from SV 4.1 to SV 5.0 SP2.

Installation Tools Provided with System Installer

The System Installer tools must be launched using the Automated Installation AUTORUN screen. This can be done via the following:

- With System Installation DVD 1 in the drive of the node where the tools are being run.
- With the contents of System Installation DVD 1 copied locally to the node where the tools are being run.

The tools can not be run from a file server.

The System Installer provides standalone tools to help in the installation and verification process.

System Planner Tool: Used to:

- **Plan a New System:** Used to specify the desired system configuration. The System Planner Tool consists of a series of dialogs where relevant information is specified, such as:

    – Location of the license file.
    – Whether or not Windows is already installed on the workstations.
    – The number of Operator Workplace and Engineering Workplace Clients.
    – The number of remote client servers.
    – Connectivity Server options.
    – Device Management options.
    – Functional Area software that will run in the system and options for each.
    – Aspect Server redundancy options.
    – AC 800M options.
    – Other Connectivity Server options.
    – Whether the system will be part of a domain or workgroup.
    – Multisystem Integration options.
    – Network and node parameters.
    – User and User Group settings.
    – Network redundancy and control network areas.
    – Workstation IP addresses.

When the planning phase is complete, node specific Setup Packages are generated. Refer to the System Planner Tool section in *Industrial IT, 800xA - System, Automated Installation (3BSE034679Rxxxx)* for more information.

- **Upgrade an Installed System from SV 4.1 to SV 5.0 SP2:** An upgrade information file, generated by the System Verifier Tool, is needed in order to use this option. The System Upgrade Guide must be run on the 800xA System version to be upgraded, while the 800xA System is running. Refer to the Upgrading an Installed System section in *Industrial IT, 800xA - System, Automated Installation (3BSE034679Rxxxx)* for more information.

Windows Firewall Configuration Tool: Windows Firewall restricts communications between a server or workstation and a network or the Internet. It might be necessary to adjust settings for some other applications that prefer an open connection. Either exceptions can be made or a port can be opened so these applications can communicate through Windows Firewall.

The Windows Firewall Configuration Tool makes the necessary exceptions and opens the necessary ports. Use this tool to configure Windows Firewall even if manually installing the 800xA Base System and Functional Area software.

In order to allow proper communications between a workstation and a network or the Internet, Windows Firewall must be disabled during 800xA installation and post installation procedures, and then enabled using the Windows Firewall Configuration Tool after all procedures are complete.

Windows Configuration Tool: Sets up Windows Operating System services and settings for the 800xA System (Windows hardening). The operation of the standalone tool is described in *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)*.

System Verifier Tool (this is not a standalone tool): After Windows is installed and configured on a node, the System Verifier Tool will check to see if the node fulfills the necessary hardware and software requirements. If any third party software is required, the System Verifier Tool will help install it or it will provide the necessary information to fulfill the requirement.

For more information on these installation tools, refer to *Industrial IT, 800xA - System, Automated Installation (3BSE034679Rxxxx)*.

System Verifier Tool vs System Checker Tool

The System Verifier Tool delivered with the System Installer verifies whether or not the hardware and software requirements are fulfilled. If the System Verifier Tool determines that required software is missing, it helps to install that software. The System Verifier Tool can only be run as part of the installation process using System Installer. It is not a standalone tool.

The System Checker Tool is a standalone tool delivered with the 800xA System. It has more features than the System Verifier Tool. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System.

The installation and use of the System Checker Tool is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**. It supports 800xA System Versions 3.x, 4.x, and 5.0, 5.0 SP1, and 5.0 SP2 (including revisions).

The System Checker Tool includes the following:

• System Checker Tool.
• System Information Collector Tool.
• System Report Analyzer Tool.

System Language Package

The 800xA System includes support for US English only. Translations of the operator interface (System 800xA Language Packages) are released separately after the main release of the 800xA System. Upgrade of a system including a Language Package requires an upgrade of the Language Package when it is released.

Refer to the Language Package release notes for information on upgrading a Language Package to SV 5.0 SP 2.

Precautions

There are third party backup/restore and disk imaging utilities that are useful when software or data becomes corrupted to the point that the node will no longer function correctly. A limited number of hardware failures can also be compensated for by using these utilities. However, it is important to understand the limitations

and ramifications associated with these utilities. In some cases (such as corrupted data, corrupted software, or hard disk failures) these utilities can be useful while in other cases (such as replacing a node) these utilities may be of limited use.

It is recommended that a third party backup/restore and/or disk imaging utility be used to save (and restore if necessary) an image of node hard disks after installation of third party software and/or after installing all software.

The 800xA System import/export utility can be used to save 800xA System information one portion at a time. However, the 800xA System backup utility is the functional equivalent of exporting all 800xA System information at one time. The critical difference between these utilities is that individually exported portions of 800xA System information can be imported back into the original system or into a completely different system while backed up 800xA System information can only be used to restore a specific system on specific nodes. The 800xA System allows for scheduled 800xA System backups. Refer to *Industrial IT, 800xA - System, Maintenance (3BSE046784Rxxxx)* for information on performing precautionary scheduled 800xA System backups.

Windows Hardening

Use the Windows Config Tool, which is part of the System Installer package, to perform automated Windows hardening for the 800xA System. Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* for more information.

Firmware Memory Consumption

When upgrading, consideration should be given to memory usage in the controller. The firmware size has grown slightly, resulting in slightly less free memory for user applications. However, this is offset by improvements in application and library handling, and for most projects, the net difference in memory usage is insignificant.

If PM851, PM856, or PM860 controllers with a small amount of free memory in are being used, refer to the instructions in *Industrial IT, 800xA - System, System Guide, Technical Data and Configuration Information (3BSE041434Rxxxx)* for information on memory requirements.

Section 2 Upgrading SV 4.1 to SV 5.0 SP2

Introduction

Upgrading the 800xA System requires the plant to be shut down. To guarantee the functionality of the upgraded system, follow these upgrade instructions carefully and perform them in the order presented.

The person performing this upgrade must use the same user account that was used during the installation of the 800xA System software, unless otherwise indicated in these instructions.

Functional Area Naming

Some 800xA Functional Area names have been changed since the SV 4.0 release. Table 1 lists the Functional Area names before and after the upgrade. The SV 4.0 Functional Area names will be used in this section up to, but not including System Upgrade (Upgrade Flow B) on page 49. The SV 5.0 SP2 Functional Areas names will be used from that point through the remainder of the section.

Table 1. Functional Area Naming

Name in SV 4.1 SP3	Name in SV 5.0 SP2
Control IT for AC 800M	800xA for AC 800M
FOUNDATION Fieldbus Device Integration	Device Management FOUNDATION Fieldbus
HART Device Integration	Device Management PROFIBUS & HART
PROFIBUS Device Integration	

Table 1. Functional Area Naming (Continued)

Name in SV 4.1 SP3	Name in SV 5.0 SP2
AC 400 Connect	800xA for Advant Master
Safeguard Connect	800xA for Safeguard

Control Builder M Compatibility Issues

Refer to the compatibility issues detailed in Appendix A, Control Builder M Compatibility Issues before beginning the upgrade.

Upgrade Flow

This section is organized so that the instructions are presented in the proper upgrade order. Do not skip any steps that pertain to 800xA software being used in the current or upgraded system. Refer to Planning for the Upgrade on page 15 for additional information and ideas on how to streamline the upgrade process.

Figure 1 shows a high level flow of the upgrade paths.

The upgrade process is broken down into three processes:

- Preparation (Figure 2).
- Operating system and third party software upgrade (Figure 3).
- 800xA System software and configuration data upgrade (Figure 4).

Each flow chart has active links, indicated by blue text, to help navigate through the document (if viewing it online). Clicking in a flow element with blue text will advance the document to the related procedure.

All paths require, after backup and before restore, installing the 800xA System software and creating the system as if it were a new installation.
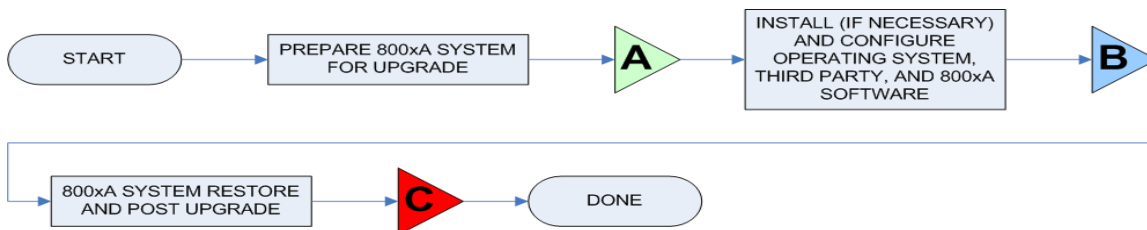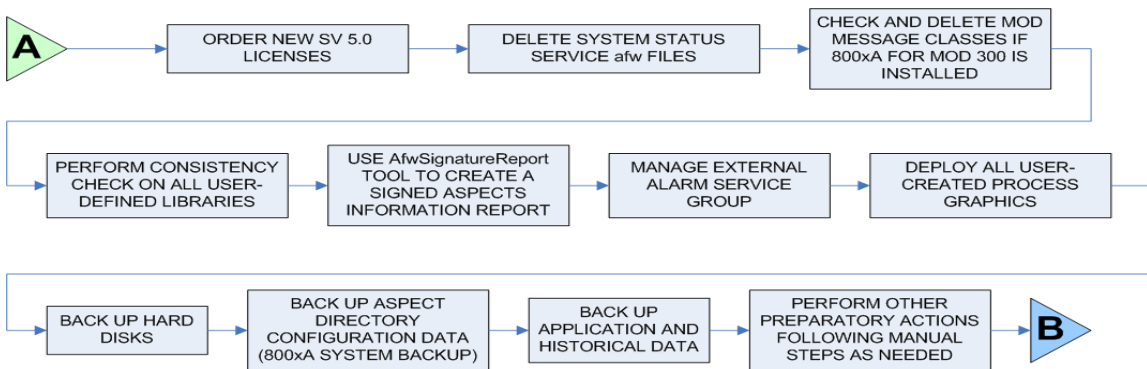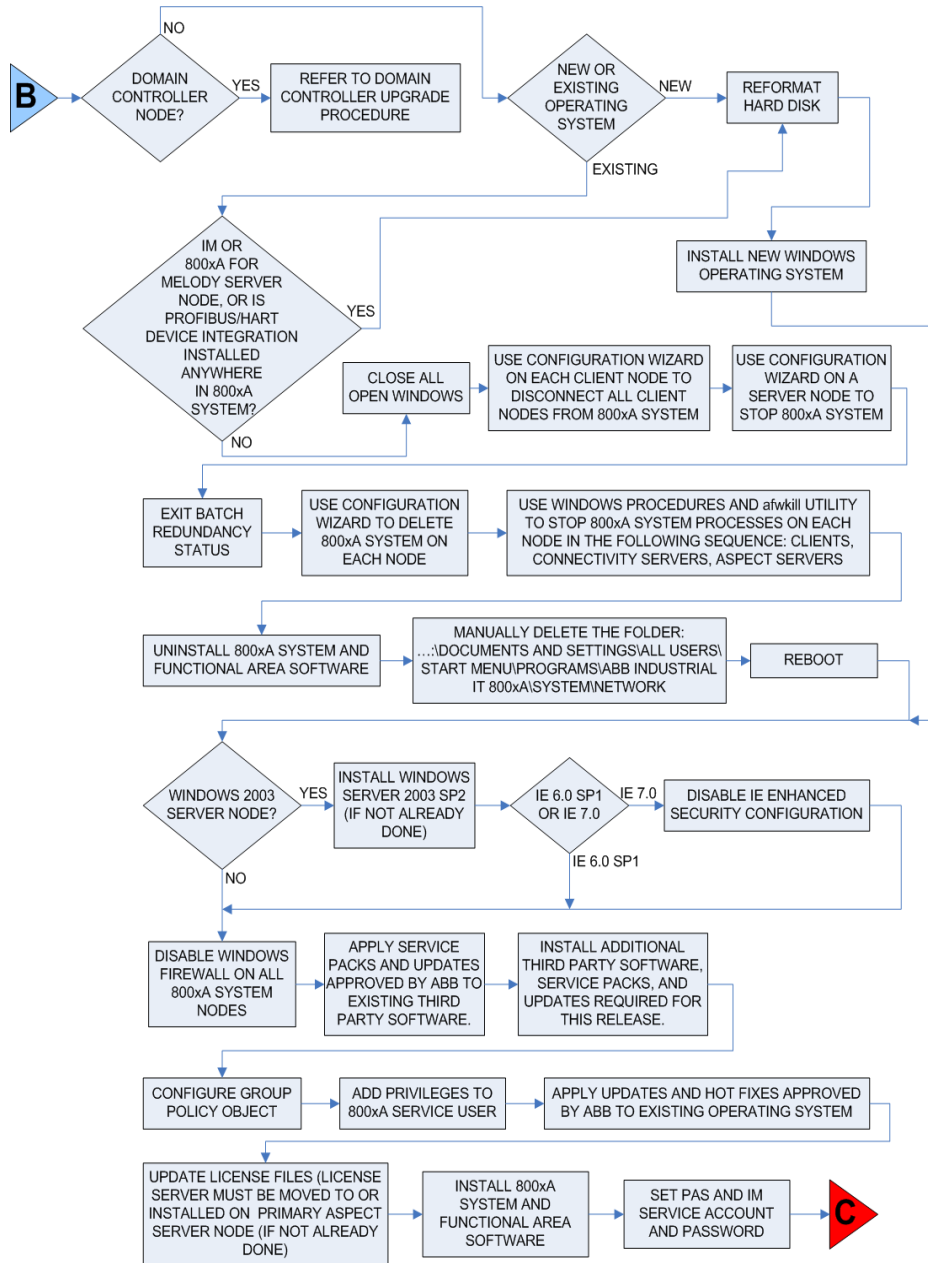

Figure 1. High Level Upgrade Flow

Figure 2. Upgrade Preparation Flow

```
         NO
    ┌──────────────┐
 B  │   DOMAIN     │ YES   ┌──────────────────┐       ┌──────────────┐  NEW   ┌──────────────┐
    │  CONTROLLER  │────── │ REFER TO DOMAIN  │       │   NEW OR     │────────│  REFORMAT    │
    │    NODE?     │       │ CONTROLLER UPGRADE│      │  EXISTING    │        │  HARD DISK   │
    └──────────────┘       │   PROCEDURE      │       │  OPERATING   │        └──────────────┘
                           └──────────────────┘       │   SYSTEM     │
                                                       └──────────────┘
                                                          EXISTING

    ┌──────────────────┐                                            ┌──────────────────────┐
    │   IM OR          │                                            │ INSTALL NEW WINDOWS  │
    │   800xA FOR      │                                            │ OPERATING SYSTEM     │
    │ MELODY SERVER    │                                            └──────────────────────┘
    │ NODE, OR IS      │ YES
    │ PROFIBUS/HART    │      ┌──────────────┐  ┌──────────────────────┐  ┌──────────────────┐
    │ DEVICE INTEGRATION│     │ CLOSE ALL    │  │ USE CONFIGURATION     │  │ USE CONFIGURATION│
    │ INSTALLED        │      │ OPEN WINDOWS │  │ WIZARD ON EACH CLIENT │  │ WIZARD ON A      │
    │ ANYWHERE         │      └──────────────┘  │ NODE TO DISCONNECT ALL│  │ SERVER NODE TO   │
    │ IN 800xA         │                        │ CLIENT NODES FROM     │  │ STOP 800xA SYSTEM│
    │ SYSTEM?          │                        │ 800xA SYSTEM          │  └──────────────────┘
    └──────────────────┘                        └──────────────────────┘
         NO
```

```
    ┌──────────────┐  ┌──────────────────┐  ┌────────────────────────────────────────┐
    │ EXIT BATCH   │  │ USE CONFIGURATION│  │ USE WINDOWS PROCEDURES and afwkill UTILITY│
    │ REDUNDANCY   │  │ WIZARD TO DELETE │  │ TO STOP 800xA SYSTEM PROCESSES ON EACH   │
    │ STATUS       │  │ 800xA SYSTEM ON  │  │ NODE IN THE FOLLOWING SEQUENCE: CLIENTS, │
    └──────────────┘  │ EACH NODE        │  │ CONNECTIVITY SERVERS, ASPECT SERVERS     │
                      └──────────────────┘  └────────────────────────────────────────┘
```

```
    ┌──────────────────────┐  ┌──────────────────────────────┐  ┌──────────┐
    │ UNINSTALL 800xA SYSTEM│ │ MANUALLY DELETE THE FOLDER:  │  │ REBOOT   │
    │ AND FUNCTIONAL AREA   │ │ …:\DOCUMENTS AND SETTINGS\ALL │  └──────────┘
    │ SOFTWARE             │  │ USERS\START MENU\PROGRAMS\ABB │
    └──────────────────────┘  │ INDUSTRIAL IT 800xA\SYSTEM\  │
                              │ NETWORK                      │
                              └──────────────────────────────┘
```

```
    ┌──────────────┐ YES ┌──────────────────┐          ┌──────────────┐ IE 7.0 ┌──────────────────┐
    │ WINDOWS 2003 │─────│ INSTALL WINDOWS  │          │  IE 6.0 SP1  │────────│ DISABLE IE ENHANCED│
    │ SERVER NODE? │     │ SERVER 2003 SP2  │          │  OR IE 7.0   │        │ SECURITY CONFIG.  │
    └──────────────┘     │ (IF NOT ALREADY  │          └──────────────┘        └──────────────────┘
         NO              │ DONE)            │              IE 6.0 SP1
                         └──────────────────┘
```

```
    ┌──────────────┐  ┌──────────────────┐  ┌──────────────────┐
    │ DISABLE WINDOWS│ │ APPLY SERVICE     │  │ INSTALL ADDITIONAL│
    │ FIREWALL ON ALL│ │ PACKS AND UPDATES │  │ THIRD PARTY SOFTWARE,│
    │ 800xA SYSTEM   │ │ APPROVED BY ABB TO│  │ SERVICE PACKS, AND│
    │ NODES          │ │ EXISTING THIRD    │  │ UPDATES REQUIRED FOR│
    └──────────────┘  │ PARTY SOFTWARE.   │  │ THIS RELEASE.    │
                      └──────────────────┘  └──────────────────┘
```

```
    ┌──────────────┐  ┌──────────────────┐  ┌──────────────────────────────┐
    │ CONFIGURE GROUP│ │ ADD PRIVILEGES TO │  │ APPLY UPDATES AND HOT FIXES  │
    │ POLICY OBJECT  │ │ 800xA SERVICE USER│  │ APPROVED BY ABB TO EXISTING  │
    └──────────────┘  └──────────────────┘  │ OPERATING SYSTEM             │
                                            └──────────────────────────────┘
```

```
    ┌──────────────────────┐  ┌──────────────┐  ┌──────────────────┐
    │ UPDATE LICENSE FILES  │  │ INSTALL 800xA│  │ SET PAS AND IM   │  ┌───┐
    │ (LICENSE SERVER MUST  │  │ SYSTEM AND   │  │ SERVICE ACCOUNT  │  │ C │
    │ BE MOVED TO OR        │  │ FUNCTIONAL   │  │ AND PASSWORD     │  └───┘
    │ INSTALLED ON PRIMARY  │  │ AREA         │  └──────────────────┘
    │ ASPECT SERVER NODE    │  │ SOFTWARE     │
    │ (IF NOT ALREADY DONE))│  └──────────────┘
    └──────────────────────┘
```
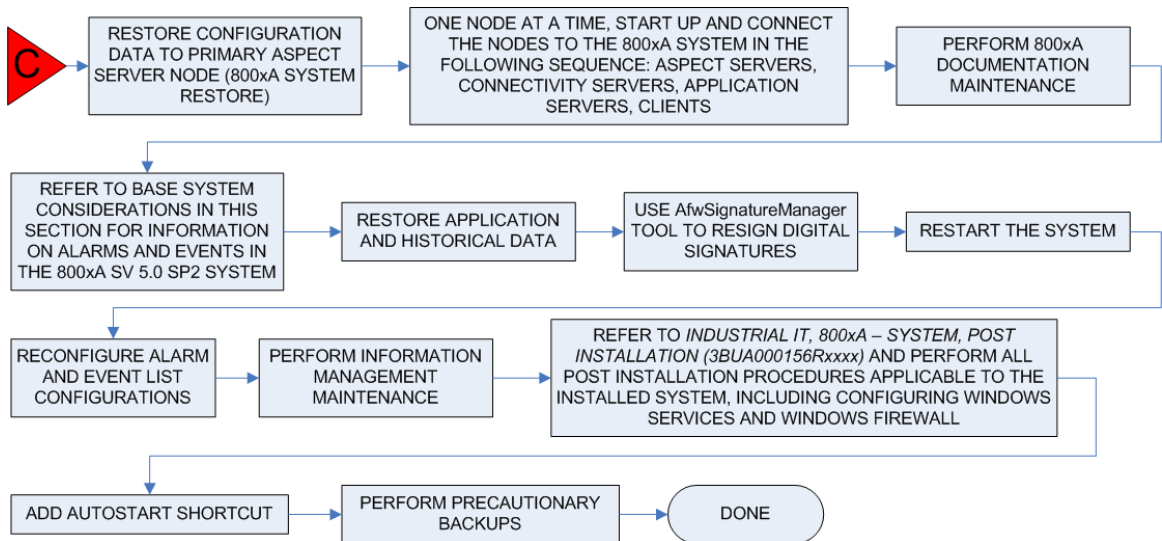
Figure 4. System Restore and Post Upgrade Flow

Central Licensing System (Upgrade Flow A)

Order new licenses for SV 5.0 SP2. The SV 4.1 licenses will not work.

800xA for MOD 300

If 800xA for MOD 300 is installed, check and delete the MOD 300 Message Class object before performing the 800xA System backup.

Delete all MOD Message Class objects below the Message Classes object located in:

Library Structure > System Messages > Message Classes

Order new SV 5.0 licenses for SV 5.0 SP2. The SV 4.1 licenses will not work.

To delete the Message Class objects is to export the Message Classes object, delete it and its descendants, and then import the Message Classes object back again.

Consistency Check

Perform a consistency check before performing the 800xA System backup. Failure to do so could result in problems when restoring the system after the upgrade.

Perform a consistency check on all user-defined libraries:

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Library Structure**.

3. Use the Object Browser to navigate to and select the Library Version aspect on each user defined library.

4. Select the **Consistency** tab.

5. Click **Check Consistency**.

6. Click **Try to Repair** if the check finds an error.

7. Repeat for all user-defined libraries.

8. Contact ABB Technical Support for assistance if there are problems.

Save Digital Signatures

The new support for version handling of aspect data will make all digital signatures in SV 4.1 invalid when upgrading to SV 5.0 SP2. To simplify the upgrade, two applications have been developed to support the re-signing of aspects in SV 5.0 SP2:

•   **AfwSignatureReport:** Used to create a report with information about signed aspects in SV 4.1.

•   **AfwSignatureManager:** Used in SV 5.0 SP2 to re-sign these aspects.

Perform the following before upgrading from SV 4.1 to SV 5.0 SP2.

1. Insert 800xA System Installation DVD 1 into the drive on a client in the SV 4.1 800xA System.

2. Copy the AfwSignatureReport.exe from the following directory on 800xA System Installation DVD 1 to a directory on the client.

   ```
   Engineering & Development\Accessories\Digital
   Signatures Upgrade Tools\SV3
   ```

3. Open a Windows Command Prompt.

4. Change to the directory where AfwSignatureReport.exe was copied.

5. Run the following command:

   ```
   AfwSignatureReport <filename>.xml
   ```

6. Save the signature report file <fileName>.xml on an external media during the upgrade.

The digital signature must be valid before saving to the report file.

External Alarm Service Group

Keep only one External Alarm Service Group and move the provider or providers to the Aspect Servers.

Deploy all User Created Process Graphics

800xA System backups containing undeployed user created process graphics will result in warning and error messages later in the upgrade process. To avoid these messages, refer to *Industrial IT, 800xA - Engineering, Graphics (3BSE030335Rxxxx)* and use the Display Tool to deploy all user created process graphics before beginning the 800xA System backup.

Backups

It is important to create backups of node hard disks and the 800xA System before starting the upgrade procedures. Valid backups insure that the system can be restored if necessary.

Hard Disk Backup

It is recommended that a third party backup/restore and/or disk imaging utility be used to save (and restore if necessary) hard disks before starting the upgrade procedures.

800xA System Backup

Refer to Consistency Check on page 26 and perform a consistency check before performing the 800xA System backup. Failure to do so could result in problems when restoring the system after the upgrade.

The Backup/Restore function makes it possible to make an online backup of a node and perform an offline restore of the same node. A full backup stores all aspect objects and aspect data (application data) in the Aspect Directory.

Verify the Batch Management Servers are operating normally before and during 800xA System backups (or usage of the Import/Export tool) of systems containing Batch Management nodes. This will make sure the backup of all batch data.

All system extensions that are part of the system must be installed and added on the node where the backup will be taken (usually the primary Aspect Server node). No changes can be made (especially to the Aspect directory) during the online backup process.

The following steps outline the 800xA system backup procedure. Refer to *Industrial IT, 800xA - System, Maintenance (3BSE046784Rxxxx)* for more detailed information.

1. Create a Full Backup Definition object in the **Maintenance Structure**.

2. Configure the **Scope** and the **Storage** tabs. Disable the **History** and **System Messages** check boxes in the **Scope** tab.

3. Check the disk space and path in the **Storage** tab of the Backup Definition aspect. A large configuration could require a minimum of five gigabytes of free space.

4. Start the backup process.

5. In case of any warning or error messages (refer to Appendix A, Warning and Error Messages), take the appropriate measure and create a new backup.

6. Record the number of aspects and objects in the system.

    a. Select the Admin Structure\Adminstrative Objects\Domains\system_name, Domain\Domain Definition aspect.

    b. Record the number of objects and aspects listed in the System Size Information area of the window.

    c. Right-click the Control Structure\control_network_name, Control Network\Control Structure aspect of one of the control networks contained in the system.

    d. Select **Properties** from the context menu.

    e. Select the **Statistics** tab.

    f. Record the number of objects listed.

    g. Right-click the **Control Structure** aspect within a controller project of the control network selected in Step c.

    h. Select **Properties** from the context menu.

    i. Record the number of objects listed.

    j. Repeat Step g through Step i for all the controller projects within the control network.

    k. Repeat Step c through Step j for every control network in the system.

    l. Right-click the Control Structure\HSE_Subnet name, HSE Subnet\Control Structure aspect of one of the HSE Subnets contained in the system.

    m. Select **Properties** from the context menu.

    n. Select the **Statistics** tab.

    o. Record the number of objects listed.

p.   Repeat Step l through Step o for every HSE Subnet in the system.

q.   Right-click the Control Structure\MB300_name, MB300
       Network\Control Structure aspect of one of the MB300 Networks
       contained in the system.

r.   Select **Properties** from the context menu.

s.   Select the **Statistics** tab.

t.   Record the number of objects listed.

u.   Repeat Step q through Step t for every MB300 network in the system.

Do not manually import or edit any information in backup files.

Pre-Upgrade Procedures

Some 800xA System software requires preparatory steps before shutting down
800xA System processes. Perform the applicable procedures in the order presented.

Control IT for AC 800M

Use the following procedure to prepare for the Control IT for AC 800M upgrade:

1.   Record the memory setting for OPC Server and Control Builder found in the
       Setup Wizard for each product.

2.   Control Builder stores its settings (systemsetup.sys) on disk in the following
       directory:

```
...\ABB Industrial IT Data\Engineer IT Data\Control
Builder M Professional
```

Copy this file to a safe media.

3.   Save OPC configurations by selecting:

       File > Save Configuration

in the OPC Server Panel.

4.   The OPC Server stores configuration files (*.cfg) and settings (systemsetup.sys) on disk. Copy these files to a safe media. The systemsetup.sys file is located in:

```
...\ABB Industrial IT Data\Control IT Data\OPC Server
for AC 800M
```

The configuration files are stored in the Files folder in the same location.

Device Management and Fieldbuses

Device Management FOUNDATION Fieldbus

User-made modifications to library objects representing FF standard blocks (these are blocks supported by the Device Type Standard FBs as indicated in the **Block Info** tab of the block class parameter dialog) will be overwritten during upgrade. If such changes have been made, they can be reconstructed manually. Refer to Device Management FOUNDATION Fieldbus on page 83.

Device Management PROFIBUS & HART

Historical data sets of Device Type Manager (DTM), exported via the Fieldbus Management aspect, along with device specific DTM files are stored as files on the Primary Aspect Server node. These files and the PROFIBUS/HART OPC Server configuration are stored after a successful 800xA System backup. The path to this folder can be found as follows:

1.   Open the Plant Explorer Workplace on the Primary Aspect Server node.

2.   Use the Structure Selector to select the **Control Structure**.

3.   Use the Object Browser to select the Root Object type.

4.   Select the FBB PH Settings aspect.

5.   Record the path information for the Primary Aspect Server found in the FBB PH Settings aspect.

6.   Use Windows Explorer to copy the folder (default: Fieldbus Builder PH) containing device specific configuration files (in the path recorded in Step 5) to the 800xA System backup folder, created as described in 800xA System Backup on page 28.

7. If the folder name of the copied folder is not Fieldbus Builder PH, it must be renamed to the default folder name (Fieldbus Builder PH) in the 800xA System backup folder.

PROFIBUS Device Types

PROFIBUS Device Types in SV 5.0 and later are based on Hardware Libraries (HWLib). This is different from previous system versions, where these Device Types were based on Hardware Definitions (HWD). As a result, the PROFIBUS Device Types used in connection with the Device Integration software must be linked to new delivered Hardware Libraries to make sure system and upgrade compatibility.

Perform the following procedure only if the exact PROFIBUS Device Type described is used. Otherwise, this procedure can be skipped.

If the *ABB_TZIDC_110-220_SP_Short* module type is used in the Control Structure of the Plant Explorer, a special upgrade procedure must be performed to make sure upgrade compatibility in SV 5.0 and later. This module is delivered with the PROFIBUS Device Integration package and its system extensions and is supported by the *ABB_TZIDC_110-220_YP0_v1_0* PROFIBUS Device Type.

The following steps requires Bulk Data Manager (BDM) (Engineering Platform) to be installed. Perform the described steps on an Engineering system node.

1. Open the Engineering Workplace and select the **Control Structure**.

2. Open the **Find Tool**.

3. In the **<Add attribute>** selection box select **Structure**.

4. In the **<Structure>** selection box select **Control Structure**.

5. In the **<Add attribute>** selection box select **Object Type**. This displays all instances available in the **Control Structure**.

6. Select the **ABB_TZIDC_110-210_SP_Short** module from the displayed list and click **Search**. If the module type is not available, this section can be skipped.

7. Open Bulk Data Manager in the **Control Structure** (right-click on the Root node and select **Advanced > Bulk Data Manager**).

8. Verify that the valid system is selected in the BDM sheet.

9. Search for and select the **ABB_TZIDC_110-220_SP_Short** module in the **Control Structure**.

10. Select `Control Properties` in the Aspect List Area and move it via the drag and drop function to the BDM sheet on cell A1 in the Preview Area.

11. A new window will open in which all parameters will be selected. Confirm the **Complete** selection by clicking **OK**.

12. Select cell A2 in the BDM sheet and enter the text **`Filter:Control Structure`**.

13. Select the project containing the **ABB_TZIDC_110-210_SP_Short** module in the **Control Structure** and move it via the drag and drop function into the BDM sheet on cell A3.

   If the module is used in different projects, the steps must be repeated for the other projects.

14. Select the **Auto filter** option in the Excel sheet (select **Data > Filter > AutoFilter** in the menu bar).

15. Select in line A in the BDM sheet, the column named **Source Object** (normally cell C1) and click **Filter**.

16. Search for and select the **ABB_TZIDC_110-210_SP_Short** module. This will now be the only module shown.

17. Enter the text **`delete`** for each listed module in the column named **Command** (normally cell A1). The Optional selection function can be used.

18. Save the changes to the 800xA System by clicking **Save All Objects**. The modules will be deleted in the **Control Structure**.

19. Remove the text **`delete`** for each listed module in the column named **Command**.

20. The captions **Short** will be exchanged to **Long** for all listed modules in the column named **Source Object**. The name will now be **ABB_TZIDC_110-210_SP_Long** for all listed modules.

21. Save the changes to the 800xA System by clicking **Save All Objects**. The modules will be created in the **Control Structure**.

800xA for AC 100

800xA for AC 100 is not detected by System Installer if this tool is used for upgrade. This means that the installation of this software must be done manually in the new system.

Perform the following to prepare for the 800xA for AC 100 upgrade:

For each 800xA for AC 100 Connectivity Server node, document the settings in the Configuration Wizard for these action groups:

*   AF 100 Network
*   AC 100 OPC Server Definitions
*   AC 100 OPC Server Station Filtering

If you have stored a local copy of the Bus Configuration Database (BCD) file in the Connectivity Server node, copy the BCD file folder to a safe location.

800xA for Advant Master and 800xA for Safeguard

Perform the following on each Connectivity Server node.

1. Make an RTA Board backup. Save the files:

*   DATHR1.CD
*   DATHR2.CD
*   DATHR3.CD

from the folder:

```
...\Program Files\ABB Industrial IT\OperateIT\AC 400
Connect\AdvantBase\Data\RTA\Init\
```

and record which files belong to which node.

2. Save the Configuration Files.

    The configuration files in the Connectivity Servers can contain special configuration settings for Alarm and Event or Data access. Refer to *800xA for*

Advant Master, Configuration (3BSE030340*) for more information about these special configuration settings.

If such changes are available in the configuration files, perform the following on each 800xA for Advant Master and 800xA for Safeguard Connectivity Server node:

Save the following files to a safe location:
– AdvDsMasterAdapter.csv
– AdvMbAeOPCServer.csv

The default location for the files is:

```
...\Program Files\ABB Industrial IT\Operate IT\AC 400
Connect\Bin
```

3. The following settings must be documented for reconfiguration.

– Time synchronization registry key (`REVERSED_SYNC_MODE`):

```
HKEY_LOCAL_MACHINE\SOFTWARE\ABB\AFW\SystemModules\
AfwTimeServerAdaptor\1.0-0\Private
```

– MB300 node and network address for RTA board in RTA board Configuration aspect.

800xA for MOD 300

Ensure that the configuration data noted in the Customized Data for Backup Appendix in *Industrial IT, 800xA System - 800xA for MOD 300, Configuration (3BUR002417Rxxxx)* has been recorded.

PLC Connect

1. If the PLC Connect IEC 60870 feature is installed and configured, the IEC configuration must be saved. Refer to the section on configuring the IEC 60870 driver in *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* for more information.

2. If the PLC Connect Communication Server Pre Treatment function is being used in the application (refer to *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* for more information), make a backup of

PreTreat2.dll. Pretreat2.dll is located in the following folder on the PLC Connect Connectivity Server:

    ...\ABB Industrial IT\Operate IT\PLC Connect\Bin

The path is the default location of the file. If it has been placed somewhere else, make a backup from that location.

3.   Make a backup of the VB application projects for PreTreat2.dll.

4.   If the Event Server Pre Treatment function is being used in the application (refer to *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* for more information), make a backup of PreEvent.dll. PreEvent.dll is located in the following folder on the PLC Connect Connectivity Server:

    ...\ABB Industrial IT\Operate IT\PLC Connect\Bin

The path is the default location of the file. If it has been placed somewhere else, make a backup from that location.

5.   Make a backup of the VB application projects for PreEvent.dll.

Engineering Studio IO Allocation

Deactivate the auto update mode in IO Allocation.

1.   Start the Engineering Workplace.

2.   Open the IO Allocation tool on any object by right-clicking on the object and selecting **Advanced > IO Allocation** from the context menu that appears.

3.   Verify that no check mark symbol is visible in the **Options > Automatic Write Allocation to CBM** menu item in the IO Allocation tool.

Asset Optimization

Preparing for the Asset Optimization upgrade requires recording some values for post upgrade and backing up data to a safe media.

Record Values for Post Upgrade

1.   Use the following procedure to record the value of the OPC Group Update Rate.

    a.   Open a Plant Explorer Workplace.

    b.   Use the Structure Selector to open the **Control Structure**.

    c.   Use the Object Browser to navigate to:

       `Root > Asset Optimization`

    d.   Select `Afw OPC-DA Asset Monitor Data Source` in the Aspect List Area.

    e.   Record the value of **OPC Group Update Rate (ms)** shown in the Preview Area. This value must be reconfigured after the upgrade.

2. If using Maximo Integration, it is necessary to record the values of the Maximo Equipment ID Provider Properties, as these values will not be upgraded. Refer to **Maximo Server Connection Properties** in the System Setup section of *Industrial IT, 800xA - Asset Optimization, Configuration (3BUA000118Rxxxx)* to access these values.

Back Up Data to Safe Media

Use the following procedure to back up Asset Optimization information (perform only the steps applicable to the system):

1. Asset Monitoring:

    Asset Monitoring directories will be found on the Asset Optimization Server node.

    a.   If Runtime Asset Monitors are being used in the system, save the Runtime Asset Monitor data directory (DeviceRunTimeMSLogicStore) to a safe media. The Runtime Asset Monitor data directory is located in:

       `...\Program Files\ABB Industrial IT\Optimize IT\Asset Optimization\AssetMonitorEnvironment\Bin`

    b.   If XY Profile Deviation Asset Monitors are being used in the system, save the XY Profile Deviation Asset Monitor data directory (XY_Reference_Profiles) to a safe media. The XY_Reference_Profiles directory is located in:

       `...\Program Files\ABB Industrial IT\Optimize IT\Asset Optimization\AssetMonitorEnvironment\Bin`

2.   Save Maximo Integration:

If using Maximo Integration, the Maximo Integration information ***must*** be saved from all Asset Optimization Server nodes. Reference the **Service Structure** for the name of the Asset Optimization Server nodes.

a.   Although the Maximo system is separate from the 800xA System, it is a good idea to back up the system in use. Follow Maximo standard practices for Maximo system backup.

b.   If the MxDef files were customized per the instructions in *Industrial IT, 800xA - Asset Optimization, Configuration (3BUA000118Rxxxx)*, back up the customized MxDef files to safe media.

The customized MxDef files are located in the following directory:

```
...\Program Files\ABB Industrial IT\Optimize IT\Asset
Optimization\ABBAO\Services\MOM\MxDefs\server_name\
app_server
```

Where:

<server_name>\<app_server> is the combination of the **MRO Server Name** and the **MRO Application Server Name** fields from the Maximo Equipment ID aspect. These fields are configured in the **Aspect System Structure** in the Maximo Equipment ID aspect. These fields allow for customization of MxDef files on the Maximo Server level as well as on the Maximo Application Server level. Refer to the Maximo documentation for an explanation of Maximo Application Servers.

For example, the resultant path to the customized MxDef files will look like:

```
...\Program Files\ABB Industrial IT\Optimize IT\Asset
Optimization\ABBAO\Services\MOM\MxDefs\Maximo5\
MxServer
```

3.   DMS Calibration Integration. If DMS Calibration Integration is used:

Restore DMS Calibration Integration information. Refer to the *Meriam Process Technologies Device Management System User's Guide* for information about restoring DMS Server data.

ℹ️ Asset Optimization DMS Calibration Integration SV 5.0 SP2 functions with DMS software Version 2.6.

PC, Network and Software Monitoring

Use the following procedure to prepare for the PC, Network and Software Monitoring upgrade.

1. If there are user defined Script, Resource, and Assembly files they need to be backed up. The user files are located in:

   ```
   ...\Program Files\ABB Industrial IT\Optimize IT\
   PC, Network and Software Monitoring\bin\Configuration\
   Scripts\User
   ```

   ```
   ...\Program Files\ABB Industrial IT\Optimize IT\
   PC, Network and Software Monitoring\bin\Configuration\
   Assemblies\User
   ```

   ```
   ...\Program Files\ABB Industrial IT\Optimize IT\
   PC, Network and Software Monitoring\bin\Configuration\
   Resources\User directory
   ```

   Copy the files in these directories to a safe location.

2. Shut down the PC, Network and Software Monitoring Server node.

   a. Use the Structure Selector to open the **Service Structure** in the Plant Explorer Workplace.

   b. Use the Object Browser to navigate to:

      Services > OpcDA_Connector, Service > SG_IT Server, Service Group > OPCDA_Provider_Node Name, Service Provider

      (where Node Name is the name of the PC, Network and Software Monitoring Server node).

   c. Select `Service Provider Definition` in the Aspect List Area.

   d. Click the **Configuration** tab to produce a view in the Preview Area.

e.   If the **Enabled** check box is enabled, disable it and click **Apply**.

SMS and e-mail Messaging

Save all GSM Device hardware information. Record information for the GSM device on the SMS and e-mail Messaging GSM Hardware Setup Worksheet shown in Table 2.

Table 2. SMS and e-mail Messaging GSM Hardware Setup Worksheet

Item	Setting/Value
Spooler Settings	
Activate Outbox Spooler	Checked (check and leave checked)
Activate Inbox Spooler	Checked (check and leave checked)
Interval for Checking for Incoming Messages	Value: _____ Seconds Minutes (circle 1)
Port Settings	
COM Port	Value: COM _____
Baud Rate	Value: _____
Data Bits	Value: _____
Parity	Value: _____
Stop Bits	Value: _____
PIN and Properties	
Query PIN	Checked or Unchecked (circle one)
PIN (only if Query PIN is checked)	Value: _____
Save PIN (only if Query PIN is checked)	Checked or Unchecked (circle one)
Own Number (telephone number of SIM card (including Country Code) in GSM hardware)	Value: _____

Table 2. SMS and e-mail Messaging GSM Hardware Setup Worksheet (Continued)

Item	Setting/Value
Initialization String for GSM Hardware	Value: _____ _____ _____ _____
General Service Properties	
Name (GSM service provider)	Value: _____
Port	Value: COM _____
SMSC	Value: _____
Default Country Code	Value: _____
Default Prefix	Value: _____
Number of Attempts	Value: _____
Splitting Service Properties	
Splitting	Checked or Unchecked (circle one)
Optimize Splitting	Checked or Unchecked (circle one)
Enumerate Splitting	Checked or Unchecked (circle one)
Narrowband Sockets	Checked or Unchecked (circle one)
Messaging Service Properties	
Add Before Message	Blank (verify and do not change)
Use for Delivery Notification Only	Unchecked (verify and do not change)
Default Option	0 (verify and do not change)
Message General Properties	
Replace CR LF for Incoming Messages	Checked or Unchecked (circle one)

Batch Management

1. Verify all scheduled batches are completed or terminated.

2. To archive batch history, select the batch history archive aspect. By default a Batch History Archive aspect is located in:

    ```
    Library Structure > Batch Management, Overviews
    ```

    The Batch History Archive window contains the **Batch Selection** and **Archive Destination** tabs. However, this aspect can be added to any 800xA system object.

    During the course of each batch process run, data that documents details about that specific batch is gathered and stored by the system in the batch database until manually removed. Data that has been archived can still be retained in the batch database. However, once data associated with a batch has been archived and placed in a safe place, the data for that batch should be removed from the batch database.

    Archiving batch data has no effect on the uniqueness of the batch ID. Even after data associated with a batch ID has been removed from the system, a record of the batch ID will be retained on the system. The batch ID can never be reused.

    Do not archive directly to or restore directly from CDs or DVDs. Archive to or restore from hard disk drives which can be backed up to CDs or DVDs using commercially available software.

3. Use the Batch Management backup/restore utility to back up and PFC color configuration information and batch IDs. Access this utility by selecting:

    Start > Programs > ABB Industrial IT > 800xA System > Batch Management > Backup Restore

    Enabling any of the options listed in the backup/restore utility enables the **Backup** and **Restore** buttons.

    The options are:

    –   PFC color configuration.
    –   Batch IDs.

When **Backup** is selected, a standard Open File window that allows browsing to any desired folder is presented. A confirmation window provides the chance to cancel before the backup file is written.

4. Disable the Batch Alarm & Event Service Group and Batch Service Group before proceeding. To disable the service groups:

   a. Open a Plant Explorer Workplace.

   b. Use the Structure Selector to open the **Service Structure**.

   c. Use the Object Browser to select:

      `Services\Alarm & Event, Service\batch_group_name, Service Group`

   d. Select `Service Group Definition` in the Aspect List Area.

   e. Select the **Configuration** tab in the Preview Area.

   f. Disable the **Enabled** check box and click **Apply**.

   g. Determine the name of the nodes that are currently Primary and Secondary Batch Servers,

   h. Use the Object Browser to select:

      `Services\Batch Service, Service\batch_group_name, Service Group`

   i. Select `Service Group Definition` in the Aspect List Area.

   j. Select the **Configuration** tab in the Preview Area.

   k. Select the provider that is currently the Secondary Batch Server.

   l. Disable the **Enabled** check box and click **Apply**.

   m. Select the provider that is currently the Primary Batch Server.

   n. Disable the **Enabled** check box and click **Apply**.

Information Management

Perform the following procedures to prepare for the Information Management upgrade.

End Microsoft Excel Process via Windows Task Manager

Use Windows Task Manager to manually end the EXCEL.EXE process.

Recording Archive Group Associations

Archive Groups are associated with Profile, Message, and Report logs.

1. Record these associations so that after the upgrade, these logs can be reassociated with their respective Archive Groups. Refer to the **Reading and Managing Archive Data** section in *Industrial IT, 800xA - Information Management, Data Access and Reports (3BUF001094Rxxxx)* to access the Archive Groups and record the information.

2. Back up the path to Archive Group Numeric Log Entry and IM Objects Entry.

ABB Process Administration Server (PAS)

Perform the following procedure to run the PAS utility.

1. Run the Process Administration Service (PAS) utility on the Information Management Application Server node. From the Windows Taskbar select:

    > **Start > Settings > Control Panel > Administrative Tools > PAS > Process Administration**

    This opens the Process Administration Service dialog.

2. Click **Stop All** to stop all processes under PAS supervision.

3. Click **Close** when the dialog indicates that all processes are stopped.

4. Use standard Windows procedures, via the Services selection from Administrative Tools in Windows Control Panel, to place the ABB Process Administration Service into manual and insure that it is stopped.

Information Management Backup and Restore Utility

Use the Information Management History Backup/Restore utility, via:

> **Start > Programs > ABB Industrial IT 800xA > Information Mgmt > History > Backup and Restore**

to create all the backup files that are required to completely back up the Information Management History database. This includes all configuration data, log data from both file-based and ORACLE-based logs, and the Aspect System definition file.

During a backup operation, all data in the Oracle database owned by the Oracle History user is exported to the specified destination and compressed into a zipped archive, along with any files that have been created to store file-based property log entries (called flat files).

The History database can be backed up to any drive on the workstation, including any mapped network drives. The database may also be divided among several drives (different files may be located on different drives on the workstation). This may occur, for example, if the History quota is exceeded on one of the drives, forcing any remaining History database files to be stored on a different drive.

To avoid any ambiguity, the backup operation produces a zipped archive of compressed History database files for each drive that contains at least some portion of the database, where each archive contains only the database files that are stored on the corresponding drive. The backup utility uses the naming convention *name-drive*.zip for the zipped archives that it produces. For example, if the History database is located entirely on the C:\ drive and you wish to back up the database to a zipped archive called hist, the backup operation will compress the database files into a zipped archive named `hist-C.zip`.

If the data files exceed two gigabytes, or if there are more than 25,000 files, then multiple zip files will be created using the following naming convention:

- First File*name-drive*.zip
- Next File*name-drive0001*.zip
- Next File*name-drive0002*.zip

When backing up the History database, make sure the disk is ready and available on the workstation on which the procedure is to occur. The log file should be checked after the backup operation to make sure that the backup operation completed successfully.

> It is recommended that the history database be cleaned before making the backup. Open a Windows Command Prompt window and enter **hsDBMaint -clean**.

Make sure the system Archive is not getting full. Temp space is required to make the backup. If the log file indicates that the Oracle export failed, use the option to export to a disk with more space.

To make a backup:

1.   Select:

> Start > Programs > ABB Industrial IT 800xA > Information Mgmt >
> History > Backup and Restore

2.   Verify the **Create Backup Files of Current Configuration** option is enabled in the IM Historian Backup/Restore Utility window.

3.   Click **Next**. A window for setting up the backup operation is displayed.

4.   Specify the location where the backup files are to be created in the New Directory Path for the Backup field. This path must already exist and the directory must be empty. If necessary, click **Browse** to create a new directory. Add a D:\HSDATA\History as an additional option.

The backup of the History data must be in a directory of its own, not the D:\HSDATA\History directory. If the data is put into the D:\HSDATA\History directory, it will get lost.

5.   Verify the Only Generate Aspect Definition File option is disabled.

6.   Click **Next**. The HsBAR Output Window is displayed.

7.   Enable the Automatically Close Upon Completion option.

8.   After the HsBAR Output Window closes, monitor the progress in the Progress Status area of the IM Historian Backup/Restore Utility window and click **Finish** when the backup is complete.

If a message appears stating that there are inconsistencies between the log configurations in the Aspect System and the log configurations in Oracle, it may be because the database was not cleaned before running the backup. Use the hsDBMaint Clean function to clean the database and then rerun the backup. If this does not fix the problem, contact ABB Technical Support for further assistance.

Saving Other Information Management Related Files

There are several other files related to Information Management to be saved as part of a total system backup.

- **History Archive Data:** For each archive device, go to the location specified by the Device Filename and copy the folders under that directory to a safe location. Do this even if automatic backup is configured.

- **History Archive State Information:** The folder that holds the last archive time and other archive state information must be copied to a safe location. The folder name is `Archive` and it is located in:

  ```
  ...\Documents and Settings\All Users\
  Application Data\ABB\IM\Archive
  ```

  Copy the entire folder.

- **Reports:** Save any report template files created in Microsoft Excel, DataDirect, and/or Crystal Reports®. Also save report output files created as a result of running these reports via the Scheduling Services.

- **Desktop Trends:** Back up trend display, ticker display, and tag explorer files.

  – Ticker files are located in:

  ```
  ...\My Documents\ABB Industrial IT\Inform IT\Desktop
  Trends\Ticker Files
  ```

  – Trend Files are located in:

  ```
  ...\My Documents\ABB Industrial IT\Inform IT\Desktop
  Trends\HTML
  ```

  – Tag Explorer files are located in:

  ```
  ...\Documents and Settings\~username\Application
  Data\ABB Industrial IT\Inform IT\Desktop Trends
  ```

- **Display Services:** Back up the directories for custom users, as well as display and user element definitions. The files are located in:

  ```
  ...\Program Files\ABB Industrial IT\Inform IT\Display
  Services\Server\Data
  ```

  Save the user-built svg and vet files.

- **DataDirect:** Back up custom text files for object, object type, and attribute menus used on the DataDirect windows. The files are located in:

```
...\Program Files\ABB Industrial IT\Inform IT\Data
Direct\etc.
```

Save the user-built text files.

Scheduler Service (Application Scheduler)

Disable Schedules before stopping the servers and performing the upgrade. The Schedules will need to be manually enabled again following the upgrade.

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Service Structure**.

3. Select the Scheduling Service Object.

4. Select the Service Definition aspect.

5. Click the **Configuration** tab.

6. Disable the **Enabled** check box and click **Apply**.

Calculations Service

Disable Calculations before stopping the servers and performing the upgrade.

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Service Structure**.

3. Select the Calculations Service Object.

4. Select the Service Definition aspect.

5. Click the **Configuration** tab.

6. Disable the **Enabled** check box and click **Apply**.

Basic History Service Data

Depending on the system, the Basic History Service data can be present on a number of different node types (Connectivity Servers, IM Servers, AO Servers, etc.). It is best to search for the directory described in this procedure on all nodes, and if there is data present, back up that data.

To save Basic History Service data:

1. Stop the Basic History Server from the **Service Structure**.

2. Use Windows Backup (not the 800xA Backup) to backup the files in the following directory:

    ```
    ...\OperateITData\History\{provider ID}
    ```

3. Start the Basic History Server again from the **Service Structure**.

Alarm and Event List Configurations

Alarm and Event handling has changed significantly from SV 4.1 to SV 5.0 SP2 (refer to Alarm and Event List Configurations on page 49). Document list configurations in the SV 4.1 system, so they can be checked against the list configurations in the SV 5.0 SP2 system.

System Upgrade (Upgrade Flow B)

The upgrade procedures differ if upgrading a Domain Controller node or if upgrading any other type of 800xA System node.

Domain Controller Nodes

The Microsoft Windows Operating Systems supported for Domain Controller nodes in SV 5.0 SP2 are:

•   Windows Server 2003 R1 with SP2.
•   Windows Server 2003 R2 with SP2.

If using Windows Server 2003 R2 with SP2, unless otherwise specified, do not enable any Windows components that are not enabled in the default installation.

The following procedures detail how to manually upgrade a Domain Controller node. There are three different scenarios:

•   Upgrading Domain Controller Node and OS without Formatting Hard Disk.
•   Upgrading Domain Controller Node with Compatible OS.
•   Upgrading Domain Controller Node by Formatting Hard Disk.

Upgrading Domain Controller Node and OS without Formatting Hard Disk

To upgrade a Domain Controller node and its Operating System from Windows 2000 Server to Windows Server 2003 without disturbing the Active Directory, follow the instructions in the following Microsoft KB Article:

http://support.microsoft.com/kb/325379

After upgrading the Operating System, perform the following procedure on the Domain Controller node:

1. Use Add/Remove Programs via Windows Control panel to uninstall 800xA System software.

    800xA System software can be identified by items that mention ABB or 800xA in Add/Remove Programs.

2. Install Windows Server 2003 SP2 on Windows Server 2003 nodes. Follow the procedures provided by Microsoft to install the Windows Operating System service packs.

3. Install Internet Explorer. Follow the procedures provided by Microsoft to install Internet Explorer.

4. Disable Internet Explorer Enhanced Security Configuration on Windows Server 2003 nodes if using Internet Explorer 7.0 (refer to Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62).

5. Disable Windows Firewall.

6. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and install additional third party software, updates, and service packs for this release approved by ABB. This document is accessible from ABB SolutionsBank.

    The System Checker Tool is a standalone tool delivered with the 800xA System. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System, including third party software. The installation and use of the System Checker is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**.

7.   Refer to Group Policy Management for Upgrades on page 63 and configure the Group Policy Object.

8.   Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and apply updates and hot fixes approved by ABB to the existing Operating System. This document is accessible from ABB SolutionsBank.

9.   Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install all required 800xA System software.

    –   ABB RNRP.
    –   ABB Diagnostic Collection Tools.
    –   ABB System Checker Tool.

10.   Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* and configure Windows Firewall.

Upgrading Domain Controller Node with Compatible OS

Perform the following procedure when upgrading a Domain Controller node with a compatible Operating System (Windows 2003 Server):

1.   Disjoin all 800xA System nodes from the Domain Controller by joining them to a Windows Workgroup.

2.   Use Add/Remove Programs via Windows Control panel to uninstall 800xA System software.

> 800xA System software can be identified by items that mention ABB or 800xA in Add/Remove Programs.

3.   Install Windows Server 2003 SP2 on Windows Server 2003 nodes. Follow the procedures provided by Microsoft to install the Windows Operating System service packs.

4.   Install Internet Explorer. Follow the procedures provided by Microsoft to install Internet Explorer.

5.   Disable Internet Explorer Enhanced Security Configuration on Windows Server 2003 nodes if using Internet Explorer 7.0 (refer to Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62).

6. Disable Windows Firewall.

7. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and install additional third party software, updates, and service packs for this release approved by ABB. This document is accessible from ABB SolutionsBank.

> The System Checker Tool is a standalone tool delivered with the 800xA System. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System, including third party software. The installation and use of the System Checker is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**.

8. Refer to Group Policy Management for Upgrades on page 63 and configure the Group Policy Object.

9. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and apply updates and hot fixes approved by ABB to the existing Operating System. This document is accessible from ABB SolutionsBank.

10. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install all required 800xA System software.

    – ABB RNRP.
    – ABB Diagnostic Collection Tools.
    – ABB System Checker Tool.

11. Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* and configure Windows Firewall.

Upgrading Domain Controller Node by Formatting Hard Disk

Perform the following procedure when upgrading a Domain Controller node by formatting the hard disk:

ℹ️ Perform the procedures detailed under the following topics in **Section 2 - Prerequisites** of *Industrial IT, 800xA - System, Installation (3BSE034678R5021)* to create the Active Directory:

- Domain Controller and DNS Server.
- Users and Groups.
- Adding Nodes to a Domain.
- Adding 800xA Domain Users to the Local Administrator Group.

Precautions:

- Disjoin all 800xA System nodes from the Domain Controller by joining them to a Windows Workgroup.

- The IP address of the original domain must be used when configuring the new Domain Controller.

- The Domain Name of the original domain must be used when configuring the new Domain Controller.

- The User and Group names of the original domain must be used when configuring the New Domain controller.

Perform the following procedure after creating the active directory:

1. Install Windows Server 2003 SP2 on Windows Server 2003 nodes. Follow the procedures provided by Microsoft to install the Windows Operating System service packs.

2. Install Internet Explorer. Follow the procedures provided by Microsoft to install Internet Explorer.

3. Disable Internet Explorer Enhanced Security Configuration on Windows Server 2003 nodes if using Internet Explorer 7.0 (refer to Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62).

4. Disable Windows Firewall.

5.   Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and install additional third party software, updates, and service packs for this release approved by ABB. This document is accessible from ABB SolutionsBank.

The System Checker Tool is a standalone tool delivered with the 800xA System. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System, including third party software. The installation and use of the System Checker is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**.

6.   Refer to Group Policy Management for Upgrades on page 63 and configure the Group Policy Object.

7.   Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and apply updates and hot fixes approved by ABB to the existing Operating System. This document is accessible from ABB SolutionsBank.

8.   Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install all required 800xA System software.

    –   ABB RNRP.
    –   ABB Diagnostic Collection Tools.
    –   ABB System Checker Tool.

Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* and configure Windows Firewall.

800xA System Nodes

The Microsoft Windows Operating Systems supported in SV 5.0 SP2 are:

Refer to *Industrial IT, 800xA - System, System Guide, Technical Data and Configuration Information (3BSE041434Rxxxx)* for specific information on what node types can be installed on each Operating System.

•   Windows XP Professional with SP2.
•   Windows Server 2003 R1 with SP2.

- Windows Server 2003 R2 with SP2.

> ⚠ If using Windows Server 2003 R2 with SP2, unless otherwise specified, do not enable any Windows components that are not enabled in the default installation.

The following rules apply:

- Any existing nodes that do not have one of these Operating Systems must be reformatted and the compatible Operating System must be installed.

- All IM (Information Management) and 800xA for Melody Server nodes being upgraded must be reformatted and the Operating System installed, even if the existing Operating System is compatible.

- All nodes being upgraded, that are not IM or 800xA for Melody Server nodes, with a compatible Operating System require that the existing Operating System be updated.

- If PROFIBUS/HART Device Integration functionality is installed in the 800xA System, all nodes being upgraded must be reformatted and the Operating System installed.

Refer to Upgrade Flow on page 22 for more information.

Existing Operating System

> ⚠ The installation will fail unless all Information Management Server, and 800xA for Melody Connectivity and Configuration Server nodes being upgraded are reformatted and the Operating System installed. This is true even if the existing Operating System is compatible. Refer to New Operating System on page 60.

If upgrading using an existing Operating System:

1. Close all open Windows.

2. Use Configuration Wizard to disconnect each client from the 800xA System. This task is only visible in the Configuration Wizard on a client node when the client node is connected to the 800xA System.

   a. Launch the Configuration Wizard.

   b. Select **Disconnect Client** and click **Next**.

    c.   Choose the 800xA System from which to disconnect the client node and click **Next**.

    d.   Click **Finish**. The client node is now disconnected from the 800xA System.

3.   Use Configuration Wizard from one of the server nodes to stop the 800xA System.

    a.   Launch the Configuration Wizard.

    b.   Select **System Administration** and click **Next**.

    c.   Select the 800xA System to stop and click **Next**.

    d.   Select **Systems** and click **Next**.

    e.   Select **Stop** in the Systems dialog and click **Next**.

    f.   Click **Finish** in the Apply Settings dialog.

4.   Exit the Batch Redundancy Status by right-clicking the Batch Redundancy Status icon in the Windows tray (P, S, or C) and choosing **Exit** from the context menu (Figure 5).

Figure 5. Stopping the Batch Redundancy Status

5.   Delete the system on each node.

    a.   Launch the Configuration Wizard.

    b.   Select **System Administration** and click **Next**.

    c.   Select the 800xA System to delete and click **Next**.

    d.   Select **Systems** and click **Next**.

    e.   Select **Delete** in the Systems dialog and click **Next**.

    f.   Click **Finish** in the Apply Settings dialog.

g. Wait a few minutes. When the Configuration Wizard appears with the Systems dialog box the deletion of the system is complete.

h. Click **Exit**.

6. The System Services listed must be stopped at each individual 800xA System node. Stop these services in a controlled manner in the following sequence:

– 800xA System Clients.
– 800xA System Connectivity Servers.
– 800xA System Aspect Servers.

a. Use standard Windows procedures, via the Services selection from Administrative Tools in Windows Control Panel, to place the following services into manual and insure that they are stopped.

– ABB Application logger.
– ABB Client License Provider.
– ABB MMS Server for AC 800M.
– ABB OPC Server for AC 800M.
– ABB ServiceManager.
– ABB System Notification Icon.
– ABB Tool Routing Service for AC 800M.

b. Use the afwkill utility (Figure 6) to make sure all processes related to the 800xA System are stopped. From the Windows Taskbar select:

Start > Programs > Accessories > Command Prompt
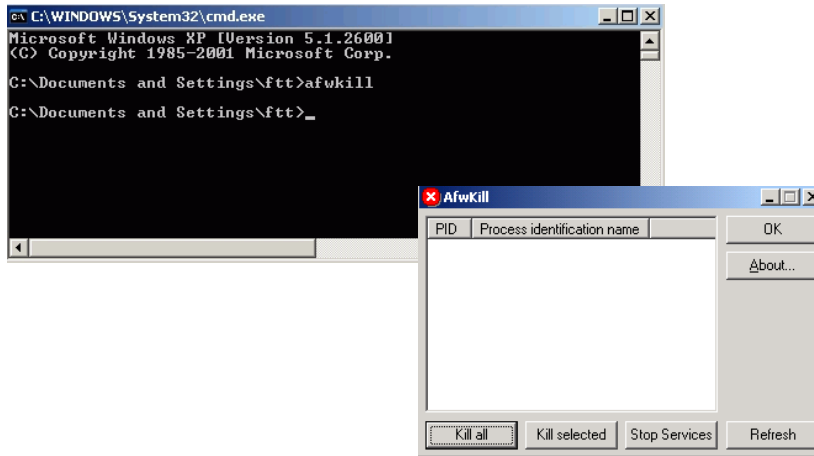
Figure 6. Running the afwkill Utility

    c.   In the Command Prompt window enter **`afwkill`**.

    d.   The afwkill window should be empty, indicating that all processes are stopped. In this case click **OK** to close.

        If processes are listed in this window, click **kill all**, then click **OK** when the window indicates all processes are stopped (empty window).

7.   Use Add/Remove Programs via Windows Control panel to uninstall 800xA System and Functional Area software. Remove the application software before the base system software.

> ℹ   There may be some 800xA software on nodes (such as 800xA RNRP on the Domain Controller node) that does not include Process Portal software. The 800xA software on these nodes also requires upgrading.

> ℹ   800xA System and Functional Area software can be identified by items that mention ABB or 800xA in Add/Remove Programs.

8.   Manually delete the following folder:

```
...:\Documents and Settings\All Users\Start Menu\
Programs\ABB Industrial IT 800xA\System\Network
```

9. Reboot the workstation after all 800xA System and Functional Area software has been removed.

10. Install Windows Server 2003 SP2 on Windows Server 2003 nodes. Follow the procedures provided by Microsoft to install the Windows Operating System service packs.

11. Install Internet Explorer. Follow the procedures provided by Microsoft to install Internet Explorer.

12. Disable Internet Explorer Enhanced Security Configuration on Windows Server 2003 nodes if using Internet Explorer 7.0 (refer to Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62).

13. Disable Windows Firewall on every node in the 800xA System.

14. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and install additional third party software, updates, and service packs for this release approved by ABB. This document is accessible from ABB SolutionsBank.:

The System Checker Tool is a standalone tool delivered with the 800xA System. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System, including third party software. The installation and use of the System Checker is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**.

15. Refer to Group Policy Management for Upgrades on page 63.

16. Refer to Adding Privileges to the 800xA Service User on page 69.

17. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and apply updates and hot fixes approved by ABB to the existing Operating System. This document is accessible from ABB SolutionsBank.

18. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install the License Server on the primary Aspect Server node and install the license file.

19. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install all required 800xA System software.

> If Production Management - Batch Management software is being installed, initialize the Batch database during installation of the Production Management - Batch Management software.

20. Refer to Setting the PAS and IM Service Account and Password on page 70 and perform that procedure before performing the 800xA System restore.

21. Refer to 800xA System Restore (Upgrade Flow C) on page 70 of this instruction and perform all necessary steps.

22. Perform all steps that pertain to the installed applications from 800xA Documentation Maintenance on page 73 through the remainder of this section in the order presented.

23. Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* and perform all applicable post installation steps, including configuring Windows Services and Windows Firewall.

24. Refer to Backups on page 28 and perform precautionary backups.

New Operating System

If upgrading using a new Operating System:

> If formatting the Domain Controller node, disconnect all 800xA System nodes from the Domain by joining them to a Windows workgroup before formatting the Domain Controller node.

> There may be some 800xA software on nodes (such as 800xA RNRP on the Domain Controller node) that does not include Process Portal software. The Operating System and 800xA software on these nodes also requires upgrading.

1. Reformat the drive.

2. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install the new Operating System.

3. Install Windows Server 2003 SP2 on Windows Server 2003 nodes. Follow the procedures provided by Microsoft to install the Windows Operating System service packs.

4. Install Internet Explorer. Follow the procedures provided by Microsoft to install Internet Explorer.

5. Disable Internet Explorer Enhanced Security Configuration on Windows Server 2003 nodes if using Internet Explorer 7.0 (refer to Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62).

6. Disable Windows Firewall on every node in the 800xA System.

7. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and install additional third party software, updates, and service packs for this release approved by ABB. This document is accessible from ABB SolutionsBank.:

The System Checker Tool is a standalone tool delivered with the 800xA System. It is designed for the purpose of checking, verifying, documenting, and troubleshooting an 800xA System, including third party software. The installation and use of the System Checker is described in *Industrial IT, 800xA - System, Tools (2PAA101888Rxxxx)*. The installation program is accessible from the Manual Installation AUTORUN screen via **Base Functionalities > Diagnostic Tools > System Checker Tool**.

8. Refer to Group Policy Management for Upgrades on page 63.

9. Refer to Adding Privileges to the 800xA Service User on page 69.

10. Refer to *Third Party Software System 800xA (3BUA000500Rxxxx)* and apply updates and hot fixes approved by ABB to the existing Operating System. This document is accessible from ABB SolutionsBank.

11. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install the License Server on the primary Aspect Server node and install the license file.

12. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* and install all required 800xA System software.

13. Refer to Setting the PAS and IM Service Account and Password on page 70 and perform that procedure before performing the 800xA System restore.

14. Refer to 800xA System Restore (Upgrade Flow C) on page 70 of this instruction and perform all necessary steps.

15. Perform all steps that pertain to the installed applications from 800xA Documentation Maintenance on page 73 through the remainder of this section in the order presented.

16. Refer to *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)* and perform all applicable post installation steps, including configuring Windows Services and Windows Firewall.

17. Refer to Backups on page 28 and perform precautionary backups.

Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0

This procedure only applies to Windows Server 2003 installations using Internet Explorer 7.0.

Windows Server 2003 with SP2 and Internet Explorer 7.0 must be installed prior to performing the following procedure.

The Internet Explorer Enhanced Security component must be disabled on all Windows Server 2003 with SP2 nodes in the 800xA System.

1. Select:

   Start > Control Panel

2. Double-click **Add/Remove Programs** to launch the Add or Remove Programs utility.

3. Click **Add/Remove Windows Components** to open the Windows Components Wizard.

4. In the Components list, disable the **Internet Explorer Enhanced Security Configuration** check box.

5. Click **Next** and then **Finish**.

Group Policy Management for Upgrades

The procedures differ depending on the environment (domain or Windows Workgroup).

Domain Environment

Perform this procedure before installing 800xA System and Functional Area software.

When upgrading from SV 4.1 to SV 5.0 SP2, it is necessary to add the SV 5.0 SP2 Group Policy on the Domain Controller node. It is also necessary to run a command on every other 800xA System node to force the new Group Policy Object from the Domain Controller down to each node.

Domain Controller Node

1. Insert 800xA System Installation DVD 1 into the drive.

2. Use Windows Explorer to locate `gpmc.msi` in the following directory:

        3rd_Party_SW\Microsoft

3. Double-click `gpmc.msi` to install the Group Policy Management Console with SP2. Follow the instructions in the Installation Wizard to complete the installation.

4. When the Group Management Console with SP 1 installation is complete, from the Windows Taskbar, select:

        Start > Run

5. Enter `dsa.msc` in the Run dialog and click **OK** to open the Active Directory Users and Computers dialog.

6. In the left pane of the Active Directory Users and Computers dialog, right-click the domain name and select **Properties** from the context menu to open the Domain Properties dialog.

7. Select the **Group Policy** tab in the Domain Properties dialog.

8.   Click **Open** to open the Group Policy Management Console.

⚠️ ***Do not*** modify the default Group Policy Object itself. Create, link and modify a new Group Policy Object.

9.   In the left pane of the Group Policy Management Console, right-click the domain name and select **Create and Link a GPO Here...** from the context menu to open the New GPO dialog.

10. Type in a name for the new Group Policy Object in the New GPO dialog; for example, `IntranetName` and click **OK** to return to the Group Policy Management Console.

11. In the right pane of the Group Policy Management Console, right-click on the new Group Policy Object and select **Edit** from the context menu to open the Group Policy Object Editor.

12. In the left pane of the Group Policy Object Editor, navigate to:

```
User Configuration > Windows Settings > Internet
Explorer Maintenance > Security
```

13. In the right pane of the Group Policy Object Editor, double-click:

```
Security Zones and Content Ratings
```

to open the Security Zones and Content Ratings dialog (Figure 7).
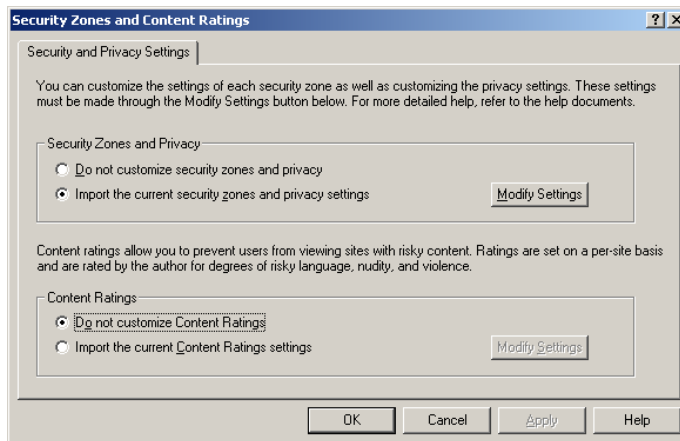
Figure 7. Security Zones and Content Ratings Dialog

14. Select **Import the current security zones and privacy settings** in the Security
     Zones and Privacy frame. Since Internet Explorer Enhanced Security was
     disabled under Disable Internet Explorer Enhanced Security Configuration for
     Windows Server 2003 Using Internet Explorer 7.0 on page 62, making this
     selection will open the Internet Explorer Enhanced Security Configuration

dialog shown in Figure 8.
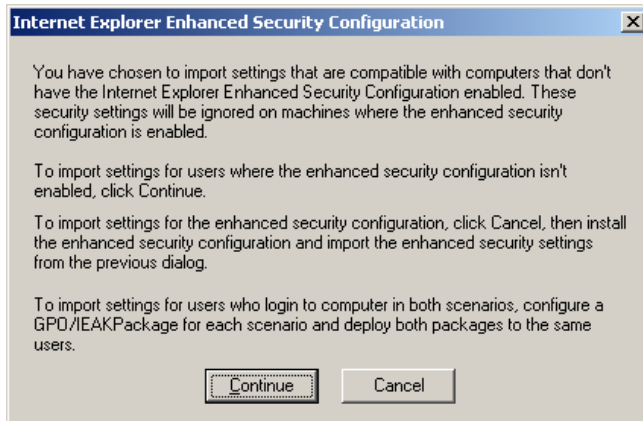
Figure 8. Internet Explorer Enhanced Security Configuration Dialog

15. Click **Continue** in the Internet Explorer Enhanced Security Configuration
    dialog to close the dialog and return to the Security Zones and Content Ratings
    dialog (Figure 7).

16. Click **Modify Settings** in the Security Zones and Content Ratings dialog to
    open the Internet Properties dialog.

17. Click the **Security** tab.

18. Select the Local Intranet icon.

19. Click **Sites** to open the Local Intranet dialog (Figure 9).
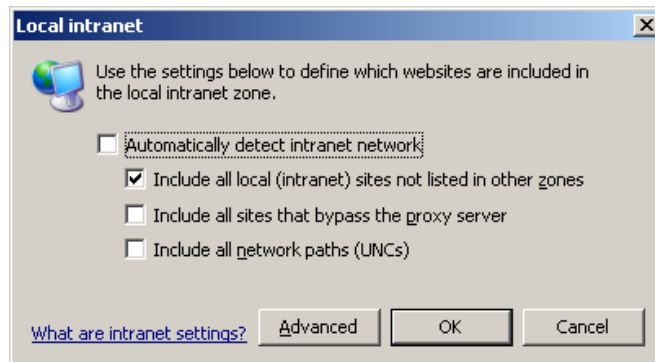
Figure 9. Local Intranet Dialog

20. Disable the **Automatically detect intranet network** check box.

21. Enable the **Include all local (intranet) sites not listed in other zones** check box.

22. Verify that all other check boxes are disabled.

23. Click OK three times to close all open dialogs.

24. Close the Group Policy Object Editor.

25. Reboot the node.

26. Return to

All Other 800xA System Nodes

1. From the Windows Taskbar, select:

> **Start > Run**

2. Enter **gpupdate /force** in the Run dialog and click **OK**. This forces the new Group Policy Object from the Domain Controller down to this node.

3.   Return to Adding Privileges to the 800xA Service User on page 69.

> If the system is expanded at a later time, this procedure must be performed on each node added during the expansion.

Windows Workgroup Environment

> Perform this procedure before installing 800xA System and Functional Area software.

This procedure must be performed on every node in the Windows Workgroup. If the system is expanded at a later time, this procedure must be performed on each node added during the expansion.

1.   From the Windows Taskbar, select:

> **Start > Run**

2.   Enter **`gpedit.msc`** in the Run dialog and click **OK** to open the Group Policy Object Editor.

3.   In the left pane of the Group Policy Object Editor, navigate to:

> `User Configuration > Windows Settings > Internet Explorer Maintenance > Security`

4.   In the right pane of the Group Policy Object Editor, double-click:

> `Security Zones and Content Ratings`

to open the Security Zones and Content Ratings dialog (Figure 7).

5.   Select **Import the current security zones and privacy settings** in the Security Zones and Privacy frame. Since Internet Explorer Enhanced Security was disabled under Disable Internet Explorer Enhanced Security Configuration for Windows Server 2003 Using Internet Explorer 7.0 on page 62, making this selection will open the Internet Explorer Enhanced Security Configuration dialog shown in Figure 8.

6.   Click **Continue** in the Internet Explorer Enhanced Security Configuration dialog to close the dialog and return to the Security Zones and Content Ratings dialog (Figure 7).

7.   Click **Modify Settings** in the Security Zones and Content Ratings dialog to open the Internet Properties dialog.

8.   Click the **Security** tab.

9.   Select the Local Intranet icon.

10.   Click **Sites** to open the Local Intranet dialog (Figure 9).

11.   Disable the **Automatically detect intranet network** check box.

12.   Enable the **Include all local (intranet) sites not listed in other zones** check box.

13.   Verify that all other check boxes are disabled.

14.   Click OK three times to close all open dialogs.

15.   Close the Group Policy Object Editor.

16.   Reboot the node.

17.   Return to

Adding Privileges to the 800xA Service User

This procedure only applies to the following node types. If these node types are not present in the system this procedure can be skipped.
• 800xA for Melody Configuration Server nodes.
• 800xA for Melody Connectivity Server nodes.
• AO Server nodes for Asset Optimization.

There are some services that run under the 800xA Service User account for the listed node types. Perform the following procedure to add the proper privileges to the 800xA Service User account.

1.   Log off the 800xA Installing User account.

2.   Log on the 800xA Service User account.

3.   Log off the 800xA Service User account.

4.   Log on the 800xA Installing User account.

Setting the PAS and IM Service Account and Password

This procedure is only necessary if Information Management is installed in the 800xA System.

The PAS and Information Management (IM) service account and password must be set, via the Information Management Configuration Assistant, before performing the 800xA System restore.

1. To launch the configuration assistant, select:

    **Start > All Programs > ABB Industrial IT 800xA >
    Information Mgmt > Configuration Assistant**

2. Select the first row, `Item 1.0 Set PAS and IM Service Account and Password` and click **Run Selected Configuration Tool**.

3. Perform the indicated actions and click **Close** in the Information Management Configuration Assistant.

> Close the Information Management Configuration Assistant after performing `Item 1.0 Set PAS and IM Service Account and Password`. The rest of the configuration steps will be performed during post installation procedures after completing the software upgrade.

800xA System Restore (Upgrade Flow C)

> The User Account that is used for 800xA System restore via the Configuration Wizard must be a member of the following groups:
> *   IndustrialITUser.
> *   IndustrialITAdmin.
> *   Local Administrators.

The backup/restore utility supports the restoring of 800xA system information. The following steps outline the 800xA system restore procedure. Refer to *Industrial IT, 800xA System, Operator Workplace, Configuration (3BSE030322Rxxxx)* for more detailed information.

1. Start the restore procedure.

> Refer to *Industrial IT, 800xA - System, Administration and Security (3BSE037410Rxxxx)* for more information on restoring the system.

a. Select:

Start > All Programs > ABB Industrial IT 800xA > System > Configuration Wizard

b. The Select Type of Configuration dialog appears. Select **Restore System** and click **Next**.

Restart the node when advised during the restore procedure.

2. Check for messages in the log file (enable the **View Log** check box in the Configuration Wizard). Refer to Appendix A, Warning and Error Messages to resolve any received warning or error messages.

3. Check the CPU load in the workstation. The System Message service may generate a high load (>90%). If this continues for longer than approximately 10 minutes, restart the service.

If a message stating that a full deploy of the Generic Control Network is needed, click **OK**.

4. One node at a time, start up all nodes again and connect them to the 800xA system in the following order:

    – Aspect Server nodes.
    – Connectivity Server nodes.
    – Application Server nodes.
    – Client nodes.

a. Use the following guidelines while connecting nodes, using the Configuration Wizard. This must be performed on the node that is going to be connected, not on the node on which the restore was performed.

b. Select **Connect Node** from the Select Type of Configuration dialog.

c. Set the current system as the default system when connecting nodes to the system.

    – In some cases, problems may be encountered when connecting nodes to the system. Verify that the system software user settings are correct using the Configuration Wizard. Restarting the node again may also solve the problem.

–   Wait until all services in the newly connected node are up and running before connecting the next node. Select the Node Administration Structure\connected_node_name\System Status Viewer aspect to monitor the status of services. If some services will not start up, restarting the node may help.

d.   Restart each node after it has been connected to the system.

Run the System Software User Settings until OK. Restart if it is not working and if the message:

```
Invalid User
```

appears.

5.   Record the number of aspects and objects in the system and compare these values to those recorded when the system was backed up.

a.   Select the `Admin Structure\Adminstrative Objects\Domains\system_name, Domain\Domain Definition` aspect.

b.   Record the number of objects and aspects listed in the System Size Information area of the window.

c.   Right-click the `Control Structure\control_network_name, Control Network\Control Structure` aspect of one of the control networks contained in the system.

d.   Select **Properties** on the context menu.

e.   Select the **Statistics** tab.

f.   Record the number of objects listed.

g.   Right-click the **Control Structure** aspect within a controller project of the control network selected in Step c.

h.   Select **Properties** on the context menu.

i.   Record the number of objects listed.

j.   Repeat Step g through Step i for all the controller projects within the control network.

k.   Repeat Step c through Step j for every control network in the system.

The number of aspects and objects after system restoration should be in the same range as those recorded during system backup, although there will likely be more.

l.   Right-click the Control Structure\HSE_Subnet name, HSE Subnet\Control Structure aspect of one of the HSE Subnets contained in the system.

m.   Select **Properties** from the context menu.

n.   Select the **Statistics** tab.

o.   Record the number of objects listed.

p.   Repeat Step l through Step o for every HSE Subnet in the system.

q.   Right-click the Control Structure\MB300_name, MB300 Network\Control Structure aspect of one of the MB300 Networks contained in the system.

r.   Select **Properties** from the context menu.

s.   Select the **Statistics** tab.

t.   Record the number of objects listed.

u.   Repeat Step q through Step t for every MB300 network in the system.

The number of aspects and objects after system restoration should be in the same range as those recorded during system backup, although there will likely be more.

800xA Documentation Maintenance

Delete all documentation aspects (denoted by an open book icon) with a category name of Application Manual, Operating Manual, Installation Manual, or Technical Reference Manual found in the **Product Type Structure**.

If any customer-specific documentation aspects have been added, it is necessary to browse through the **Product Type Structure** and delete the 800xA documentation aspects individually so that customer-specific documentation will not be accidentally deleted.

Use the Find Tool in the Plant Explorer Workplace to find the documentation aspects.

The System Instructions system extension must be removed (unregistered). To unregister the System Instructions system extension from the 800xA system:

1. Use Windows Explorer to navigate to:

   ```
   ...:\Program File\ABB Industrial IT\Operate IT\Process
   Portal A\bin
   ```

2. Double-click `AfwRemoveSystemInstructions.exe` to execute the program.

Base System Considerations

There are considerations that must be taken into account with respect to alarms and events when working with the SV 5.0 SP2 System. It is important to read and understand the information about Alarm Categories in *Industrial IT, 800xA - System, Administration and Security (3BSE037410Rxxxx)*.

Connections between Alarm List and Alarm and Event OPC Server

This connection is valid only for upgrading of Alarms and Events.

SV 4.1 has one layer between the clients (e.g. an alarm list) and the OPC Alarm and Event Server that provides the alarms. This layer is realized by the Alarm and Event Service, as shown in Figure 10.

T05252B
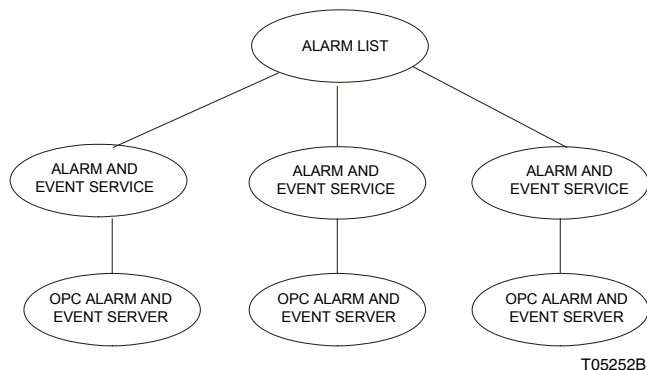
Figure 10. Alarm and Event Service Layer for SV 4.1

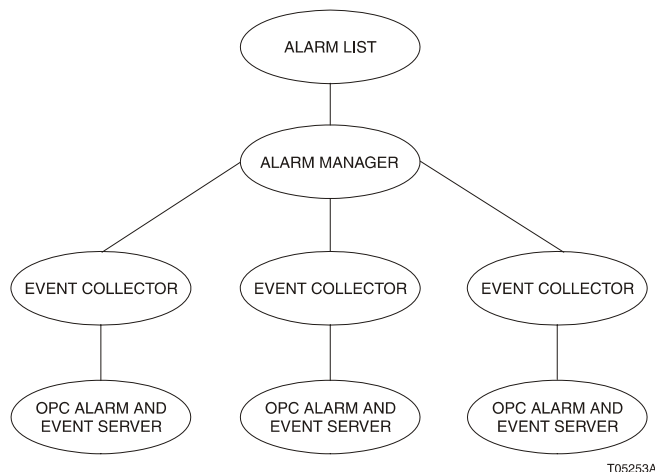SV 5.0 SP2 has two layers, realized by the Alarm Manager which is on top of the Event Collector as shown in Figure 11.

Figure 11. Alarm Manager and Event Collector Layers for SV 5.0 SP2

Automatic Configuration

The object tree below the Alarm and Event Service is recreated below the Event Collector Service. The required library objects are also created.

The Alarm Manager Service is automatically configured. Some manual configuration is also required.

Manual Configuration

Manual configuration consists of several actions.

Configure the Event Collector Service

Manual configuration is required for Event Collectors connected to Connectivity Servers (such as, but not limited to, AC 800M).

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Service Structure**.

3. Use the Object Browser to navigate to:

    `Services > Event Collector, Service Group`

    and expand the tree.

4. Select a Service Group for a Connectivity Server.

5. Select `Service Group Definition` in the Aspect List Area.

6. Select the **Special Configuration** tab in the Preview Area.

7. Check to see if the item in the **Collection Definition** drop-down list box is the the new one that is to be used with SV 5.0 SP2. (The name should not end with (SV3)).

8. If the Collection Definition is not the new one that is to be used with SV 5.0 SP2, change the value so that it is and click **Apply**.

9. Select the **Configuration** tab.

10. Disable the **Enabled** check box and click **Apply**.

11. Enable the **Enabled** check box and click **Apply**. This will restart the Service Group.

12. Repeat this procedure for all Connectivity Server Service Groups.

Organize the Library Objects

The upgrade code creates one library object per Alarm and Event Service Group that was found in the backup. The library objects are located below the Alarm Collection Definitions object in **Library Structure**. The intention, however, is that there should be one library object per OPC Alarm and Event Server type that exists in the system, because the library object describes the capabilities of an OPC Alarm and Event Server. All groups working towards a specific OPC Alarm and Event Server type can share one library object.

After an upgrade, the structure should be organized so that it complies with this intention. Do not forget to update the settings that refer to the library object in the Event Collector Service Groups, in the **Special Configuration** tab of the Service Group Definition aspect.

Check the Alarm Manager Service Configuration

In SV 4.1, it is possible to have a number of Alarm and Event Service groups, all with individual configurations. In SV 5.0 SP2, these groups are replaced with one group. Consequently, the individual configurations are replaced with one configuration. This common configuration is automatically generated from the individual configurations and should be checked, because:

•   There are one or more new parameters that should be configured.

•   Backed up data may be ambiguous. One Alarm and Event Service group might have another configuration than another group in the backed up system.

•   Modifications might need to be made.

The configuration is found in the **Special Configuration** tab of the Service Group Definition aspect of the Alarm Manager Service group (Figure 12).

TC07437B
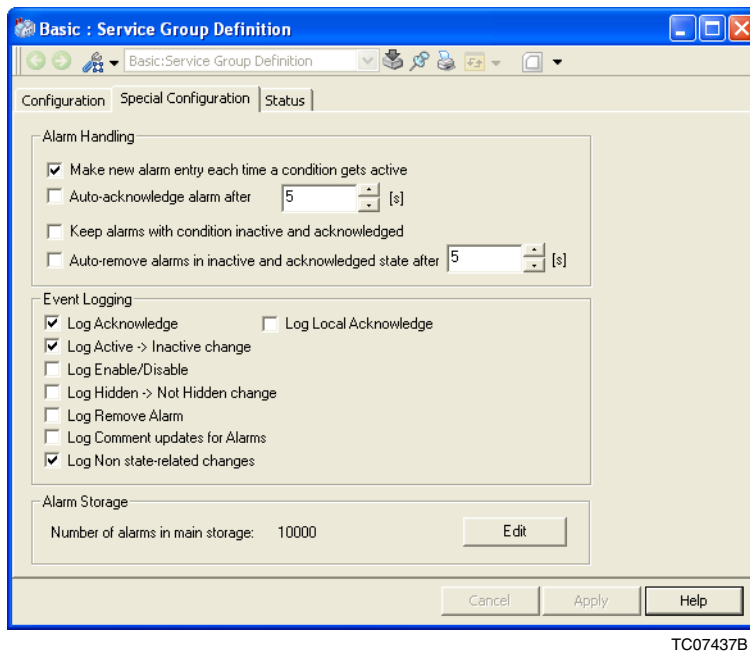
Figure 12. Service Group Definition Aspect (Special Configuration Tab)

Add Redundancy For Alarm Manager

The upgrade creates one service provider for the Alarm Manager, configured to execute in the node in which the upgrade takes place. If the backed up system had redundant Aspect Servers, it is recommended to add service providers for the Alarm Manager according to the same configuration as for other services that execute in Aspect Servers. However, this should be done after the server nodes have been connected to the system.

Restoring Application and Historical Data

The remainder of this section describes how to restore historical data and the necessary data for each Functional Area.

Device Management and Fieldbuses

If the system contains Fieldbus devices, the Restore Device Types procedures must be performed before restoring the Control Builder M project or the upgrade will fail. The Control Builder M upgrade can be done only once.

After installation of SV 5.0 SP2 software all third party software for Device Type Objects used in the previous system version must be reinstalled. Additionally PROFIBUS Device Type Objects used in the Control Builder M project must be adapted to new delivered Hardware Libraries. Check that all licenses are valid for the restore, even for third party devices.

Restore Fieldbus Device Types

The procedures in the System Restore Wizard function in the Device Library Wizard must be performed for Fieldbus Device Types before restoring the Control Builder M project, otherwise the upgrade will fail. The Control Builder M upgrade can only be performed once.

The following steps for Fieldbus Device Types need to be carried out on every system node, except thin client nodes. Perform the System Restore Wizard's procedure on the nodes in the following sequence:

- Aspect Servers (including redundant Aspect Servers).
- Connectivity Servers (including redundant Connectivity Servers).
- Application Servers.

- Clients.

1. Start the Device Library Wizard. Select:

     Start > All Programs > ABB Industrial IT 800xA > Device Mgmt >
     Device Library Wizard

   -or-

   double-click the Device Library Wizard icon on the desktop.

2. Navigate to:

   Device Type Administration > System Restore Wizard

   and choose the first option in the System Restore Wizard as shown in Figure 13
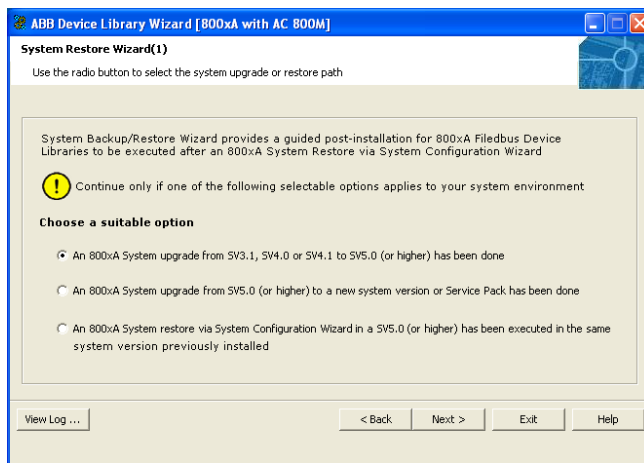   and click **Next**.

Figure 13. System Restore Wizard (1)

3. Choose whether or not this system node has been reformatted as shown in Figure 14 and click **Next**.
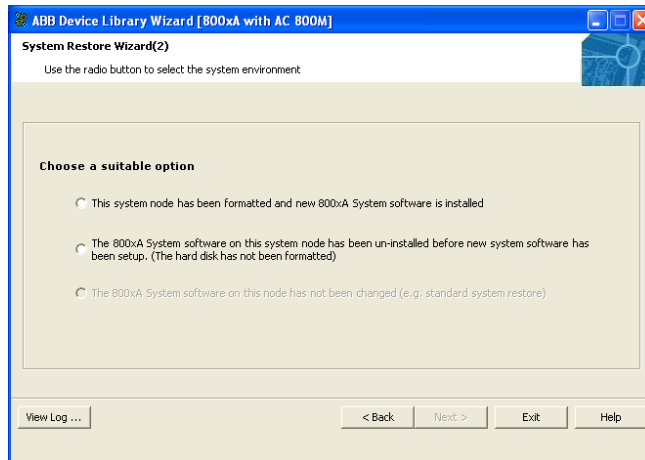

Figure 14. System Restore Wizard (2)

> If the system node has not been reformatted (second option), the following steps are not necessary when PROFIBUS Device Types are not present in the system node. In this case, the Device Library Wizard will perform an update of Fieldbus Device Types (refer to Update Fieldbus Device Types on page 82).

4. Depending on which fieldbus protocol is used in the previous system version environment, insert one of the delivered Device Library system DVDs in the DVD drive (e.g. Device Library HART – DVD).

5. Click **Browse** and navigate to the DVD drive.

6. When the drive has been selected in the Browse for folder dialog, click **OK** in that dialog and then **Next** in the ABB Device Library Wizard.

7. The Device Library Wizard scans the 800xA System for fieldbus device types that are already used and compares the results with the contents of the DVD. Device Types available in the 800xA System and the DVD are shown in the

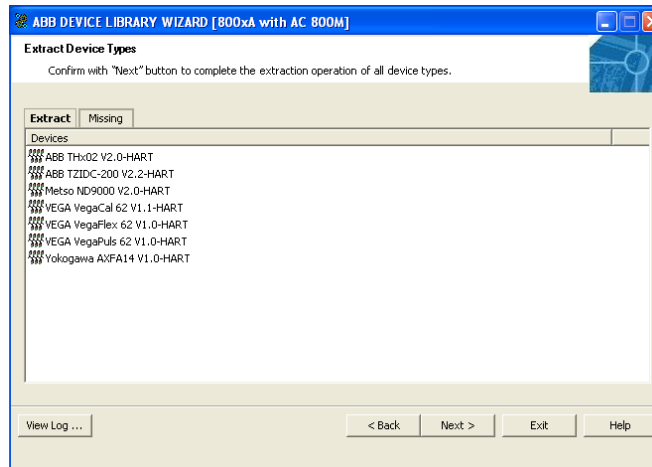Extract tab of the Device Library Wizard (Figure 15).

Figure 15. Extract Device Type Files

8. Click **Next** to start the extraction process.

9. Device Types available in the 800xA System but not on the DVD are displayed in the **Missing** tab. If there are any Device Types showing in the **Missing** tab, **Next** in the Device Library Wizard is disabled. Navigate to the Browse dialog by clicking **Back** and inserting a new Device Library DVD in the DVD drive.

10. Repeat this procedure until all Device Types are extracted to the 800xA System node and the **Missing** tab does not list any device types.

11. If the Device Library DVDs do not contain all Device Types used in the previous system version, the missing Device Types must be downloaded from ABB SolutionsBank.

It is only possible to complete the Wizard if all Device Types have been successfully extracted.

12. When the extraction process is completed successfully, the Device Types need to be re-installed on the 800xA System node. Click **Next** to launch the Re-

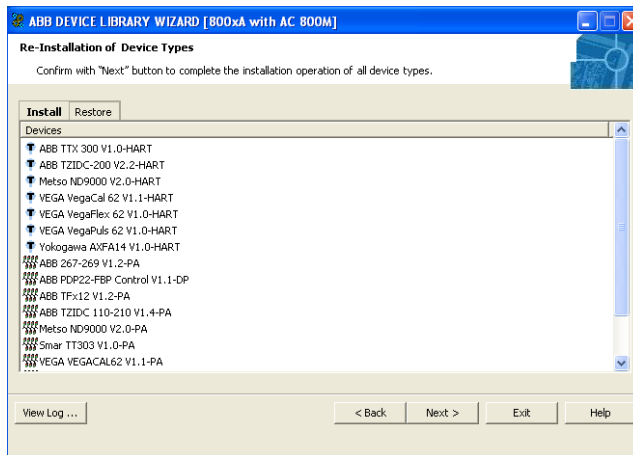installation of Device Types dialog shown in Figure 16.

Figure 16. Re-install Device Types Dialog

13. Follow the Device Library Wizard procedure to complete the installation. The Device Library Wizard will automatically navigate to the main window after the process is completed.

14. Exit the Device Library Wizard and repeat the procedure on the other 800xA System nodes, if applicable.

Update Fieldbus Device Types

If the system node has not been reformatted (second option in Figure 14), all Device Types that exist in the 800xA System node and need updated are displayed in the
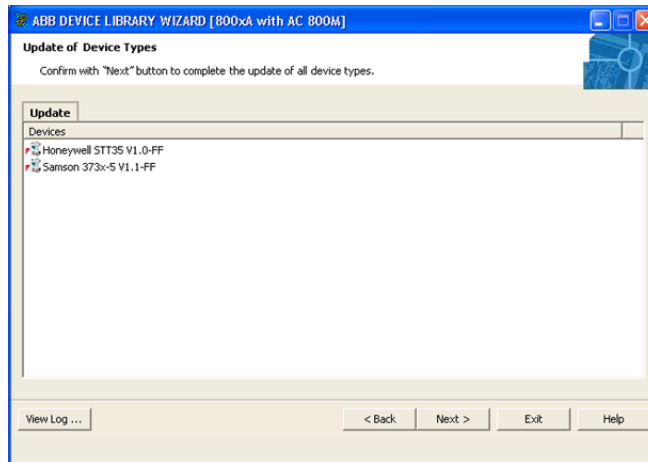
Update tab (Figure 17).

Figure 17. Update of Device Types Dialog

1. Click **Next** to launch the update.

2. The Selection Summary dialog will appear showing the Device Types to be updated. Click **Next** to continue.

3. Follow the Device Library Wizard procedure to complete the installation. The Device Library Wizard will automatically navigate to the main window after the process is completed.

Device Management FOUNDATION Fieldbus

Perform the following to complete upgrading Device Management FOUNDATION Fieldbus.

1. **Update LD 800HSE Linking Devices:** Update all LD 800HSE linking devices to the latest firmware version released for this system environment following the update procedure described in the user instructions for the particular device.

   Refer to *Field IT, Foundation Fieldbus Linking Device, LD 800HSE, Version Table (3BDS009910)* in ABB SolutionsBank for the latest linking device firmware released for this system environment.

   From Downloads Explorer, navigate to:

   > Control Products and Systems/800xA/Device Management Foundation Fieldbus/Foundation Fieldbus Linking Device LD800HSE

2. Check, Save, and Upload FF Libraries:

   a. Open a Plant Explorer Workplace.

   b. Use the Structure Selector to open the **Object Type Structure**.

   c. Use the Object Browser to navigate to:

      `FF Libraries Object Type Group`

   d. Select `FF Upload` in the Aspect List Area.

   e. Click **Open Library in Fieldbus Builder FF**.

   f. Open the library in Fieldbus Builder FF.

   g. Click **Edit Library**.

   h. Right-click **FF H1 Device Library** in the Libraries dialog of the Fieldbus Builder FF.

   i. In the Parameter dialog, click **Reload Standard Dictionary** and browse to the following directory:

   j. `...\Fieldbus Builder FF\ff`

   k. Select **STANDARD.DCT** and click **Open** and then **OK**.

   l. Check the libraries for plausibility and store them in Fieldbus Builder FF.

   m. Exit Fieldbus Builder FF.

   n. Return to the Plant Explorer Workplace and click the **Library Upload** tab in the Preview Area.

o.   Click **Upload FF Library**.

p.   After a successful upload, the green traffic light symbol indicates that the FF libraries have been synchronized.

3.   Optional: Reconstruct User-made Changes to Library Objects representing FF Standard Blocks:

ℹ️   This step is only required if changes were made to library objects representing FF standard blocks.

During upgrade, **user-made changes to library objects representing FF standard blocks have been overwritten**. Important substitutions have been logged.

a.   If such changes were made, display the substitutions as follows:

–   Open a Plant Explorer Workplace.

–   Use the Structure Selector to open the **Object Type Structure**.

–   Use the Object Browser to navigate to:

     `FF Libraries Object Type Group`

–   Select `FF Upload` in the Aspect List Area.

–   Select **Warnings** tab.

b.   For reconstructing user-made changes, reapply the changes to the library objects manually.

4.   Update FF Libraries for HSE Subnet (Library Update).

ℹ️   Perform the following procedure for each HSE Subnet.

a.   Open a Plant Explorer Workplace.

b.   Use the Structure Selector to open the **Control Structure**.

c.   Use the Object Browser to navigate to:

     `HSE Subnet`

d.   Select `FF Upload` in the Aspect List Area.

e.   Click the **Library Update** tab in the Preview Area.

    f.   Click **Update Library**.

5.   Check, Save, Commission, and Upload the HSE Subnet.

Perform the following procedure for each HSE Subnet.

    a.   Open a Plant Explorer Workplace.

    b.   Use the Structure Selector to open the **Control Structure**.

    c.   Use the Object Browser to navigate to:

         `HSE Subnet`

    d.   Select `FF Upload` in the Aspect List Area.

    e.   Click the **HSE Subnet Reference** tab in the Preview Area.

    f.   Click **Open Subnet in Fieldbus Builder FF**.

    g.   Click **Edit Subnet**.

    h.   **Check whole project** for plausibility and save the configuration in Fieldbus Builder FF.

    i.   Perform device assignment for all linking devices LD 800HSE.

    j.   Perform precommissioning/commissioning for all objects for which this is necessary (discernible from engineering status).

To assign all H1 devices in one step, use the **Assign all devices** function from the HSE Subnet context menu: **Object > Assign all devices...**

For downloading use the online dialog from the HSE Subnet context menu: **Object > Online Dialog...**

    k.   Exit Fieldbus Builder FF and save changes if prompted to do so.

    l.   Return to the Plant Explorer Workplace and click the **HSE Subnet Upload** tab in the Preview Area.

    m.   Click **Upload HSE Subnet**.

    n.   After a successful upload, the green traffic light symbol indicates that the HSE Subnet has been synchronized.

800xA for AC 800M

ℹ️ After upgrading a configuration containing one Engineering and one Production system to SV 5.0 SP2, the Control Builder M projects in the two systems should be made identical using the Import/Export tool, Engineering Repository, or by recreating the Engineering System using Backup/Restore before engineering work is restarted. Otherwise there will be a lot of false differences on the AC 800M aspects reported in the import difference report when moving solutions between the systems.

There may be Control Builder M compatibility issues when upgrading from SV 4.1 to SV 5.0 SP2. Review the issues detailed in SV 4.1 to SV 5.0 SP2 Compatibility Issues on page 124 before proceeding

Use the following procedure to restore 800xA for AC 800M information:

1. Configure the memory setting for OPC Server and Control Builder (found in the Setup Wizard for each product) to the saved and recorded values.

2. Control Builder stores its settings (systemsetup.sys) on disk in the following directory:

    ```
    ...\ABB Industrial IT Data\Engineer IT Data\Control
    Builder M Professional
    ```

    Add the file saved on the safe media to the system.

3. New handling for Hardware Types was introduced in SV 5.0. All hardware types are now packaged in libraries. Because of this all Control Builder projects must be upgraded according to the following steps.

ℹ️ If the application contains FOUNDATION Fieldbus, HART, or PROFIBUS specific configurations, perform post upgrade procedures for Device Types via the Device Library Wizard (refer to Device Management and Fieldbuses on page 78) before upgrading the project in Control Builder M.

  a. Start an empty Control Builder M .

  b. Select:

      Tools > Maintenance > Upgrade Project > from Control Builder Professional 3.4 or later

    c.   Select the Control Builder project to upgrade. This step will take a while. All hardware objects in the **Control Structure** are redirected by Control Builder to use hardware types from libraries. If the project contained custom hardware definition files, libraries with corresponding hardware types are automatically created by Control Builder.

    d.   Repeat Step a through Step c for all Control Builder projects in the system.

    e.   When all Control Builder Projects are upgraded the old hardware types should be deleted from the **Object Type Structure**.

        In the Plant Explorer Workplace, navigate to the **Object Type Structure** and browse to:

```
Object Types > Control System > AC800M/C Connect -
Controller Hardware
```

        Right-click the `Controller Hardware` object and select **Delete**.

4.   Modify the application program according to applicable issues in SV 4.1 to SV 5.0 SP2 Compatibility Issues on page 124.

5.   Load the controllers with their firmware and applications. Change Analysis Mismatches may be shown for objects in the Standard Libraries during the first download after the upgrade. Possible mismatches are:

```
Mismatch: Variable has changed data type.
Mismatch: Variable not found.
Mismatch: Control Module not found.
```

The mismatches reflect internal changes in the Standard Libraries. No Cold Retain Values will be lost. Click **Next Mismatch** to continue.

6.   The OPC Server stores configuration files (*.cfg) and settings (systemsetup.sys) on disk. Add the files saved on the safe media to the system. The systemsetup.sys file is located in:

```
...\ABB Industrial IT Data\Control IT Data\OPC Server
for AC 800M
```

The configuration files are stored in the Files folder in the same location.

7. Restore OPC configurations by selecting **File > Load Configuration** in the OPC Server Panel.

ℹ Remember to enable autoloading of the configuration and provide the correct path to the file.

800xA for AC 100

ℹ 800xA for AC 100 is not detected by System Installer if this tool is used for upgrade. This means that the installation of this software must be done manually in the new system.

Perform the following post upgrade procedure for 800xA for AC 100:

If you have made a copy of the Bus Configuration Database (BCD) folder in the pre-upgrade procedure, copy the saved BCD file folder to the upgraded Connectivity Server node.

• For each Connectivity Server node, restore the 800xA for AC 100 settings documented in the pre-upgrade procedure.

800xA for Advant Master and 800xA for Safeguard

Perform the following on each Connectivity Server node:

1. Copy the saved files:

    – DATHR1.CD
    – DATHR2.CD
    – DATHR3.CD

    to the folder:

        ...\Program Files\ABB Industrial IT\OperateIT\AC 400
        Connect\AdvantBase\Data\RTA\Init\

    to the node where they belong.

2. Update the Configuration Files.

    For each Connectivity Server, compare the following files saved in a safe location during the 800xA for Advant Master pre-upgrade phase:
    – AdvDsMasterAdapter.csv

– AdvMbAeOPCServer.csv

with the installed version of the files at the following location:

```
...\Program Files\ABB Industrial IT\Operate IT\AC 400
Connect\Bin
```

If any customization was done to the old files, update the installed version of the files with the corresponding changes.

3. Open the MB 300 RTA Settings dialog in Configuration Wizard and reconfigure:

– MB 300 Node and Network Numbers.

– Check 800xA as Clock Master in case the time synchronization key REVERSED_SYNC_MODE was enabled before.

4. Always Restart the RTA board.

5. The Audible property must be 0 for events and 1 for alarms 800xA for Advant Master version 4.1 SP1 RU6 and newer. Refer to *Industrial IT, 800xA - System, Configuration (3BDS011222Rxxxx)* for configuration of audible alarms.

Safeguard standardevent 300 - 326 does not comply with this rule before 800xA for 800xA for Advant Master Version 5.0 SP2. The Event numbers where the Audible property should be changed from 1 to 0 are:

– EVENT302.
– EVENT305.
– EVENT310.
– EVENT312.
– EVENT320.
– EVENT321.
– EVENT322.
– EVENT325.

800xA for MOD 300

Perform the following post upgrade procedures for 800xA for MOD 300.

1. Re-initialize PAS System Services on the Connectivity Server.

The PAS System Services will not start until the communications settings are initialized as described in the following steps.

2. Initialize the OMF settings to start system services. Use the Administrative Tools in Windows Control Panel to select:

     PAS > Settings

     This displays the Communications Configuration Tool.

     The message: `Would you like to revert back to saved settings?`

     is displayed if settings were previously saved. To restore the previous settings, perform Step a through Step d.

     a. Select **Yes** at the message: `Would you like to revert back to saved settings?`

         This opens the Communication Settings display.

     b. Select **OK** on the Communication Settings display to save the settings and close the window.

     c. Select **OK** to the message: `Settings have been saved . ...`

     d. Select **OK** when the message appears that indicates the settings have been changed. A restart is always required if the Control Network Setting, OMF Memory, or TCP/IP enabled setting are changed.

3. Restart Windows at this time.

4. Reverse_Time synch will be disabled following the re-installation of PAS. If the Connectivity Server node sets the time on the Real-Time Accelerator Board (RTAB), Reverse_Time_Synch must be enabled. Refer to the 800xA for MOD 300 section in *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)*.

5. If any objects were customized, those changes must be implemented again on objects delivered with 800xA for MOD 300 Version 5.0 SP2.

6. If a new Operating System has been installed as part of the upgrade, update the registry settings previously recorded. Refer to *Industrial IT, 800xA System - 800xA for MOD 300, Configuration (3BUR002417Rxxxx)*.

PLC Connect

Perform the following post upgrade procedures for PLC Connect.

Modify Installation for IEC60870 or Basic Project Objects

If either the IEC60870 or Basic Project Objects features were installed:

1. Use standard Windows procedures to access Add/Remove Programs in Windows Control Panel.

2. Select ABB PLC Connect.

3. Select Change/Modify.

4. The InstallShield Wizard for PLC Connect appears. Refer to *Industrial IT, 800xA - System, Installation (3BSE034678Rxxxx)* to select and install the desired features.

5. If the IEC60870 feature is installed refer to *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* and reload the saved IEC configuration.

Restoring PreTreat2.dll

To restore PreTreat2.dll:

1. If the PLC Connect Communication Server Pre Treatment function is being used in the application, copy `PreTreat2.dll` from the backup location to the same folder as it was backed up from on the PLC Connect Connectivity Server. If the default folder is used, that location is:

        ...\ABB Industrial IT\Operate IT\PLC Connect\Bin

2. Register the `PreTreat2.dll` file (refer to *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* for more information).

3. Restart the PLC Connect Connectivity Server for the changes to take effect.

4. Restore the VB project for PreTreat2.dll.

Restoring PreEvent.dll

To restore PreEvent.dll:

1. If the PLC Connect Event Server Pre Treatment function is being used in the application, copy `PreEvent.dll` from the backup location to the same folder as it was backed up from on the PLC Connect Connectivity Server. If the default folder is used, that location is:

    ```
    ...\ABB Industrial IT\Operate IT\PLC Connect\Bin
    ```

2. Register the `PreEvent.dll` file (refer to *Industrial IT, 800xA System - PLC Connect, Configuration (3BSE035041Rxxxx)* for more information).

3. Restart the PLC Connect Connectivity Server for the changes to take effect.

4. Restore the VB application project for PreEvent.dll.

Redeploy the PLC Connect Configuration

To redeploy the PLC Connect configuration:

1. Use the Structure Selector to open the **Control Structure** in the Plant Explorer Workplace.

2. Use the Object Browser to navigate to the first Generic Control Network object.

3. Select `Deploy` in the Aspect List Area.

4. Press the SHIFT key and click **Deploy** in the Preview Area to make sure that a full deploy is done.

5. The deploy begins and the progress is displayed in the Preview Area. The deploy is completed when Deploy ended is displayed.

6. Repeat the procedure for any additional Generic Control Network objects.

Engineering Studio

Post upgrade procedures for Engineering Studio include those for IO Allocation, Engineering Templates, and Function Designer.

IO Allocation

> Before working with the IO Allocation function in an upgraded system, check all Control Builder Name aspects of CBM_Signal instances to see if they contain a valid name.
>
> All Control Builder Name aspects having an empty name or a name not introduced by synchronization from the Name aspect must be corrected accordingly. This can be performed using a Bulk Data Manager worksheet that reads out Name and Control Builder Name. The same worksheet can be used to write back the Name.

> The following procedure is only required if HART devices and IO signals will be merged into one object.

SV 5.0 SP2 supports merging of Hart devices and IO signals within one object. If Hart devices and IO signals will be merged into one object refer to *Industrial IT, 800xA - Engineering, Engineering Workplace, Basic Engineering Functions (3BDS011223Rxxxx)*.

> The following procedure is only required when working with IO Allocation and if properties of IO boards have been changed directly in Control Builder M.

IO Allocation has enabled new properties (e.g. *Inverted*) to be accessible for CBM_SignalParameter/CBM_PulseSignalParameter. These properties are initialized with a default value. If properties have been changed directly in the Hardware Editor of Control Builder M (as they were not supported by IO Allocation) these changes are not reflected in CBM_SignalParameter/CBM_PulseSignalParameter aspects after the upgrade. Therefore, when the menu **Write Allocation into CBM** is performed, values may be overwritten with their default value. After upgrading, select controller by controller and perform the menu **Read Allocation from CBM**, which reads the property values from Control Builder M and updates the signal objects.

Engineering Templates for Bulk Data Manager (BDM)

Engineering Templates are typically used from scratch, meaning data is dropped into the templates. The result is used for information or documentation. In this case no upgrade is required, because the installation of Engineering Studio 5.0 SP2 exchanges the Engineering Templates in:

```
...\Documents and Settings\All Users\Desktop
```

However, if a worksheet containing data has been saved in the file system for writing back to the 800xA System after upgrade, either:

- Newly create the worksheet based on an Engineering Template delivered with Engineering Studio 5.0 SP2.

     -or-

- Update the worksheet according to the description in:

     ```
     ...\Documents and Settings\All Users\Desktop\
     Engineering Templates\ Upgrade Description Engineering
     Templates.doc
     ```

Function Designer

Modified Aspects of Function Designer System Extension. The Function Designer system extensions:

The Function Designer system extensions:

- Function Designer.
- Function Designer for AC800M Connect.
- Function Designer for AC 800M SB2 Libraries.
- Function Designer for Fieldbus Builder PROFIBUS/HART.

mainly consist of:

- Functional Planning Object Types, including a Function Settings aspect at the Settings Object Type Group.

- Extension Libraries that add Function Designer Aspects to Object Types (Control Modules, Function Blocks, ...) created by basic libraries (AC 800M Connect, AC 800M SB2 Libraries, etc.).

After having loaded such a system extension in the SV 4.1 800xA System some of these aspects may have been modified; for example, to adapt Function Settings, or to change the color or layout of Function Blocks in Function Diagrams.

During the 800xA System upgrade to SV 5.0 SP2 the system extensions of the new system are loaded. To keep the information about modified aspects, all aspects that

had been created by a Function Designer system extension, but later on modified are listed in the Configuration Wizard log, and are written to Afw files, e.g.:

> ...\Function Designer\bin\Upgrade\313To501\Function Designer.afw

> ...\Function Designer\bin\Upgrade\313To501\Function Designer for Ac800M Connect.afw

> ...\Function Designer\bin\Upgrade\313To501\Function Designer for Ac800M SB2Libs.afw

> ...\Function Designer\bin\Upgrade\313To501\Function Designer for FB P/H.afw

The only way to bring these modifications back into the SV 5.0 SP2 800xA System is to manually merge the changes. Do not import the Afw files above into the SV 5.0 SP2 800xA System, because some additional properties/data might get lost. In the case of Function Settings, look for each settings property in the SV 4.1 800xA System and do the modifications again in the SV 5.0 SP2 800xA System. In the case of modified Function Aspects (e.g. Diagram Template, Component Template), check the modifications done in the SV 4.1 800xA System and do the modifications again in the SV 5.0 SP2 800xA System.

Upgrade Diagram References and Diagram Variables. In the SV 5.0 SP2 800xA System (opposite to the SV 4.1 800xA System) Diagram References and Diagram Variables are by default created as Symbol Objects. This is not true for Diagram References and Diagram Variables created during upgrade (restore) from SV 4.0 800xA Systems. Convert them from Aspect Objects to Symbol Objects by use of the conversion function described in the following procedure.

ℹ️ Differences between Aspect Objects and Symbol Objects are described in *Industrial IT, 800xA -Engineering, Engineering Workplace, Function Designer (3BDS011224Rxxxx).*

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Object Type Structure**.

3. Use the Object Browser to navigate to:

        Object Types > Functional Planning > Settings

4. Select `Function Upgrade` in the Aspect List Area to open the Function Upgrade aspect in the Preview Area.

5. Enable the **Convert Diagram References/Variables from Aspect Objects to Symbol Objects** check box and click **Apply**.

6. Click Run Upgrade to perform the upgrade.

ℹ️ This function is not suitable in the case of additional aspects on input/output references, e.g. Graphic Elements, for typical diagrams with input/output references that will get copied and connected via the Bulk Data Manager.

Check and Repair AES Variable Table (Applications, Controllers Diagrams/SCMs, and Diagram (Cm) Types). This function can be used to:

• Correct possible inconsistent data used for display of online values and external cross references.

• Delete obsolete data and reduce aspect size.

Perform the following procedure to use this application.

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Object Type Structure**.

3. Use the Object Browser to navigate to:

> `Object Types > Functional Planning > Settings`

4. Select `Function Upgrade` in the Aspect List Area to open the Function Upgrade aspect in the Preview Area.

5. Enable the **Check and Repair AES Variable Table (Applications, Controllers, Diagrams/SCMs, and Diagram (Cm) Types)** check box and click **Apply**.

6. Click **Run Upgrade** to perform this upgrade.

ℹ️ Execute Check and Repair AES Variable Table in order to make the environment support work for Function Designer.

Asset Optimization

Use the following procedure after upgrading Asset Optimization. Perform the steps applicable to the system.

1. Asset Monitoring:

    Asset Monitoring directories **must** be restored on the Asset Optimization Server node.

    a. Reconfigure the value of the OPC Group Update Rate:

    – Open a Plant Explorer Workplace.

    – Use the Structure Selector to open the **Control Structure**.

    – Use the Object Browser to navigate to:

        `Root > Asset Optimization`

    – Select `Afw OPC-DA Asset Monitor Data Source` in the Aspect List Area.

    – Update the value of **OPC Group Update Rate (ms)** in the Preview Area with the value recorded under Record Values for Post Upgrade on page 36 and click **Apply**.

    b. If Runtime Asset Monitors are being used in the system, restore the Runtime Asset Monitor data directory (DeviceRunTimeMSLogicStore). The Runtime Asset Monitor data directory is located in:

        `...\Program Files\ABB Industrial IT\Optimize IT\Asset Optimization\AssetMonitorEnvironment\Bin`

    The saved data contains the Runtime Asset Monitor data present at the time of the save. Use the Runtime Asset Monitor faceplate to reset the asset monitors by adding the lost time to their accumulated run time or with some known values based on other records. Any alarms that were occurring during the backup should be ignored.

    c. If XY Profile Deviation Asset Monitors are being used in the system, restore the XY Profile Deviation Asset Monitor data directory (XY_Reference_Profiles). The XY_Reference_Profiles directory is located in:

```
...\Program Files\ABB Industrial IT\Optimize IT\Asset
Optimization\AssetMonitorEnvironment\Bin
```

2. Maximo Integration:

    ℹ️ If using Maximo Integration, the Maximo Integration information *must* be restored on all Asset Optimization Server nodes. Reference the **Service Structure** for the Asset Optimization Server.

    a. If the MxDef files were customized, restore the MxDef files to the following directory:

    ```
    ...\Program Files\ABB Industrial IT\Optimize IT\Asset
    Optimization\ABBAO\Services\ MOM\MxDefs\
    ```
    server_name**app_server**

    Where:

    <server_name>\<app_server> is the combination of the **MRO Server Name** and the **MRO Application Server Name** fields from the Maximo Equipment ID aspect. These fields are configured in the **Aspect System Structure** in the Maximo Equipment ID aspect. These fields allow for customization of MxDef files on the Maximo Server level as well as on the Maximo Application Server level. Refer to Maximo documentation for an explanation of Maximo Application Servers.

    For example, the resultant path to the customized MxDef files will look like:

    ```
    ...\Program Files\ABB Industrial IT\Optimize IT\Asset
    Optimization\ABBAO\Services\MOM\MxDefs\Maximo5\
    MxServer
    ```

    Refer to *Industrial IT, 800xA - Asset Optimization, Configuration (3BUA000118Rxxxx)* for more information on MxDef files.

    b. It is necessary to configure the values of the Maximo Equipment ID Provider Properties, as these values are not upgraded. These values should have been recorded in Step 2 under Record Values for Post Upgrade on page 36. Refer to **Maximo Server Connection Properties** in the **System Setup** section of *Industrial IT, 800xA - Asset Optimization, Configuration (3BUA000118Rxxxx)* to configure these values.

3.   DMS Calibration Integration. If using DMS Calibration Integration:

ℹ️   Asset Optimization DMS Calibration Integration SV 5.0 SP2 functions with
    DMS software Version 2.6.

   a.   Restore DMS Calibration Integration information. Refer to the *Meriam
        Process Technologies Device Management System User's Guide* for
        information about restoring DMS Server data.

   b.   Perform an 800xA > DMS synchronization to insure that the 800xA
        objects correctly map to the Devices within DMS.

4.   Asset Monitors that are assigned (via the Configure option drop-down list box
     on the Asset Monitor Instance on an Object) to a particular AO Server object
     and Asset Optimization Server aspect (by Object name:Aspect name pair), will
     not be correctly configured after the upgrade. The AOServer property will be
     unconfigured and the following error message will appear:

        Unable to resolve AO Server for this Asset Monitor
        configuration

     This must be resolved before the Asset Monitor Logic can be loaded into an
     AO Server:Asset Optimization Server for execution. Refer to the **Object Type
     Structure** for Asset Optimization, Object Type Group:AO Server, Object Type.

5.   In the **Control Structure**, open the AOServer1, AOServer object, Asset
     Optimization Server aspect.

   a.   Service Hostname MUST be configured. It may be necessary to navigate
        into the **Service Structure** to the AssetMonitoring Service Provider to set
        the Node and enable the service. There is a navigation button for
        convenience.

   b.   Target State should be Service, i.e. Engine is running.

   c.   On all objects that have Asset Monitor aspects, check the **Asset Monitor**
        tab in the Config View of the aspect for the Server Assignment and
        Assigned to. These fields may upgrade as blank or unassigned.

6.   After a restore of a SV 5.0 SP2 system, the Asset Optimization Server (Monitor
     Server/Engine) is running. The **AO Server** tab of the Asset Monitoring Server
     aspect will show a status of good: AM Engine running.

a. Clicking the **Asset Monitors** tab and selecting **AMs assigned to this AO Server** will show that the values in the Status column are `NOT Loaded, enabled`.

b. Click **Load all AMs** to reload all enabled Asset Monitors assigned to this AO Server.

7. In earlier versions of Asset Optimization, all Asset Optimization alarms were written as alarm category soft alarm. Starting with Asset Optimization SV 5.0, these soft alarms are replaced with two new categories: Asset Condition Alarm and Asset Monitoring Status Alarm. Therefore, any existing Alarm and Event Lists that filtered on soft alarms for the purpose of viewing Asset Optimization alarms, must have their filters changed.

8. Starting with Asset Optimization SV 5.0, Object Type Inheritance is supported. That is, an Asset Monitor on the Object Instance will inherit its configuration from the Asset Monitor in the Object Type if it was created via the Copy to all instances property check in the Type Definition aspect. When importing an SV 4.1 configuration, the configuration inheritance changes shown in Table 3 will be made:

Table 3. Configuration Inheritance Changes

Type	Change
Asset Monitor is on the Object Type.	This Asset Monitor will be set to inherit from the Asset Monitor category.
	For each of the 4 configuration tabs (**Asset Monitor**, **Conditions**, **Asset Parameters**, and **Input Records**) the configuration inheritance values will be set to their pre SV 5.0 SP2 values.

Table 3. Configuration Inheritance Changes (Continued)

Type	Change
Asset Monitor is on the instance of the generic object.	This Asset Monitor will be set to inherit from the Asset Monitor category.
Asset Monitor in the instance that has Object Type. Corresponding Asset Monitor does not exist in the Object Type.	For each of the 4 configuration tabs (**Asset Monitor**, **Conditions**, **Asset Parameters**, and **Input Records**) the configuration inheritance values will be set to their pre SV 5.0 SP2 values.
Asset Monitor in the instance that has Object Type. Corresponding Asset Monitor exists in the object type and the **Copy to all instances** check box is disabled in the **Aspect Control** tab of the Object Type Definition aspect.	
Asset Monitor in the instance that has Object Type. Corresponding Asset Monitor exists in the object type and the **Copy to all instances** check box is enabled in the **Aspect Control** tab of the Object Type Definition aspect.	This Asset Monitor will be set to inherit from the Asset Monitor of the Object Type. For each of the 4 configuration tabs (**Asset Monitor**, **Conditions**, **Asset Parameters**, and **Input Records**) if the configuration matches the configuration in Object Type, inheritance values will be set to TRUE, else to FALSE.

9. SV 4.1 supported assigning Asset Monitors on the same object to the different Asset Monitoring Servers. SV 5.0 SP2 requires that all Asset Monitors on the object be assigned to the same AO Server. When upgrading from SV 4.1 to SV 5.0 SP2, the AO Server for all Asset Monitors will be set to **Default**. All Asset Monitors that were assigned to **None** in SV 4.1 will be marked as disabled in SV 5.0 SP2. If the user needs to load balance Asset Monitors between two different AO Servers, this should be done via the **Assign Asset Monitors to this AO Srv** context menu item in the AO Server aspect. Refer to *Industrial IT, 800xA - Asset Optimization, Configuration (3BUA000118Rxxxx)* for more information.

PC, Network and Software Monitoring

1. If user defined Script, Resource, and Assembly files were backed up, copy the saved files from the safe media to the following directories:

    ```
    ...\Program Files\ABB Industrial IT\Optimize IT\
    PC, Network and Software Monitoring\bin\Configuration\
    Scripts\User
    ```

    ```
    ...\Program Files\ABB Industrial IT\Optimize IT\
    PC, Network and Software Monitoring\bin\Configuration\
    Assemblies\User
    ```

    ```
    ...\Program Files\ABB Industrial IT\Optimize IT\
    PC, Network and Software Monitoring\bin\Configuration\
    Resources\User
    ```

2. Perform the following steps on the PC, Network and Software Monitoring Server node.

    ℹ️ The following steps assume that the required system extensions were loaded on the primary Aspect Server node.

    a. Use the Structure Selector to open the **Service Structure** in the Plant Explorer Workplace.

    b. Use the Object Browser to navigate to the:

        ```
        Services > OpcDA_Connector, Service > SG_IT Server
        ```

        object. If there is no object to navigate to, skip to Step l (letter l, not number 1).

    c. Open the OPCDA_Provider_<servername> object and double-click on the Service Provider Definition aspect.

    d. On the **Configuration** tab, enable the **Enabled** check box and click **Apply**. The **Current** field should change to `Service`.

    e. Use the Structure Selector to open the **Control Structure**.

    f. Use the Object Browser to navigate to the IT Server object.

    g. Double-click `OPC Data Source Definition` in the Aspect List Area.

h.   Click on the **Service Group** drop-down menu and select the SG_IT Server.

i.   Click on the OPCDA_Provider_<servername> which was configured in step Step c.

j.   Click **Apply**.

k.   Skip to Step 3.

l.   Use the Structure Selector to open the **Control Structure**.

m.   Use the Object Browser to navigate to the IT Server object.

n.   Double-click OPC Data Source Definition in the Aspect List Area.

o.   Select **New**.

p.   Click **Add** and select the appropriate Service Provider from the list.

q.   Click **OK** twice.

r.   Click **Apply**.

3.   The IT General Setup aspect is used to point the IT OPC Server Network Object to the Asset Optimization Server for Asset Optimization, and the Asset Monitor Data Source. If Asset Optimization software is installed and loaded, then the following configuration is required:

a.   Use the Structure Selector to open the **Control Structure**.

b.   Use the Object Browser to navigate to:

   IT Server, IT OPC Server Network

c.   Select IT General Setup in the Aspect List Area.

d.   Refer to the **IT General Setup Aspect** topic in *Industrial IT, Asset Optimization - PC, Network and Software Monitoring - Configuration (3BUA000447Rxxxx)* and configure the Asset Optimization Server and Asset Optimization Data Source.

e.   Click **Apply**.

4.   Migrate the IT Asset Monitors. If Asset Optimization **and** PC, Network and Software Monitoring were installed on the SV 4.1 System, then the following

must be done for any existing IT Assets that had IT Asset Monitors configured for them.

a. Use the Find Tool in the Plant Explorer Workplace to locate all the IT Asset Monitor aspect instances in the **Control Structure**.

b. Right-click on each of the found aspects and select **Goto Object**.

c. Delete the IT Asset Monitor aspect.

d. Open the IT Device Manager aspect and click **Generate** to recreate the IT Asset Monitor.

e. Repeat Step c and Step d for each object in the Find list.

f. Use the Object Browser to navigate to:

```
Root, Domain > Asset Optimization, Asset Optimization >
AO Server 1, AO Server
```

g. Select `Asset Optimization Server` in the Aspect List Area.

h. In the **AO Server** tab enable the Enable check box and click **Apply**.

i. In the **Asset Monitors** tab, click **Load all AMs**.

SMS and e-mail Messaging

Reconfigure the GSM Device hardware information recorded in the save operation (refer to SMS and e-mail Messaging on page 40).

ℹ️ It may be necessary to stop and start the Messenger Server Service in the **Service Structure** after the SMS and e-mail Messaging restore operation.

ℹ️ During the upgrade, a second Messenger Service Group and Messenger Service Provider will be created in the **Service Structure**. For instance:

Messenger SG_1, Service Group
Messenger SP_1, Service Provider

If there is already a Messenger Service Group and Messenger Service Provider configured, the new one may be deleted.

Batch Management

Verify that the primary Batch Server is in primary mode (P is displayed in the Windows Taskbar) and the secondary Batch Server is in secondary mode (S displayed in the Windows Taskbar). If the proper modes are not displayed, enable the Batch Service Group before proceeding.

To enable the Batch Service Group:

1. Open a Plant Explorer Workplace.

2. Select the **Service Structure**.

3. Select the Services\Batch Service, Service\batch_group_name, Service Group\Service Group Definition aspect.

4. Select the Configuration tab.

5. Select the provider that is currently the secondary Batch Server.

6. Enable the **Enabled** check box and click **Apply**.

7. Select the provider that is currently the primary Batch Server.

8. Enable the **Enabled** check box and click **Apply**.

Batch data can be reloaded to the batch database from wherever it was archived. Once the restored data is in the batch database, it can be viewed using the Batch History Overview window.

Do not restore directly from CDs or DVDs. Restore from hard disk drives which can be restored from CDs or DVDs using commercially available software.

Restoring Batches

To restore batch history, select the batch history restore aspect. By default a Batch History Restore aspect is located in Library Structure\Batch Management\Overviews. However, this aspect can be added to any 800xA System object. The Batch History Restore window is displayed.

To restore batches:

1. Click **Pick Files**.

2. Select the batch files to be restored in the standard Windows Open window.

3.   Click **OK**.

4.   Repeat Step 1 through Step 3 until all the desired batch files are selected.

5.   Click **Restore**.

Use the **Remove from List** and **Clear All** buttons to delete the selected batch or all the batches from the list.

Click **View Log** to view a record of the actions taken during the last restore operation.

Use the Batch Management backup restore utility to restore PFC color configuration information and batch IDs. Access this utility by selecting:

Start > All Programs > ABB Industrial IT 800xA >
Production Mgmt - Batch > Restore Utility

Enabling any of the check boxes listed in the Restore Utility enables **Restore**.

The labeled check boxes are:

•   PFC color configuration.
•   Batch IDs.

When **Restore** is clicked, a warning is presented that states that the restore operation will overwrite the selected parts of the configuration database. The parts of the database that are overwritten are dependent on the option selections. A standard Windows open file window that allows browsing to any desired folder is presented. A configuration window provides the chance to cancel before the file is restored.

Selecting the Alarm Server

To select the Alarm Server:

1.   Open a Plant Explorer Workplace.

2.   Use the Structure Selector to open the **Service Structure**.

3.   Use the Object Browser to select:

```
Services > Event Collector, Service >
Batch_AE_Service, Service Group
```

4.   Select `Service Group Definition` in the Aspect List Area.

5.   Select the **Special Configuration** tab in the Preview Area.

6.   Select Produce IT Batch OPC AE Server in the Alarm Server field.

7.   Click **Apply**.

> Always perform the Toolbar configuration and shutdown script procedure as described in the Production Management section of *Industrial IT, 800xA - System, Post Installation (3BUA000156Rxxxx)*.

Basic History Service

Restore the Basic History Service data as follows. Perform this procedure on every node where the Basic History Service is running.

1.   Stop the Basic History Server from the **Service Structure**.

2.   Read {Provider ID} from the properties of the Basic History Server. This information may be needed when matching servers.

3.   If it is necessary to keep historical data for the time since the system was started after the upgrade, move the Basic History log files in the following directory to a temporary directory:

```
...\OperateITData\History\{provider ID}
```

These files will be inserted by using the Archive Tool as described in Step 7.

4.   Delete all files under:

```
...\OperateITData\History\{provider ID}
```

5.   Restore the files from the backup of Basic History Service Data to:

```
...\OperateITData\History\{provider ID}
```

6.   Start the Basic History Service from the **Service Structure**.

7.   If Step 3 was performed:

a.   Open the AdvHtArchiveTool located by default in the following directory:

```
...\Program Files\ABB Industrial IT\Operate IT\Process
Portal A\bin
```

b.   Use the File/Select/Open Archive command and browse to the directory containing the history log files.

Information Management

Perform the following post upgrade procedures for Information Management.

> ⚠ When creating the Oracle instance, select **I am upgrading from SV3.x or SV4.x** in the Configuration File Options dialog to prevent the wizard from creating a history database. This will prevent History from starting until after the History Database is restored.

Reconfiguring the IM Log Configuration

After restoring a system containing IM logs, the Service Group for the IM log template configuration might be missing. The IM log templates must be checked, and if the Service Group is missing, a new Service Group must be configured.

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Library Structure**.

3. Use the Object Browser to navigate to:

    ```
    History Log Templates, History Log Template Library >
    Default Log Templates, History Log Template Library
    ```

4. Select a log template.

5. Select `Log Template` in the Aspect List Area.

6. Select the **Log Definition** tab in the Preview Area.

7. If the Service Group in the Service Group drop-down list box is missing, it must be reconfigured. The Service Group drop-down list box contains all History servers defined in the system. Use this list to specify the server where this log will reside.

8. Repeat this procedure for all of the log templates.

Information Management History Backup/Restore Utility

Use the Information Management History Backup/Restore utility, via:

> **Start > ABB Industrial IT 800xA > Information Mgmt > History > Backup and Restore**

to restore the Information Management History database and synchronize the Aspect Directory contents with the current Information Management History database configuration.

During the restore, the existing database is dropped, and a new one is created. Mount points and additional table spaces are created based on the database being restored. Oracle data is imported, and the file-based property logs are copied back into the system. Unless a different mount point is specified, the History database will be restored to its original location (its location prior to being backed up).

The History database can be restored from any drive on the workstation, including any mapped network drives. The restore utility will first search a specified location for zipped archives matching a specific name and fitting the form *name-drive***.zip** (such as hist-C.zip, hist-A.zip, and hist-D.zip), and will then restore the compressed database files contained within the archives to their respective original locations (their locations prior to being backed up).

Considerations. When restoring the History database, make sure the disk is ready and available on the node on which the procedure is to occur. Also, make sure that no applications are accessing the Oracle database. The log file should be checked after the restore operation to make sure that the restore operation completed successfully.

Running the Information Management History Backup/Restore Utility

To restore a backed up History database:

The path to PAS now changed to **Control Panel > Administrative Tools**.

This procedure can also be performed by using the pasgui command in the Run dialog (**Start > Run**).

1. Use PAS to stop all Information Management processes and the Inform IT History service provider for this node.

    a. Use the Windows Taskbar to select:

        Start > Programs > Administrative Tools > PAS > Process Administration

      b.   Click **Stop All** in the PAS dialog. This will stop the Inform IT History Service Provider.

> If it is suspected that the Inform IT History Service Provider has not stopped, it can be stopped now by selecting the Inform IT History Service Provider for this node in the **Service Structure**, selecting the **Configuration** tab on the Service Provider Definition aspect, disabling **Enabled**, and clicking **Apply**.

2.   Make sure that no third party applications access the Oracle database during the restore operation.

3.   Select:

> **Start > All Programs > ABB Industrial IT 800xA > Information Mgmt > History > Backup and Restore**.

4.   Verify **Restore configuration from a backup file(s)** is enabled in the Welcome to IM Historian Backup and Restore Utility dialog.

5.   Click **Next**. IM Historian Database Restore dialog appears as shown in Figure 18.
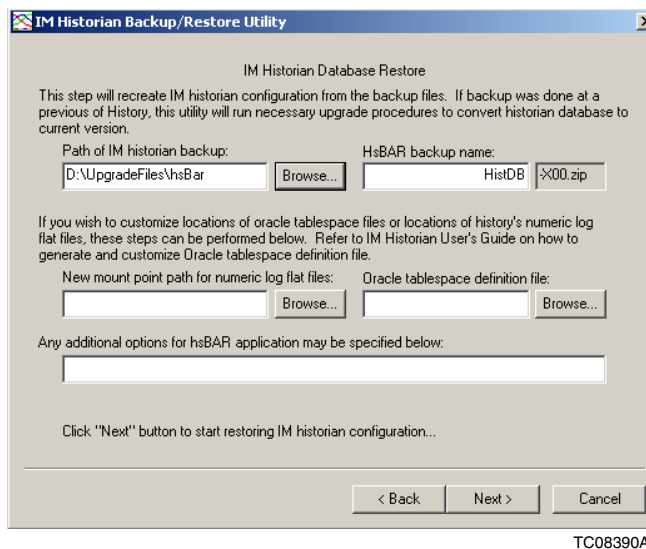
TC08390A

Figure 18. IM Historian Database Restore Dialog

6. Specify the location of the backup files in the **Path of IM historian backup:** field (Figure 18).

If new mount points need to be specified for file-based logs and/or a new Oracle tablespace definition file, click **Browse**.

7. Click **Next**. The HsBAR Output Window appears.

8. Enable the **Automatically close upon completion** check box.

9. Monitor the progress in the Progress Status area of the IM Historian Backup/Restore Utility window. Ignore the error messages indicating errors deleting aspect.

    Shortly after the message indicating the import is complete, the database conversion tool will run automatically. Feedback will be provided in the HsBAR window.

    Shortly after the message indicating the database conversion is complete, the history synchronization tool will run automatically. Again, feedback will be provided in the HsBAR window.

If the restore operation fails with Oracle Error Message 1652 - `Unable to extend tmp segment in tablespace tmp` - it may be due to a large OPC message log which exceeds the tmp tablespace capacity during the restore operation.

Use the Database Instance Maintenance wizard to increase the tmp tablespace. The default initial size is 128 MB with a maximum extended size of 256 MB. The maximum size can be increased using the Oracle Instance Wizard in maintenance mode. Retry the restore operation until it runs successfully.

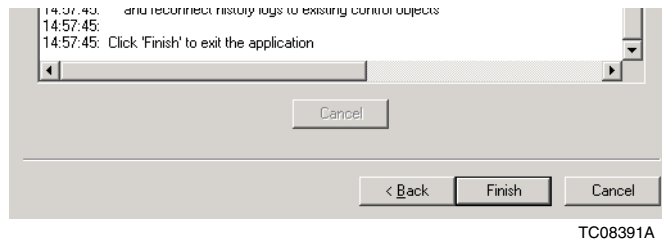10. Click **Finish** when a message stating the execution is complete is displayed as shown in Figure 19.

TC08391A

Figure 19. Execution is Complete Message

If the Progress Status dialog has warning messages with possible solutions as indicated in Figure 20, read the possible solutions carefully, then click **Finish** and proceed with the solution that best fits your problem. Refer to the Information Management Release Notes for further guidelines.
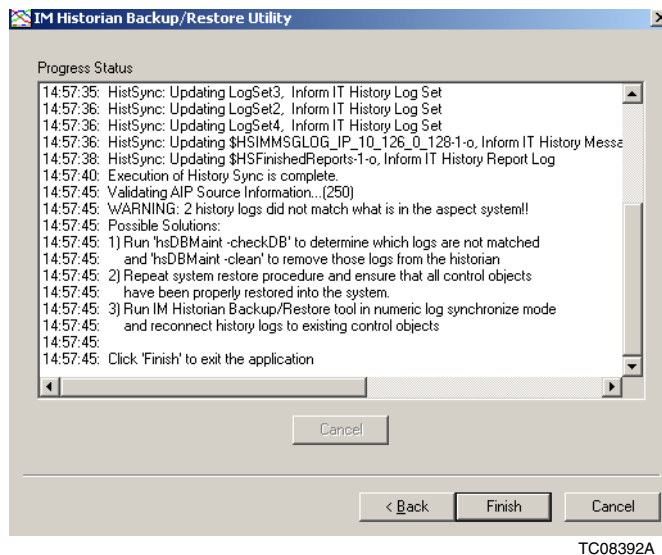

TC08392A

Figure 20. Progress Status Dialog

Start Inform IT History Provider

1. Start all processes under PAS supervision. This will start the Inform IT History Service Provider.

    ℹ️ If it is suspected that the Inform IT History Service Provider has not started, it can be started now by selecting the Inform IT History Service Provider for this node in the **Service Structure**, selecting the **Configuration** tab on the Service Provider Definition aspect, selecting **Enabled**, and clicking **Apply**.

2. Restart the Basic History Service Provider for this node:

    a. Select the Basic History Service Provider object for the Information Management node in the **Service Structure** in the Plant Explorer.

    b. Select the Service Provider Definition aspect.

    c. Select the **Configuration** tab.

    d. Disable the **Enabled** option.

    e. Click **Apply**.

    f. Enable the **Enabled** option.

    g. Click **Apply**.

Restoring Other Information Management Related Files

There are several other files related to Information Management that need to be restored as part of total system restore.

ℹ️ Refer to Saving Other Information Management Related Files on page 46 for Desktop Trends, Display Services, and DataDirect file locations.

*   **History Archive Data:** For each archive device, copy the appropriate folders from the safe media to the location specified by the Device Filename.

*   **History Archive State Information:** Stop the Industrial IT Archive service in the **Service Structure**. Copy the folder that holds the last archive time and other archive state information from the safe media to:

    ```
    ...\Documents and Settings\All Users\Application
    Data\ABB\IM\Archive
    ```

    Restart the Industrial IT Archive service.

- **Reports:** Restore any report template files created in Microsoft Excel, DataDirect, and/or Crystal Reports. Also restore report output files created as a result of running these reports via the Scheduling Services.

- **Desktop Trends:** Restore trend display, ticker display, and tag explorer files.

- **Display Services:** Restore the directories for custom users, as well as display and user element definitions.

- **DataDirect:** Restore custom text files for object, object type, and attribute menus used on the DataDirect windows.

- **Check Archive Path Specifications:** If the disk configuration has changed from the previous system to the new system (i.e. letter designations for disks have changed: C, D, E, etc.), check the archive device configurations to make sure the Archive Path specification points to the correct disk drive and directory, as shown in Figure 21.
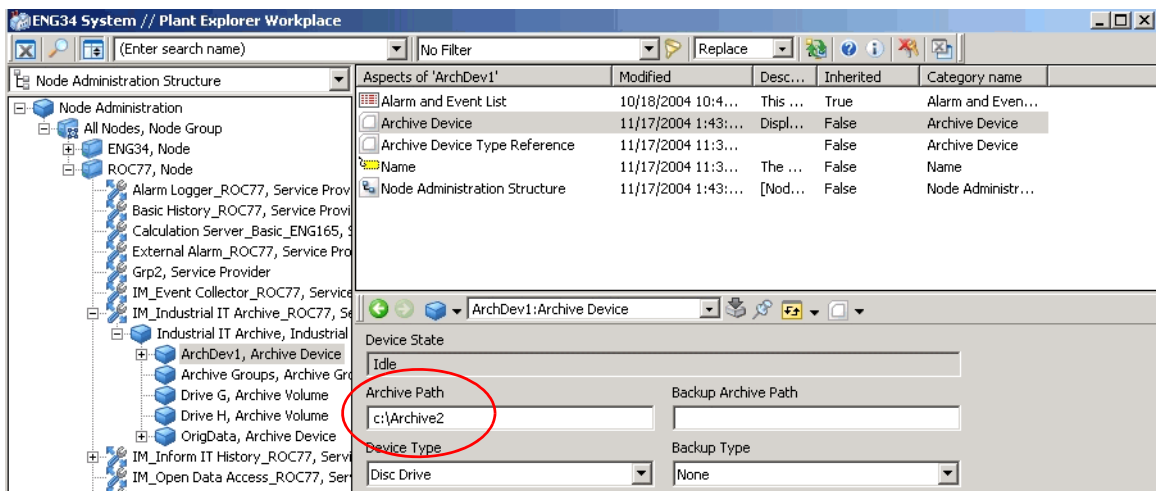
Figure 21. Checking the Archive Path Specification

Restoring Archive Group Associations

Profile, Message, and Report logs must be reassociated with their respective Archive Groups. This information was recorded before beginning the upgrade.

Refer to *Industrial IT, 800xA - Information Management, Configuration (3BUF001092Rxxxx)* to access the Archive Groups and restore the Archive Group associations.

Updating Archive Logs

Absolute names are now included as part of the archive storage. Archive links now use an absolute reference that is independent of the name of the log. Run the archive maintenance to update the _RST log references to use the absolute log reference.

> This procedure is not necessary if archives are not being used.

> This procedure only needs to be performed one time no matter how many Information Management nodes are in the system.

1. Open a Plant Explorer Workplace.

2. Use the Object Browser to navigate to:

    IM Node > `Archive Service Provider`

3. Click `Archive Service Aspect` in the Aspect List Area.

4. Click **Maintenance** in the Preview Area to launch the Maintain Archive References dialog box.

5. Click **Validate Archive Logs**.

6. Run a consistency check on all log configurations.

SoftPoint Service

The SoftPoint configuration must be deployed after the upgrade.

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Control Structure** in the Plant Explorer Workplace.

3. Use the Object Browser to navigate to `Softpoint Generic Control Network` for the node where you want to deploy the SoftPoints.

4.   Select `Deploy` in the Aspect List Area. This aspect provides a listing of configuration changes that have occurred since the last deployment, and indicates whether it requires a full or incremental deployment.

Incremental deploys only those changes that have been made since the last deployment and is the typical selection. A prompt indicates when a Full deploy is required.

5.   Click **Deploy** to start the deploy process. During this time, SoftPoint processing is suspended, and current values and new inputs are held. This process is generally completed within five minutes, even for large configurations. Completion of the deploy process is indicated by `Deploy ended`.

Calculations Service

The Const keyword is no longer allowed within the VBScript source code of the calculation; therefore, edit Calculations that use the Const Statement.

Calculations that were disabled prior to the upgrade must be enabled by enabling the **Enabled** check box in the Calculations dialog. Refer to the section on Calculations in *Industrial IT, 800xA - Information Management, Operation (3BUF001094Rxxxx)*.

To enable the Calculations Service:

1.   Open a Plant Explorer Workplace.

2.   Use the Structure Selector to open the **Service Structure**.

3.   Select the Calculations Service Object.

4.   Select the Service Definition aspect.

5.   Click the **Configuration** tab.

6.   Enable the **Enabled** check box and click **Apply**.

Scheduling Service (Application Scheduler)

Schedules that were disabled prior to the upgrade must be enabled by enabling the **Enabled** check box in the Scheduling dialog. Refer to the section on Scheduling in *Industrial IT, 800xA - Information Management, Operation (3BUF001094Rxxxx)*.

To enable the Scheduling Service:

1. Open a Plant Explorer Workplace.

2. Use the Structure Selector to open the **Service Structure**.

3. Select the Scheduling Service Object.

4. Select the Service Definition aspect.

5. Click the **Configuration** tab.

6. Enable the **Enabled** check box and click **Apply**.

Resigning Digital Signatures in SV 5.0 SP2

To resign digital signatures in SV 5.0 SP2:

1. Use Windows Explorer to locate `AfwSignatureManager.exe` in the following directory:

    ```
    ...\<Base System install directory>/bin
    ```

2. Double-click `AfwSignatureManager.exe` to launch the Signature Manager.

3. Use the **File** menu to open the Signature Report file saved before the upgrade.

4. When a signer is selected in the **Signer** column, the **Aspects Signed** table will show all aspects signed by this signer and information indicating whether the signature was valid in the SV 4.1 System or not.

5. Select the aspects to re-sign and click **Sign**.

6. A Signature dialog will appear in which to validate the signature.

Use Ctrl+Shift+Click to select multiple aspects to sign in one operation.

Restart the System

Restart the system after performing all post upgrade procedures.

Reconfigure Alarm and Event List Configurations

In SV 5.0 SP2, in most cases, the SourceName column contains GUIDs. The recommendation in SV 5.0 SP2 is to reconfigure the Alarm and Event List configurations to use the ObjectName column instead of the SourceName column.

Alarm and Event handling has changed significantly from SV 4.1 to SV 5.0 SP2 (refer to Alarm and Event List Configurations on page 49). Check the list configurations in the SV 5.0 SP2 system against those recorded for the SV 4.1 system under Alarm and Event List Configurations on page 49.

Information Management Maintenance

Perform this procedure on all Information Management Server nodes.

1.   Open a Plant Explorer Workplace.

2.   Use the Structure Selector to open the **Node Administration Structure**.

3.   Use the Object Browser to navigate to:

         All Nodes, Node Group > *IM Node* > Inform IT History_*IM
         Node*, Service Provider > Inform IT History Object,
         Inform IT History Object

4.   Select Inform IT History Control in the Aspect List Area.

5. Expand the `Maintenance` tree in the Preview Area and select
    `Synchronization`. The Inform IT History Manager shown in Figure 22
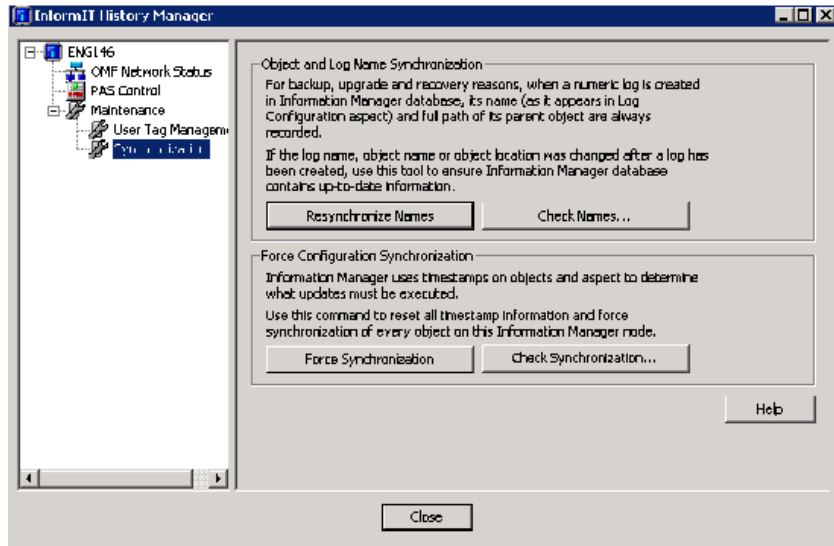   appears in the Preview Area.

Figure 22. Inform IT HIstory Manager

6. Click **Check Names**.

7. A blank dialog should appear. If it does, click **OK**. If it does not click
    Resynchronize Names.

8. Click **Check Synchronization**.

9. A blank dialog should appear. If it does, click **OK**. If it does not click **Force
    Synchronization**.

Configure Windows Services and Windows Firewall

Perform all applicable post installation steps in *Industrial IT, 800xA - System, Post
Installation (3BUA000156Rxxxx)*, including configuring Windows Services and
Windows Firewall.

Add Autostart Shortcut

It it is desired to enable the autostart of the Operator Workplace on client nodes, perform the following:

1. Define a default workplace.

2. The shortcut must be created from the ABB Workplace login window.

3. The shortcut is located in:

   ```
   ...:\Documents and Settings\UserName\Start
   Menu\Programs\Startup
   ```

4. Right-click the shortcut and select **Properties** from the context menu.

5. Add the following to the shortcut target:

   ```
   /WS
   ```

   -or-

   ```
   /WaitForSystem
   ```

6. Click **OK**.

System Backup

Make a complete backup of the upgraded system as described in Backups on page 28.

Appendix A Control Builder M Compatibility Issues

Introduction

This appendix lists the compatibility issues when upgrading from the various system versions to SV 5.0 SP2.

SV 4.1 to SV 5.0 SP2 Compatibility Issues

Table 4 lists and describes Control Builder M compatibility issues, including

solutions to the issues, when upgrading from SV 4.1 to SV 5.0 SP2.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues

Application	Issue	Solution
Force I/O from SIL2 applications prohibited	In order to better enforce the counting of maximum number of forces in High Integrity Controllers, the possibility to force I/O signals directly from code has been removed. This means that no writing will be allowed to the .Forced component of an IO data type in a SIL1-2 or SIL3 application. It will result in a compile error.	The only possibility to force I/O in a SIL application will be via the Safe Online Write function (confirmed write) from operator graphics.This restriction will also improve the response time when resetting forces in the controller.The reset of individual forced signals from code will still be possible by using the new firmware function ResetForcedValue(), which is introduced in SV5.0 SP2. This implies that constructions where variables of IO data type (i.e. BoolIO, RealIO, DWordIO, or DintIO) are copied or connected via out parameters in function blocks, will no longer work. However, parameter passing via in or in_out parameters is not affected.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Discontinued functions for Safe MMS communication (function blocks)	Due to the restriction described in Force I/O from SIL2 applications prohibited, the SIL2 marking of function blocks writing to IO data types has been removed. The affected function blocks are: • MMSRead4BoolIO. • MMSRead4DintIO. • MMSRead4RealIO. Consequently, these function blocks can not be used in SIL applications but will still be available for use in non-SIL applications. The corresponding definition function blocks (MMSdef4xxxxIO) will still be available from SIL applications and consequently reading IO from SIL to non-SIL applications will still be possible.	In SIL applications it is recommended to replace the MMSRead4xxxxIO with the MMSRead4xxxx function blocks and only transfer the Value component of the IO data type.
Safety Operator User Group	An operator must be a member of the Safety Operator User Group to be able to write data to objects running in a SIL application in the controller.	Make the operator a member of the Safety Operator User Group.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
No Time Sync warning in controller	Some controllers might get a `No time sync` warning in the controller log after upgrade to SV5.0 SP2.	Set the CS Protocol Type for controllers that are not intended to be synchronized **No Synch** in order to avoid the warning.
Accessing Local Variables in Function Blocks.	It has been possible to access local variables in Function Blocks from surrounding code. According to the IEC 61131-3 standard, local variables shall only be accessible within the containing software element. A compilation error is given if local variables are accessed from the outside.	Correct any such warnings before performing the download. Local variables used in this fashion need to be changed to parameters instead.
Code sorting loops treated as errors.	Code sorting loops in applications are by default considered as errors in SV 5.0 SP2. It is not possible to compile and download an application if it contains code sorting loops.	First, try to correct the sorting loops. Refer to Interpret and Correct Code Loop Errors in *Industrial IT, 800xA - Control and I/O, Application Programming, Introduction and Design (3BSE043723Rxxxx)*. Another alternative is to change the compiler switch for Code Sorting Loops: 1. Mark the project in Project Explorer. 2. Right-click and select **Settings > Compiler Switch**. 3. Set the global Loops in Control Modules switch to **Warning**.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Applications having integer literal values too large as initial values.	Compile error 1040 might appear in Control Builder projects that previously did not contain any compile errors. Control Builder now makes more stringent compiler checks on initial values for variables. It previously allowed illegal (too large) integer literal values as initial values. The actual used value was zero.	Correct the compile error. e.g. by entering a smaller, legal value on the literal.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Self defined serial communication using the Serial Communication Library.	The Serial Communication Library has undergone a major internal redesign that in some cases may lead to compatibility issues.	**Use of firmware functions:** Firmware functions used for serial communication handling are no longer supported. This means that user-built libraries where these firmware functions have been used, can no longer be used. The no longer supported firmware functions are: • OpenDevice • UpdateDeviceSetup, • SetDeviceClearRead • CloseDevice. • ReadStringDevice • ReadLineDevice • WriteStringDevice **Improvement were made in the following areas:** • Clear buffer when entering the listen operation of the *SerialListen* function block. • If the *SerialWriteWait* function block is triggered when the timeout has elapsed, the read/listen buffer is cleared in between the retry operations in connection to the write operation. • **Behavior of the SerialWriteWait function block in previous versions:** If the function block is triggered after the application stopping phase is entered, the function block propagates the status code -15 via the Status -parameter.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Self defined serial communication using the Serial Communication Library. (continued)	The Serial Communication Library has undergone a major internal redesign that in some cases may lead to compatibility issues. (continued)	If the power fails, and a function block was in a pending state, the Status *-5331* is derived from it after the controller is powered up again. • **Behavior of the *SerialWriteWait* function block in previous versions:** If the function block was triggered after the application stopping phase was entered, the function block should normally propagate status code -15. But this was masked, and instead, after the finished application change, the function block automatically retriggered the write operation.

	The Serial Communication Library has undergone a major internal redesign that in some cases may lead to compatibility issues. (continued)	**Printing a string longer than 140 characters:**
		The behavior of the *SerialWrite* operation is no longer synchronous. Therefore, the possibility to call one and the same function block time after time to print a longer string than 140 characters is no longer supported. Instead, do like the following:
		
		To be able to print a string longer than the maximum length of 140 characters, call subsequent function blocks in order:
		Write1(Req := TRUE,
		         Id := Id,
		          EndChar := EndChar_Write1,
		          Done => Done_Write1,
		          Error => Error_Write1,
		          Status => Status_Write1,
		          Sd := Sd_Write1);
		Write2(Req := TRUE,
		         Id := Id,
		          EndChar := EndChar_Write2,
		          Done => Done_Write2,
		          Error => Error_Write2,
		          Status => Status_Write2,
		          Sd := Sd_Write2);
		Printing the two strings Sd_Write1 + Sd_Write2

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Compiler warnings occur if there is a risk for task collisions.	If there is a risk that tasks can collide in the controller, a warning will be displayed during compilation. The compilation warning will look like: `Warning 9155: Controller_1:HW Task Normal and Fast may have colliding start times`	Apply proper task offsets so that the tasks can no longer collide.

Table 4. SV 4.1 to SV 5.0 SP2 Control Builder M Compatibility Issues (Continued)

Application	Issue	Solution
Applications using SattBus on TCP/IP.	SattBus on TCP/IP will not work after the upgrade. The COMLI communication function blocks have been used also for SattBus on TCP/IP, but this is no longer the case. A new library including a set of new function blocks should be used instead.	Change the application to use function blocks and data types from SattBusCommLib as follows: Function Blocks BeforeAfter COMLIConnectComliSBConnect COMLIReadComliSBRead COMLIReadCycComliSBReadCyc COMLIReadPhysComliSBReadPhys COMLIWriteComliSBWrite COMLIWriteDTComliSBWriteDT Data Types BeforeAfter Comm_Channel_COMLI Comm_Channel_ComliSB
Some project constants have been removed from SupervisionBasicLib (cSinit.*), BasicLib (cEnable.*), and SupervisionLib (cInit.*). Refer to Removed Project Constants on page 134 for a list of the removed project constants.	1. If these project constants have been used in code there will be compile errors after upgrading the project. 2. If the value of the project constants was changed in the project in SV5.0 SP1a, it will lead to changed behavior of the code after the upgrade, because these project constants have been used as default values on parameters.	1. Change to the correct literal value in the places where the project constants are used. 2. Check if the value of the removed project constant was changed in the project in SV5.0 SP1a. This can be done by opening the Project Constants dialog after the upgrade and seeing if the project constants are listed. In that case the parameters previously using the project constant as a default value must be manually connected to a literal with the corresponding value.

Removed Project Constants

Some project constants have been removed from SupervisionBasicLib (cSinit.*), BasicLib (cEnable.*), and SupervisionLib (cInit.*).

SupervisionBasicLib (cSinit.*)

- cSinit.Latch shall be replaced by 'true'.
- cSinit.LevelHH shall be replaced by '80.0'.
- cSinit.LevelH shall be replaced by '60.0'.
- cSinit.LevelL shall be replaced by '40.0'.
- cSinit.LevelLL shall be replaced by '20.0'.

BasicLib (cEnable.*)

Table 5. BasicLib (cEnable)

cEnable.InputOverUnderRange		bool	Default value in library BasicLib 1.4-11 (bool): false
cEnable.OutputOverUnderRange		bool	Default value in library BasicLib 1.4-11 (bool): false

SupervisionLib (cInit.*)

Table 6. SupervisionLib (cInit.)*

cInit.AckreqAtErr		bool	Default value in library SupervisionLib 2.3-7 (bool): false
cInit.AckReqToReset		bool	Default value in library SupervisionLib 2.3-7 (bool): false
cInit.ActOnError		bool	Default value in library SupervisionLib 2.3-7 (bool): false
cInit.AEClass		dint	Default value in library SupervisionLib 2.3-7 (dint): 1

Table 6. SupervisionLib (cInit.*) (Continued)

cInit.AEConfigCableBreak		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AEConfigDetectorFault		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AEConfigDiffInput		dint	Default value in library SupervisionLib 2.3-7 (dint): 1
cInit.AEConfigDiffOutput		dint	Default value in library SupervisionLib 2.3-7 (dint): 3
cInit.AEConfigErr		dint	Default value in library SupervisionLib 2.3-7 (dint): 1
cInit.AEConfigH		dint	Default value in library SupervisionLib 2.3-7 (dint): 1
cInit.AEConfigHH		dint	Default value in library SupervisionLib 2.3-7 (dint): 1
cInit.AEConfigL		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AEConfigLoopFault		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AEConfigMaintenance		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AEConfigPrewarn		dint	Default value in library SupervisionLib 2.3-7 (dint): 1
cInit.AEConfigShortCircuit		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.AESevCableBreak		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevDetectorFault		dint	Default value in library SupervisionLib 2.3-7 (dint): 800

Table 6. SupervisionLib (cInit.*) (Continued)

cInit.AESevDiffInput		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevDiffOutput		dint	Default value in library SupervisionLib 2.3-7 (dint): 300
cInit.AESevErr		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevFeedback		dint	Default value in library SupervisionLib 2.3-7 (dint): 300
cInit.AESevH		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevHH		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevL		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevLoopFault		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevMaintenance		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevPrewarn		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AESevReleased		dint	Default value in library SupervisionLib 2.3-7 (dint): 300
cInit.AESevShortCircuit		dint	Default value in library SupervisionLib 2.3-7 (dint): 800
cInit.AlarmLimit		real	Default value in library SupervisionLib 2.3-7 (real): 40.0
cInit.ConfirmedLimitH		dint	Default value in library SupervisionLib 2.3-7 (dint): 2

Table 6. SupervisionLib (cInit.*) (Continued)

cInit.ConfirmedLimitHH		dint	Default value in library SupervisionLib 2.3-7 (dint): 0
cInit.ConfirmedLimitOr		bool	Default value in library SupervisionLib 2.3-7 (bool): true
cInit.DelayTime		time	Default value in library SupervisionLib 2.3-7 (time): TIME#10s
cInit.EnableCommonReset		bool	Default value in library SupervisionLib 2.3-7 (bool): true
cInit.EnableRangeConversion		bool	Default value in library SupervisionLib 2.3-7 (bool): false
cInit.Latch		bool	Default value in library SupervisionLib 2.3-7 (bool): true
cInit.LevelCableBreak		real	Default value in library SupervisionLib 2.3-7 (real): 1.0
cInit.LevelDetectorFault		real	Default value in library SupervisionLib 2.3-7 (real): 3.0
cInit.LevelDiff		real	Default value in library SupervisionLib 2.3-7 (real): 10.0
cInit.LevelLoopFault		real	Default value in library SupervisionLib 2.3-7 (real): 3.5
cInit.LevelMaintenance		real	Default value in library SupervisionLib 2.3-7 (real): 2.5
cInit.LevelShortCircuit		real	Default value in library SupervisionLib 2.3-7 (real): 19.0
cInit.OneLevelH		real	Default value in library SupervisionLib 2.3-7 (real): 10.0
cInit.OneLevelL		real	Default value in library SupervisionLib 2.3-7 (real): 5.0

Table 6. SupervisionLib (cInit.*) (Continued)

cInit.OutputResetDelay		time	Default value in library SupervisionLib 2.3-7 (time): TIME#1s
cInit.PrewarningLimit		real	Default value in library SupervisionLib 2.3-7 (real): 5.0
cInit.RedIncDecLim		real	Default value in library SupervisionLib 2.3-7 (real): 10.0
cInit.ResetTime		time	Default value in library SupervisionLib 2.3-7 (time): TIME#5s
cInit.ResponseTime		time	Default value in library SupervisionLib 2.3-7 (time): TIME#5s
cInit.RText		string	Default value in library SupervisionLib 2.3-7 (string): 'R'
cInit.TwoLevelH		real	Default value in library SupervisionLib 2.3-7 (real): 20.0
cInit.TwoLevelHH		real	Default value in library SupervisionLib 2.3-7 (real): 60.0
cInit.UseLevelPar		bool	Default value in library SupervisionLib 2.3-7 (bool): True

Appendix B Online Upgrade Controller Level

Introduction

The information in this appendix is intended only as a high level introduction to the online upgrade of the controller level. Detailed information appears in the controller and control software instructions.

Online Upgrade Controller Level

Redundant AC 800M controllers can be upgraded with new firmware versions online. Online upgrade is initiated from Control Builder by a nine-step wizard. Refer to the Maintenance and Troubleshooting section in *800xA - Control and I/O, Basic Control Software, Introduction and Configuration (3BSE035980RRxxxx)* for more information.

In order to use online upgrade for the controller level:

- Refer to *Industrial IT, 800xA - Control and I/O, Control Software for AC 800M, Release Notes (3BSE021377Rxxxx)* for the controller versions that support online upgrade.

- AC 800M Controllers require the workstation and server level to be of the same or higher 800xA System version/revision.

- AC 800M Controllers must be redundant. A redundant controller consists of two redundant processing units connected to I/O modules or CI modules.

- AC 800M Controller firmware and its CI modules can be upgraded independently.

    - AC 800M controller firmware and the SM810 (safety) CI module must be upgraded simultaneously.

- Different AC 800M Controllers with different 800xA System versions/revisions can coexist. This allows for extensions of an 800xA System with new AC 800M Controllers or other new 800xA System functionality without having to upgrade all existing controllers.

    – Starting from SV 5.0, upgrading to newer versions of Control Builder and/or OPC Server does not require a controller upgrade. Controllers with different firmware versions can coexist in the same network, and newer versions of Control Builder and OPC Server can connect to controllers of older versions (not older than SV 5.0). Refer to *Industrial IT, 800xA - Control and I/O, Control Software for AC 800M, Release Notes (3BSE021377Rxxxx)* for the controller versions that support coexistence.

    – Hardware types can coexist in different 800xA System versions/revisions in the same 800xA System.

    – Controllers that need to take advantage of new functionality are the only ones that have to be upgraded. Other controllers can remain untouched. This backwards compatibility is typically kept for two previous system versions.

- Upgrading nonredundant AC 800M Controllers is accomplished with minimized plant disturbance by stopping and upgrading one controller at a time. The workstation and server level can still be upgraded online, as long as the conditions are met for performing an online upgrade on the workstation and server level.

Hot swap is the method to be used for a nonredundant AC 800M controller with redundant CI modules and unchanged controller firmware.

Flowchart for Upgrading Controller Level

Figure 23 shows the upgrade flow for the controller level.
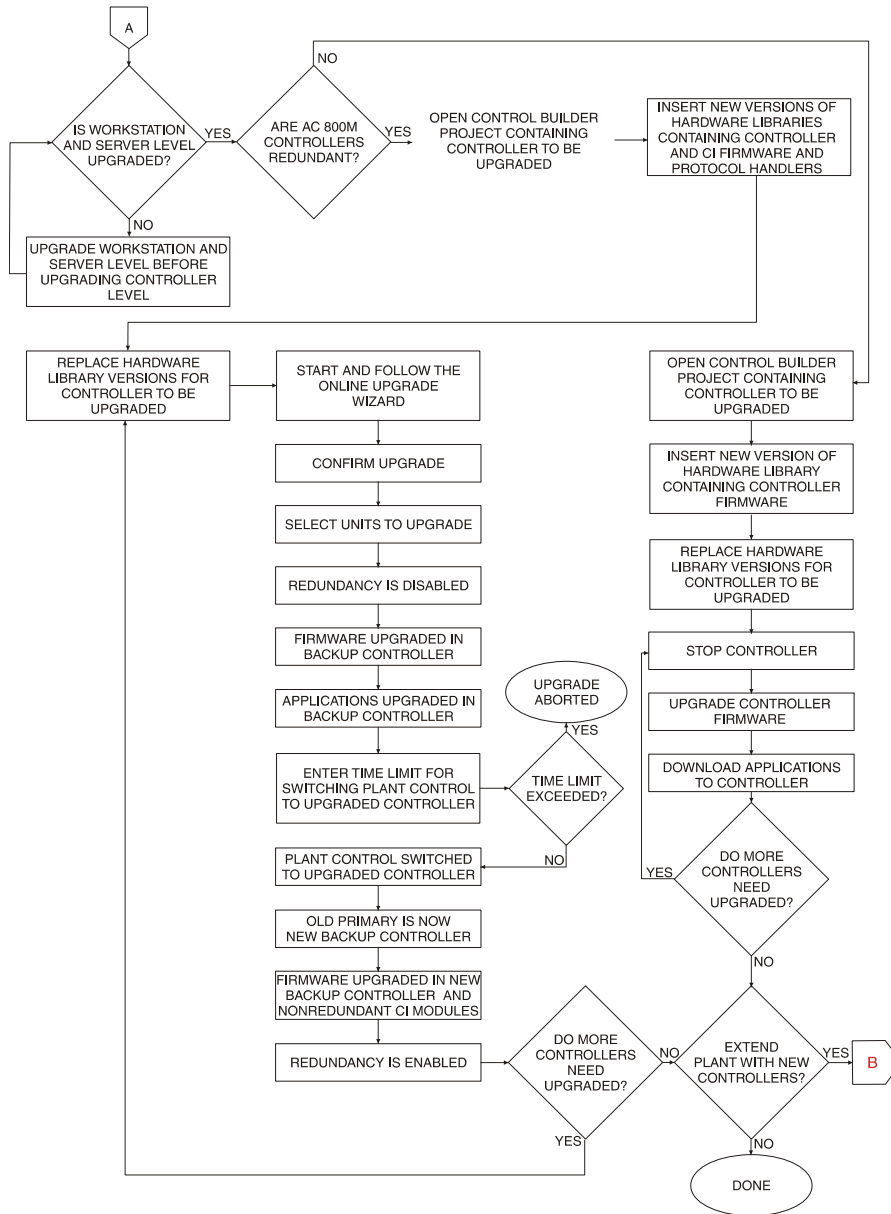
Figure 23. Online Upgrade Flowchart for Controller Level

Flowchart for Extending Controller Level

Figure 24 shows the flow for extending the controller level to add new AC 800M Controllers with the latest 800xA System version/revision to an existing plant with or without upgrading the existing AC 800M Controllers.
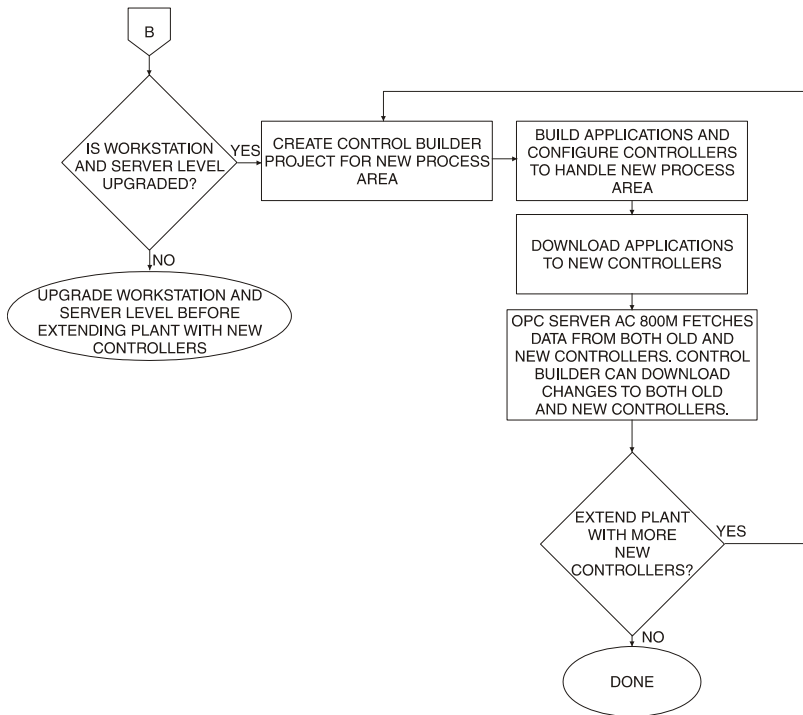
Figure 24. Flowchart for Extending Plant with New Controllers

Contact us

www.abb.com/800xA
www.abb.com/controlsystems

2PAA113553-600

Power and productivity
for a better world™

ABB