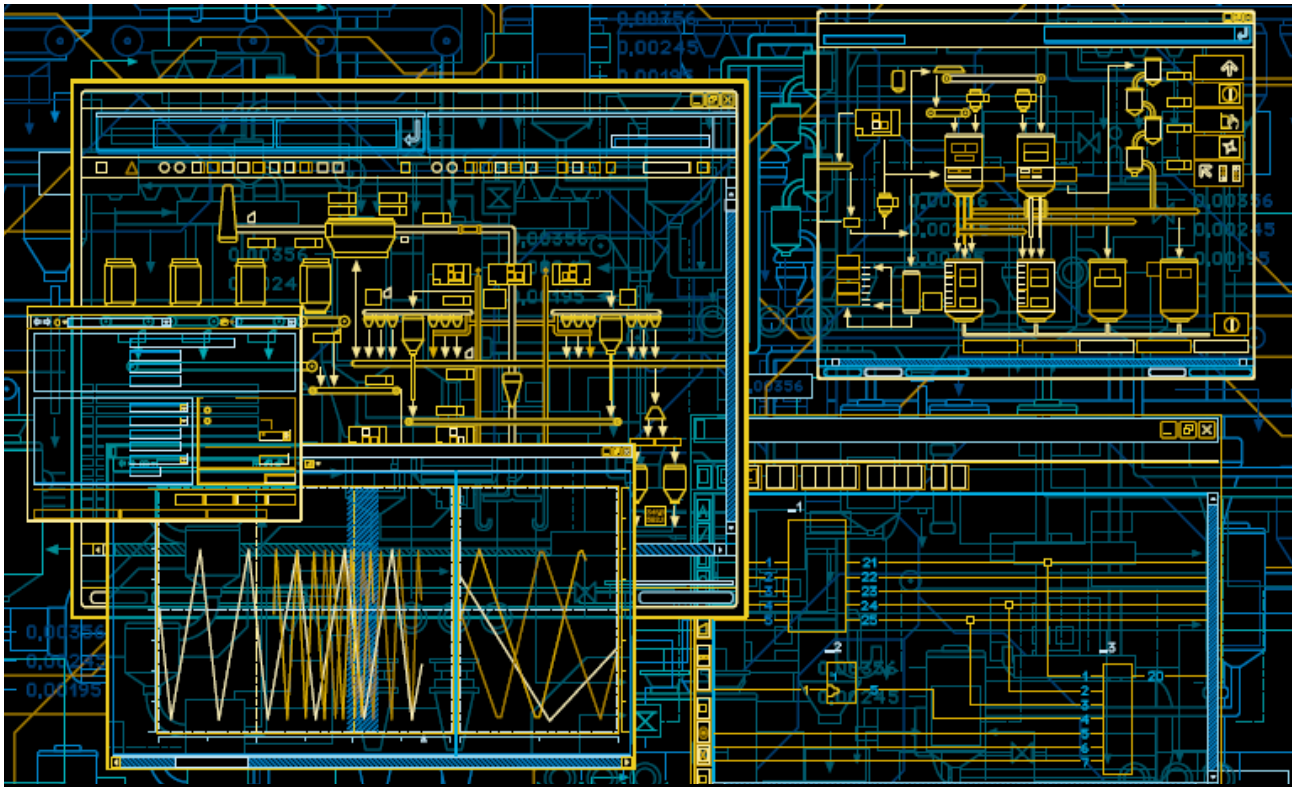


System 800xA Safety
AC 800M High Integrity Safety Manual

System Version 5.1

Power and productivity
for a better world™

System 800xA Safety
AC 800M High Integrity
Safety Manual

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. ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB product(s) described in this publication. 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.

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 89/336/EEC and in Low Voltage Directive 72/23/EEC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2003-2012 by ABB.
All rights reserved.

Release: November 2012
Document number: 3BNP004865-513 RevA Nov 2012

Safety Summary



Electrostatic Sensitive Device
Devices labeled with this symbol require special handling precautions as described in the installation section.

GENERAL WARNINGS

Equipment Environment
All components, whether in transportation, operation or storage, shall be in a noncorrosive environment.
A complete overview of environmental conditions is given in the user manuals *AC 800M Controller Hardware, 3BSE036351** on page 41 and *S800 I/O Getting Started, 3BSE020923** on page 41.

Electrical Shock Hazard During Maintenance
Disconnect power or take precautions to insure that contact with energized parts is avoided when servicing.

Network Security
The 800xA system shall be protected against deliberate, illegal intrusion. It is the responsibility of the user of the safety system to establish and maintain adequate network security measures adapted to the level of openness in the particular installation.

Safety Summary (continued)

SPECIFIC WARNINGS

Warnings related to Equipment Requirements on page 49:

For Normally De-energized Outputs, alarming is the only system reaction upon detected failures, hence an alternative alarming path shall be established by e.g connecting an external alarm device to a DO880 output configured as NE. on page 49

Warnings related to Information Requirements on page 50:

Requirements and instructions marked with the Warning symbol in this manual shall be adhered to for the system to remain in compliance with the requirements of the certification. on page 50

The user shall verify that installed versions of hardware and software modules are in compliance with the valid version of 'Annex2 of the Report on the certificate Z10 08 10 29902 005. This certificate is issued by TÜV Product Service GmbH. on page 50

Warnings related to Organization and Resources on page 52:

It is the responsibility of the end user of the product to ensure that all organizational units involved during any phase of the Safety Life Cycle of the product, possess sufficient competency. on page 52

Warnings related to Safety Lifecycle Activities on page 57:

Requirements in the application specific standards listed in the chapter Applicable Specifications on page 38 and other relevant and valid application standards shall be adhered to (e.g.EN 54, EN298). on page 57

Warnings related to Process Interface Selection on page 67:

For safety critical functions, only certified I/O modules shall be used. If non- certified I/O modules are connected to a SIL2 Application, a warning is given, but download of the Application is allowed upon engineer's approval. For SIL3 applications, download is prevented. on page 67

Safety Summary (continued)

Warnings related to AI880A High Integrity Analog Input Module on page 68:

The HART functionality of AI880A is approved to be interference free, for non safety critical use. on page 68

The use of HART routing of AI880A during operation of the plant, shall be restricted by configuration or by operational procedures. on page 68

Warnings related to AI880A as DI - Loop Supervised Digital Input Module on page 68:

If the AI880A as DI - Loop Supervised Digital Input Module is used with an external field loop resistor network, this resistor network shall be configured in accordance with the guidance in the user manual “S800 I/O - Modules and Termination Units, 3BSE020924* page 41”. on page 69

Warnings related to DI880 High Integrity Digital Input Module on page 69:

The sequence of event functionality of DI880 is certified interference free, for non safety critical use. on page 69

If an input loop of DI880 is externally powered, the loop shall be equipped with a current limiting device in the signal line. The current shall be limited to 200 mA. on page 69

Safety Summary (continued)

Warnings related to DO880 High Integrity Digital Output Module on page 70:

Normally De-energized DO880 channels can only be used in High Demand applications provided the demand rate of the process exceed 10 minutes. on page 70

Normally De-energized DO880 channels used in loops were a false trip directly cause a hazardous event (e.g. fire extinguishing with CO2) are restricted to SIL2 if the field device has a response time that is shorter than 10ms. on page 70

Normally De-energized DO880 channels are meant to be used with latched field devices where no continuous energized safe state is required. on page 70

Normally De-energized DO880 channels shall not be used in EN954-1 applications. on page 70Normally Energized DO880 channels used in EN954-1 applications; Category 4 is supported from DO880 product revision G, older product revisions support Category 3. on page 70

When Normally Energized or Normally De-energized DO880 channels are configured as inverted outputs, see Table 13, care must be taken to handle the fact that at application delete the reaction of the outputs will activate the inverted function. Application delete occurs when manually deleting an application or manually selecting cold re-start at re configuration. Inverted out channels are not allowed in SIL3 applications. on page 70

For channels of the DO880 module configured as Normally Energized Degraded Mode (NE-DM), the Safety Integrity Level is SIL3 Low demand, or reduced to SIL2 High demand during the Degraded Mode time (72 hours). on page 71

Safety Summary (continued)

Warnings related to Power Supply on page 72:

The AC 800M HI and the connected S800 I/O system (including field power) shall be supplied from a SELV or PELV power supply connected through the power voter SS823. Provided that each power supply contain or are equipped with double over voltage protection (two independent means of limiting the output voltage to max 30 VDC), the SS823 can be omitted. on page 72

If any field device connected to the AC 800M HI is externally powered, the device shall be supplied from a SELV or PELV power supply connected through the power voter SS823. Provided that each power supply contains or is equipped with double over voltage protection (two independent means of limiting the output voltage to max 30 VDC), the SS823 can be omitted. When externally powered transmitters are connected to the analog input module AI880A via a fuse rated 60V/<= 0.1A, the SS823 can be omitted for loops up to SIL2. on page 72

Warnings related to Operator Interface on page 72:

If used, the Reset all Forces input shall be connected to an impulse type panel button. on page 73

Safety Summary (continued)

Warnings related to Software Architecture on page 79:

Modification of SIL3 application/task connection shall always be followed by a cold restart of the controller. The need for changing task connections can be avoided by changing task properties. on page 79

For all safety critical Applications, correct SIL shall be selected in Control Builder M Professional. on page 80

Some of the function block types in MMSCommLib for communication between applications in the same controller, are certified SILx Restricted. This means that they are allowed to be used in SIL classified applications, but the communicated data can not be used for safety critical functions. on page 80

For exchanging safety critical data between Applications, the Control Modules MMSDefxxx and MMSReadxxx shall be used. The Valid parameter of the MMSReadxxx shows whether the data can be trusted. In case of invalid data, the application shall bring the related safety functions to safe state. on page 81

The Control Modules MMSDefxxx and MMSReadxxx are designed to be executed every scan of the application, hence any conditional execution (for example, use of ExecuteControlModules() inside an if statement) shall be avoided. on page 81

When establishing a safety critical communication link, the UniqueID parameter represents the safety identification of the data and shall be unique within the plant network. The UniqueID shall be identical in the MMSDefxxx and MMSReadxxx. on page 81

The Control Modules MMSReadxxx provides parameters SILOutx showing the SIL level of the communicated data. The application shall ensure that the data origins from the same or higher SIL before it can be used in any way that can interfere with the safety action of the SIL classified Application. on page 81

Data originating from SILxRestricted System Functions/Library types and data originating from NONSIL marked parameters (see Appendix A, Certified Libraries), shall not be communicated via the MMSDefxxx Control modules. If this restriction is violated in a SIL3 application, it might result in a Safety Shutdown of the related AC 800M HI controller(s). on page 81

Safety Summary (continued)

When safety critical signals are communicated between Applications (in the same or different controllers), the FDRT of the communication subsystem shall be configured to match the process safety time of the controlled process. Requirements for process safety time given in relevant application standards (e.g. EN 298) shall be considered and fulfilled. on page 82

In Applications where inputs reside in other Applications (and other controllers), the design shall take into consideration the possibilities that the “remote” inputs can be forced independent of the Force Control setting of the “local” Application. on page 83

A philosophy for using either positive or negative logic shall be established and followed consistently for the whole plant. Naming of variables should reflect this philosophy to avoid confusion. on page 84

A philosophy for using retain/cold retain values shall be developed based on the characteristics of the process to be controlled. The philosophy shall be followed consistently for the whole plant. on page 84

If automatic restart of the process after a power failure is not desired, the application program shall contain mechanisms to achieve the desired behavior. on page 85

The input modules certified for use in safety critical applications can be configured to enter a predefined safe value upon a detected failure. The modules can also be configured to “keep current value” upon a failure, when this option is used, the application shall be designed to handle the process safely upon faulty input signals. Keep current value is not allowed in machine safety applications. on page 85

The application program shall be designed to handle faulty input and output signals in accordance with the safety requirements for the plant. on page 86

To avoid dangerous situations at controller restart, care shall be taken during application design, e.g. by using the IO.Status value to interlock unwanted start-up actions. on page 86

When working with arithmetic operators and Mathematical System functions, the user must take care to avoid illegal parameters, out-of-range and overflow situations. on page 86

Safety Summary (continued)

Warnings related to Programming Languages and Libraries on page 86:

For an overview of certification level and safety restrictions for System Functions and Library Types, see Appendix A, Certified Libraries. on page 87

It is not allowed to use Functions, Function Blocks or Control Modules marked as SILxRestricted in a way that can influence the safety function of a SIL classified application. If such code affects an output from a SIL3 application, it might result in a Safety Shutdown. on page 88

It is not allowed to use output parameters from Function Blocks or Control Modules marked with NONSIL in the parameter description in a way that can influence the safety function of a SIL classified application. If such code affects an output from a SIL3 application, it might result in a Safety Shutdown. on page 88

If a faceplate with possibility for operator changes to objects in a SIL classified application is to be created, the guidelines for Confirmed Write support in chapter Access Management Settings on page 111 shall be followed. on page 88

Warnings related to Control Builder M Professional - Settings and Restrictions on page 89:

If the EN (Enable) input on functions and function blocks is used in FBD, great care shall be taken to avoid unintentional stop of application execution. on page 91

Warnings related to Controller Settings and Restrictions on page 91:

When setting the “Application type” due care shall be taken to the properties of the process to be controlled by the AC 800M HI. on page 93

FDRT (Fault Detection and Reaction Time) is the maximum time from an internal error occur in the controller, to the defined action is taken. This time shall be set according to the process safety time and the demand rate of the controlled process. on page 93

Safety Summary (continued)

Warnings related to I/O Module Settings on page 100:

To ensure safe operation and adaptation to the process, AI880A High Integrity Analog Input Module, shall be configured according to the directions in Table 10. Safety Related Settings of AI880A on page 100. on page 100

To ensure safe operation and adaptation to the process, AI880A as DI - Loop Supervised Digital Input Module shall be configured according to the directions in Table 11. Safety Related Settings of AI880A as DI - Loop Supervised on page 103. on page 102

To ensure safe operation and adaptation to the process, DI880 shall be configured according to the directions in Table 12. Safety Related Settings of DI880 on page 104. on page 104

To ensure safe operation and adaptation to the process, DO880 shall be configured according to the directions in Table 13. Safety Related Settings of DO880 on page 105. on page 105.

Warnings related to Configuration of DRT and FDRT on page 107

The Demand Response Time, DRT and Fault Detection and Reaction Time, FDRT of a loop can be calculated using the figures in Table 14. Response times for SIL2 systems on page 107.FDRT for SIL3 loops can be calculated using the formula described in FDRT for SIL3 loops page 108 on page 107

Warnings related to *FDRT for SIL3 loops* on page 108

When FDRT is required to be shorter then the configured diagnostic cycle time (FDRT) user must in the application code connect channel error from the I/O in such a way that the affected loop is brought to safe state. on page 109

Safety Summary (continued)

Warnings related to *FDRT for SIL3 loops* on page 108

During Warm Download and Hot Insert of SM811 the calculated shorter FDRT is superseded by the configured diagnostic cycle time (FDRT). It is the responsibility of the end user, via organizational measures, ensuring that this can be done in a safe way. on page 109

Warnings related to Access Management Settings on page 111:

The “maximum number of forces” property shall be set based on the characteristics of each application and the operation philosophy of the plant. on page 112

The SIL Access level shall be configured based on the characteristics of each variable and the operation philosophy of the plant. on page 113

Warnings related to User Defined Diagnostics on page 114:

If parameter errors on function blocks or control modules shall lead to a system reaction, this shall be programmed in the application program. on page 114

Warnings related to Software Verification on page 117:

The Source Code Report shall be carefully reviewed to verify correct application programming. on page 117

Warnings related to Modification Testing on page 118:

Modifications affecting I/O connections shall be verified by testing in the running AC 800M HI controller. on page 118

Safety Summary (continued)

Warnings related to Installation and Commissioning on page 119:

If required environmental conditions during operation are not yet established, interim measures shall be taken to avoid damage of the equipment. on page 119

To ensure a safe mechanical installation and assembling of the equipment at installation site, the guidance described in the user manuals AC 800M Controller Hardware, 3BSE036351* page 41 and S800 I/O Getting Started, 3BSE020923* page 41 shall be followed. on page 119

To ensure a safe electrical installation and power up of the equipment at installation site, the guidance described in the user manuals 800xA System, Site Planning, 3BUA000258* page 41, AC 800M Controller Hardware, 3BSE036351* page 41 and S800 I/O Getting Started, 3BSE020923* page 41 shall be adhered to. on page 120

Warnings related to Program Download and Startup on page 120:

During online download (normal application update or LEG), the user shall take appropriate precautions dependant of the properties and the time demands of the process under control. on page 120

To ensure a safe download and startup of applications to the AC 800M HI, the steps described in Table 17. Program Download Procedure on page 121 shall be performed. on page 121

Warnings related to Program Download with LEG on page 123:

Program Download with LEG to an AC 800M HI is not allowed if any changes to the controller configuration is made. on page 123

To ensure a safe program Download with LEG to the AC 800M HI, the steps described in Table 18. Program Download with LEG Procedure on page 123 shall be performed. on page 123

The displayed data in the evaluation report on the Control Builder M Professional screen can not be used to validate the safety function of the application. on page 124

Safety Summary (continued)

Warnings related to Operation Procedures on page 127:

The operation procedures shall emphasize the operator's responsibility to verify his operations by checking the Confirm Operation dialog. on page 128

If the HART routing functionality of AI880A is not restricted by the configuration settings of the module, the operation procedures shall include restrictions for use of this function. on page 129

Warnings related to Maintenance Procedures on page 129:

In redundant DO880 configurations, faulty DO880 modules shall be removed from the system within the repair time of 72 hours. on page 130

Online replacement (Hot Insert) of the SM811 will lead to a short stop of the SIL3 applications. The stop time is limited by the configured FDRT. on page 130

Safety Summary (continued)

Warnings related to Application Modifications on page 132:

To verify that no unintended changes to the SIS part of the system are done, always examine the difference report before download, (see Difference Report on page 115). on page 132

Warnings related to Firmware Upgrade on page 132:

To ensure a safe Firmware Upgrade of a stopped AC 800M HI, the steps described in Table 19. Firmware Upgrade Procedure on page 133 shall be performed. on page 133

Before Online Upgrade is started, check that the “Online Upgrade Handover Limit” is set in accordance with the time demands of the process under control. on page 134

Online Upgrade of an AC 800M HI is not allowed if any changes to the controller configuration or application is made. on page 135

To ensure a safe Online Upgrade of firmware in a running AC 800M HI, the sequence described in Table 20. Online Upgrade Procedure on page 136 shall be performed. on page 135

Safety Summary (continued)

SPECIFIC CAUTIONS

Cautions related to Equipment Requirements on page 49:

If the AC 800M HI is used without an 800xA Operator Workplace, the system alarm output (O2) on the SM810/SM811 shall be connected to an external alarm device in order to alarm detected errors, see Physical I/O for Operator and Maintenance Personnel Interaction on page 72. This is also recommended when using 800xA Operator Workplace in order to achieve a diverse alarming path. on page 49

Cautions related to System Structure Selection on page 61:

The local built-in electrical ModuleBus cannot be used in configurations with redundant AC 800M HI. on page 65

Redundant AC 800M HI processor units, require redundant optical Cluster Modems. on page 65

In redundant AC 800M HI systems, the CEX-Bus shall always be connected via the CEX-Bus Interconnection Unit, BC810. on page 66

Cautions related to Process Interface Selection on page 67:

If the input loops of AI880A are externally powered, or another risk of applying 24V to the signal line is present, the loop should be equipped with a fuse (rated <= 0.1A) in the signal line to avoid possible overheating of the shunt stick during fault situations. on page 68

If the input loops of AI880A as DI are externally powered, or another risk of applying 24V to the signal line is present, the loop should be equipped with a fuse (rated <= 0.1A) in the signal line to avoid possible overheating of the shunt stick during fault situations. on page 69

Safety Summary (continued)

Cautions related to Site Planning on page 75:

To ensure a safe and reliable mechanical installation and assembling of the equipment at installation site, the guidance described in the referred manuals shall be adhered to. If not all recommendations given in these manuals are strictly followed, the responsibility lies with the user to demonstrate an equivalent safe and reliable assembling and installation of the equipment. on page 75

Cautions related to Software Architecture on page 79:

To avoid availability problems due to transient high traffic situations in the TCP/IP communication, the Timeout parameter of the MMSReadxxx Modules should be set to 5 seconds. on page 82

To avoid time-out/invalid data on peer-to-peer links during Online Upgrade of firmware, the 'OLUTimeOut' parameter of the MMSReadxxx Modules shall be set to at least 10 seconds longer than the 'Online Upgrade Handover Limit' configured in the corresponding server (controller) to be upgraded. on page 82

Do not configure cold retain on parameters of SILxRestricted types and NONSIL marked parameters used in SIL3 applications. Doing so will obstruct automatic start after a Power Failure of the system. on page 84

Cautions related to Mechanical Completion on page 119:

Before connecting any external devices to the AC 800M HI, voltage level and polarity shall be verified. on page 120

Cautions related to Online Upgrade on page 134:

To avoid time-out/invalid data on peer-to-peer links, the 'Access Enable' input in all clients shall be activated. on page 135

Safety Summary (continued)

TABLE OF CONTENTS

About This Book

General....28
- Purpose and Scope of the Manual....28
- Intended User....29
- Manual Organization....29

Warning, Caution, Information, and Tip Icons....30
Document Conventions....31
Terminology....31
Applicable Specifications....38
- Laws and Directives....38
- General Safety Standards....38
- Additional Approvals for Safety Compliance....39
- Application Standards (to the extent applicable)....40
- Withdrawn Standards....40

Related Product Documentation....41

Section 1 - Introduction

Safety Principles....43
Product Overview....46
- Mode of Operation....48
- Redundancy....48

Prerequisites and Requirements....49
- Equipment Requirements....49
- Information Requirements....50
- Restrictions for Use of the System....50

Section 2 - Management of Functional Safety

Organization and Resources 52
Safety Planning 52
Implementation and Monitoring 52
Assessment, Auditing and Revisions 53
Auditing and Revision Procedures 55
Configuration Management 56

Section 3 - Safety Lifecycle Activities

Process Hazard and Risk Assessment 57
Allocation of Safety Functions 58
Safety Requirement Specifications 59
System Design and Engineering 61
System Structure Selection 61
Redundancy 64
Redundant AC 800M HI Controller (PM865 with SM810/SM811) 64
Redundant Optical ModuleBus 65
Redundant Electrical ModuleBus 65
Redundant High Integrity I/O Modules 65
Redundant CEX-Buses 66
Redundant Power Supply 66
Process Interface Selection 67
Allocation of I/O Modules 67
AI880A High Integrity Analog Input Module 68
AI880A as DI - Loop Supervised Digital Input Module 68
DI880 High Integrity Digital Input Module 69
DO880 High Integrity Digital Output Module 69
Allocation of I/O Channels 71
Communication Interfaces 71
Power Supply 71
Operator Interface 72
Physical I/O for Operator and Maintenance Personnel Interaction 72
800xA Operator Workplace 74

Maintenance/Engineering Interface 74
Site Planning 74
Enclosures 75
Application Software 76
Safety Lifecycle 76
Application Safety Requirement Specification 77
Safety Validation Planning 77
Application Design and Development 77
General 77
Software Architecture 78
Programming Languages and Libraries 85
Control Builder M Professional - Settings and Restrictions 88
Controller Settings and Restrictions 90
I/O Module Settings 99
Configuration of DRT and FDRT 106
Access Management Settings 110
User Defined Diagnostics 113
Configuration Management 113
Test and Verification 114
Source Code Report 114
Difference Report 114
Test Mode 115
Simulation 115
Hardware Testing 115
Software Module Testing 116
Software Verification 116
Software Integration Testing 116
Integration of Application Software with the System Hardware 116
System Integration Testing 117
Modification Testing 117
Installation and Commissioning 118
Transportation and Storage 118

Mechanical Completion 118
Electrical Completion 118
Program Download and Startup 119
Program Download 120
Program Download with LEG 122
Controller Restart 123
Commissioning Test Activities 124
Safety Validation 125
Operation and Maintenance 126
Operation and Maintenance Planning 126
Operation Procedures 126
Maintenance Procedures 128
Routine Maintenance 128
Fault Finding and Repair 128
Training and Qualifications 130
Proof Testing and Inspection 130
Modification during Operation 131
Application Modifications 131
Firmware Upgrade 131
Upgrade of stopped controllers 132
Online Upgrade 133
Configuration Management 136
Decommissioning 136

Appendix A - Certified Libraries

Introduction 139
System Functions 140
Library Types 146
AlarmEventLib 147
BasicLib 147
FireGasLib 149
IconLib 149
MMSCommLib 150

ProcessObjBasicLib 152
ProcessObjExtLib 154
SerialCommLib 156
SignalBasicLib 156
SignalLib 157
SignalSupportLib 158
SupervisionBasicLib 159
SupervisionLib 161

Appendix B - Certified Hardware Components

Safety Certified Hardware Components 163
Safety Relevant Hardware Components 164
Interference free Hardware Components 166

INDEX

About This Book

General

Purpose and Scope of the Manual

This manual provides guidelines and safety considerations related to all safety lifecycle phases of an AC 800M HI. The recommendations and requirements in this manual shall be considered and implemented during design, installation, commissioning, operation and decommissioning of the product.
The manual is an integral part of the AC 800M HI certification and has been approved by TÜV.

The manual is structured to comply with the safety lifecycle described in IEC 61511, and addresses all phases from initial concept, design, implementation, operation and maintenance through to decommissioning of an installation.
The scope of the manual is limited to activities related to the engineering and operation of an AC 800M HI, but where special requirements or expectations to the output from earlier phases (e.g. process hazard and risk assessment) exist, they are listed. Similarly the manual does not describe all requirements to an engineering project execution, but relates the AC 800M HI specific requirements to such a process as described in IEC 61511.
The manual contains requirements for quality systems, documentation and competence; these requirements are NOT replacement for the user company's quality systems, procedures and practices.
Local statutory regulations, should they be stricter, shall always take precedence over this manual.



The safety instructions of this manual take precedence over corresponding instructions given in other user manuals to the system.



For detailed technical information and operation instructions, the reader is referenced to Related Product Documentation on page 41.

Intended User

This manual is intended for all people involved in the complete lifecycle of the AC 800M HI, including those responsible for planning of safety activities. The safety lifecycle of the AC 800M HI, comprise all activities from the equipment arrives from the factory until it is safely disposed after the operation period.

Manual Organization

This manual is organized in three sections as described below; this introduction gives a short summary of the content of each section as guidance to the reader.

Section 1 - Introduction

Describes general safety principles applicable to the AC 800M HI and its use. This section also contains a brief overview of the main characteristics and intended use of the AC 800M HI.

Section 2 - Management of Functional Safety

Provides input to the management activities that are necessary to ensure that the functional safety objectives are met during all phases of the lifecycle of the AC 800M HI.

Section 3 - Safety Lifecycle Activities

Contains guidelines and requirements related to the use of the AC 800M HI during all phases of its lifecycle. To make information available as easy and intuitive as possible to the user, this section is organized in accordance with the safety lifecycle process as defined in IEC 61511. E.g. information related to commissioning work is found in the sub-clause “Installation and Commissioning”.

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 that could result in *electrical shock.*



Warning icon indicates the presence of a hazard that could degrade the safety function of the system, hence result in *personal injury or death.*



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.

Information marked with the Tip icon is regarded as guidance of good practice, but not required.

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.

Document Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Terminology

A complete and comprehensive list of Terms is included in the Industrial^{IT} Extended Automation System 800xA, Engineering Concepts instruction (3BDS100972*). The listing included in Engineering Concepts includes terms and definitions as they 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 may be included here as part of this document.

The following terms and abbreviations are defined either by IEC 61508/IEC 61511 (in **bold**) or by ABB.

Term	Description
AC 800M HI	AC 800M High Integrity
AI	Analog Input
AK 1-6	Anforderungs Klasse 1 to 6 (Requirement Class, RC) according to the withdrawn standards DIN V 19250 / DIN V VDE 0801.
Application	User-defined logic. Used in Control Builder M Professional to denote a "container" for executable programs and data that are grouped together.
BPCS	Basic Process Control System (IEC 61511)
CAT	Category of safety related equipment according to the withdrawn standard EN-954-1.
CC	Continuous Control output, no "trip" direction is defined. Safe state is defined as de-energize.
CEX-Bus	Communication Expansion Bus

Term	Description
Channel	Element or group of elements that independently perform(s) a function.
CM	Cluster Modem
Common cause failure	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure.
Controller configuration	Hardware configuration or setup of a controller, including configuration of I/O, communication, access variables, resources/tasks (interval time, priority, etc.) in addition to the I/O connection.
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Critical Loop	Consist of all components involved in reading inputs (from the terminal of the input module), executing safety application and controlling the outputs (to the terminals of the output module).
CTA	Compiler Test Application, an automatically generated Application used to verify that the IEC61131-3 compiler works properly.
DRT, Demand Response Time	Time from a demand to a sub-system and until the correct state on this sub-system output, is achieved.
DI	Digital Input
Diversity	Different means of performing a required function.
DO	Digital Output
ESD	Emergency ShutDown
F&G	Fire and Gas (detection system)
Failure	The termination of the ability of a functional unit to perform a required function.

Term	Description
Fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
Fault avoidance	Use of techniques and procedures, which aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults (NOTE: Assuming safety functions, not process availability issues).
FBD	Function Block Diagram
FDRT, Fault Detection and Reaction Time	The maximum time from an error occurs to the defined action is taken.
Force	Forcing an I/O variable causes a stop in the automatic update, and manual entry of values is possible. When an input channel is forced, the forced value is passed to the Application. When an output channel is forced, the forced value is passed to the output module.
FPGA	Field Programmable Gate Array
FPL	Fixed Program Language (IEC 61511)
FSA	Functional Safety Assessment
FVL	Full Variability Language (IEC 61511)
Gray channel	Part of a system or function where any potential influence on safety is detected externally from the gray channel by the safety system.
Hot replacement	Replacement of hardware that may be done with power connected to the unit.
IL	Instruction List

Term	Description
Interference free	Hardware and software functions certified to be used in AC 800M HI for non safety related functions.
LD	Ladder Diagram
LEG	Load Evaluate Go: A function to enable dynamic comparison between running application and new application.
Logic solver (IEC 61511)	That portion of either a BPCS or SIS that performs one or more logic function(s). Note: Sensors and final elements are not part of the logic solver.
LVL	Limited Variability Language (IEC 61511)
Mode of operation	- Low demand: where the frequency of demands for operation on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency. - High demand or continuous: where the frequency of demands for operation on a safety-related system is greater than one per year or greater than twice the proof-test frequency.
MTU	Module Termination Unit
NC	Normally Closed
ND	Normally De-energized output, energize to trip Safe state is defined as de-energize.
NE	Normally Energized output, de-energize to trip Safe state is defined as de-energize.
NO	Normally Open
On-line replacement	Replacement of hardware/software parts without affecting the process under control.

Term	Description
PELV	Protected Extra Low Voltage (earthed SELV) An electrical system in which the voltage cannot exceed ELV (IEC 61131-2: 60V DC) under single fault conditions except earth faults in other circuits, (IEC 61140 ch. 3.26.2).
PFD	Probability of Failure on Demand
POU	Program Organization Unit
Proof Test	Test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality.
PST	The Process Safety Time is defined as the time a process can withstand an incorrect control signal.
Random hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.
RCU	Redundancy Control Unit (part of redundant PM86x)
RCU-link	Cable to be connected between two redundant PM86x modules.
Redundancy	Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information.
RRF	Risk Reduction Factor
Safety Critical	Hardware and Software functions classified SIL1-3.
Safety function	Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the equipment under control, in respect of a specific hazardous event.
Safety integrity	Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Term	Description
Safety integrity level	Discrete level for specifying the safety integrity requirements, in IEC 61508 and IEC 61511, level 4 has the highest level of safety integrity and level 1 the lowest.
Safety Layer	An additional layer on top of a communication protocol (additional to the ISO layers) realized in the safe environment. The intention is to cover all potential faults described in the deterministic fault model, without analyzing in detail all elements of the communication link. These elements can then be viewed as a gray channel.
Safety lifecycle (IEC 61511)	Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.
SELV	Safety Extra Low Voltage An electrical system in which the voltage cannot exceed ELV (IEC 61131-2: 60V DC) under single fault conditions including earth faults in other circuits, (IEC 61140 ch. 3.26.1).
SFC	Sequential Function Chart
SFC - Simultaneous Sequence	A SFC structure that allows several branches to execute simultaneously.
SFC - Sequence Selection	A SFC structure that allows execution in only one of several alternative branches.
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function (IEC 61511)
SIL	Safety Integrity Level according to IEC 61508 and IEC 61511.
SIL2	Hardware and software functions certified according to SIL2 to be used to control safety devices in a safety system.

Term	Description
SIL2 Restricted	The Function, Function Block or Control Module can be used in a SIL1-2 Application, but the data from the outputs may not be used in the critical loop.
SIL3	Hardware and software functions certified according to SIL3 to be used to control safety devices in a safety system.
SIL3 Restricted	The Function, Function Block or Control Module can exist in a SIL3 Application, but the data from the outputs shall not be used in the critical loop even if a safety layer is added.
SIS	Safety Instrumented System (IEC 61511)
SOE	Sequence Of Event
ST	Structured Text
Sub-system	Part of a system (e.g. component as I/O module, I/O system or software “package”).
Synch Link	Cable to be connected between two redundant SM811 modules.
Task	A task is an execution control element that is capable of starting, on a periodic basis, the execution of a set of POUs (Programs, Function blocks, functions, etc.).
Validation (IEC 61511)	Activity of demonstrating that the SIF(s) and SIS(s) under consideration after installation meet in all respects the safety requirements specification.
Verification (IEC 61511)	Activity of demonstrating for each phase of the relevant safety lifecycle by analysis and/or tests, that, for specific inputs, the output meet in all respects the objectives and requirements set for the specific phase.

Term	Description
VMT	Virtual Machine Test, an automatically generated Application used to verify certain functions in the AC 800M HI.
Watchdog	Combination of diagnostics and an output device (e.g. a switch) for monitoring of the correct operation and taking action upon detection of an incorrect operation.

Applicable Specifications

This product meets the following laws and standards.

Laws and Directives

2006/95/EEC	Low Voltage Directive
2004/108/EEC	EMC Directive
93/68/EEC and amendments	CE marking Directive
98/37/EC	Safety of Machinery (to the extent applicable)
94/9/EC – ATEX directive	Electrical and mechanical equipment and protective systems, which may be used in potentially explosive atmospheres

General Safety Standards

IEC 61508	1999/ 2000	Functional safety of electrical/electronic/programmable electronic safety-related systems
ISO 13849-1	2006	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design
IEC 62061	2005	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN 954-1	1996	Safety of machinery - Safety-related parts of control systems

EN 61131-2	2007	Programmable controllers – equipment requirements and test
EN 60204-1	2006	Safety of machinery - Electrical equipment of machines Part 1: General requirements (to the extent applicable)
EN 61000-6-4	2007	Generic standard - Emission for industrial environments
EN 61000-6-2	2005	Generic standard - Immunity for industrial environments
IEC 60079-0 Ed. 3.1(1)	2004	Electrical apparatus for explosive gas atmospheres Part 0: General requirements
IEC 60079-15 Ed. 2.0(1)	2001	Electrical Apparatus for Potentially Explosive Atmospheres Type of Protection n

(1) The AC 800M HI is designed in accordance with this standard. The standard is not included in the certification.

Additional Approvals for Safety Compliance

UL 508	1998	Industrial Control Equipment
UL 1998	2004	Standard for Software in Programmable Components
FM 7605(1))	1999	Programmable Logic Control based Burner Management Systems
CSA 22.2.NO.142-M1987(2)	2000	Process Control Equipment
EN 50178	1997	Electronic equipment for use in power installations

(1) Only a selected number of AC 800M HI boards are certified according to FM7605
(2) The AC 800M HI is designed in accordance with this standard. The standard is not included in the certification.

Application Standards (to the extent applicable)

IEC 61511	2003	Functional safety - Safety Instrumented Systems for the process industry sector
ISA S84.01	2004	Application of safety instrumented systems for the process industries
ISO 10418 (API RP 14c)(1)	1993	Petroleum and natural gas industries – offshore production platforms – Analysis, design, installation and testing of basic surface safety systems
EN 50156-1	2004	Electrical equipment for furnaces
EN 298 Ch 8,9,10	2003	Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
EN 54-2 and -4	1997	Fire detection and fire alarm systems
NFPA 72	2007	National Fire Alarm Code
NFPA 79	2007	Electrical Standard for Industrial Machinery
NFPA 85 Ch 4.6.3	2007	Boiler and Combustion Systems Hazards Code (compilation of 8501 – 8506)
prENV 1954(1)	1995	Internal and external fault behavior of safety-related electronic parts of gas appliances

(1) The AC 800M HI is designed in accordance with this standard. The standard is not included in the certification.

Withdrawn Standards

DIN V 19250 (withdrawn)(1)	1994	Fundamental safety aspects to be considered for measurement and control equipment
DIN V VDE 0801 inc. A1 (withdrawn)(1)	1990	Principles for computers in safety-related systems
DIN VDE 0116 (withdrawn)(1)	1989	Electrical equipment for furnaces

(1) The AC 800M HI is designed in accordance with this withdrawn standard.

Related Product Documentation

A complete list of all documents applicable to the 800xA Industrial^{IT} Extended Automation System is provided in Released User Documents, 3BUA000263*. This document lists applicable Release Notes and User Instructions. It is provided in PDF format and is included on the Release Notes/Documentation media provided with your system. Released User Documents are updated with each release and a new file is provided that contains all user documents applicable for that release with their applicable document number. Whenever a reference to a specific instruction is made, the instruction number is included in the reference.

The table below lists all product documents referenced in this instruction.

Category	Title	Description
System	800xA System, Site Planning, 3BUA000258*	User's guide
	System 800xA 5.1 Network Configuration, 3BSE034463*	Design and Configuration
	800xA System Guide, 3BSE041434*	Technical Data and Configuration Information
Hardware	AC 800M Controller Hardware, 3BSE036351*	Hardware and Operation
	S800 I/O Getting Started, 3BSE020923*	User's guide
	S800 I/O - Modules and Termination Units, 3BSE020924*	User's guide
	800xA - Safety, Reliability and Availability Data, 3BSE034876*(1)	User's guide

Category	Title	Description
Software	System 800xA Control 5.1 AC 800M Configuration, 3BSE035980*	Introduction and Configuration
	System 800xA Control 5.1 AC 800M Planning, 3BSE043732*	Introduction and Design
	System 800xA Control 5.1 AC 800M Binary and Analog Handling, 3BSE035981*	Analog and Binary Handling
	AC 800M 5.1 Communication Protocols, 3BSE035982*	Protocols and Design
	System 800xA 5.1 Rev A Release Notes New functions and known problems, 2PAA107250-510*	Release Notes

(1) The document is not distributed on media, but available through ABB web services.

Section 1 Introduction

Safety Principles

In most situations, safety is best achieved by an inherently safe process design whenever practicable. When this is not practicable, the residual risk shall be identified and handled by one or more protective systems.
The overall safety requirements of a process are identified by carrying out hazard and risk assessment, the identified safety requirements are allocated to safety functions and related protection systems (protection layers). Depending on the number of protection layers identified, and the risk reduction they provide, the need for a Safety Instrumented System (SIS) may arise. For each identified safety function the Safety Integrity Level (SIL) shall be identified.

The AC 800M HI is certified to handle safety functions with SIL2 and SIL3 requirements.

Important characteristics of the SIS are the response time during normal operation; Demand Response Time (DRT), and the response time during internal faults; Fault Detection and Reaction Time (FDRT) for single channel 1oo1D systems. For AC 800M HI this is the SIL2 configuration. These characteristics of the SIS relates to the Process Safety Time (PST) of the process to be controlled. For definitions of terms and abbreviations like DRT, FDRT and PST, see Terminology on page 31.

As the initiator and actuator response time varies for various devices, the SIS shall be configured to guarantee a logic solver FDRT (see Figure 1 below) to meet the process requirements according to the applicable industrial standards. In the 1oo2D System structure (SIL3) first faults are controlled by the system architecture. This means first faults are detected and reacted upon within the application interval time. In the 1oo2D System Structure the FDRT is not used to comply with requirements to detect faults within the Process Safety time.

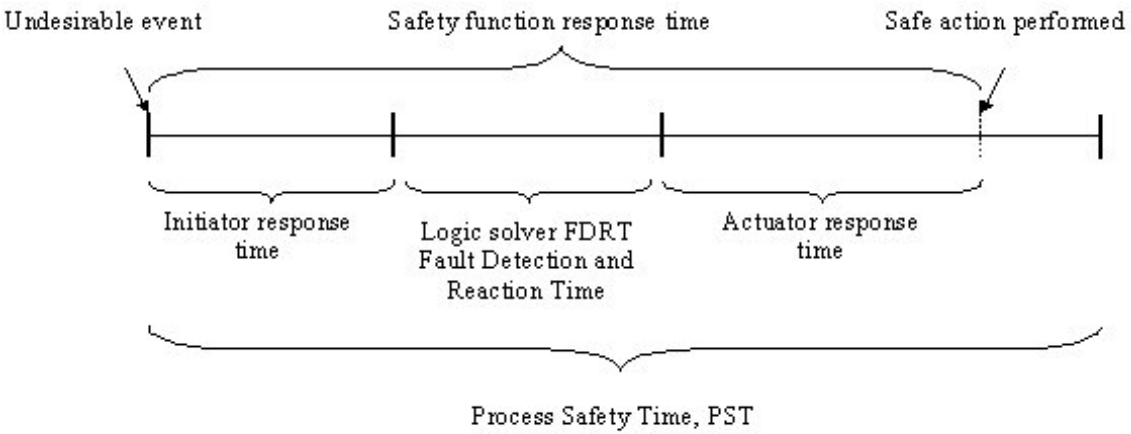


Figure 1. Process Safety Time (PST)

Note to Figure 1:

When configuring the logic solver, the initiator response time does not need to be considered, hence the time required to bring the process to safe state upon an internal fault in the AC 800M HI is only dependent of the FDRT and the actuator response time.

FDRT < PST - Actuator Response Time

The AC 800M HI supports an FDRT down to one second.

For more information, see Configuration of DRT and FDRT on page 107.

The DRT of the logic solver, is the time for processing an event in the input sub-system, scan the input sub-system, execute the functional logic, update the output sub-system and processing the desired action in the output sub-system. (Initiator and actuator response times are not included).

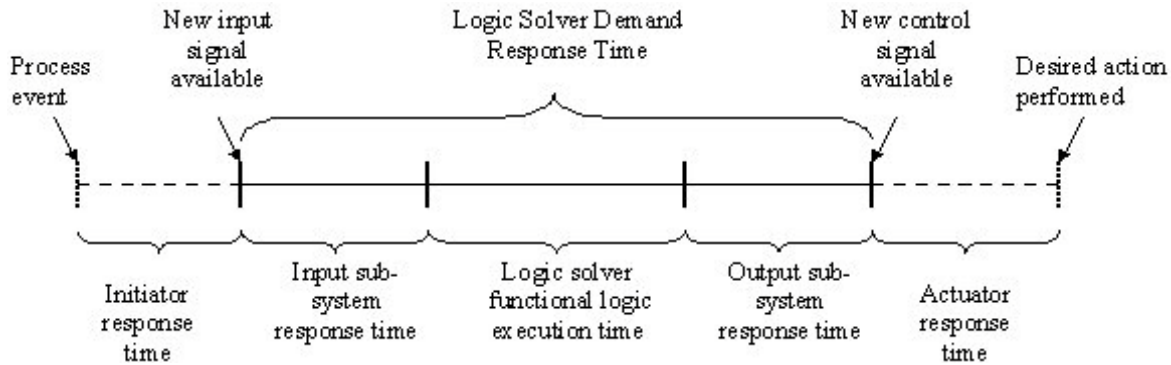


Figure 2. Demand Response Time

The DRT of the AC 800M HI is mainly dependent on the size and the interval time of the application(s) and the number of I/O modules used. For a small application (with no complex calculations) and with a limited set of I/O modules (e.g. one cluster), a DRT down to 40 ms is possible.

Product Overview

This section contains a brief overview of the main characteristics and intended use of the AC 800M HI.

The AC 800M HI is certified to comply with the requirements of Safety Integrity Level 1 - 3 according to IEC 61508.

Additionally, a set of other relevant safety/application standards are supported by the AC 800M HI, see Applicable Specifications on page 38.

When configured as a SIL1-2 systems, the AC 800M HI is realized in a 1oo1D structure by combining application execution in the PM865 with diagnostic and monitoring functions of the SM810/SM811.

When configured as a SIL3 systems, the AC 800M HI is realized in a 1oo2D[1] structure by executing application in both PM865 and SM811 (SM810 can not be used in SIL3 systems).

The SM810 can be used in systems containing applications classified up to SIL2, while the SM811 can be used for both SIL1-2 and SIL3 applications.

The S800 I/O High Integrity modules (AI880A, AI880A as DI, DI880 and DO880) are certified for use in SIL1-3 safety functions as single modules[2]. This is achieved by using an internal diverse redundant structure with diverse execution and mutual supervision.

The AC 800M HI offers a certified control environment that can host a combination of non-SIL classified BPCS functions and SIL1-3 classified safety functions in the same controller. In order to enable this, a SIL classification of user applications is introduced.
All functions/types in standard libraries usable in SIL classified applications are marked SIL2, SIL2 Restricted, SIL3 or SIL3 Restricted.

Communication modules and protocols that are not certified for safety critical use as well as non certified I/O modules, are possible to use in SIL classified applications for non safety critical functions, e.g. process feedback, status indications, etc.

1. 1oo2D for Safety action.
2. For configuration requirements, see Process Interface Selection on page 67.

External influence to the AC 800M HI is controlled by the Access Management package that contains functionality to allow human interactions from tools or operator stations in a safe and pre-configured way.

The general topology, in which the AC 800M HI is totally integrated, is shown in Figure 3.

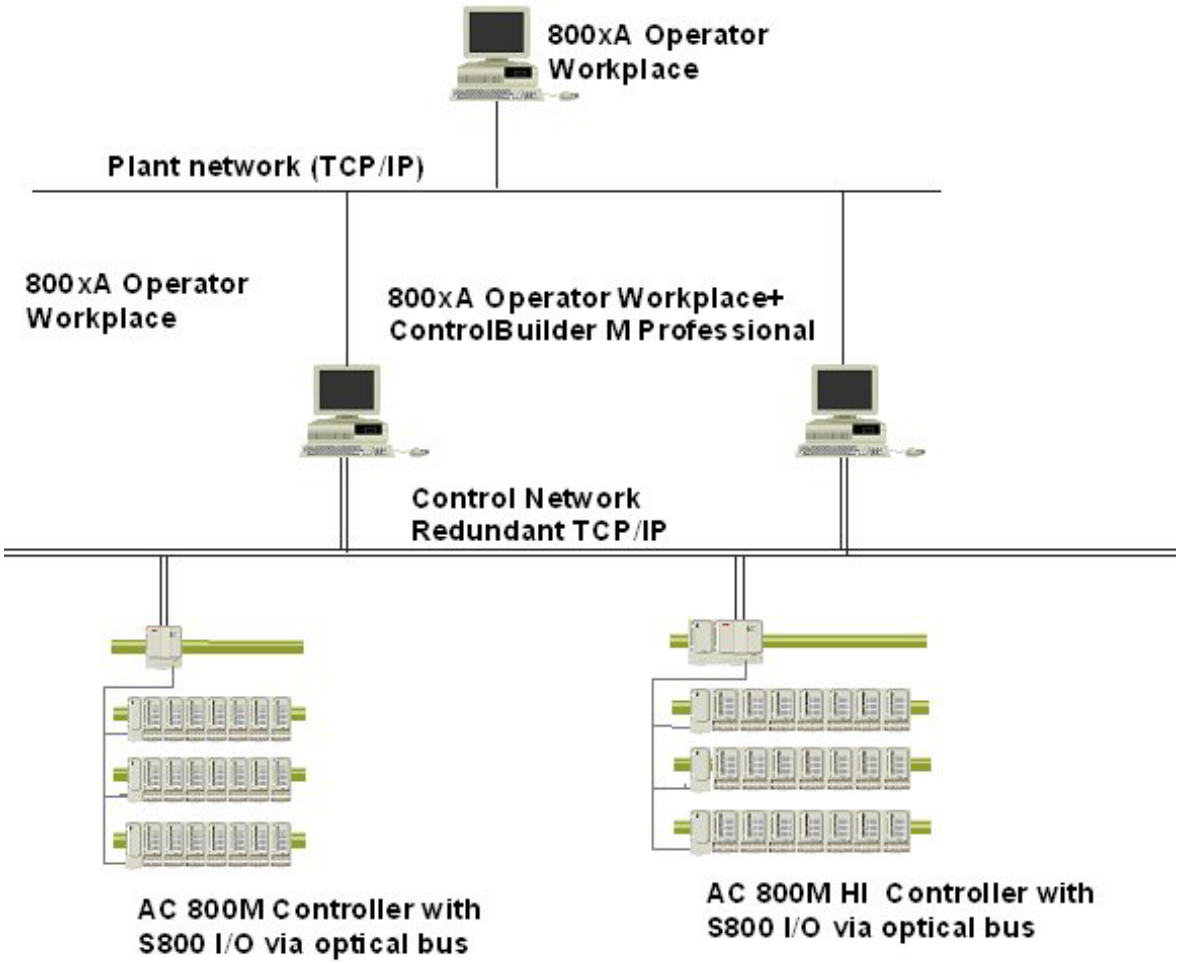


Figure 3. System Topology

Mode of Operation

The Mode of Operation is the way in which the Safety Related System will be used with respect to frequency of demands upon it. Two modes of operation are defined in IEC 61508:

Low Demand Mode: where the frequency of demands for operation made on a safety related-system is no greater than one per year and no greater than twice the proof-test frequency;

High Demand or Continuous Mode: where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-test frequency.

AC 800M HI can be used to control both Low Demand and High Demand safety functions, provided the safe state is defined as stop/de-energize[1].

The AC 800M HI can be configured with a “fault detection and reaction time” as low as one second.

Redundancy

AC 800M HI does not require any redundancy for safety integrity reasons. However, the controller and I/O system can be designed for any optimization of system availability (system uptime) by individually being configured with redundant input modules, redundant CPU/communication modules and/or redundant output modules.

1. For conditions related to DO880, see DO880 High Integrity Digital Output Module on page 70

Prerequisites and Requirements

Equipment Requirements

The following equipment is required in order to program, configure, install, verify and operate the AC 800M HI controller.

- For systems containing SIL3 applications, the SM811 is required.
  Systems equipped with the SM810, can be configured with non-SIL and SIL1-2 applications only.
  Systems equipped with the SM811 can be configured with non-SIL, SIL1-2 and SIL3 applications.
- The Control Builder M Professional shall be used for engineering and application download. It can also be used for monitoring the application during operation.
- The 800xA Operator Workplace is available as operator interface. By means of the “Confirmed Online Write” function, safe write to application variables is allowed (configurable) during operation of the plant.
  Confirmed Online Write operations to a SIL3 application, requires PPA System Version 5.0 SP2 or newer.



The AC 800M HI is suitable for unsupervised operation, i.e. it can operate without Control Builder M Professional or 800xA Operator Workplace connected.



If the AC 800M HI is used without an 800xA Operator Workplace, the system alarm output (O2) on the SM810/SM811 shall be connected to an external alarm device in order to alarm detected errors, see Physical I/O for Operator and Maintenance Personnel Interaction on page 72. This is also recommended when using 800xA Operator Workplace in order to achieve a diverse alarming path.



In order to enable all safety diagnostics, AC800M HI must be used with at least one SIL marked Task and Application.



For Normally De-energized Outputs, alarming is the only system reaction upon detected failures, hence an alternative alarming path shall be established by e.g connecting an external alarm device to a DO880 output configured as NE.

Information Requirements



Requirements and instructions marked with the **Warning** symbol in this manual shall be adhered to for the system to remain in compliance with the requirements of the certification.

Required user documentation is listed in the chapter Related Product Documentation on page 41.

Special attention shall be paid to the *System 800xA 5.1 Rev A Release Notes New functions and known problems, 2PAA107250-510** for the actual version of the AC 800M HI. This document contains information on compatibility questions, any known failures in the system, user manuals and other “last minute” information.



The user shall verify that installed versions of hardware and software modules are in compliance with the valid version of ‘Annex2 of the Report on the certificate Z10 08 10 29902 005.(1) This certificate is issued by TÜV Product Service GmbH.

(1) Available through ABB web services.

This document describes the safety aspects of the components listed in the above mentioned Annex2. For other safety related and/or certified products in an installation shall the Safety Manual related to the respective product be adhered to.

In case of any remarks or questions to the content of this manual, or the products described, please contact your local ABB representative.

Restrictions for Use of the System

Environmental restrictions and considerations are described in chapter Site Planning on page 75.

Section 2 Management of Functional Safety

This section provides guidelines and input to the management activities that are necessary to ensure that the functional safety objectives are met during all phases of the lifecycle of a safety system.

In addition to guidelines given here, the relevant application standards should be considered and fulfilled.

The management activities with respect to Functional Safety shall be identified, documented and planned as part of an overall Quality and Safety Plan.

The Policy and Strategy for achieving safety shall be identified and defined together with the means for evaluating its achievement and shall be communicated within the organization.
The policy and strategy shall contain:

- SIL Statement
- Project category statement (size, scope, complexity, management)
- Safety Verification strategy
- Safety Validation strategy
- Safety Assessment strategy
- Handling of non-certified components

A Safety Management System shall be in place; this could be integrated with the Basic Quality Management System of the organization.

Organization and Resources

The organizational structure with Roles and Responsibilities shall be defined and clearly communicated and understood by all involved parties. For each role, unambiguous accountabilities shall be defined.

Persons, departments, organizations and other units involved in safety related activities including but not limited to design, engineering, installation, configuration, test, commissioning, maintenance and operation shall have sufficient level of safety knowledge, technical knowledge, skills an relevant experience to carry out the activities for which they are accountable.



It is the responsibility of the end user of the product to ensure that all organizational units involved during any phase of the Safety Life Cycle of the product, possess sufficient competency.

A qualification process shall be established in order to specifically qualify persons, departments, organizations and other units that are involved during the lifecycle of the safety system.

As the AC 800M HI can comprise both unclassified process control applications and SIL classified applications in the same controller, the organization and procedures shall reflect the different requirements that apply.

Safety Planning

Safety Planning shall take place to define required activities, along with the persons, departments, organizations or other units responsible to carry out these activities.

Safety Planning shall include those activities that are specifically addressing Management of Functional Safety.

Implementation and Monitoring

- Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of qualified recommendations arising from:
  - Hazard analysis and Risk Assessment
  - Assessment and Auditing activities

  - Verification activities
  - Validation activities
  - Post-incident and Post-accident activities
- Procedures shall be implemented for monitoring the safety performance of the system during the operation phase. Performance shall be verified against the requirements given in the Safety Requirement Specification.
  Emphasis shall be put on:
  - Component failure rates
  - Demand rates (compared with the initial assumptions made)
  - Systematic failures (including operator and maintenance aspects)
- Procedures shall be implemented to verify the adequacy of the quality management system of all sub suppliers.

Assessment, Auditing and Revisions

A procedure shall be defined and executed for a Functional Safety Assessment (FSA), in such a way that a judgment can be made as to the functional safety and safety integrity achieved by the Safety Instrumented System.

Functional Safety Assessment aims to evaluate whether necessary provisions are made during the assessed lifecycle to ensure that required Functional Safety is or will be achieved. The procedure shall require an assessment team to be appointed that includes the technical, application and operations expertise needed for the particular installation. The procedure shall cover:

- Assessment Team organization and independency
- FSA Planning (Scope)
- FSA Minimum requirements (Scope)
- Development and production tools
- Recording and Reporting including specification of document templates
- Requirements for Follow-up

Functional Safety Assessment Team

The organization of the FSA Team and the criteria for selection of team members shall be well defined. To increase objectivity, the FSA team shall have a defined level of independency with respect to the actual project team. At least the FSA team leader shall be from an independent organization. Depending on the organization of the company and the internal skills within the company, the company may use their own resources to meet requirements for an independent organization.

Functional Safety Assessment Planning

The stages in the safety lifecycle at which the Functional Safety Assessment activities are to be carried out shall be identified during safety planning.
The number, size and scope of FSA should be defined upon specific circumstances that shall be defined. The circumstances and the method to select FSA scope shall be defined.

Functional Safety Assessment - Minimum Requirements

One Functional Safety Assessment, as a minimum, shall be carried out to make sure that the hazards arising from the process and its associated equipment are properly controlled. It shall be carried out prior to the startup of the process and shall confirm that:

- Hazard and risk assessment has been carried out, and recommendations are implemented and resolved
- Project design procedures are properly implemented
- The SIS is in accordance with the safety requirement specification
- The operation, maintenance and emergency procedures to the SIS are in place
- The validation planning is appropriate and validation activities are completed
- The training activities of maintenance and operating personnel are completed

Functional Safety Assessment of Development and Production Tools

Where development and production tools are used for any safety lifecycle activity, they shall themselves be subject to a Functional Safety Assessment.

Functional Safety Assessment Reporting

The result of the Functional Safety Assessment shall be available together with any recommendation coming from this assessment.

FSA reporting shall be clarified for the actual phase. Responsibilities and Accountabilities for both the content of the report as well as for responses to the report shall be defined. A standardized FSA report template shall be defined that include a defined distribution.

Auditing and Revision Procedures

Audits, revisions or inspections aim to check whether required provisions (procedures) for achievement of functional safety are implemented and are working properly.

Procedures shall be defined and executed for auditing compliance with the following requirements:

- Requirements for categories of Safety Audits
- Requirements for frequency of Safety Audits
- Requirements for qualifications of Audit personnel
- Requirements for Audit planning including Audit strategy
- Requirements for recording and reporting
- Requirements for follow-up

Auditing and Revision, Procedures for Management of Modifications

Management of Modifications is essential and sensitive to Functional Safety – especially over time. Audits and revisions of procedures for management of modifications are therefore vital.
Although this requirement mostly is interpreted to specifically address the operation phase, the other phases should also be covered.

Configuration Management

Configuration Management aims to manage and maintain traceability of devices through the lifecycle of the SIS.

The user of the system shall establish a practice to maintain an overview of software and hardware versions of the installed equipment, as well as versions of application software and libraries.

If the system is configured as a combined BPCS and SIS, the configuration management procedures shall identify the different requirements for handling subsystems of different SIL.

Procedures shall be established for preventing unauthorized items from entering service.

Section 3 Safety Lifecycle Activities

The content of this section is organized in accordance with the safety lifecycle process as defined in IEC 61511. For each phase of the lifecycle, guidelines, instructions and requirements related to the use of the AC 800M HI are given.

Adherence to these instructions is necessary to meet the requirements of the general safety standards listed in Applicable Specifications on page 38.

Application specific standards may contain additional requirements to configuration and application design, such requirements are not reflected in this manual.



Requirements in the application specific standards listed in the chapter Applicable Specifications on page 38 and other relevant and valid application standards shall be adhered to (e.g.EN 54, EN298).

For detailed operation instructions, the reader is referenced to Related Product Documentation on page 41.

Process Hazard and Risk Assessment

Process Hazard and Risk Assessment is performed to determine the hazards and associated risks of the process to be controlled. The need for risk reduction, and required safety functions shall be identified.

The results from such analysis are necessary input for the subsequent phases of the engineering and operation of a SIS.

A hazard and risk assessment shall be carried out on the process and its associated equipment, and shall result in:

- Undesirable event specification, description and causes, (including human errors)
- Consequences and likelihood of undesirable events

- Consideration of conditions (process phases, process upset, shutdowns)
- Determination of requirements for additional risk reduction
- Assumptions made during analysis (demand rates, failure rates, operational constraints or human intervention)
- Description of measures taken to reduce hazards and risk
- Allocation of safety functions to layers of protection
- Identification of safety instrumented functions

It may be necessary to perform Hazard and Risk assessment at several stages of the project.

The hazard and risk assessment shall be recorded in such a way that relationship between the above items is clear and traceable.

The extent of risk reduction necessary will vary depending on application, legal requirements and on an evaluation of the cost-value achievement.

Allocation of Safety Functions

In order to determine the need for a SIS and its SIL, it is necessary to consider what other protection layers exist and their level of protection.

The Allocation of Safety Functions is necessary input for the subsequent phases of engineering a SIS.

The Risk Reduction Factor shall be determined for the different layers of protection. The Allocation process shall also include allocation of Safety Instrumented Functions to individual SIS and subsystems.

From the allocation process the Risk Reduction Factor (RRF) requirement will be derived for the Safety Instrumented Functions (SIF). The SIL for the Safety Instrumented Functions shall be set taking into account the required RRF.
The Safety Integrity Level requirement is related only to the complete Safety Instrumented Function that is defined and allocated for the actual identified hazard. The distinction between Risk and Safety Integrity should be noted. Risk is a measure of the frequency and consequence of a specified hazardous event. Safety Integrity is a measure of the likelihood that the SIF (or other protection functions) will provide the specified safety function when demanded.

Demand Mode of Operation

For safety-instrumented functions where the demand rate is specified to be once per year or less, Table 3 in part 1 of IEC61511 will be used for defining the safety integrity level.

Continuous Mode of Operation.

For safety-instrumented functions where the demand rate is specified to be more than once per year or greater than twice the proof test frequency, Table 4 in part 1 of IEC61511 will be used for defining the safety integrity level.

Safety Requirement Specifications

The Safety Requirement Specification is the main input for the design of the SIS. The requirements may be collected in one single document or a collection of several documents and drawings. The requirements should be expressed in such a way that they are clear, precise, verifiable, maintainable and feasible with respect to all phases of the lifecycle.

Normally the Safety Requirement Specification will cover the following items:

- A description of all the safety instrumented functions.
- Common cause failures shall be identified and taken into account.
- Safe state shall be defined for each identified SIF.
- Any individually safe states which, when occurring concurrently, create a separate hazard shall be identified.
- Source of demand and demand rate for the SIF shall be identified.
- Proof test interval for each SIF.
- The response time for the SIS to bring the process to a safe state.
- The safety integrity level and the mode of operation for each SIF.
- A description of SIS process measurements and their trip points.
- A description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves.

- The functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissive.
- Requirements for manual shutdown when applicable.
- Requirements related to energize or de-energize to trip.
- Requirements for resetting the SIS after shutdown.
- The maximum spurious trip rate shall be specified.
- Failure modes and desired response of the Safety Instrumented System.
- Any specific requirements related to starting up and restarting the SIS.
- All interfaces between the SIS and any other system as well as operators.
- The modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode.
- The application software safety requirements as listed in Application Safety Requirement Specification on page 78.
- Requirements for overrides, inhibits and bypasses.
- Any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS, taking account for all relevant human factors.
- The mean time to repair that is feasible for the SIS.
- Potential dangerous combinations of output states of the SIS.
- The extremes of all environmental conditions likely to be encountered by the SIS.
- Normal and Abnormal modes of Plant operation.
- Requirements for any SIF necessary to survive a major accident event.

System Design and Engineering

System Structure Selection

The AC 800M HI, including its I/O system can be designed for any optimization of system availability (system uptime) by individually being configured with redundant input modules, redundant CPU/communication modules and/or redundant output modules.

The AC 800M HI does not require any redundancy for safety integrity reasons

If the safety functions of the plant require more than one AC 800M HI, for capacity or geographical reasons, they can interchange safety critical data by means of the certified peer-to-peer communication. For more information, see Communication Interfaces on page 71.

Figure 4 and Figure 5 shows example of single and redundant configurations, the various modules and redundancy options are described below.

For installation requirements and details on configuration possibilities, refer to the user manuals *AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41*.

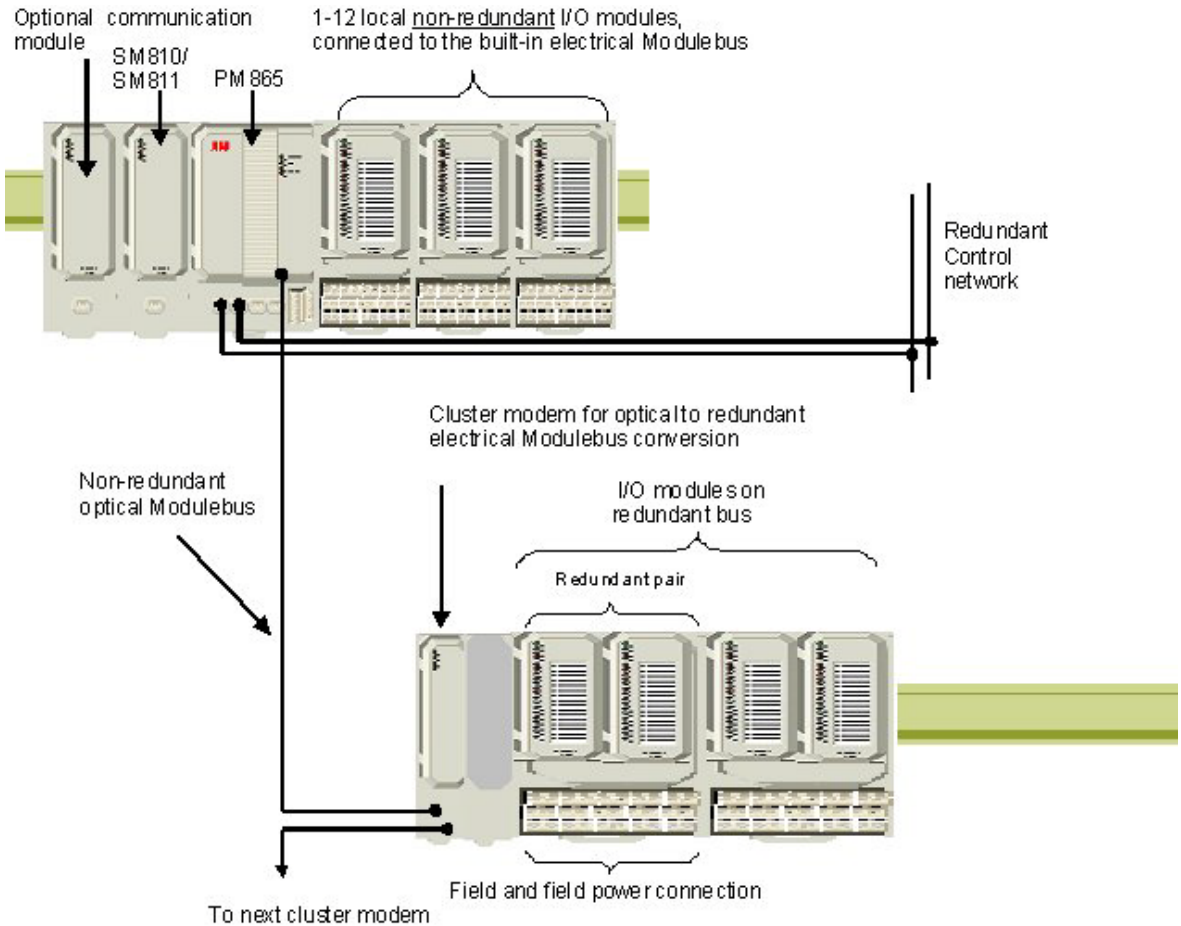


Figure 4. Single AC 800M HI System

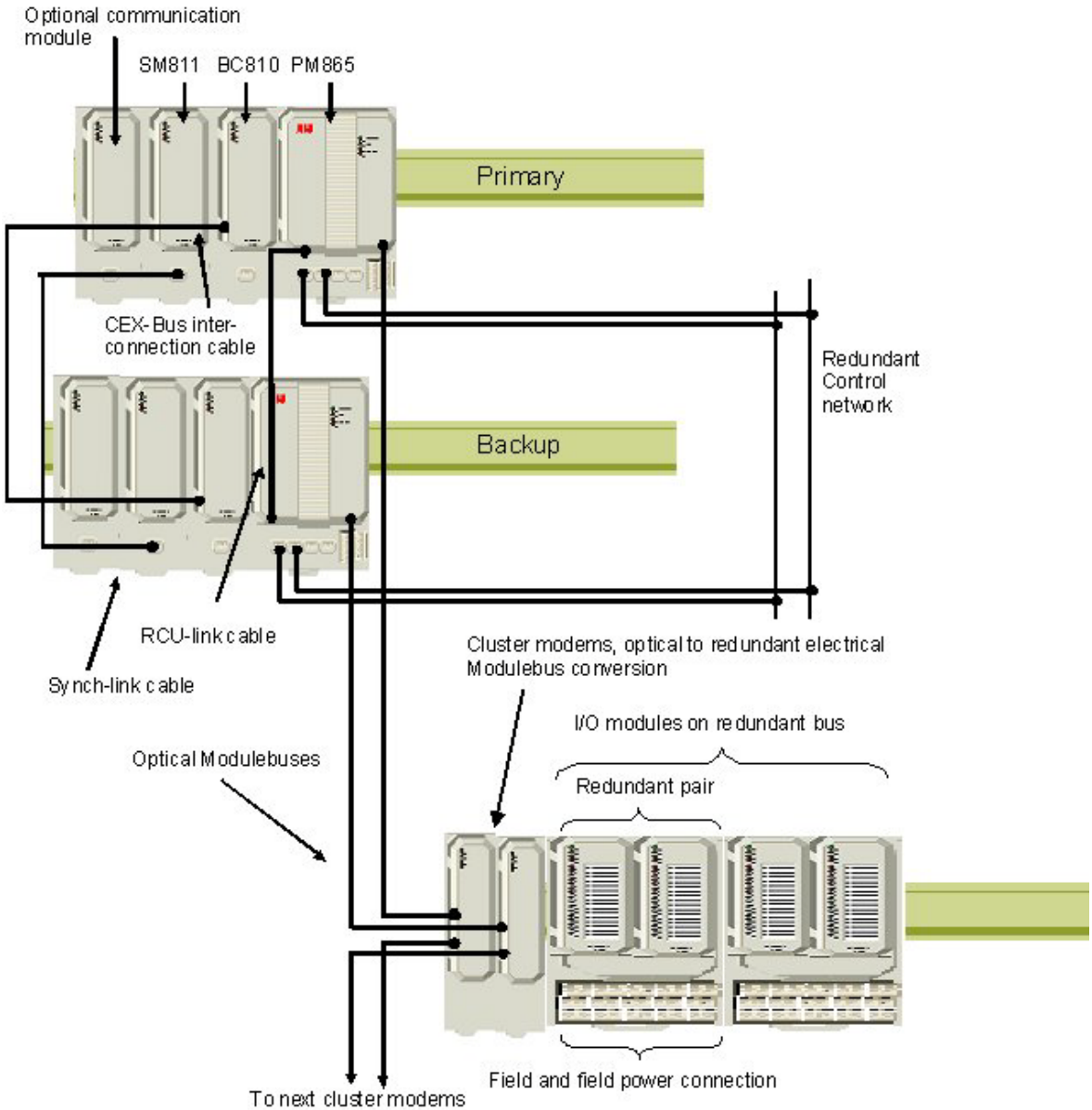


Figure 5. Redundant AC 800M HI System

Redundancy

The redundancy scheme implemented enables increased availability and fault tolerance on:

- Controller
- Communication expansion bus (CEX-Bus)
- Communications modules on the CEX-Bus
- Optical ModuleBus (when controller redundancy is used)
- Optical Cluster Modems (when controller redundancy is used)
- Electrical ModuleBus (not the local built-in electrical ModuleBus)
- I/O modules
- Power Supply

Below is a summary of the possibilities available for each component and sub-system.

Redundant AC 800M HI Controller (PM865 with SM810/SM811)

By adding a secondary PM865 and SM810/SM811[1] in backup mode, full redundancy is achieved on controller level.

After a power-on, the PM865 with the “upper-end” of the redundancy cable undertake the primary role and the other becomes the backup. The redundancy concept ensures that the backup PM865 is cyclically updated and kept “synchronized” by the primary PM865 over the RCU-link (single link).
This redundancy concept guarantees a takeover time of maximum 10 ms (typically 4-6 ms).

The SM810/SM811 is not configured to operate in primary or backup mode. Instead both modules are actively performing the same tasks. In a configuration with two SM810/SM811s both modules are continuously updated by the primary PM865, but only one of the SM810/SM811s is used for input data (read from). This concept enables almost instant takeover upon internal fault detection in one SM810/SM811.

1. Redundant systems containing SIL3 applications shall be equipped with SM811 modules interconnected with the Synch Link cable.

The Synch Link between the two SM811s is used for synchronization during an Online Upgrade or Hot Insert operation of a SM811.

A Processor Module fail-over does NOT imply a change of SM810/SM811 or communication units connected via the CEX-Bus. Also the primary I/O modules are kept (communication is switched to the other set of cluster modems) thus preventing e.g. leaps in analog input signals.

The local built-in electrical ModuleBus cannot be used in configurations with redundant AC 800M HI.

Redundant AC 800M HI processor units, require redundant optical Cluster Modems.

Redundant Optical ModuleBus

In redundant AC 800M HI systems, the redundant optical Cluster Modems enables redundant ModuleBus communication. Each PM865 is connected to one Cluster Modem. If one of the optical buses fails, communication is maintained by switching to the other AC 800M HI processor unit, this does not imply a switch over to redundant I/O modules.

Redundant Electrical ModuleBus

This is achieved by using optical Cluster Modems and Module Termination Units (MTUs) designed for housing redundant I/O modules. To take advantage of redundant electrical ModuleBus, one also needs to use two I/O modules, because an I/O module is only connected to one of the electrical ModuleBuses.

Failures related to an electrical ModuleBus causes the Cluster Modem(s) to switch to the second electrical ModuleBus. As a consequence, primary I/O modules are changed.

Redundant High Integrity I/O Modules

Requires use of optical Cluster Modems and MTUs intended for redundant I/O modules.

If redundant MTUs are used, the I/O modules can be configured for “Hot Replacement mode”.
In this configuration, the redundant slot in the MTU is left empty, and a new I/O module can be inserted upon detected channel fault(s).

The AC 800M HI treats input and output modules differently:

Input Modules

The controller assigns one of the input modules in a redundant pair as primary and the other one as backup. The input values and their status are read from the primary module and will be treated as valid until the module reports channel- or module fault, or until the communication is interrupted.

The backup module in the pair is accessed from time to time (typically every 10th scan of the primary) to determine the status of the channels, the module itself and the electrical ModuleBus.

Upon a channel fault on the primary module, the controller switches to the backup module and assigns it as the primary; the previous primary module will be stopped.

Output Modules

Digital outputs in a redundant pair are both active, both modules are always accessed one after the other in sequence. Both modules are therefore given the same values and both modules controls the outputs (and the field), which enables uninterrupted control of the outputs in case of a channel, module or electrical ModuleBus fault.

Redundant CEX-Buses



In redundant AC 800M HI systems, the CEX-Bus shall always be connected via the CEX-Bus Interconnection Unit, BC810.

The BC810 offers a way to section the CEX-Bus into two independent segments. This improves the availability in systems with redundant communication interfaces.

Redundant Power Supply

The AC 800M HI systems can be equipped with redundant power supplies.

Process Interface Selection

Allocation of I/O Modules

The S800 I/O system can be connected via the direct electrical ModuleBus (only available for single I/O modules), via the optical ModuleBus or via ProfiBus.

Note that the certified I/O modules are supported by ModuleBus only.

Each I/O cluster can contain a maximum of 12 single I/O modules, alternatively 6 redundant pairs, hence limiting the total number of modules to 12.
A maximum of 8 clusters (including the local electrical) can be connected to one AC 800M HI.

Certified and non-certified I/O modules can be connected to the same cluster.

For safety critical functions, only certified I/O modules shall be used. If non-certified I/O modules are connected to a SIL2 Application, a warning is given, but download of the Application is allowed upon engineer's approval. For SIL3 applications, download is prevented.

For information on the S800 I/O system, refer to the user manuals *S800 I/O Getting Started, 3BSE020923* page 41* and *S800 I/O - Modules and Termination Units, 3BSE020924* page 41*.

The following I/O modules are certified for safety critical use in AC 800M HI:

- AI880A High Integrity Analog Input Module
- AI880A as DI - Loop Supervised Digital Input Module
- DI880 High Integrity Digital Input Module
- DO880 High Integrity Digital Output Module

See relevant chapters below for a summary of the safety related characteristics of each module.

For information on configuration details for each I/O module, see I/O Module Settings on page 100.

AI880A High Integrity Analog Input Module

The module is certified SIL3 for the input range 4-20 mA.

The certification is valid in both single and redundant configurations.

The AI880A module supports routing of HART signals to the connected transmitters. It is important to be aware that the HART protocol supports functions that can change the behavior of the connected transmitters, like calibration and simulation.
If this functionality is to be used during operation of the plant, the utilization shall be supported by organizational procedures to maintain the safety integrity of the installation. The AI880A module can be configured to restrict the HART routing in three levels (full, read only, disabled).



The HART functionality of AI880A is approved to be interference free, for non safety critical use.



The use of HART routing of AI880A during operation of the plant, shall be restricted by configuration or by operational procedures.



If the input loops of AI880A are externally powered, or another risk of applying 24V to the signal line is present, the loop should be equipped with a fuse (rated <= 0.1A) in the signal line to avoid possible overheating of the shunt stick during fault situations.



Inverted channels from AI880A are not allowed in SIL3 applications.

AI880A as DI - Loop Supervised Digital Input Module

The AI880A module can be configured for “Loop Supervised Digital Input”.
The module is certified SIL3.
The certification is valid in both single and redundant configurations.

When used as Loop Supervised Digital Input, the module can handle input signals with defined levels for open circuit, logic low state, logic high state and short circuit. The function Loop Supervised Digital Input can also be used with field devices

without defined levels for loop diagnostics if an additional resistor network is added. The resistor network is considered to be a part of the field device, this shall be considered when certifying a safety loop according to IEC 61511. The resistor network should be placed close to the field device.



If the AI880A as DI - Loop Supervised Digital Input Module is used with an external field loop resistor network, this resistor network shall be configured in accordance with the guidance in the user manual "*S800 I/O - Modules and Termination Units, 3BSE020924* page 41"*.



If the input loops of AI880A as DI are externally powered, or another risk of applying 24V to the signal line is present, the loop should be equipped with a fuse (rated <= 0.1A) in the signal line to avoid possible overheating of the shunt stick during fault situations.



Inverted channels from AI880A used as DI are not allowed in SIL3 applications.

DI880 High Integrity Digital Input Module

The module is certified SIL3 for normally closed input loops (i.e. open for alarm). The certification is valid in both single and redundant configurations.

The DI880 module support Sequence Of Event (SOE) recording with a resolution of 1 ms, the accuracy of the recording is 1.3 ms.



The sequence of event functionality of DI880 is certified interference free, for non safety critical use.



If an input loop of DI880 is externally powered, the loop shall be equipped with a current limiting device in the signal line. The current shall be limited to 200 mA.



Inverted channels from DI880 are not allowed in SIL3 applications.

DO880 High Integrity Digital Output Module

The module is certified SIL3 for output channels configured as NE (Normally Energized), and ND (Normally De-energized).
For both output types, safe state is defined as de-energize; i.e. upon fatal errors (as CPU, power failure, loss of contact with controller), all outputs will be de-energized.

The DO880 module can be used in both Low Demand and High Demand applications, with the following restrictions:



Normally De-energized DO880 channels can only be used in High Demand applications provided the demand rate of the process exceed 10 minutes.



Normally De-energized DO880 channels used in loops were a false trip directly cause a hazardous event (e.g. fire extinguishing with CO2) are restricted to SIL2 if the field device has a response time that is shorter than 10ms.



Normally De-energized DO880 channels are meant to be used with latched field devices where no continuous energized safe state is required.



Normally De-energized DO880 channels shall not be used in EN954-1 applications.



Normally Energized DO880 channels used in EN954-1 applications; Category 4 is supported from DO880 product revision G, older product revisions support Category 3.



When Normally Energized or Normally De-energized DO880 channels are configured as inverted outputs, see Table 13, care must be taken to handle the fact that at application delete the reaction of the outputs will activate the inverted function. Application delete occurs when manually deleting an application or manually selecting cold re-start at re configuration. Inverted out channels are not allowed in SIL3 applications.

The certification is valid in both single and redundant configurations.

Individual channels of the DO880 module, can be configured and used in Normally Energized Degraded Mode (NE-DM) (function included from DO880 product revision G).

In this mode the de-energizing of the output upon an internal channel fault will be delayed for 72 hours.

When used in “Hot Replacement mode”, the NE-DM function allows for replacement of units with internal channel errors without interfering with the process.

For channels of the DO880 module configured as Normally Energized Degraded Mode (NE-DM), the Safety Integrity Level is SIL3 Low demand, or reduced to SIL2 High demand during the Degraded Mode time (72 hours).

Allocation of I/O Channels

If a safety function is equipped with redundant instrumentation, it is recommended for availability reasons to distribute the signals to different I/O modules wherever practical.

Communication Interfaces

The AC 800M HI comprises peer-to-peer communication via the control network; the communication is certified for safety critical use. Actually this function is a “peer-to-multiple-peer” communication, i.e. data made available for communication in one controller, can be read from multiple controllers.
This peer-to-peer communication can be established by using the MMS control modules designed for this purpose, for more details, see Software Architecture on page 79.

Other available communication interfaces are certified interference free, i.e. they can be used in the AC 800M HI and the data communicated on them can be used in both SIL and non-SIL Applications, but only for non safety critical functions.

For information on available communication interfaces refer to the user manual *AC 800M 5.1 Communication Protocols, 3BSE035982* page 42*.

The following communication interfaces are available for use with the AC 800M HI controller: CI853, CI854A, CI855, CI856, CI857, CI867, CI868 and CI872.

Power Supply

For information on available power solutions and recommended configurations, please refer to the user manuals *AC 800M Controller Hardware, 3BSE036351* page 41*.

It is strongly recommended to use separate power supplies for powering System Units and powering Field Equipment.



The AC 800M HI and the connected S800 I/O system (including field power) shall be supplied from a SELV or PELV power supply connected through the power voter SS823.
Provided that each power supply contain or are equipped with double over voltage protection (two independent means of limiting the output voltage to max 30 VDC), the SS823 can be omitted.

The above warning is also valid for 24 V supply to the Rechargeable External Battery Unit; SB822.



If any field device connected to the AC 800M HI is externally powered, the device shall be supplied from a SELV or PELV power supply connected through the power voter SS823.
Provided that each power supply contains or is equipped with double over voltage protection (two independent means of limiting the output voltage to max 30 VDC), the SS823 can be omitted.
When externally powered transmitters are connected to the analog input module AI880A via a fuse rated 60V/<= 0.1A, the SS823 can be omitted for loops up to SIL2.

Operator Interface

Physical I/O for Operator and Maintenance Personnel Interaction

The SM810/SM811 module in the AC 800M HI Processor Unit provides digital inputs and digital outputs intended for connection to panels for operators and maintenance personnel.

- Digital Inputs
  - Reset all Forces (I1)
  - Access Enable (I2)
  - Hot Insert (I3) (only on SM811)
- Digital Outputs
  - Any Force Active (O1)
  - System Alarm (O2)

For connection details, refer to the user manual *AC 800M Controller Hardware, 3BSE036351* page 41.*

The **Access Enable** input needs to be active to allow download to the AC 800M HI. Also write operations to variables configured as “confirm and access enable” are restricted by this input.[1]
This input should be connected to a key switch in the operator’s panel.
The function block *ForcedSignals* and Control Module *ForcedSignalsM* provides the status of the **Access Enable** input for use in Application programs and for presentation on 800xA Operator Workplace and Control Builder M Professional.

The **Reset All Forces** input provides a possibility to reset the force property of all forced I/O channels connected to SIL marked Applications.



It is under the End Users responsibility how to handle the key for the **Access Enable** input key switch and how to release passwords for 800xA Operator Workplace and Control Builder M Professional.



The **Reset All Forces** input is acting on the local controller only; a plant wide reset facility can be established using the peer-to-peer communication.



If used, the **Reset all Forces** input shall be connected to an impulse type panel button.

For a more detailed description of this functionality, see Access Management Settings on page 111.

1. Only valid for variables in a SIL marked Application.

The **Hot Insert** input is for allowing the user to insert a new SM811 (or restart a stopped one) in a redundant system containing SIL3 application(s).
This input shall be connected to an impulse type panel button.



The **Hot Insert** input is disabled during normal operation, hence incidental activation will have no effect.



During hot insert of SM811 unit the **Access Enable** input key must be turned On ("enabled"), otherwise the inserted SM811 will not be updated.

The digital outputs can be used for activating external visual or audible indications. The **Any Force Active** output is activated if any I/O variable in a SIL marked Application is forced. This output should be used for indication to operators.

For information about configuring the **System Alarm** output, see Controller Settings and Restrictions on page 91.

800xA Operator Workplace

For SIL Applications, the AC 800M HI provides protection against unauthorized writing from other computers on the control network. This protection layer is named “Confirmed Write” and consists of a special communication protocol securing that correct operation is performed on correct object.
Any attempt to write to variables and parameters belonging to a SIL Application will be stopped by the AC 800M HI if the “Confirmed Write” protocol is not used.

800xA Operator Workplace supports the “Confirmed Write” protocol and can be used for both viewing and modifying variables in AC 800M HI. The possibility to modify variables in SIL Applications are also restricted by the “SIL Access Control”, see Access Management Settings on page 111.

Maintenance/Engineering Interface

The instructions and procedures given in this manual require the use of Control Builder M Professional for engineering and application download. Various front-end applications like Reuse Assistant or Bulk Data Manager can be utilized, but the Control Builder M Professional shall be used as the interface to the AC 800M HI.

The IEC 61131-3 application code shall be compiled before it is downloaded to the AC 800M HI.

When using an external tool for I/O configuration of an application, it is required that this application is not sharing IO channels on IO boards that are already used by other applications. This shall be verified by the Difference Report

Regardless of which editors or programming tools that are utilized to produce the application source code, the compilation and download shall be done with the Control Builder M Professional. The procedure described in Program Download and Startup on page 120 shall be followed.

All data is stored in the Aspect directory of the 800xA system. The engineering environment supports multiple users, built in functionality for reserving data entities for modification prevents two users from modifying the same data simultaneously.

Site Planning

Guidelines for planning the installation of an AC 800M HI system are given in the user manuals *800xA System, Site Planning, 3BUA000258* page 41, AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41.* These manuals are giving guidelines and requirements for environmental conditions, cables, power supply and grounding.

To ensure a safe and reliable mechanical installation and assembling of the equipment at installation site, the guidance described in the referred manuals shall be adhered to.
If not all recommendations given in these manuals are strictly followed, the responsibility lies with the user to demonstrate an equivalent safe and reliable assembling and installation of the equipment.

Enclosures

The AC 800M HI modules are of protection class IP20 and each module is individually CE-marked. In office environment, they can be used without any additional enclosure. In normal industrial environment it is necessary to provide a higher protection class than IP20 by adding a suitable enclosure.

For more information, refer to the user manual *AC 800M Controller Hardware, 3BSE036351* page 41*.

Application Software

The term software in this sub-section refers to application software developed in one of the languages defined by IEC 61131-3 or in control modules, including controller and I/O configurations. For more information on available languages see Programming Languages and Libraries on page 86.

Safety Lifecycle

Activities shall be defined and planned for design, development and test/verification of the application software until it is integrated with the hardware and ready for installation and commissioning as described in Installation and Commissioning on page 119.

The following chapters give guidelines and input to these activities when working with the AC 800M HI.

- Software Architecture on page 79
- Programming Languages and Libraries on page 86
- Control Builder M Professional - Settings and Restrictions on page 89
- Controller Settings and Restrictions on page 91
- I/O Module Settings on page 100
- Access Management Settings on page 111
- Configuration Management on page 114
- Software Module Testing on page 117
- Software Integration Testing on page 117
- Integration of Application Software with the System Hardware on page 117
- System Integration Testing on page 118
- Modification Testing on page 118

Application Safety Requirement Specification

The Application Safety Requirement Specification is the main input for the design of the application software. This specification normally contains more detailed and specific requirements to the software development than present in the SIS Safety Requirement Specification (see Safety Requirement Specifications on page 59). The Application Safety Requirement Specification may be included in the SIS Safety Requirement Specification.

The requirements should be expressed in such a way that they are clear, precise, verifiable, maintainable and feasible with respect to all phases of the lifecycle.

Normally the Application Safety Requirement Specification will cover the following items:

- Safety functions to be supported
- Capacity and response time
- Interfaces to operators and other equipment
- Modes of operation of the process
- Actions on faulty process inputs
- Testing of external devices (sensors, actuators and final elements)
- Software self testing (e.g. watch dogs and range checking)
- Periodic testing of the SIF during operation

Safety Validation Planning

The Safety Validation of the application software shall be planned in accordance with the descriptions in Safety Validation on page 126.

Application Design and Development

General

This chapter provides guidelines and requirements on what to consider and which configuration settings to perform during application design, programming and handling of the AC 800M HI.

For instructions on how to perform the different tasks, please refer to the user manuals *System 800xA Control 5.1 AC 800M Planning, 3BSE043732* page 42 System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42* and *System 800xA Control 5.1 AC 800M Binary and Analog Handling, 3BSE035981* page 42.*

Software Architecture

Applications

The term Application is used in Control Builder M Professional to denote a "container" for executable programs and variables that are grouped together.

The control software for a system can be divided into Applications based on functionality, process characteristics, geographical conditions or other plant specific criteria.

The different applications shall be connected to "tasks" in the controller, determining the interval time of the different parts of the applications.



A SIL marked Application can only be connected to a task with corresponding SIL, and a non-SIL marked Application can only be connected to a non-SIL marked task.



A SIL3 application can only be connected to one task.
This is checked during compilation and download is prevented if the condition is not fulfilled.



Modification of SIL3 application/task connection shall always be followed by a cold restart of the controller. The need for changing task connections can be avoided by changing task properties.

Rules and guidelines on how to utilize the features of AC 800M HI and the Control Builder M Professional to achieve a good design of the application software is described in the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

When engineering the AC 800M HI controller, two Applications and one Library are automatically created.

- "CTA" is the Compiler Test Application, used to make sure that the IEC 61131-3 compiler works properly (this application is not downloaded to the controller).
- "VMTxx..." is a diagnostics Application used to verify certain functions of the AC 800M HI. The name of this Application is made up of the prefix VMT_ and the name of the controller.
- VMTLib is the Virtual Machine Test library, containing types used when running the VMT Application.



The CTA and VMT Applications and Library are for diagnostic purpose. They are automatically created and included; hence should not be deleted or altered in any way. However, if manually changed, they are automatically restored before download.

Combined SIL and non-SIL Classified Applications

The AC 800M HI allows SIL classified functions (e.g. SIS) and non-SIL classified functions (like BPCS) to be programmed and executed in the same controller. In such configurations the SIL and non-SIL functions shall be programmed in different Applications.
In Control Builder M Professional, the SIL is selected for each Application. The selection of SIL automatically activates the relevant restrictions and limitations that apply.



For all safety critical Applications, correct SIL shall be selected in Control Builder M Professional.

Communication Between Applications

The Library MMSCommLib contains a range of function blocks for interchanging data between two SIL marked applications, or between SIL marked and non-SIL marked applications based on the gray-channel concept.



Some of the function block types in MMSCommLib for communication between applications in the same controller, are certified SILx Restricted. This means that they are allowed to be used in SIL classified applications, but the communicated data can not be used for safety critical functions.

MMSCommLib does also contain a range of Control Modules for safe communication between SIL marked applications. By means of these modules, a certified link between SIL marked applications can be established for exchanging safety critical data.
Data communicated in this way between two SIL marked applications, is allowed to be used for safety critical functions. For a list of available modules, and their certification level, see MMSCommLib on page 150.



The SIL3 certified MMSDefHI and MMSReadHI are suitable for use in SIL 2 applications as well as in SIL3 applications.



For exchanging safety critical data between Applications, the Control Modules MMSDefxxx and MMSReadxxx shall be used. The **Valid** parameter of the MMSReadxxx shows whether the data can be trusted. In case of invalid data, the application shall bring the related safety functions to safe state.



The Control Modules MMSDefxxx and MMSReadxxx are designed to be executed every scan of the application, hence any conditional execution (for example, use of ExecuteControlModules() inside an if statement) shall be avoided.



When establishing a safety critical communication link, the **UniqueID** parameter represents the safety identification of the data and shall be unique within the plant network(1). The **UniqueID** shall be identical in the MMSDefxxx and MMSReadxxx.

(1) The Unique ID is created within the safe environment and transferred from the server to the client inside every data package for safe verification of correct connection.



The Control Modules MMSReadxxx provides parameters **SILOutx** showing the SIL level of the communicated data. The application shall ensure that the data origins from the same or higher SIL before it can be used in any way that can interfere with the safety action of the SIL classified Application.



Data originating from SILxRestricted System Functions/Library types and data originating from NONSIL marked parameters (see Appendix A, Certified Libraries), shall not be communicated via the MMSDefxxx Control modules. If this restriction is violated in a SIL3 application, it might result in a Safety Shutdown of the related AC 800M HI controller(s).



When safety critical signals are communicated between Applications (in the same or different controllers), the FDRT of the communication subsystem shall be configured to match the process safety time of the controlled process. Requirements for process safety time given in relevant application standards (e.g. EN 298) shall be considered and fulfilled.

FDRT of the communication subsystem can be calculated by means of the formulas given below. Different modules have different time supervision mechanisms, hence calculation formulas differ as well.

For the module MMSReadHI the FDRT can be calculated as follows:

FDRT = Timeout + Interval $Time_{Client}$

For the modules MMSRead128BoolM, MMSRead16BoolM, MMSRead2DintM, MMSRead2DwordM, MMSRead2RealM, MMSRead64BoolM the FDRT can be calculated as follows:

FDRT =Timeout + (FaultCount+1) * Interval $Time_{Client}$ + 100ms.

Example: Using Timeout = 1.400ms, FaultCount = 2 and Interval $Time_{Client}$ = 500ms.
FDRT for the communication = 1.4sec + (2+1)*0.5sec + 0.1sec = 3.0 sec.

The parameter *FaultCount* defines the number of cycles *Valid* shall remain TRUE when inconsistencies are found in the data-set (range: 2 - 5).

The parameter *Timeout* defines the max allowed transport delay (in milliseconds) from server to client (range: from [2*Client task interval time] to 10000).



To avoid availability problems due to transient high traffic situations in the TCP/IP communication, the Timeout parameter of the MMSReadxxx Modules should be set to 5 seconds.



To avoid time-out/invalid data on peer-to-peer links during Online Upgrade of firmware, the ‘OLUTimeOut’ parameter of the MMSReadxxx Modules shall be set to at least 10 seconds longer than the ‘Online Upgrade Handover Limit’ configured in the corresponding server (controller) to be upgraded.

As the Force Control functionality described in Access Management Settings on page 111 is defined to act on I/O variables per Application, the force flag of an input residing in a “remote” Application is not part of the “number of forces” count for the “local” application.



In Applications where inputs reside in other Applications (and other controllers), the design shall take into consideration the possibilities that the “remote” inputs can be forced independent of the Force Control setting of the “local” Application.

Communication Between Controllers

The Function Block types and Control Modules described above for communication between applications internal in one AC 800M HI controller, can also be utilized for communication between Applications residing in different controllers on the control network.



The peer-to-peer link between controllers requires the internal clock of the controllers to be kept synchronized (not needed for MMSDefHI and MMSReadHI).

For details about configuring clock synchronization see *System 800xA 5.1 Network Configuration, 3BSE034463* page 41*



If the system detects communication error too often, this might be caused by damaged communication cables/connections or by EMC problems and should be corrected immediately to maintain the availability of the installation.



The functionality of Control Builder M Professional to distribute parts of an application to several controllers, cannot be utilized for the AC 800M HI. All parts of an Application shall reside in the same controller.

Positive or Negative Logic

In most safety applications, the field loops are energized when the plant is in normal operation, and de-energized during a trip situation.
The AC 800M HI provides the possibility to invert the Boolean in- and out- signals when configuring the I/O modules, hence enabling use of positive[1] logic, independent of the characteristics of the field devices. Inverted out channels are not

1. Positive logic means that logic zero is the state during normal operation; logic one will activate a trip of the process under control. Negative logic means that logic one is the state during normal operation; logic zero will activate a trip of the process under control.

allowed in SIL3 applications using DO880 see warning in section DO880 High Integrity Digital Output Module on page 70.

It is recommended to use positive logic, to increase readability of the application code.



A philosophy for using either positive or negative logic shall be established and followed consistently for the whole plant. Naming of variables should reflect this philosophy to avoid confusion.

Use of Retain Variables

Variables can be given the attributes *retain* or *cold retain*. Depending on these attributes, the values of the variables are either maintained or lost upon warm restart, cold restart or power failure.



Do not configure *cold retain* on parameters of SILxRestricted types and NONSIL marked parameters used in SIL3 applications. Doing so will obstruct automatic start after a Power Failure of the system.



Parameters in Function Blocks with the attribute *by_ref*, will follow the retain behavior of the referenced variable.

One obvious use of cold retain variables is storing of operator changeable parameters.

For more information on the behavior of the AC 800M HI upon the different start modes, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.



A philosophy for using retain/cold retain values shall be developed based on the characteristics of the process to be controlled. The philosophy shall be followed consistently for the whole plant.

Use of Project Constants

Project Constants are intended for standardizing parameters in projects. E.g a configuration parameters of several Control Module instances can be connected to a project constant to achieve the same configuration settings on a group of instances.



If a project constant connected to initial value of a retain parameter (or variable) is changed online, the change will not take effect on existing instances until a cold restart is performed.

Power Failure

After a short power failure, a warm restart of the controller is performed, provided that the battery in the controller backs up the memory.
NonSIL and SIL1-2 applications are warm restarted with their *retain* values stored in the battery backed memory of the PM865.
SIL3 applications are cold restarted using *'SIL3 Application Start Values'* which are *cold retain* values cyclically stored with a configured interval time, see Controller Settings and Restrictions on page 91.

Some safety applications might be of such a nature that an automatic restart is not desired after a power failure. The AC 800M HI offers a system function named "FirstScanAfterPowerUp" which can be used in the IEC 61131-3 application to control the behavior of outputs after a power failure restart. It is also important to make sure that a full scan of the I/O is performed before the Outputs are activated.



If automatic restart of the process after a power failure is not desired, the application program shall contain mechanisms to achieve the desired behavior.

I/O Signal Failure



The input modules certified for use in safety critical applications can be configured to enter a predefined safe value upon a detected failure. The modules can also be configured to "keep current value" upon a failure, when this option is used, the application shall be designed to handle the process safely upon faulty input signals. Keep current value is not allowed in machine safety applications.

Dependant of the safety requirements of the process under control, specific attention shall be paid to faults on the digital output modules. Faults on a DO-module that will cause shutdown of final elements shall force respective logic outputs (IO variable) to safe state and shall require a reset to reactivate the actual output

channels. If the process under control allows automatic reset of safety instrumented functions after shutdown, this step can be omitted.



The application program shall be designed to handle faulty input and output signals in accordance with the safety requirements for the plant.



To avoid dangerous situations at controller restart, care shall be taken during application design, e.g. by using the IO.Status value to interlock unwanted start-up actions.



Application storage on a Compact Flash Card or download from a Compact Flash Card is not supported for AC 800M High Integrity controllers as the integrity of data storage and retrieval can not be verified.

Exceptional values in arithmetic operators and functions

The AC 800M HI comprise several System Functions and Arithmetic Operators intended for performing mathematical calculations and comparisons of integer and real values.



When working with arithmetic operators and Mathematical System functions, the user must take care to avoid illegal parameters, out-of-range and overflow situations.

Programming Languages and Libraries

For mandatory- and user-configurable language restrictions, see Control Builder M Professional - Settings and Restrictions on page 89.

The IEC 61511 defines three classes of software languages for use in a SIS; these are **fixed program language** (FPL), **limited variability language** (LVL) and **full variability language** (FVL).

The languages of the AC 800M HI are classified as shown in the table below.

Table 1. Classification of IEC 61131-3 languages

Language	Description	Classification	Allowed SIL in AC 800M HI
FBD	Function Block Diagram	LVL	Non-SIL, SIL 1 - 3
SFC	Sequential Function Chart	LVL	Non-SIL, SIL 1 - 2
ST	Structured Text	LVL	Non-SIL, SIL 1 - 3(1)
IL	Instruction List	FVL	Non-SIL
LD	Ladder Diagram	LVL	Non-SIL

(1) Structured Text with the subset defined for SIL2 and SIL3 is classified as LVL.

The international standard IEC 61511 supports development and modification of application software using an LVL up to SIL3. Application programmers working with higher SIL, or using an FVL are referenced to IEC 61508.

In AC 800M HI the languages IL (Instruction List) and LD (Ladder Diagram) are not allowed for use in SIL classified applications.

In AC 800M HI the language SFC (Sequential Function Chart) are not allowed for use in SIL 3 classified applications.

The Control Builder M Professional is supplied with predefined libraries containing “System Functions”, “Function Block Types” and “Control Module Types”.
A subset of these functions and types is certified for use in SIL classified applications.

For an overview of certification level and safety restrictions for System Functions and Library Types, see Appendix A, Certified Libraries.

Some of the elements are marked with SIL2 Restricted or SIL3 Restricted, in the Control Builder M Professional these elements are identified with a special icon.

The color of the SIL-digit in the icon is grey on a restricted element compared to the black digit on regular SIL-classified types and functions.



It is not allowed to use Functions, Function Blocks or Control Modules marked as SILxRestricted in a way that can influence the safety function of a SIL classified application.
If such code affects an output from a SIL3 application, it might result in a Safety Shutdown.

For restricted types and functions, user documentation or online help will give specific information related to each element.

Some of the Certified Function Block Types and Control Module Types, contains SILx Restricted sub-objects. Output parameters originating from such sub-objects are marked with NONSIL in the parameter description, such parameters shall not be used in a way that can influence the safety functions of a SIL classified application.



It is not allowed to use output parameters from Function Blocks or Control Modules marked with NONSIL in the parameter description in a way that can influence the safety function of a SIL classified application.
If such code affects an output from a SIL3 application, it might result in a Safety Shutdown.

User Defined Libraries

It is possible for the user to make project-, or industry-specific libraries for use in the automation solutions. It is the responsibility of the editor of such libraries to secure the functionality and quality of the library elements.

User defined library elements can be SIL marked (at the users own responsibility) to enable use in SIL classified applications. Such libraries shall comply with the guidelines for application programming given in this manual. This also applies when copying SIL marked library types independent if they are modified or not.



If a faceplate with possibility for operator changes to objects in a SIL classified application is to be created, the guidelines for Confirmed Write support in chapter Access Management Settings on page 111 shall be followed.



A SIL marked application can only contain SIL classified types and functions with same or higher SIL.

Library Management

When working with libraries, it is important to be aware of how libraries are version handled, how libraries are connected, and what happens if a certain library is changed.

Libraries may exist in multiple versions in the same project, but not in the same application.



A new version of a library shall be connected to all applications where it will be used.

Control Builder M Professional - Settings and Restrictions

The IEC 61131-3 application code shall be compiled before it is downloaded to the AC 800M HI. The compilation and download is performed with Control Builder M Professional.
The compiler checks that all restrictions and rules necessary to achieve the intended SIL of the application are adhered to.
The restrictions built into the compiler are dependent on the mandatory SIL and upon user selectable Compiler Switch settings. The SIL mark of the used Library-elements/Types determines which level of restrictions that are enforced. For example additional compiler switches added to SIL 1-3 element will be enforced also in a NONSIL application. The possible Compiler Switch settings are described in Table 2. Compiler Switches on page 89.;

Table 2. Compiler Switches

Switch	Description	Global (Non-SIL)	SIL 1 - 2	SIL 3
Simultaneous Execution in SFC(1)	Simultaneous sequences in SFC	**A**/E/W	E	E
Loops In ST	Loops in Structured Text (FOR, WHILE, REPEAT and EXIT)	**A**/E/W	E	E
Nested If or Case	Nested IF and CASE statements in ST	**A**/E/W	**A**/E/W	**A**/E/W

Table 2. Compiler Switches

Switch	Description	Global (Non-SIL)	SIL 1 - 2	SIL 3
Implicit Cast(2)	Automatic conversion of data types (e.g. int. to real)	**A**/E/W	A/**E**/W	A/**E**/W
Instruction List language	Instruction List	**A**/E/W	E	E
Ladder Diagram language	Ladder Diagram	**A**/E/W	E	E
SFC Language	Sequential Function Chart	**A**/E/W	**A**/E/W	E
Loops in Control Modules(3)	Code sorting loops	A/**E**/W	A/**E**/W	A/**E**/W
Force I/O from code	Restricts the possibility to change the “Forced” component of IO Variables	**A**/E/W	E	E
Multiple calls to the same Function Block	Checks for multiple calls to the same FB instance within a POU	A/E/**W**	A/E/**W**	A/**E**/W
None or multiple calls to ExecuteControlModules	Checks for correct use of this function.	A/E/**W**	A/E/**W**	A/**E**/W

(1) This switch does not affect the “sequence selection” functionality of SFC.
(2) In SIL applications it is highly recommended to set this switch to Error.
(3) In SIL applications it is highly recommended to keep the default setting (Error) for this switch.

Notes to Table 2. Compiler Switches on page 89

– “**A**”: - **Allowed**, checking of the rule is not activated.

– “**W**”: - Gives a **Warning** if the rule is violated, acknowledge required before download is allowed.

– “**E**”: - Gives an **Error** if the rule is violated, download is blocked.
The default settings are marked with boldface letters in the table.

– Some of the switches can be disabled for libraries, even if they are activated for general application.



If the EN (Enable) input on functions and function blocks is used in FBD, great care shall be taken to avoid unintentional stop of application execution.



The RETURN function (including variants such as RETCN) is not allowed in the AC 800M HI, this is checked during compilation and download is prevented.

Controller Settings and Restrictions

The internal diagnostic and the fault reaction of AC 800M HI can be adapted to the actual process by various settings. Table 3. Controller Settings on page 91, Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96 below shows available settings on controller level, while Table 9. Settings on Task Level on page 99 shows available settings on task level. Note to Table 3. Controller Settings on page 91: The settings described affect the whole controller.

Table 3. Controller Settings

Function	Description	Options	Default
Fatal Overrun Reaction	Determines the system reaction to a fatal overrun of a task.	Reset Controller	Reset Controller
Fatal Overrun Limit	Defines the number of consecutive overruns to activate the fatal overrun reaction.	1 - 10	10
Application type	Type of the actual process to be controlled.	Normally Energized/ Shutdown Normally De-energized/ Supervision	Normally Energized/ Shutdown

Table 3. Controller Settings (Continued)

Function	Description	Options	Default
FDRT (Diag.Cycle)(3)	Fault Detection and Reaction Time. (Diagnostic Cycle time)	1000 - 60000 msec (1 - 60 seconds)	3000 msec (3 seconds)
Update interval	Interval for saving "SIL3 Application Start Values"(1)	1 - 24 hours	24 hours
Online Upgrade Handover Limit	Defines the maximum time the controller are allowed to not update its outputs during an Online Upgrade of Firmware(2).	3000 -10000 msec	3000 msec

(1) Interval for saving SIL 3 Application values to be used upon a Power Failure Restart. For more information see the heading *Power Failure* in chapter Software Architecture on page 79.
(2) For more information description below and in chapter Online Upgrade on page 134.
(3) See Section Safety Principles on page 43.

Overrun of a task is defined as the situation when the task has not finished its current execution before it is scheduled to execute again. This overrun situation is not applicable to SIL classified tasks, because the latency monitoring described below will detect and react to the situation before an overrun can occur.

Detection of **Fatal Overrun** is reported as a high-severity error. The Error Handler Configuration described in Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96 below determines the system reaction.

The **Application type** selection determines the fault reaction of the system.
If "Normally De-energized/ Supervision" is selected, the controller will continue its operation during some error situations that would lead to a halt of the controller if "Normally Energized/ Shutdown" were selected.
A typical example of a "Normally Energized/ Shutdown" type of application is

process shutdown systems like ESD. Typical examples of “Normally De-energized/ Supervision” type of application is supervision and mitigation systems like F&G.



When setting the “Application type” due care shall be taken to the properties of the process to be controlled by the AC 800M HI.



FDRT (Fault Detection and Reaction Time) is the maximum time from an internal error occur in the controller, to the defined action is taken. This time shall be set according to the process safety time and the demand rate of the controlled process.



Setting the FDRT to a shorter time than necessary will reduce the performance of the system.

During Online Upgrade of firmware in the AC 800M HI, the application controlling the process is stopped for a short period of time. During this time period the output signals are not updated, but keep their current values. The duration of this time is depending of the configured **Online Upgrade Handover Limit**.
For most processes it is possible to find a process state, or a period of time when the configured FDRT can be exceeded without creating any hazardous situation. Based on such a judgement of the process, the Online Upgrade Handover Limit can be set in accordance with the following formula.

- Online Upgrade Handover Limit =
  Max acceptable Output freeze time - 2 x actual Task Interval Time - 2 x ModuleBus scan time.

If the configured FDRT are to be maintained also during an Online Upgrade session, the Online Upgrade Handover Limit shall be set in accordance with the following formula:

- Online Upgrade Handover Limit =
  FDRT - 2 x the longest Task Interval Time - 2 x ModuleBus scan time.

The maximum length of the time period the outputs are not updated can be determined by using the following formula:

- Output freeze time = Online Upgrade Handover Limit + 2 x the actual Task Interval Time + 2 x ModuleBus scan time.

The AC 800M HI has an “Error Handler” to handle faults discovered by the different diagnostic systems in a consistent manner. In order to adapt to different needs, the user can configure the Error Handler reaction as described in Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96 below.

The Error Handler can be addressed from IEC 61131-3 application code as described in User Defined Diagnostics on page 114.

Depending on the “Application type” setting of the system (see Table 3. Controller Settings on page 91), the Error Handler has different default settings, see Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96.

Table 4. Error Reaction, Normally Energized/Shutdown Applications

Error Type	System Diagnostics				Execution				I/O			
Action / Severity	Log	Event	Reset Controller	System Alarm Output	Log	Event	Reset Controller	System Alarm Output	Log	Event	Reset Controller	System Alarm Output
1 - Low												
2 - Medium												
3 - High	M	M	M	D	M	M	M	D	M	M	M	D
4 - Critical	M	M	M	D	M	M	M	D	M	M	M	D
5 - Fatal	M	M	M	D	M	M	M	D	M	M	M	D

Notes to Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95:

- “M” in the table denotes the predefined Minimum setting of the system that cannot be changed.
- “D” in the table denotes Default settings that can be changed.
- The open fields shows where additional reactions might be configured.
- The severity level, error types and possible actions are described in Table 6. Error Handler Severity Levels on page 97, Table 7. Error Handler - Error Types on page 97 and Table 8. Error Handler - Actions on page 98

Table 5. Error Reaction Normally De-energized/Supervision Applications

Error Type	System Diagnostics				Execution				I/O			
Action / Severity	Log	Event	Reset Controller	System Alarm Output	Log	Event	Reset Controller	System Alarm Output	Log	Event	Reset Controller	System Alarm Output
1 - Low												
2 - Medium	M				M							
3 - High	M	M		D	M	M		D				D
4 - Critical	M	M	M	D	M	M	M	D	M	M	M	D
5 - Fatal	M	M	M	D	M	M	M	D	M	M	M	D

Notes to Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96:

- “M” in the table denotes the predefined Minimum setting of the system that cannot be changed. page 95
- “D” in the table denotes Default settings that can be changed. page 95
- The open fields shows where additional reactions might be configured. page 95
- The severity level, error types and possible actions are described in Table 6. Error Handler Severity Levels on page 97, Table 7. Error Handler -

Error Types on page 97 and Table 8. Error Handler - Actions on page 98 page 95.

Table 6. Error Handler Severity Levels

Severity	Description
1 – Low	Minor, of diagnostic or informative sort. Does not affect the system safety or the functionality of the reporting module.
2 – Medium	Some error, I/O channel failure, communication failed Does not affect the system safety but the functionality in the reporting module.
3 – High	Severe error but not critical, I/O module failure. May affect the system safety. The functionality in the reporting module is affected. Redundancy may maintain the function of the system.
4 – Critical	Safety critical, task stalled or SM810/SM811 failed, ModuleBus stalled. Affects the system safety; the whole reporting “subsystem” has failed.
5 – Fatal	Safety critical failures (software) that lead to shutdown of the complete system, including redundant controller (if installed).

Table 7. Error Handler - Error Types

Error Type	Description
System Diagnostics	SM810/SM811, protocol handler, CEX module, redundancy problems. General system errors e.g. full queues, lost communication.
Execution	Is used for errors regarding IEC 61131-3 application execution, e.g. latency, overrun, sequence verification, CRC (memory corruption), etc. Can also be activated from user defined diagnostics by using function blocks or control modules, see User Defined Diagnostics on page 114.
I/O	I/O channel error, faulty I/O module.

Table 8. Error Handler - Actions

Actions	Description
Log	An entry is written in the system log.
Event	Event message to operator, presented in event list.
Reset Controller	If the error is originated in the PM865, the controller is set in “empty controller” mode and application programs are erased. Log files are preserved. If a healthy standby PM865 exist, a switch over will take place, otherwise the High Integrity outputs will be de-energized (safe state) after the configured timeout time. If the error is located in the SM810/SM811, the SM is halted. If a healthy standby SM exist, a switch over will take place, otherwise the High Integrity outputs will be de-energized (safe state) after the configured timeout time.
System Alarm Output	The “System Alarm” output on the SM810/SM811 is activated.

Additional to the settings on controller level some system reactions are configurable on task level; see the table below.

Table 9. Settings on Task Level

Function	Description	SIL task	NonSIL task
Enable Latency Supervision	For non-SIL tasks, the latency monitoring can be disabled.	Fixed ON	Selectable
Accepted Latency	Determines maximum accepted latency of a task in % of configured interval time.	Range: 1 - 100% Min:10 ms	Range: 1 - 100% Min:10 ms
Debug Mode (Single Run)	Function used to debug non-SIL applications.	Fixed OFF	Configurable

Notes to Table 9. Settings on Task Level on page 99:

Detection of too long Latency of a Non-SIL task is reported as an error of severity “high”. The Error Handler Configuration described in Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96 determines the system reaction.

Detection of too long Latency of a SIL classified task is reported as an error of severity “critical”. The Error Handler Configuration described in Table 4. Error Reaction, Normally Energized/Shutdown Applications on page 95 and Table 5. Error Reaction Normally De-energized/Supervision Applications on page 96 determines the system reaction.

The task priority *Time Critical* is not allowed for any task in the AC 800M HI. This is checked during compilation and download is prevented.

SIL3 tasks shall have higher priority than SIL2 tasks which again shall have higher priority than tasks running non-SIL applications in the same controller. This is checked during compilation and download is prevented.

It is not recommended to have any task running on the same or higher priority than the VMT task. This is checked during compilation, a warning is given, but download is not prevented.

Shortest allowed interval time for any task in the AC 800M HI is 10 ms for SIL2 and 20ms for SIL3.

Shortest allowed ModuleBus scan time in the AC 800M HI is 5 ms.

I/O Module Settings

Details on how to configure the I/O modules are described in the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*, and in Control Builder M Professional, online help. The characteristics of the individual I/O modules are described in the user manual *S800 I/O - Modules and Termination Units, 3BSE020924* page 41*.

This section deals with safety related settings of the High Integrity I/O.

AI880A High Integrity Analog Input Module

To ensure safe operation and adaptation to the process, AI880A High Integrity Analog Input Module, shall be configured according to the directions in Table 10. Safety Related Settings of AI880A on page 100.

Table 10. Safety Related Settings of AI880A

Parameter	Description
Safety Accuracy	Denotes the maximum drift of the measured value before a channel is marked faulty.(1) Shall be set in accordance with the tolerances of the configured trip limits for the process. The unit to be entered is % of measuring range. Default is “1.9%” (2).
HART Mode	The HART protocol supports commands that can affect the 0-20 mA output from the connected transmitter, hence to avoid jeopardizing the safety function of the transmitter, changing this parameter shall be restricted by operational procedures or be set to “Read only” or “disabled” during the operation phase of the plant. Default is “Read Only”.

Table 10. Safety Related Settings of AI880A

Parameter	Description
ModuleBus timeout	Denotes the time from communication with the input module is lost until the connected variables are error marked. Shall be set in accordance with the process safety time of the fastest loop connected, but not shorter than 4 times the configured ModuleBus scan time. To allow online upgrade of firmware the setting must be minimum “512ms”. Default is “512 ms”.
Activate channel no yy	All I/O channels having a variable connected shall be set active to avoid channel error. Default is “True”.
ISP Control channel no yy	The characteristics of the process shall be evaluated to determine the safe action when an input signal is lost. This parameter shall be set to “Keep Current Value” or “Use ISP Value” accordingly. Default is “Keep Current Value”.
ISP Value channel no yy	Denotes the value the channel will go to upon error, provided the “ISP Control...” property is set to “Use ISP Value”. The safe value of this parameter shall be set based on the characteristics of the process. Default is “0.0”
Filter time channel no yy	When setting this parameter, the process safety time of the loop shall be considered. Default is “no filtering”.
Signal range channel no yy	The certification for AI880A is valid for the signal range 4-20 mA. For not used channels, the range shall be set to 0-20 mA to avoid channel fault. Default is “4-20 mA”.
Field Power Output Trigger Level ch no yy	AI880A is monitoring the power fed to the transmitter, default setting is 18,5 Volt. If the connected field device has deviating requirements, this parameter shall be set accordingly.

Table 10. Safety Related Settings of AI880A

Parameter	Description
Set NAMUR range 3.6, 3.8-20.5, 21.0 mA ch no yy	When this parameter is set to True, the error marking of the channel is delayed with 4 seconds. When the parameter is False, error marking is done without delay. When setting this parameter, the process safety time of the loop shall be considered. When this parameter is “False”, the over- and underrange limits shall be entered by the user. Default is “False”.
Inverted (property)	Under the property tab it is possible to invert each variable connected to a analogue channel. This property shall be set in accordance with the positive/negative logic philosophy of the plant, see Software Architecture on page 79. Default is “False”.Inverted channels from AI880A are not allowed in SIL3 applications. page 68

(1) Normal accuracy of AI880A without faults is 0.1%.
(2) Setting this value lower than default, might in dynamic processes, cause intermittent channel fault.

AI880A as DI - Loop Supervised Digital Input Module



To ensure safe operation and adaptation to the process, AI880A as DI - Loop Supervised Digital Input Module shall be configured according to the directions in Table 11. Safety Related Settings of AI880A as DI - Loop Supervised on page 103.

Table 11. Safety Related Settings of AI880A as DI - Loop Supervised

Parameter	Description
ModuleBus timeout	Denotes the time from communication with the input module is lost until the connected variables are error marked. Shall be set in accordance with the process safety time of the fastest loop connected, but not shorter than 4 times the configured ModuleBus scan time. To allow online upgrade of firmware the setting must be minimum “512ms”. Default is “512 ms”.
Activate channel no yy	All I/O channels having a variable connected shall be set active to avoid channel error. Default is “True”.
ISP Control channel no yy	The characteristics of the process shall be evaluated to determine the safe action when an input signal is lost. This parameter shall be set to “Keep Current Value” or “Use ISP Value” accordingly. Default is “Keep Current Value”.
ISP Value channel no yy	Denotes the value the channel will go to upon error, provided the “ISP Control...” property is set to “Use ISP Value”. The safe value of this parameter shall be set based on the characteristics of the process. Default is “False”
Filter time channel no yy	When setting this parameter, the process safety time of the loop shall be considered. Default is “no filtering”.
Open circuit alarm level channel no yy	The limit can be configured by selecting a fixed value in the range of 0.0 mA and 4.0 mA. Default is “1.0mA”.
Limit for change false – true ch no yy	The limit can be configured by selecting a fixed value in the range of 1.6 mA to 5.8 mA. Default is “4.2mA”.
Inverted (property)	Under the property tab it is possible to invert each variable connected to a digital channel. This property shall be set in accordance with the positive/negative logic philosophy of the plant, see Software Architecture on page 79. Default is “False”.Inverted channels from AI880A used as DI are not allowed in SIL3 applications. page 69

DI880 High Integrity Digital Input Module



To ensure safe operation and adaptation to the process, DI880 shall be configured according to the directions in Table 12. Safety Related Settings of DI880 on page 104.

Table 12. Safety Related Settings of DI880

Parameter	Description
ModuleBus timeout	Denotes the time from communication with the input module is lost until the connected variables are error marked. Shall be set in accordance with the process safety time of the fastest loop connected, but not shorter than 4 times the configured ModuleBus scan time. To allow online upgrade of firmware the setting must be minimum “512ms”. Default is “512 ms”.
Activate channel no yy	All I/O channels having a variable connected shall be set active to avoid channel error. Default is “True”.
ISP Control channel no yy	The characteristics of the process shall be evaluated to determine the safe action when an input signal is lost. This parameter shall be set to “Keep Current Value” or “Use ISP Value” accordingly. Default is “Keep Current Value”.
ISP Value channel no yy	Denotes the value the channel will go to upon error, provided the “ISP Control...” property is set to “Use ISP Value”. The safe value of this parameter shall be set based on the characteristics of the process. Default is “False”.
Filter time channel no yy	When setting this parameter, the process safety time of the loop shall be considered. Default is “50 ms”.
Inverted (property)	Under the property tab it is possible to invert each variable connected to a digital channel. This property shall be set in accordance with the positive/negative logic philosophy of the plant, see Software Architecture on page 79. Default is “False”.Inverted channels from DI880 are not allowed in SIL3 applications. page 69

DO880 High Integrity Digital Output Module



To ensure safe operation and adaptation to the process, DO880 shall be configured according to the directions in Table 13. Safety Related Settings of DO880 on page 105.

Table 13. Safety Related Settings of DO880

Parameter	Description
ModuleBus timeout	Denotes the time from communication with the controller module is lost until the outputs of DO880 are brought to the safe state (de-energized). Shall be set in accordance with the process safety time of the fastest loop connected, but not shorter than 4 times the configured ModuleBus scan time. To allow online upgrade of firmware the setting must be minimum “512ms”. Default is “512 ms”.
Activate channel no yy	All I/O channels having a variable connected shall be set active to avoid channel error. To avoid channel faults on not used channels, the loop supervision should be disabled (see Trig limit parameters below) or the channel should be set not active (false). Default is “True”.
Output mode channel no yy	If the process requires a manual interaction to activate the output after a short circuit situation, this parameter shall be set to “latch on short”. Default is “latch on short”.

Table 13. Safety Related Settings of DO880

Parameter	Description
Normal State channel no yy	Defines the channel behavior upon detection of a channel fault (by means of internal redundancy the channels have a fault tolerance of 1). • Normally energized (NE), de-energize to trip: Output will be de-energized if an internal channel error is detected. • Normally de-energized (ND), energize to trip: Output will follow the output value demanded by the controller if an internal channel error is detected. • Continuous Control (CC): Same behavior as ND. • Normally energized Degraded Mode (NE-DM), de-energize to trip: Output will follow the output value demanded by the controller (for 72 hours) if an internal channel error is detected. 72 hours after detection of an internal channel error the output is de-energized. For all output types, safe state is defined as de-energize; i.e. upon fatal errors, (as CPU, power failure, loss of contact with controller), all outputs will be de-energized. Default is “Normally energized (NE)”.
Trig limit open energized channel no yy	Shall be adapted to the connected field device and loop characteristics to enable loop supervision. Default is “5 mA”.
Trig limit short energized channel no yy	Shall be adapted to the connected field device and loop characteristics to enable loop supervision. Default is “600mA”.
Trig limit open de-energized channel no yy	Shall be adapted to the connected field device and loop characteristics to enable loop supervision. Default is “1300 Ohm”.

Table 13. Safety Related Settings of DO880

Parameter	Description
Trig limit short de-energized channel no yy	Shall be adapted to the connected field device and loop characteristics to enable loop supervision. Shall not be set to 0 Ohm (disabled) for Normally de-energized channels. Default is “40 Ohm”.
Inverted (property)	Under the property tab it is possible to invert each variable connected to a digital channel. This property shall be set in accordance with the positive/negative logic philosophy of the plant, see Software Architecture on page 79. Default is “False”. Inverted Outputs are not allowed in SIL3 applications, see DO880 High Integrity Digital Output Module on page 70

Configuration of DRT and FDRT



The Demand Response Time, DRT and Fault Detection and Reaction Time, FDRT of a loop can be calculated using the figures in Table 14. Response times for SIL2 systems on page 107.FDRT for SIL3 loops can be calculated using the formula described in FDRT for SIL3 loops page 108

For a more detailed description of the DRT and FDRT, see Safety Principles on page 43.
In addition to the figures for each individual module in a loop, the behavior of the ModuleBus upon faults shall be considered. If one telegram on the ModuleBus is lost or corrupted, two retries are done before communication is stopped or switched to the redundant unit (if existing).

DRT and FDRT response time for SIL2 systems

Table 14. Response times for SIL2 systems

	DRT	FDRT(1)
DI880	1.3 ms (max)	50 ms (max)
AI880A	10 ms (max)(2)	50 ms (max)

Table 14. Response times for SIL2 systems

	DRT	FDRT(1)
DO880-NE	15 ms (max)	50 ms (max)
DO880-ND	15 ms (max)	3s (max)
AC 800M HI Processor Unit Application interval time	Configurable min. 10 ms	Configurable min. 1000 ms
ModuleBus scan time	Configurable 5 - 300 ms	3 times the configured scan time

(1) Max. FDRT value for AI/DI/DO should include one Modulebus scan.
(2) Demand Response Time for AI880A does not include the delay caused by the input hardware filter, for more information see S800 I/O Modules and Termination Units 3BSE020924*.

FDRT for SIL3 loops

For SIL3 loops the configured diagnostic cycle time (FDRT) setting can be replaced, by a shorter FDRT calculated according to the formula below. The use of a shorter calculated FDRT assumes that the user takes care of the safety reaction, bringing the affected loop to a safe state. The configurd diagnostic cycle time (FDRT) can be set higher but it is still active, setting shall be based on requirement for the SIL2 loops.

$FDRT_{max}$= (Input error detection) + 2*(Application interval time) + (Output error detection)

The (Input error detection) is given by the maximum value of one of the following parameters:

- Modulebus scan time.
- DI880 or AI880A FDRT from Table 14. Response times for SIL2 systems on page 107.

The largest value of the two parameters shall be used in the calculation see Table 15. SIL3 FDRT Example 1 on page 110 and Table 16. SIL3 FDRT example 2

on page 111.



When FDRT is required to be shorter then the configured diagnostic cycle time (FDRT) user must in the application code connect channel error from the I/O in such a way that the affected loop is brought to safe state.

Output error detection is given by the maximum value of the following parameters:

Modulebus scan time.

Modulebus time-out timer.

DO880-NE or DO880-ND FDRT from Table 14.

The largest value of the three parameters shall be used in the calculation see Table 15. SIL3 FDRT Example 1 on page 110 and *Table 16. SIL3 FDRT example 2 on page 111*



During Warm Download and Hot Insert of SM811 the calculated shorter FDRT is superseded by the configured diagnostic cycle time (FDRT). It is the responsibility of the end user, via organizational measures, ensuring that this can be done in a safe way.

Example 1 small system 3 I/O boards 20ms Application interval time using the formula.

$FDRT_{max}$= (Input error detection) + 2*(Application interval time) + (Output error detection)

:

Table 15. SIL3 FDRT Example 1

Parameter	Value	Input system	Output system	SIL3 FDRT
Modulebus scan time	5ms	3*5ms =15ms is smaller then DI880 FDRT of 50ms Resulting value to be used in the FDRT calculation is 50ms	3*5ms = 15ms is smaller then Modulebus time-out of 16ms. DO880-NE FDRT is the largest resulting value to be used in calculation is 50ms	Input system 50ms Output system 50ms 2*Application 40ms FDRT 140ms (max)
Modulebus time-out timer	16ms			
DO880-NE FDRT from Table 14	50ms			
DI880 FDRT from Table 14	50ms			
Application interval time	20ms			

Example 2 system 20 I/O boards 100ms Application interval time using the formula.
$FDRT_{max}$= (Input error detection) + 2*(Application interval time) + (Output error detection)

Table 16. SIL3 FDRT example 2

Parameter	Value	Input system	Output system	SIL3 FDRT
Modulebus scan time	45ms	3*45ms =135ms is larger then DI880 FDRT of 50ms Resulting value to be used in the FDRT calculation is 135ms	3*45ms = 135ms is larger then Modulebus time-out of 128ms. DO880-NE FDRT is smaller then both resulting value to be used in calculation is 135ms	Input system 135ms Output system 135ms 2*Application 200ms FDRT 470ms (max)
Modulebus time-out timer	128ms			
DO880-NE FDRT from Table 14	50ms			
DI880 FDRT from Table 14	50ms			
Application interval time	100ms			

Access Management Settings

Force Control

The AC 800M HI supports supervision and control with the number of forces entered during operation.

To enable forcing of I/O variables in a SIL classified application, the “maximum number of forces” property for the actual application shall be configured (default is 0). This setting is available for each SIL classified application.



The “maximum number of forces” property shall be set based on the characteristics of each application and the operation philosophy of the plant.



If the "maximum number of forces" property is lowered care must be taken. If the value is set lower than the actual number of active forces in the application the result will be a safe shutdown.



The “maximum number of forces” property is only available in offline mode, and requires a download to take effect in the controller.

The force control acts on the “force” property of I/O variables (BoolIO, RealIO, DintIO and DwordIO) connected to I/O modules (both inputs and outputs). No other variables containing a force property will be affected by the force control, neither will any variable not connected to an I/O channel be affected.



In SIL classified applications, the “force” property of I/O variables connected to I/O modules can not be set by the application code. Such constructions will give a compilation error and download is prevented.

The force property of I/O variables can be reset from application code by using the System Function *ResetForcedValues*, the Function Block *ForcedSignals* or the Control Module *ForcedSignalsM*.

The SM810/SM811 provides a digital input **Reset All Forces**, giving a possibility to reset the force property of all I/O channels connected to SIL marked Applications in the whole controller.
For more information about the “Reset all Forces” input, see Physical I/O for Operator and Maintenance Personnel Interaction on page 72.

SIL Access Control

The possibility to change the content of variables in SIL applications in the AC 800M HI is restricted by the “Confirmed Write” and “SIL Access” functionality.

The “Access Level” shall be configured for all variables that shall be possible to modify online from the 800xA Operator Workplace. Available settings are (Read only), (Confirm and Access Enable) and (Confirm).

- Read Only: Not possible to modify online, only viewing is possible.
- Confirm and Access Enable: Enables modification of values by means of the “Confirm Operation” dialog, provided the “Access Enable” input is enabled, see Physical I/O for Operator and Maintenance Personnel Interaction on page 72.
- Confirm: Enables modification of values by means of the “Confirm Operation” dialog.



The SIL Access level shall be configured based on the characteristics of each variable and the operation philosophy of the plant.

Default setting when instantiating a type is Read Only. Opening up for modification of a variable should only be done after careful considerations.

Confirmed Write Support

Confirmed Write Support is a function for enabling secure operation on objects in a SIL classified application. The Confirmed Write Support function brings up a **Confirm Operation** dialog, enabling the operator to verify and acknowledge the operation to be performed, see Operation Procedures on page 127, Figure 6 for example on the **Confirm Operation** dialog.

When creating a new type with operator faceplate for use on 800xA Operator Workplace, support for the confirmed write function shall be implemented to enable operators to change values of the object (in SIL classified applications).
This is done by adding a Confirmed Write Support aspect to the object to be operated (in addition to configuring the SIL Access Control as described above).

The faceplate and the configuration of the Confirmed Write Support aspect shall be designed so it is easy for the operator to recognize object, property and value in the **Confirm Operation** dialog. Texts displayed in the **Confirm Operation** dialog shall uniquely identify the operation to be performed.

User Defined Diagnostics

All SIL marked library types (Function Blocks and Control Modules) that include range check of input values, have an output parameter (ParError). The ParError is indicated on operator faceplates. If any system reaction is needed, this parameter shall be used in an application program to perform the desired action.



If parameter errors on function blocks or control modules shall lead to a system reaction, this shall be programmed in the application program.

Errors detected by the user defined diagnostic functions, can be reported to the system internal Error Handler by means of the Function Block *ErrorHandler* or Control Module *ErrorHandlerM*. In this way it is possible to achieve a consistent handling of all error types. The internal Error Handler functionality and configuration possibilities are described in Controller Settings and Restrictions on page 91.

Configuration Management

Procedures for Configuration Management shall be established and used during the whole lifecycle of the application software.

Configuration Management comprise the running of an inventory list, showing the version of all SIS hardware (AC 800M HI with all connected interface and I/O modules) and software modules, as well as the version of all utility software like Control Builder M Professional, 800xA Operator Workplace and other tools utilized.

The following list is intended as input to the Configuration Management procedure:

- Identify the stage where formal configuration control shall be implemented
- Prevent unauthorized items (hardware and software) from entering service
- Tracking of changes resulting from observations and audits
- Tracking of work around and other temporary solutions
- Handling of revisions of input documentation

Test and Verification

This chapter contains guidelines on how testing and verification can be divided into sub tests performed during different phases of a project.

For planning and execution of regression testing after modifications, see the chapter Modification Testing on page 118.

Source Code Report

The source code report shows the complete source code for the current project in the Control Builder M Professional. Independent of what editor is used to create the code, the report is presented in “xml” format.
The report shall be used to verify that the intended functionality is realized in the application code.

The source code report can be presented at any stage of the project, or during online operation of the system.

If a printed/saved Source Code Report is needed, this can be obtained from the menu: **Remote System>Show Downloaded Items>Source Code Report**.

For more details about the source code report, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Difference Report

The difference report is generated after compilation and is presented before download to the AC 800M HI. The format and data is equal to that of the source code report, but only source code (and differences) for changed Applications and Controller Configurations is displayed. E.g. if the project contains two Applications App1 and App2, and only App1 has been changed since last download, only source code for App1 will be displayed.

When a download is performed, the difference report will be saved for future reference.

For more details about the difference report, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Test Mode

Test Mode can be used for offline testing of applications. Executing code in Test mode means that the code will be compiled and executed locally in the PC.

The difference report cannot be used in Test Mode.

For more details about Test mode, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Simulation

Simulation means that code is downloaded and executed in a simulation controller.

SIL classified applications can be simulated in SoftController running in HI mode.
The AC 800M HI cannot be configured as a simulation controller.

To enable download to a simulation controller, both the applications and the actual controller in the hardware tree shall be marked with “simulate”.

In a simulation controller, the normal updating of I/O values from the I/O modules is stopped, enabling simulated test values to be entered. This can be done manually from Control Builder M Professional, or by a test program executing in the simulation controller.

To avoid dangerous situations, the following restrictions apply:

A simulation marked application, or an application containing a simulation marked program, can only be downloaded to a simulation marked controller.

For more details about Simulation, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Hardware Testing

Testing shall be performed on the project specific hardware to show that the hardware is assembled and configured correctly and works according to its specifications.

Software Module Testing

Testing of project specific Function Blocks and Control Module types shall be performed to verify their specified functionality.

The logic functions of such types can be verified in *Test Mode* or *Simulation* as described above, while execution time and memory consumption shall be verified in an AC 800M HI.

Software Verification

Before formal testing commence, the *Source Code Report* shall be generated and reviewed, see Source Code Report on page 115.



The *Source Code Report* shall be carefully reviewed to verify correct application programming.

This review will secure that the actual source code realizes the intended functionality. The need for testing (and the probability for finding errors) will be significantly reduced, provided a proper desk check is performed on the source code report.

Software Integration Testing

These tests shall demonstrate that all application software modules and components interact correctly with each other and with the underlying embedded software.

Software Integration testing can be done either by using the AC 800M HI or by means of the *Test Mode* or *Simulation* functions described above.

Integration of Application Software with the System Hardware

These tests shall verify that all software and hardware modules of an AC 800M HI function together and interface with each other as a complete system.

These tests shall verify I/O configurations and other external interfaces. Correct function of redundant components shall be verified.

These tests shall be performed using the AC 800M HI hardware.

System Integration Testing

If the project contains functions that are dependent of more than one controller, or other external systems, these functions shall be verified in a complete system setup, comprising all involved sub systems.
These kinds of tests can be done in a staging area or after installation in the actual plant.

Modification Testing

Impact Analysis

If modifications are done to hardware or software parts that already are tested, an impact analyze shall be performed to identify all parts of the system that might be influenced by the modification.
For application changes, the “difference report” presented after compilation (see Difference Report on page 115) provides information that will be useful in verifying the completeness of the impact analysis.

Functional Testing

The changed parts of the system shall be tested according to the procedures originally used for such testing the first time. If the modification is done on a Function Block type or Control Module type, functional re-testing shall be performed on the instances of the type.

Regression Testing

Regression testing shall be performed to verify that no unintended effects of the modification have occurred. Such regression testing shall cover all parts of the system identified in the impact analysis. The level of regression testing shall be determined based on a competent judgment of the extent and the complexity of the performed modification.



Modifications affecting I/O connections shall be verified by testing in the running AC 800M HI controller.

For additional considerations regarding modifications during the operation period, refer to Modification during Operation on page 132.

Installation and Commissioning

Transportation and Storage

Requirements for environmental conditions during transportation and storage are described in the user manual *AC 800M Controller Hardware, 3BSE036351* page 41*.

Mechanical Completion

Upon receipt of the equipment at the site of installation, it is important to secure satisfactory environmental conditions.



If required environmental conditions during operation are not yet established, interim measures shall be taken to avoid damage of the equipment.

For a complete overview of environmental conditions, see the user manuals *AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41*.

After packaging and transportation material is removed, the equipment shall be checked for any visual signs of physical damage during transportation.



To ensure a safe mechanical installation and assembling of the equipment at installation site, the guidance described in the user manuals *AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41* shall be followed.

If not all recommendations given in these manuals are strictly followed, the responsibility lies with the user to demonstrate an equivalent safe and reliable assembling and installation of the equipment.

Electrical Completion

During installation of cables and powering of the system, all connections to external equipment and field instruments should be disconnected to avoid damage of equipment in case of wrong polarities or voltage levels.

Earth connections shall be in place and verified before power is connected to the system.

The power source shall be connected and verified for polarity and voltage level before power is turned on to the system.



To ensure a safe electrical installation and power up of the equipment at installation site, the guidance described in the user manuals *800xA System, Site Planning, 3BUA000258* page 41, AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41* shall be adhered to.



Before connecting any external devices to the AC 800M HI, voltage level and polarity shall be verified.

Program Download and Startup

Applications can be downloaded to a stopped/empty controller, or online to a running controller without interfering with the running process.

The system offers a licensed option “Load Evaluate Go”, in short LEG. This is a function to enable comparison between the modified application and the old application before the old application is replaced. For downloads using this option see Program Download with LEG on page 123.



During online download (normal application update or LEG), the user shall take appropriate precautions dependant of the properties and the time demands of the process under control.

The application that is controlling the process is stopped, and the 1131-task execution is delayed for a short period of time during the download. During this time period the output signals are not updated, but keep their current values.

The maximum length of the time period the outputs are not updated can be determined by using the following formulas:

- If the task Interval time is <= FDRT:
  3 times the FDRT.
- If the task Interval time is > FDRT:
  FDRT + 3 times the task Interval time.

If the stop period exceeds the limit determined by the formulas, the controller is halted and the outputs are automatically brought to the safe state.

After the first download of a SIL marked application to an AC 800M HI controller, subsequent downloads are protected by the “Access enable” input on the SM810/SM811, see description under Operator Interface on page 72.

The “Access enable” input shall be enabled to allow download to an AC 800M HI controller (valid for SIL and non-SIL applications).

Note: If the AC 800M HI is empty or running only non-SIL applications, this restriction is not valid.

Program Download

For details on how to perform program download, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

To ensure a safe download and startup of applications to the AC 800M HI, the steps described in Table 17. Program Download Procedure on page 121 shall be performed.

Table 17. Program Download Procedure

Step	Action
1	Enable download to the relevant controller(s) by activating the “Access enable” input(s). Note: It is recommended to perform a download to one AC 800M HI at the time.
2	Select the controller(s) to be updated in Control Builder M Professional.
3	Select warm or cold restart for each application (the first time a download is performed, cold restart is automatically selected), based on the *retain value* philosophy described in Application Design and Development on page 78.
4	If there are any compilation errors or warnings displayed, a careful judgment shall be done prior to continuing (or canceling) the download (not possible to continue with errors).

Table 17. Program Download Procedure (Continued)

Step	Action
5	The difference report(1) (2)presented on the screen shall be carefully analyzed. Verify that all the intended changes are correctly implemented and do also verify for all SIL marked applications that no unintended changes are done. If cold restart is selected, the Source Code Report part of the difference report contains an item named **Cold Retain and Instance specific values.** Verify for all SIL marked applications that applied cold retain values are correct before continuing with the download. Select continue or cancel.
6	If the download is interrupted before completion, a new download shall be performed.
7	After the download, open the “Show Downloaded Items” display and verify that the correct versions of all applications and controller configurations are downloaded and running, by comparing the compilation date and signature for each item with the corresponding information found in the “difference report” or “source code report”.
8	Check that all tasks in AC 800M HI are running with sufficient margin to the specified interval time.
9	Perform testing as planned during engineering, see Test and Verification on page 115.
10	The system is considered operating safe when these steps are performed.

(1) The first time an application is downloaded, the difference report is empty, for more information, see Difference Report on page 115.

(2) If “continue” is selected after analyzing the presented differences, the difference report will be saved for future reference.

Program Download with LEG

For details on how to perform Program Download with LEG, refer to the user instructions delivered with your licensed option.
The Program Download with LEG option is not available for SIL3 systems.



Program Download with LEG to an AC 800M HI is not allowed if any changes to the controller configuration is made.



To ensure a safe program Download with LEG to the AC 800M HI, the steps described in Table 18. Program Download with LEG Procedure on page 123 shall be performed.

Table 18. Program Download with LEG Procedure

Step	Action
1	Select “evaluation” in the restart mode dialog. The new application version will be started with retain values from the old application version.
2	Enable download to the relevant controller by activating the “Access enable” input.
3	Select the application to be updated.
4	If there are any compilation errors or warnings displayed, a careful judgment shall be done prior to continuing (or canceling) the download (not possible to continue with errors).
5	Analyze the result of the Task Analysis tool to predict the execution of tasks in controllers before downloading the application to a controller. If significant changes has been made adjust the expected execution time for more accurate analysis result.
6	The difference report(1) presented on the screen shall be carefully analyzed. Verify that all the intended application changes are correctly implemented and do also verify that no unintended changes are done. There shall be no changes to the controller configuration. Select continue or cancel.
7	If the download is interrupted before completion, a new download shall be performed.

Table 18. Program Download with LEG Procedure

Step	Action
8	Analyze the evaluation report presented on the screen to determine whether process control shall be switched to the new application or not. It is also possible to cancel the download and continue operation with the old application.
9	After the LEG session is finished (new or old application is running), open the “Show Downloaded Items” display and verify that the correct versions of all applications and controller configurations are downloaded and running, by comparing the compilation date and signature for each item with the corresponding information found in the “difference report” or “source code report”.
10	Check that all tasks in AC 800M HI are running with sufficient margin to the specified interval time.
11	Perform testing as planned during engineering, see Test and Verification on page 115.
12	The system is considered operating safe when these steps are performed.

(1) If “continue” is selected after analyzing the presented differences, the difference report will be saved for future reference. For more information, see Difference Report on page 115.



The displayed data in the evaluation report on the Control Builder M Professional screen can not be used to validate the safety function of the application.

Controller Restart

Pressing the INIT button manually restarts the controller. A short press (less than 3 seconds) results in a cold restart, hence only variables with the attribute cold retain are maintained.

A long press on the INIT button results in a complete reset of the controller and a new download of all applications is needed. Also in this case, variables with the attribute cold retain are maintained, provided they are stored in the aspect server.

A power failure, in combination with too low battery capacity in the controller, will have the same effect as a long press on the INIT button.



It is recommended to verify that the intended re-start (warm- or cold re-start) has been performed by using the controller log.

Commissioning Test Activities

Commissioning test activities shall include field devices and other external components needed to perform a complete function. The aim of the test is to verify that all components work together in their real environment.

Procedures for handling deviations identified during the commissioning testing shall be established. The procedures shall cover necessary impact analyses and re-engineering activities to be able to handle all deviations safely, also if the deviation origins from an early engineering phase, or from input documents to the engineering. For guidance in testing of such modifications, see Modification Testing on page 118.

If parts of the safety functions controlled by the AC 800M HI are put operational, while other parts are still under commissioning, procedures shall be established to secure the integrity of the operational parts.

Safety Validation

The objective of the safety validation is to validate, through inspection and testing that all safety functions are in operation as specified.
Specific validation procedures shall be developed for the actual plant; this chapter contains some items to consider when developing the procedures.

Verify that all safety functions are tested and in operation.

Verify that tests are done to demonstrate correct system behavior upon loss of utilities like electrical power, air or hydraulics.

Verify that tests are done to demonstrate correct system behavior upon fault of redundant parts.

Verify that tests are done to demonstrate correct system behavior upon loss of communications.

Verify that a correct backup of all software exists and are stored securely.

Verify that all relevant documentation is updated and stored securely.

The validation should include the following items to ensure that all temporary degradations of the safety functions are removed:

- Verify that all applications are marked with the correct SIL mark
- Verify that no warnings are presented during compilation and download
- Verify that all forces and bypasses in the application software are removed
- Verify that all temporary bypasses and overrides in the hardware, including field loops are removed.
- Verify that all system components (including redundant parts) are running without any error LEDs, or error messages.
- Verify that all temporary filtering of “system alarms from hardware units” are removed, (setting on object level in the hardware editor).

Operation and Maintenance

This subsection contains information on how to maintain the required SIL of each safety instrumented function during the operation period.

Operation and Maintenance Planning

Operation and maintenance planning for the SIS shall be carried out, this requirement ensures that functional safety continues beyond the design, production, installation and commissioning of the system. Guidance and procedures shall be provided to enable the organization responsible for Operation and Maintenance to maintain the intended safety levels of the safety instrumented functions.

The Operation and maintenance plan shall include:

- Start-up and shutdown procedures of the process
- Procedures for normal operation
- Maintenance activities for sensors, actuators and other field devices
- Maintenance activities for the SIS
- Allocation of responsibilities for the various tasks

Operation Procedures

Procedures shall be established to secure safe operation of the SIS under all process conditions and states.

As described in chapter Access Management Settings on page 111, the operator's possibility to change values in an AC 800M HI can be configured to fit the operation philosophy of the plant. The configured behavior of the system shall be reflected in the operation procedures.

The utilization of the **Access Enable** key switch and the **Reset all Forces** panel button as described in Physical I/O for Operator and Maintenance Personnel Interaction on page 72 shall be reflected in the operation procedures.

All operations on an object in a SIL application, shall be confirmed by the operator by selecting **yes** in the **Confirm Operation** dialog, see Figure 6 below.

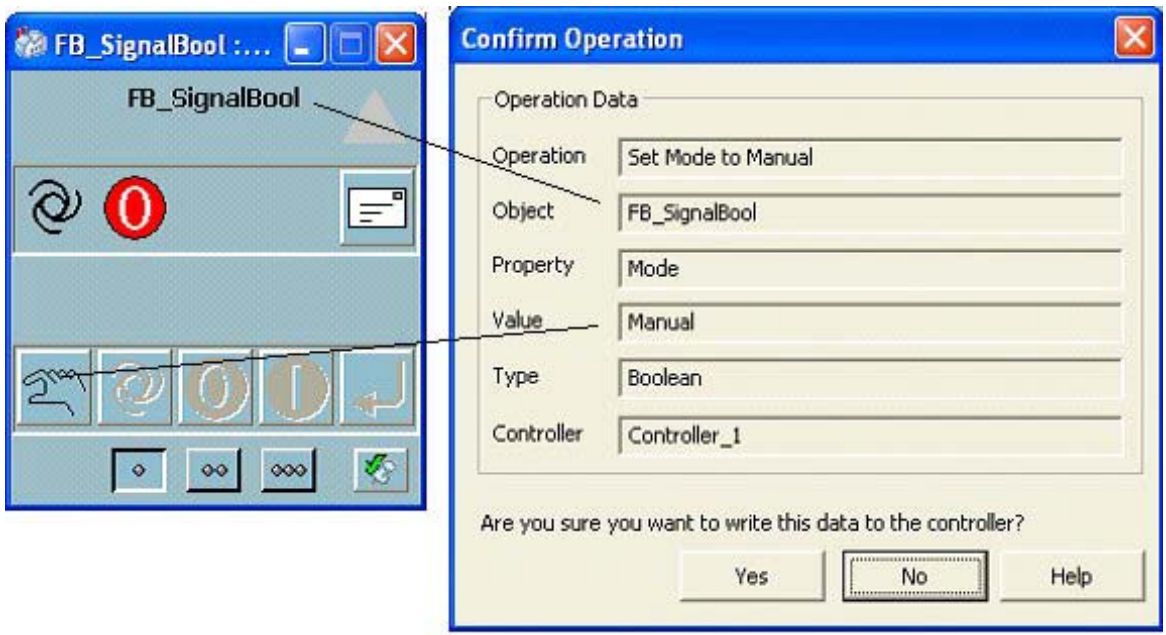


Figure 6. Confirm Operation Dialog

Notes to Figure 6:

The **Confirm Operation** dialog has a timeout and has to be acknowledged within 90 seconds. After 90 seconds the confirm button is dimmed and it's only possible to cancel the write operation.

It is the operator's responsibility to verify that the operation performed in the faceplate corresponds to the operation indicated in the **Confirm Operation** dialog, which is the system's interpretation of the intended operation.

The operation procedures shall emphasize the operator's responsibility to verify his operations by checking the **Confirm Operation** dialog.

All operators authorized to use the **Confirmed Operation** dialog, shall be part of the <Safety Operator Group> in the 800xA Operator Workplace.

Alarm acknowledge is not invoking the **Confirm Operation** dialog, nor is it dependent of the SIL access setting, i.e. there is no restriction on acknowledging alarms in SIL applications.



It is not possible to enable/disable alarms in a SIL classified application from the Alarm List on the 800xA Operator Workplace.



If the HART routing functionality of AI880A is not restricted by the configuration settings of the module, the operation procedures shall include restrictions for use of this function.

Maintenance Procedures

Routine Maintenance

Procedures shall be established for performing necessary maintenance to the SIS, see also guidelines given in Proof Testing and Inspection on page 131.
The procedures shall include measures to be taken to maintain the safety functions during testing, or if necessary, what additional steps need to be implemented to reduce the risk during testing.

Procedures for performing maintenance to connected field devices (including interfacing components, cabling etc.) shall describe necessary precautions to avoid hazardous situations to arise.
If unintended activation of the device can imply any danger, measures external to the AC 800M HI shall be planned (e.g disconnect power or activate mechanical interlocks).

Procedures shall also be established to secure that test equipment used during maintenance activities are properly calibrated and maintained.

For requirements for routine maintenance of the AC 800M HI, see user manuals *AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41*.

Fault Finding and Repair

The AC 800M HI has extensive self-test and diagnostic functions that report all detected failures promptly. The consequence of a faulty module depends on the nature of the fault and the level of redundancy installed in the actual configuration:

- If available, the system maintains safety by switching to a redundant unit.
- If no redundant unit is available, the AC 800M HI deactivates its outputs and thus the process is brought to the safe state.

Procedures shall be developed and implemented to govern the reaction to detected faults in the SIS. The following warnings and information shall be reflected;



In redundant DO880 configurations, faulty DO880 modules shall be removed from the system within the repair time of 72 hours.

Online Replacement of SM811 (Hot Insert)

When the Hot Insert button is pressed, the SIL 3 applications are stopped, and the 1131-task execution is delayed for a short period of time. During this period the output signals are not updated, but keep their current values. The stop time is normally << 1 second and always limited by the configured FDRT.



Online replacement (Hot Insert) of the SM811 will lead to a short stop of the SIL3 applications. The stop time is limited by the configured FDRT.



If the configured FDRT is exceeded, the Hot Insert procedure will be interrupted, and the application is started again.

Hot insert will also occur after power failure of one CEX segment.



Reported faults should be repaired promptly to re establish the availability of the installation.



The Control Builder M Professional can be used for monitoring values in the AC 800M HI, but it is not possible to change values in SIL classified applications.

For information and guidelines related to fault finding and module replacement, see the user manuals *AC 800M Controller Hardware, 3BSE036351* page 41* and *S800 I/O Getting Started, 3BSE020923* page 41*.

Training and Qualifications

The general guidelines regarding qualifications and allocation of responsibilities given in chapter Organization and Resources on page 52 apply.

The training of operators shall emphasize:

- The safety functions implemented in the SIS
- The hazards the SIS is protecting against
- Routines and procedures for operation of bypass switches
- Routines and procedures for operation of manual shutdown/activation switches
- Procedures for action upon SIS diagnostic alarms

The training of maintenance personnel shall be adapted to the level of maintenance they will perform. Routine testing of field devices requires different skills than faultfinding and module replacement in the SIS.

Proof Testing and Inspection

In most system configurations there will be some elements of the SIF that will not be covered by the system's automatic diagnostic functions (e.g. sensors, actuators and field wiring). To avoid fault accumulation within those elements, periodic proof testing of the safety instrumented functions shall be conducted. The proof test interval shall be calculated using PFD calculations. This will probably result in different test intervals for different parts of the SIS.

The proof test interval required for the AC 800M HI is:

- 8 years for central processing unit (PM865 and SM810/SM811)
- 8 years for I/O system and other peripherals

These test intervals are used in *800xA - Safety, Reliability and Availability Data, 3BSE034876* page 41*[1].

The safety instrumented system (including field devices) shall be visually inspected at regular intervals, to detect any observable damages.

Records and procedures for handling findings from both proof testing and inspections shall be created.

1. The document is not distributed on media, but available through ABB web services. page 42

Modification during Operation

Application Modifications

In order to maintain the safety integrity level of the safety system during the operation period, it is of vital importance that proper procedures for modifications are established and implemented.
Such procedures shall secure that all modifications to the SIS are properly planned, reviewed and approved prior to implementing the change.

The following list is intended as items to consider when establishing procedures for modification during operation:

- Impact analysis to identify all influenced parts of the system
- Properly trained and qualified personnel
- Guidelines described in System Design and Engineering on page 61
- Guidelines described in Application Software on page 77
- Guidelines described in Modification Testing on page 118
- Will the modification be implemented while the process is running?
  - Evaluate the need for temporary measures to maintain safety integrity during the implementation.
  - Evaluate the need for temporary measures to avoid process upsets during the implementation.
- Procedure Program Download and Startup on page 120

If the system is configured as a combined BPCS and SIS, changes can be done to the BPCS part without affecting the SIS.



To verify that no unintended changes to the SIS part of the system are done, always examine the difference report before download, (see Difference Report on page 115).

Firmware Upgrade

Firmware is the system software in controller CPUs and units such as SM810/SM811 and communication interfaces on the CEX-Bus. Upgrading of

firmware is done by downloading new versions from Control Builder M Professional.



Firmware Upgrade from Compact FLASH is not supported for AC 800M HI.

Firmware can be upgraded in a stopped/empty controller, or online in a running controller without interfering with the running process.



Online Upgrade is only possible for redundant AC 800M HI controllers.

Upgrade of stopped controllers



To ensure a safe Firmware Upgrade of a stopped AC 800M HI, the steps described in Table 19. Firmware Upgrade Procedure on page 133 shall be performed.

Firmware of single AC 800M HI can only be upgraded when the AC 800M HI contains no application programs.

Prior to removing an application from an AC 800M HI, cold retain values can be saved to the aspect directory.

Table 19. Firmware Upgrade Procedure

Step	Action
1	Save cold retain values to the aspect directory (if needed).
2	Select the controller to be upgraded.
3	Reset the controller by pressing the Reset-button on PM865 for more then 3 seconds, in a redundant configuration both PM865 have to be reset simultaneously.
4	Select the unit to be upgraded (PM865 or SM810/SM811).
5	Select the firmware version to be downloaded.

Table 19. Firmware Upgrade Procedure

Step	Action
6	After the download, the controller is restarted (automatically), then open the “Show Firmware Information” display and verify that the correct versions of firmware are downloaded.
7	Download the application to the controller by following the procedure described in Program Download and Startup on page 120.

For details on how to perform the above tasks, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Online Upgrade

Redundant AC 800M HI controllers (PM865 and SM810/SM811) can be upgraded with new firmware versions online.

Online Upgrade is not possible on versions prior to System Version 5.0 SP1 CC1.

During Online Upgrade, redundancy is disabled, hence hardware failures occurring during this operation might lead to process upset.

The application controlling the process is stopped, and the 1131-task execution is delayed for a short period of time during the upgrade. During this period of time the output signals are not updated, but keep their current values.

The parameter Online Upgrade Handover Limit defines the maximum allowed time consumption for the hand over, see Controller Settings and Restrictions on page 91.

Before Online Upgrade is started, check that the “Online Upgrade Handover Limit” is set in accordance with the time demands of the process under control.

If the defined Online Upgrade Handover Limit is exceeded, the Online Upgrade procedure will be interrupted, and a roll-back of control to the Primary will take place.

If the controller to be upgraded contains one or more server(s) for safe communication link(s) to other controller(s) (clients), care shall be taken to avoid

process upsets in the clients due to timeout of the safe link (Control modules MMSDefxxx and MMSReadxxx).
The MMSReadxxxM modules (client) contains a parameter (OluTimeOut) for setting a special timeout during Online Upgrade of the server.
When an Online Upgrade is initiated in a controller hosting an MMS server, all the peer to peer clients receive information about this (through the safe link) and provided the “Access Enable” input is activated, the OluTimeOut is used for monitoring the communication.



To avoid time-out/invalid data on peer-to-peer links, the ‘Access Enable’ input in all clients shall be activated.



During Online Upgrade, short delays in the communication with the 800xA Operator Workplace might lead to e.g. interrupts in trend values and short alarm delays.

After the first download of a SIL marked application to an AC 800M HI controller, subsequent downloads are protected by the “Access enable” input on the SM810/SM811, see description under Operator Interface on page 72.
Download of SIL3 applications are always protected by the “Access enable” input.



The “Access enable” input shall be enabled to allow Online Upgrade to an AC 800M HI controller.



Online Upgrade of an AC 800M HI is not allowed if any changes to the controller configuration or application is made.



To ensure a safe Online Upgrade of firmware in a running AC 800M HI, the sequence described in Table 20. Online Upgrade Procedure on page 136 shall be performed.

Table 20. Online Upgrade Procedure

Step	Action
1	Enable download to the relevant controller(s) by activating the “Access enable” input(s).
2	Verify that the ‘OluTimeOut’ parameter of all clients to safe MMS communication is sufficiently long and activate ‘Access Enable’ on the client(s).
3	Verify that the “ModuleBus timeout” parameter of all IO modules are set to minimum 512ms.
4	Select the controller(s) to be updated in Control Builder M Professional.
5	Perform the Online Upgrade by following the 9-step wizard of Control Builder M Professional as described in the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.
6	The difference report(1) presented on the screen shall be carefully analyzed. 1. Verify that no changes is made to the controller configuration. 2. Verify that no changes is made to the safety application. 3. Verify correct versions of hardware-Libraries. 4. The only difference should be related to new or updated libraries. 5. Select continue or cancel.
7	After the upgrade, then open the “Show Firmware Information” display and verify that the correct versions of firmware are downloaded.
8	Open the “Show Downloaded Items” display and verify that the correct versions of all applications and controller configurations are downloaded and running, by comparing the compilation date and signature for each item with the corresponding information found in the “difference report” or “source code report”.

Table 20. Online Upgrade Procedure

Step	Action
9	Check that all tasks in AC 800M HI are running with sufficient margin to the specified interval time.
10	Press the “Hot Insert” button to regain synchronization of the backup SM811 (only for redundant SIL3 systems).
11	Perform testing as planned during engineering, see Test and Verification on page 115.
12	The system is considered operating safe when these steps are performed.

(1) If “continue” is selected after analyzing the presented differences, the difference report will be saved for future reference. For more information, see Difference Report on page 115.

For details on how to perform the above tasks, refer to the user manual *System 800xA Control 5.1 AC 800M Configuration, 3BSE035980* page 42*.

Configuration Management

For modifications done during operation, it is vital to continue the Configuration Management established during the engineering phase. See Configuration Management on page 114.

Decommissioning

Prior to decommissioning the system, proper planning and procedures shall be established.

An analysis shall be performed to determine the impact on functional safety from the proposed decommissioning activities. The assessment shall consider:

- Functional safety during execution of the decommissioning activities
- Impact on adjacent operating units and facilities
  - Including interfaces to other safety instrumented systems
- Sequence of decommissioning

  - Is there a need to keep parts of the safety functions operational during some stages of the decommissioning?

- Identify need for establishing temporary safety measures during the decommissioning activities.

All parts of the safety system shall be disposed according to national laws and regulations regarding environmental aspects.

Appendix A Certified Libraries

Introduction

The Control Builder M Professional is supplied with predefined libraries of “System Functions”, “Function Block Types” and “Control Module Types”. This appendix provides lists of library elements that are certified for use in SIL marked applications, the classifications are:

- **SIL3**
  Can be used in SIL3, SIL1-2 and NonSIL applications, the *Restriction* column in the tables below might give limitations in the use.
- **SIL3 restricted**
  Can be used in SIL3, SIL1-2 and NonSIL applications, the outputs from these elements shall not be used in a way that can influence the safety function of a SIL classified application.
- **SIL2**
  Can be used in SIL1-2 and NonSIL applications, the *Restriction* column in the tables below might give limitations in the use.
- **SIL2 restricted**
  Can be used in SIL1-2 and NonSIL applications, the outputs from these elements shall not be used in a way that can influence the safety function of a SIL classified application.

The SIL2 Restricted and SIL3 Restricted elements are identified in Control Builder M Professional with a special icon. The color of the SIL-digit in the icon is grey on a restricted element compared to the black digit on regular SIL-classified types and functions.

Other library elements supplied with the system, but not listed here, are intended for use in non-SIL marked applications in the AC 800M HI controller.

The types are described in Control Builder M Professional Online Help.

System Functions

Due to limited support for the data types *string* and *date_and_time* in SIL3 applications, it is not allowed to use these data types in code that can influence the safety function of a SIL3 classified application.
If such code affects an output from a SIL3 application, it might result in a Safety Shutdown.

Variables of type *string* and *date_and_time* shall only be used for presentation purposes.

Table 21. System Functions

System Function	Certification	Restrictions
abs	SIL3	
add	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
addsuffix	SIL3	
and	SIL3	
ASCIIStructToString	SIL3 Restricted SIL2	
bool_to_dint	SIL3	
bool_to_dword	SIL3	
bool_to_int	SIL3	
bool_to_real	SIL3	
bool_to_string	SIL3 Restricted SIL2	
bool_to_uint	SIL3	
bool_to_word	SIL3	
Bool16ToDint	SIL3	
Bool32ToDint	SIL3	

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
date_and_time_to_string	SIL3 Restricted SIL2	
dint_to_bool	SIL3	
dint_to_dword	SI 3	
dint_to_int	SIL3	
dint_to_real	SIL3	
dint_to_string	SIL3 Restricted SIL2	
dint_to_time	SIL3	
dint_to_uint	SIL3	
dint_to_word	SIL3	
div	SIL3	
dword_to_bool	SIL3	
dword_to_dint	SIL3	
dword_to_int	SIL3	
dword_to_real	SIL3	
dword_to_string	SIL3 Restricted SIL2	
dword_to_uint	SIL3	
dword_to_word	SIL3	
eq	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
ExecuteControlModules	SIL3	
expt	SIL3	

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
FirstScanAfterApplicationStart	SIL3	
FirstScanAfterPowerUp	SIL3	
ge	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
GetActualIntervalTime	SIL3	
GetApplicationSIL	SIL3	
GetIntervalTime	SIL3	
GetSystemDT	SIL3 Restricted SIL2 Restricted	
gt	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
int_to_bool	SIL3	
int_to_dint	SIL3	
int_to_dword	SIL3	
int_to_real	SIL3	
int_to_string	SIL3 Restricted SIL2	
int_to_uint	SIL3	
int_to_word	SIL3	
le	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
len	SIL3 Restricted SIL2	
limit	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
lt	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
match	SIL3 Restricted SIL2	
max	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
min	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
mod	SIL3	
move	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
mul	SIL3	
mux	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
ne	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
not	SIL3	
or	SIL3	
ReadStatusZeroDivInt	SIL2	
ReadStatusZeroDivReal	SIL2	
real_to_bool	SIL3	
real_to_dint	SIL3	
real_to_dword	SIL3	
real_to_int	SIL3	
real_to_string	SIL3 Restricted SIL2	

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
real_to_time	SIL3	
real_to_uint	SIL3	
ResetForcedValue	SIL3	
rol	SIL3	
ror	SIL3	
sel	SIL3	
serial_string_append_ASCII	SIL2	
serial_string_append_Hex	SIL2	
serial_string_find_ASCII	SIL2	
serial_string_get_ASCII	SIL2	
serial_string_Hex_to DWORD	SIL2	
serial_string_left	SIL2	
serial_string_mid	SIL2	
serial_string_put_ASCII	SIL2	
serial_string_replace_Hex	SIL2	
serial_string_right	SIL2	
shl	SIL3	
shr	SIL3	
sqrt	SIL3	
string_to_bool	SIL3 Restricted SIL2	
string_to_date_and_time	SIL3 Restricted SIL2	

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
string_to_dint	SIL3 Restricted SIL2	
string_to_dword	SIL3 Restricted SIL2	
string_to_int	SIL3 Restricted SIL2	
string_to_real	SIL3 Restricted SIL2	
string_to_time	SIL3 Restricted SIL2	
string_to_uint	SIL3 Restricted SIL2	
string_to_word	SIL3 Restricted SIL2	
sub	SIL3	SIL3 Restricted/SIL2 when used with type *string* and type *date_and_time*
SystemDTToLocalDT	SIL3 Restricted SIL2 Restricted	
time_to_dint	SIL3	
time_to_real	SIL3	
time_to_string	SIL3 Restricted SIL2	
Timer	SIL3	
TimerElapsed	SIL3	
TimerElapsedMS	SIL3	
TimerHold	SIL3	
TimerReset	SIL3	

Table 21. System Functions (Continued)

System Function	Certification	Restrictions
TimerStart	SIL3	
uint_to_bool	SIL3	
uint_to_dint	SIL3	
uint_to_dword	SIL3	
uint_to_int	SIL3	
uint_to_real	SIL3	
uint_to_string	SIL3 Restricted SIL2	
uint_to_word	SIL3	
word_to_bool	SIL3	
word_to_dint	SIL3	
word_to_dword	SIL3	
word_to_int	SIL3	
word_to_string	SIL3 Restricted SIL2	
word_to_uint	SIL3	
xor	SIL3	

Library Types

Some of the Certified Function Block Types and Control Module Types, contains SILx Restricted sub-objects. Output parameters originating from such sub-objects are marked with NONSIL in the parameter description, such parameters shall not be used in a way that can influence the safety functions of a SIL classified application. The Library types are programmed using the ST language.

AlarmEventLib

Table 22. AlarmEventLib, Function Block Types

Function Block Types	Certification	Restrictions
AlarmCond	SIL3 Restricted	
AlarmCondBasic	SIL3 Restricted	
ProcessObjectAE	SIL2 Restricted	
SignalAE	SIL3 Restricted	
SimpleEventDetector	SIL3 Restricted	
SystemAlarmCond	SIL2 Restricted	

Table 23. AlarmEventLib, Control Module Types

Control Module Types	Certification	Restrictions
AlarmCondBasicM	SIL2 Restricted	
AlarmCondM	SIL2 Restricted	

BasicLib

Table 24. BasicLib, Function Block Types

Function Block Types	Certification	Restrictions
ACOFAct	SIL2	
ACOFAct3P	SIL2	
ACOFActDeact	SIL2	
ACOFActDeact3P	SIL2	
CTD	SIL3	

Table 24. BasicLib, Function Block Types (Continued)

Function Block Types	Certification	Restrictions
CTU	SIL3	
CTUD	SIL3	
ErrorHandler	SIL3	
F_Trig	SIL3	
ForcedSignals	SIL3	
PulseGenerator	SIL2	
R_Trig	SIL3	
RS	SIL3	
SampleTime	SIL2	
SR	SIL3	
TimerD	SIL2	
TimerOffHold	SIL2	
TimerOnHold	SIL2	
TimerOnOffHold	SIL2	
TimerPulseHold	SIL2	
TimerPulseHoldDel	SIL2	
TimerU	SIL2	
TOf	SIL3	
TOn	SIL3	
TP	SIL3	
Trigger	SIL2	

Table 25. BasicLib, Control Module Types

Control Module Types	Certification	Restrictions
CCInputGate	SIL2	
CCOutputGate	SIL2	
ErrorHandlerM	SIL2	
ForcedSignalsM	SIL2	
GroupStartObjectConn	SIL2	

FireGasLib

Table 26. FireGasLib, Control Module Types

Control Module Types	Certification	Restrictions
CO2	SIL2	Contains one or more NONSIL output(s)
Deluge	SIL2	Contains one or more NONSIL output(s)
FGOutputOrder	SIL2	Contains one or more NONSIL output(s)
Sprinkler	SIL2	Contains one or more NONSIL output(s)

IconLib

Control Module Types

All Control Module types in IconLib are for presentation purpose only. They are all certified for use in SIL2 and SIL3 marked applications.

MMSCommLib

Table 27. MMSCommLib, Function Block Types

Function Block Types	Certification	Restrictions
MMSConnect	SIL3 Restricted	See restriction for use under heading *Communication Between Applications* in chapter Software Architecture on page 79.
MMSDef4Bool	SIL2 Restricted	
MMSDef4BoolIO	SIL2 Restricted	
MMSDef4Dint	SIL2 Restricted	
MMSDef4DintIO	SIL2 Restricted	
MMSDef4Real	SIL2 Restricted	
MMSDef4RealIO	SIL2 Restricted	
MMSRead4Bool	SIL2 Restricted	
MMSRead4Dint	SIL2 Restricted	
MMSRead4Real	SIL2 Restricted	

Table 28. MMSCommLib, Control Module Types

Control Module Types	Certification	Restrictions
MMSDef128BoolM	SIL2	See restriction for use under heading *Communication Between Applications* in chapter Software Architecture on page 79.
MMSDef16BoolM	SIL2	
MMSDef2DintM	SIL2	
MMSDef2DwordM	SIL2	
MMSDef2RealM	SIL2	
MMSDef64BoolM	SIL2	
MMSDefHI	SIL3	
MMSRead128BoolM	SIL2	
MMSRead16BoolM	SIL2	
MMSRead2DintM	SIL2	
MMSRead2DwordM	SIL2	
MMSRead2RealM	SIL2	
MMSRead64BoolM	SIL2	
MMSReadHI	SIL3	

ProcessObjBasicLib

Table 29. ProcessObjBasicLib, Function Block Types

Function Block Types	Certification	Restrictions
BiCore	SIL2	
BiDelayOfCmd	SIL2	
BiSimple	SIL2	
DetectOverrideBi	SIL2	
DetectOverrideUni	SIL2	
DetectOverrideVoteBi	SIL2	
DetectOverrideVoteUni	SIL2	
Jog	SIL2	
PrioritySup	SIL2	
UniCore	SIL2	
UniDelayOfCmd	SIL2	
UniSimple	SIL2	

Table 30. ProcessObjBasicLib, Control Module Types

Control Module Types	Certification	Restrictions
BiSimpleM	SIL2	
DisplayOverrides	SIL2	
FaceplateBiSimple	SIL2	
FaceplateBiSimpleM	SIL2	
FaceplateUniSimple	SIL2	

Table 30. ProcessObjBasicLib, Control Module Types

Control Module Types	Certification	Restrictions
FaceplateUniSimpleM	SIL2	
IconProcObj	SIL2	
InfoOverrideBi	SIL2	
InfoOverrideBiM	SIL2	
InfoOverrideBiSimple	SIL2	
InfoOverrideUni	SIL2	
InfoOverrideUniM	SIL2	
InfoOverrideUniSimple	SIL2	
InfoParBi	SIL2	
InfoParBiGroupStart	SIL2	
InfoParBiM	SIL2	
InfoParUni	SIL2	
InfoParUniGroupStart	SIL2	
InfoParUniM	SIL2	
UniSimpleM	SIL2	

ProcessObjExtLib

Table 31. ProcessObjExtLib, Function Block Types

Function Block Types	Certification	Restrictions
Bi	SIL2	Contains one or more NONSIL output(s)
LevelDetection	SIL2	
MotorBi	SIL2	Contains one or more NONSIL output(s)
MotorUni	SIL2	Contains one or more NONSIL output(s)
OETextBi	SIL2	
OETextUni	SIL2	
OETextValveUni	SIL2	
Uni	SIL2	Contains one or more NONSIL output(s)
ValveUni	SIL2	Contains one or more NONSIL output(s)

Table 32. ProcessObjExtLib, Control Module Types

Control Module Types	Certification	Restrictions
BiM	SIL2	Contains one or more NONSIL output(s)
FaceplateBi	SIL2	
FaceplateBiM	SIL2	
FaceplateMotorBi	SIL2	
FaceplateMotorBiM	SIL2	
FaceplateMotorUni	SIL2	
FaceplateMotorUniM	SIL2	
FaceplateUni	SIL2	

Table 32. ProcessObjExtLib, Control Module Types

Control Module Types	Certification	Restrictions
FaceplateUniM	SIL2	
FaceplateValveUni	SIL2	
FaceplateValveUniM	SIL2	
GroupStartIconBi	SIL2	
GroupStartIconMotorBi	SIL2	
GroupStartIconMotorUni	SIL2	
GroupStartIconUni	SIL2	
GroupStartIconValveUni	SIL2	
InfoParMotorBi	SIL2	
InfoParMotorBiM	SIL2	
InfoParMotorUni	SIL2	
InfoParMotorUniM	SIL2	
InfoParValveUni	SIL2	
InfoParValveUniM	SIL2	
MotorBiM	SIL2	Contains one or more NONSIL output(s)
MotorUniM	SIL2	Contains one or more NONSIL output(s)
UniM	SIL2	Contains one or more NONSIL output(s)
ValveUniM	SIL2	Contains one or more NONSIL output(s)

SerialCommLib

Table 33. SerialCommLib, Function Block Types

Function Block Types	Certification	Restrictions
SerialConnect	SIL2 Restricted	
SerialListen	SIL2 Restricted	
SerialListenReply	SIL2 Restricted	
SerialSetup	SIL2 Restricted	
SerialWrite	SIL2 Restricted	
SerialWriteWait	SIL2 Restricted	

SignalBasicLib

Table 34. SignalBasicLib, Function Block Types

Function Block Types	Certification	Restrictions
SignalBasicBool	SIL3	
SignalBasicInBool	SIL3	
SignalBasicInReal	SIL3	
SignalBasicOutBool	SIL3	
SignalBasicReal	SIL3	

SignalLib

Table 35. SignalLib, Function Block Types

Function Block Types	Certification	Restrictions
SignalBool	SIL2	Contains one or more NONSIL output(s)
SignalInBool	SIL2	Contains one or more NONSIL output(s)
SignalInReal	SIL2	Contains one or more NONSIL output(s)
SignalOutBool	SIL2	Contains one or more NONSIL output(s)
SignalReal	SIL2	Contains one or more NONSIL output(s)
SignalSimpleInReal	SIL2	

Table 36. SignalLib, Control Module Types

Control Module Types	Certification	Restrictions
SDLevelAnd4	SIL2	
SDLevelBranch4	SIL2	
SDLevelM	SIL2	Contains one or more NONSIL output(s)
SDLevelOr4	SIL2	
SignalBoolCalcInM	SIL2	Contains one or more NONSIL output(s)
SignalBoolCalcOutM	SIL2	Contains one or more NONSIL output(s)
SignalInBoolM	SIL2	Contains one or more NONSIL output(s)
SignalInRealM	SIL2	Contains one or more NONSIL output(s)
SignalOutBoolM	SIL2	Contains one or more NONSIL output(s)
SignalRealCalcInM	SIL2	Contains one or more NONSIL output(s)
SignalRealCalcOutM	SIL2	Contains one or more NONSIL output(s)

Table 36. SignalLib, Control Module Types

Control Module Types	Certification	Restrictions
SignalSimpleInRealM	SIL2	Contains one or more NONSIL output(s)
Vote1oo1Q	SIL2	Contains one or more NONSIL output(s)
VoteBranch4	SIL2	
VotedAnd4	SIL2	
VotedBranch4	SIL2	
VotedOr4	SIL2	
VoteXoo2D	SIL2	Contains one or more NONSIL output(s)
VoteXoo3Q	SIL2	Contains one or more NONSIL output(s)
VoteXoo8	SIL2	Contains one or more NONSIL output(s)

SignalSupportLib

Table 37. SignalSupportLib, Function Block Types

Function Block Types	Certification	Restrictions
DiffNormalDetection	SIL3	
ErrorDetection	SIL3	
FBSupervision	SIL3	
GTLevelDetection	SIL3	
LPFilter	SIL3	
LTLevelDetection	SIL3	
ModeControl	SIL3	

Table 37. SignalSupportLib, Function Block Types

Function Block Types	Certification	Restrictions
OutBoolControl	SIL3	
OutValveControl	SIL3	
SRedundantIn	SIL3	
SsampleTime	SIL3	
StatusCollection	SIL3	

SupervisionBasicLib

Table 38. SupervisionBasicLib, Function Block Types

Function Block Types	Certification	Restrictions
SDBool	SIL3	Contains one or more NONSIL output(s)
SDInBool	SIL3	Contains one or more NONSIL output(s)
SDInReal	SIL3	Contains one or more NONSIL output(s)
SDLevel	SIL3	Contains one or more NONSIL output(s)
SDOutBool	SIL3	Contains one or more NONSIL output(s)
SDReal	SIL3	Contains one or more NONSIL output(s)
SDValve	SIL3	Contains one or more NONSIL output(s)
StatusRead	SIL3	

Table 39. SupervisionBasicLib, Control ModuleTypes

Control Module Types	Certification	Restrictions
FaceplateSDBool	SIL3	
FaceplateSDInBool	SIL3	
FaceplateSDInReal	SIL3	
FaceplateSDOutBool	SIL3	
FaceplateSDReal	SIL3	
FaceplateSDValve	SIL3	
InfoAlarmSDInReal	SIL3	
InfoBarSDReal	SIL3	
InfoHistSDBool	SIL3	
InfoHistSDReal	SIL3	
InfoParSDAlarm	SIL3	
InfoParSDBool	SIL3	
InfoParSDBoolAlarm	SIL3	
InfoParSDError	SIL2	
InfoParSDInReal	SIL3	
InfoParSDOutBool	SIL3	
InfoParSDOutBoolAlarm	SIL3	
InfoParSDReal	SIL3	
InfoParSDValve	SIL3	

SupervisionLib

Table 40. SupervisionLib, Control Module Types

Control Module Types	Certification	Restrictions
Detector1Real	SIL2	Contains one or more NONSIL output(s)
Detector2Real	SIL2	Contains one or more NONSIL output(s)
DetectorAnd	SIL2	
DetectorAnd16	SIL2	
DetectorAnd4	SIL2	
DetectorAnd8	SIL2	
DetectorBool	SIL2	Contains one or more NONSIL output(s)
DetectorBranch	SIL2	
DetectorBranch16	SIL2	
DetectorBranch4	SIL2	
DetectorBranch8	SIL2	
DetectorLoopMonitored	SIL2	Contains one or more NONSIL output(s)
DetectorOr	SIL2	
DetectorOr16	SIL2	
DetectorOr4	SIL2	
DetectorOr8	SIL2	
DetectorRemote	SIL2	Contains one or more NONSIL output(s)
DetectorVote	SIL2	
OrderBranch	SIL2	
OrderBranch16	SIL2	
OrderBranch4	SIL2	

Table 40. SupervisionLib, Control Module Types (Continued)

Control Module Types	Certification	Restrictions
OrderBranch8	SIL2	
OrderMMSDef16	SIL2	
OrderMMSRead16	SIL2	
OrderOr	SIL2	
OrderOr16	SIL2	
OrderOr4	SIL2	
OrderOr8	SIL2	
OutputBool	SIL2	Contains one or more NONSIL output(s)
OutputOrder	SIL2	Contains one or more NONSIL output(s)
OverrideControlInterface	SIL2	
OverviewConversion	SIL2	
SiteOverview	SIL2	
SiteOverviewMMSDef	SIL2	
SiteOverviewMMSRead	SIL2	
SiteOverviewOr4	SIL2	
SupervisionOverview	SIL2	

Appendix B Certified Hardware Components

For information on version numbers of the certified modules, please refer to the valid version of Annex 2 to the TÜV certification report, see Information Requirements on page 50.

Safety Certified Hardware Components

The following system components are certified. This allows the components to be used to process safety critical signals and functions:

Table 41. Safety-related hardware components

Module	Description
AI880A	Safety Analog Input Module with Hart support
DI880	Safety Digital Input Module
DO880	Safety Digital Output Module
PM865	Processor Module
SM810	Safety Module
SM811	Safety Module (required for SIL3 systems)
SS823	Power Voting Unit with over voltage protection

Safety Relevant Hardware Components

The following system components are certified ‘safety-relevant’, i.e. they are supporting hardware to be attached to the safety system

In addition to the components listed here are their corresponding MTUs, ModuleBus and CEX-Bus inlets, outlets and termination units, cables etc. listed in relevant user manuals, possible to connect to and use in the safety system:

Table 42. Safety-relevant hardware components

Module	Description
TB825	Optical Media Converter for long distance ModuleBus
TB826	Optical Media Converter for long distance ModuleBus
TB840/TB840A	Cluster Modem for redundant electrical ModuleBus
BC810	CEX-Bus interconnection unit
TP830	Base-Plate, PM865
TP855	Base-plate, SM810
TP857	Base-plate, BC810
TP868	Base-plate, SM811
TU807	Single MTU for TB840/TB840A (single el. ModuleBus)
TU810	Single MTU for DI880 / DO880, single ModuleBus
TU812	Single MTU for DI880 / DO880, single ModuleBus
TU814	Single MTU for DI880 / DO880, single ModuleBus
TU830	Single MTU for DI880 / DO880, single ModuleBus
TU834	Single MTU for AI880A, single ModuleBus
TU838	Single MTU for DI880, single ModuleBus extension
TU840	Redundant MTU for TB840/TB840A (redundant electrical ModuleBus)

Table 42. Safety-relevant hardware components (Continued)

Module	Description
TU841	Redundant MTU for TB840/TB840A (single electrical ModuleBus)
TU842	Redundant MTU for DI880 / DO880
TU843	Redundant MTU for DI880 / DO880
TU844	Redundant MTU for AI880A
TU845	Redundant MTU for AI880A
TU848	Redundant MTU for TB840/TB840A (redundant electrical ModuleBus, redundant power connections)
TU849	Redundant MTU for TB840/TB840A (single electrical ModuleBus, redundant power connections)

Interference free Hardware Components

The following hardware components are interference free. They are possible to connect to or use in the safety system but they are not suitable to process safety critical functions or signals.

In addition to the components listed here are their corresponding MTUs, ModuleBus and CEX-Bus inlets, outlets and termination units, cables etc. listed in relevant user manuals, possible to connect to and use in the safety system.

Table 43. Interference free hardware components

Module[1]	Description
AI80x	Compact Analog Input Modules
AI81x / AI82x / AI83x / AI84x / AI890/AI893/AI895	Standard Analog Input Modules
AO80x	Compact Analog Output Modules
AO81x / AO82x / AO84x / AO890 / AO895	Standard Analog Output Modules
CI853	Serial communication – RS 232
CI854A	Communication Interface for ProfiBus-DP/V1
CI855	Communication Interface for Master Bus 300
CI856	Communication Interface for S100 I/O
CI857	Communication Interface for Insum
CI867	Communication Interface for Modbus TCP
CI868	IEC 61850 Communication Interface
CI872	Communication Interface for MOD5
DI80x	Compact Digital Input Modules
DI81x / DI83x / DI84x / DI890	Standard Digital Input Modules

Table 43. Interference free hardware components (Continued)

Module(1)	Description
DO80x	Compact Digital Output Modules
DO81x /DO84x / DO890	Standard Digital Output Modules
DP82x / DP84x	Standard Digital Pulse Counter Modules
SB821	Battery back-up unit
SB822	Battery back-up unit, rechargeable
SD821	Power supply 120/230V AC mains supply (24V DC/2.5A)
SD822	Power supply 120/230V AC mains supply (24V DC/5A)
SD823	Power supply 120/230V AC mains supply (24V DC/10A)
SD831	Power supply 120/230V AC mains supply (24V DC/2.5A)
SD832	Power supply 120/230V AC mains supply (24V DC/5A)
SD833	Power supply 120/230V AC mains supply (24V DC/10A)
SD834	Power supply 120/230V AC mains supply (24V DC/20A)
TC562	Short-distance modem (RS-232)
TP853	Base-plate for CI853 / CI855 / CI857
TP854	Base-plate for CI854A
TP856	Base-plate for CI856
TP867	Base-plate for CI867 and CI868

(1) This table applies only for I/O modules that are specified for field voltages lower than or equal to 24 V d.c. I/O modules specified for higher voltages are described in Table 44.

The following hardware components are interference free. However, they shall not be used on ModuleBus cluster 0, (the built-in electrical ModuleBus) and they shall not be used in any ModuleBus cluster in combination with the safety-related DO880 modules:

Table 44. Interference free hardware components

Module	Description
DI802 / DI803	Compact Digital Input Modules
DI811 / DI820 / DI821 / DI831 / DI885	Standard Digital Input Modules
DO802	Compact Digital Output Modules
DO820 / DO821	Standard Digital Output Modules

INDEX

Numerics

800xA Operator Workplace 73 to 74, 112, 127 to 128

A

Access Control 111
Access Enable 72, 126
Access Management 110
AI880A 68, 99, 101, 106
Any Force Active 72 to 73
Application 78, 82, 90
application software 76
Aspect directory 74

B

BC810 66
BPCS 79, 131
Bulk data manager 74

C

CASE 88
Caution 30
CEX 64, 66
cold restart 83
cold retain 83, 121
Commissioning 124
communication 71, 79, 82
compiler 88
Compiler Test Application 79
Configuration Management 56, 113
Confirm Operation 112, 126
Confirmed Write 74, 87, 111 to 112
Confirmed Write Support 112
Continuous Mode 59
Control Builder M Professional 74, 88
Control Module Types 86
Control Modules 80
Controller Restart 123
CTA 79

D

Demand Mode 59
DI880 69, 103, 106
diagnostic 113, 128
difference report 114, 121, 123, 135
Digital Inputs 72
Digital Outputs 72
DO880 69, 104, 106
documentation 41
download 120
DRT 43, 106

E

EN 90
Enable Input 90
enclosure 75
environment 50, 75, 118
Error Handler 93, 98, 113
ESD 92
EXIT 88

F

F&G 92
FDRT 43, 81, 91, 106
Filter time 100, 102
Firmware 91, 131

FirstScanAfterPowerUp 84
FOR 88
Force Control 82, 110
ForcedSignals 73
FPL 85
Function Block Types 86
FVL 85

H

HART 68, 99, 128
hazard 57
Hot Insert 129

I

I/O Signal Failure 84
Impact Analysis 117, 131
Implicit Cast 89
Information 30
installation 118
Instruction List 89
Interval Time 81
ISP 100, 102 to 103

L

Ladder Diagram 89
Languages 85
Latency 98
Libraries 85, 87
logic 82
Loops In ST 88
LVL 85

M

MMS 71
MMSDefxxx 80, 134
MMSReadxxx 80, 134
modifications 131
ModuleBus 65, 99, 103 to 104, 107

N

NAMUR 101
ND 105
NE 105
Nested If or Case 88
Normally de-energized 105
Normally energized 105
number of forces 82, 110

O

OLU 81
Online Upgrade 133
Overrun 90

P

peer-to-peer 71, 82
PELV 35, 71 to 72
PM865 64, 130
positive logic 82
power failure 83
proof test 130
PST 43

Q

Quality Management System 51

R

RCU 64
redundancy 48, 64, 128
REPEAT 88
Reset all Forces 72, 126
restart 84, 120, 123
restrictions 50, 88, 90
Retain Variables 83, 121
RETCN 90
RETURN 90
Reuse assistant 74
risk 57
Risk Reduction Factor 58

S

S800 I/O system 67
Safety Accuracy 99
Safety Functions 58
safety lifecycle 28, 57
Safety Management System 51
Safety Requirement Specification 59, 77
Safety Validation 77, 125
SELV 35 to 36, 71 to 72
Sequence Of Event 69
SFC 88
shunt stick 68 to 69
SIL 79, 87, 129, 134, 136
SIL Access Control 74, 111
Simulation 115
Simultaneous Execution in SFC 88
SIS 57, 131
Site Planning 74
SM810 46, 49, 64, 96, 111, 120, 130
SM811 37, 46, 49, 64, 72, 96, 108, 111, 120, 130
SoftController 115
source code report 114, 116, 121
SS823 71
System Alarm 72 to 73, 94
System Functions 86

T

T 28
task 98
Test Mode 115
Time Critical 98
Tip 30
training 130

U

UniqueID 80
user defined diagnostic 113
user defined libraries 87
user manuals 41

V

Virtual Machine Test 79
VMT 79
VMTLib 79

W

warm restart 84
Warning 30
WHILE 88

Contact us

ABB AB
Control Technologies
Västerås, Sweden
Phone: +46 (0) 21 32 50 00
e-mail: processautomation@se.abb.com
www.abb.com/controlsystems

ABB Automation GmbH
Control Technologies
Mannheim, Germany
Phone: +49 1805 26 67 76
e-mail: marketing.control-proucts@de.abb.com
www.abb.de/controlsystems

ABB S.P.A.
Control Technologies
Sesto San Giovanni (MI), Italy
Phone: +39 02 24147 555
e-mail: controlsystems@it.abb.com
www.abb.it/controlsystems

ABB Inc.
Control Technologies
Wickliffe, Ohio, USA
Phone: +1 440 585 8500
e-mail: industrialitsolutions@us.abb.com
www.abb.com/controlsystems

ABB Pte Ltd
Control Technologies
Singapore
Phone: +65 6776 5711
e-mail: processautomation@sg.abb.com
www.abb.com/controlsystems

ABB Automation LLC
Control Technologies
Abu Dhabi, United Arab Emirates
Phone: +971 (0) 2 4938 000
e-mail: processautomation@ae.abb.com
www.abb.com/controlsystems

ABB China Ltd
Control Technologies
Beijing, China
Phone: +86 (0) 10 84566688-2193
www.abb.com/controlsystems

Copyright © 2012 by ABB.
All rights reserved.

3BNP004865-513 RevA

Power and productivity
for a better world™