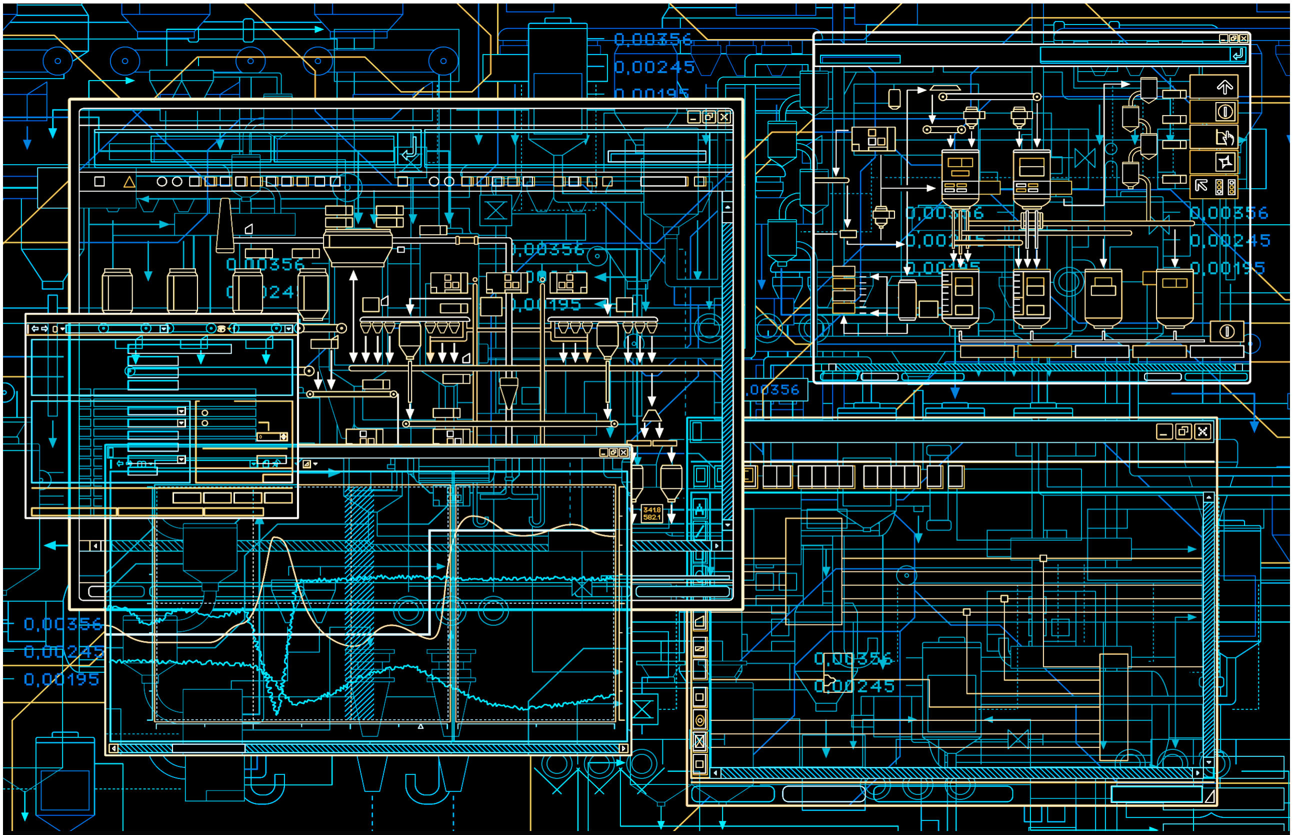

System 800xA

Operations
Safety Operator Warnings

System Version 6.0

Power and productivity
for a better world™

System 800xA

Operations
Safety Operator Warnings

System Version 6.0

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

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

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

Products described or referenced in this document are designed to be connected, and to communicate information and data via a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect the system, its products and networks, against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB verifies the function of released products and updates. However system/product owners are ultimately responsible to ensure that any system update (including but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) is compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment they are deployed.

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

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

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

This manual applies only in conjunction with the System 800xA Safety AC 800M High Integrity Safety Manual (3BNP004865-601) and AC 800M Burner Library Safety and User Manual (3BSE079156-600).

TRADEMARKS

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

Release: September 2016
Document number: 2PAA110888-601

Table of Contents

About This User Manual

General 7
User Manual Conventions 7
Related Documentation 8

Section 1 - Safety Operator Warnings

System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP004865-601 9
System 800xA Network Configuration, 3BSE034463* 23
System 800xA Administration and Security, 3BSE037410* 23
System 800xA Technical Data and Configuration, 3BSE041434* 23
System 800xA Operator Manual, 2PAA111131* 23
System 800xA Multisystem Integration, 3BSE037076* 24
AC 800M Controller Hardware, 3BSE036351* 24
S800 I/O Getting Started, 3BSE020923* 26
S800 I/O Modules and Termination Units, 3BSE020924* 28
System 800xA Safety 6.0 AC 800M High Integrity Reliability and Availability, 3BSE034876 28
System 800xA Control 6.0 AC 800M Configuration, 3BSE035980* 29
System 800xA Control 6.0 AC 800M Planning, 3BSE043732* 30
System 800xA Control 6.0 AC 800M Binary and Analog Handling, 3BSE035981* 30
AC 800M 6.0 Communication Protocols, 3BSE035982* 30
System 800xA Release Notes New Functions and Known Problems, 2PAA111899-60031
System 800xA Release Notes Fixed Problems, 2PAA112277-600 31
System 800xA Release Notes New Functions and Known Problems, 2PAA111899-60132
System 800xA Release Notes Fixed Problems, 2PAA112277-601 32
System 800xA Release Notes New Functions and Known Problems, 2PAA111899-60233
System 800xA Release Notes Fixed Problems, 2PAA112277-602 33

Section 2 - Safety Operator Warnings - BurnerLib

AC 800M Burner Library Safety and User Manual, 3BSE079156-600 35
System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP004865* 41
System 800xA Control 6.0 AC 800M Getting Started, 3BSE041880* 41
System 800xA Operations 6.0, 3BSE036904* 41

Revision History

Introduction 43
Revision History 43

About This User Manual

General

Any security measures described in this User Manual, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

This user manual lists the safety operator warnings and electrical warnings as described in the *System 800xA Safety AC 800M High Integrity Safety Manual (3BNP004865-601), AC 800M Burner Library Safety and User Manual (3BSE079156-600)*and the various user manuals referenced in the Safety Manual.

To fulfill the Safety of Machinery Directive 2006/42/EC, ensure that this manual and *System 800xA Operator Manual (2PAA111131*)* are translated into your local official community language.

User Manual 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.

Warning Icon

This user manual includes Warning, 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 warning symbol 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 result in *personal injury.*

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.

Related Documentation

A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in System 800xA Released User Manuals and Release Notes (3BUA000263*).

System 800xA Released User Manuals and Release Notes (3BUA000263*) is updated each time a document is updated or a new document is released. It is in PDF format and is provided in the following ways:

- Included on the documentation media provided with the system and published to myABB/My Control System when released as part of a major or minor release, Service pack, Feature Pack, or System Revision.
- Published to myABB/My Control System when a User Manual or Release Note is updated in between any of the release cycles listed in the first bullet.

A product bulletin is published each time *System 800xA Released User Manuals and Release Notes (3BUA000263*)* is updated and published to myABB/My Control System.

Section 1 Safety Operator Warnings

This section provides a list of all the safety operator warnings in System 800xA.

The references in this manual pertaining to page numbers, section names, section numbers, tables, and figures correspond to the references in the original user manuals.

System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP004865-601

This section lists the warnings mentioned in the *System 800xA Safety AC 800M High Integrity Safety Manual (3BNP004865-601).*

Warnings

Electrostatic Sensitive Device

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

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* and S800 I/O Getting Started, 3BSE020923*.

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.

Intended User

The End-User shall comply with all restrictions and conditions for the safety system that are provided by the Safety Manuals or by other mandatory documents referred to by the Safety Manual. This includes all aspects of installation, configuration, operation and maintenance.

Equipment Requirements

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. Mitigation of the failure requires additional safety measures.

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.

The user shall verify that installed versions of hardware, software modules and documentation System 800xA Safety AC 800M High Integrity Manual (3BNP004865*) and System 800xA Safety AC 800M High Integrity, Reliability and Availability (3BSE034876*) are in compliance with the valid version of System 800xA Safety AV84798C-A_A Annex A, TÜV Certificate report, (3BSE074100) of the Report on the certificate Z10 13 07 29902 006. Annex A is also referred to from the Machine Safety certificate M6A 13 07 29902 008.[1] These certificates are issued by TÜV Product Service GmbH.

[1] Available through ABB web services.

Organization and Resources

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.

Safety Lifecycle Activities

Requirements in the application specific standards listed in the chapter Applicable Specifications and other relevant and valid application standards shall be adhered to (e.g. EN 54, EN 298, EN 1037 and EN ISO 13850).

Allocation of I/O Modules

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.

AI880A High Integrity Analog Input Module

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.

AI880A as DI - Loop Supervised Digital Input Module

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*.

DI880 High Integrity Digital Input Module

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.

DO880 High Integrity Digital Output Module

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 EN ISO 13849 applications.

Normally Energized DO880 channels used in EN ISO 13849 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 15. Safety Related Settings of DO880, care must be taken to handle the fact that at application delete, or removal of the I/O connection, 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.

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).

Power Supply

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.

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. The fuse is only needed when using the TY801. If TY805 is used the fuse can be omitted.

Operator Interface

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

Software Architecture

Change of task connection of a SIL3 application shall always be followed by a cold restart of the controller.

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

Communication Between Applications using IAC

All SIL Communication Variables must have an ISP value connected. Keep Current Value is not allowed.

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 IAC CV. If this restriction is violated in a SIL3 application, it might result in a Safety Shutdown of the related AC 800M HI controller(s).

SIL IAC between SoftControllers are not affected by the configured ExpectedSIL. Care should be taken when changing from simulated to nonsimulated safety controllers.

When establishing a safety critical communication link using IAC, the UniqueID parameter represents the safety identification of the data and it is the user's responsibility to ensure that it is unique within the available System networks.[1]

[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

Note! Remember to change the UniqueIDs if PPA systems are cloned (e.g. in case of multiple PPA systems on the same network).

For IAC communication between different PPA Systems, the IP addresses must be explicitly defined.

It is the end users responsibility to make sure that before doing the Manual Acknowledge on the related IAC Acknowledge Group the process can be started safely. Auto Acknowledge is not allowed for Machine Safety applications. If Auto Acknowledge is used it is the end-users responsibility to make sure the process can start safely.

For Machine Safety applications, acknowledgment of IAC communication shall require the 'Access Enable' to be enabled. This means that the CVAckISP control module must be configured with AccessLevel set to ConfirmWriteAndAccessEnable. It is also not allowed to use the bool inputs ResetGroup or ResetAllGroups, nor cascaded groups of CVAckISP modules, for Machine Safety.

One IAC Acknowledge Group can have a maximum of 32 Communication Variables connected. If structured variables are used the maximum number of structured components connected is 32.

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

Communication between different SIL using IAC

It is the end-users responsibility to ensure that the Lower SIL signals are well reviewed and tested, to verify that they do not interfere with the safety function.

Communication Between Controllers using MMSCommLib

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 cannot be used for safety critical functions.

For exchanging safety critical data between Applications using MMS, 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. Conditional execution may extend the TimeOut and FDRT.

When establishing a safety critical communication link using MMS, the UniqueID parameter represents the safety identification of the data and it is the users responsibility to ensure that it is unique within the available System networks [1]. The UniqueID shall be identical in the MMSDefxxx and MMSReadxxx.

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 SafetyShutdown of the related AC 800M HI controller(s).

When safety critical signals are communicated between Applications (in the same or different controllers), the $\mathrm{FDRT}_{\mathrm{MMS}}$ of the communication subsystem shall be calculated 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.

The Control Module MMSReadHI provides acknowledge functionality which is default disabled. If the acknowledge functionality is enabled it is the end users responsibility to be aware of that the Valid parameter will be set to True when the communication is restored. Acknowledge functionality shall be disabled for Machine Safety applications.

[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.

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.

Positive or Negative Logic

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

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.

Power Failure

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.

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.

Usage of Compact Flash Card

If the Compact Flash Card is not empty and properly formatted, it must be removed from the High Integrity controller before the reset button is pressed to perform a cold restart.

Exceptional values in arithmetic operators and functions

When working with arithmetic operators and Mathematical System functions, the user must take care to avoid illegal parameters, out-of-range, and overflow situations. This can be facilitated by using the RealInfo function for variables of data type Real.

The RealInfo should be used when there is a risk of overflow when making calculation with the data type Real. The function RealInfo should be used just after a calculation to check if the result is OK. If the result is not OK the user has to handle this in an appropriate way.

Programming Languages and Libraries

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

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.

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.

The Split and Join elements shall not be used in SIL Diagrams, since reverse components are not transferred. If needed, single (forward) components can be retrieved using dot notation, i.e. the (structured) signal can be branched, and a component from one of the branches can be connected to application logic.

User Defined Libraries

It’s the user’s responsibility that the SIL marked library elements fulfills the relevant safety standards and complies with the guidelines for application programming given in this manual. This also applies when copying SIL marked library types independent of whether they are modified or not.

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

Alarm and Event functionality is SIL2 Restricted/SIL3 Restricted and user-defined types shall not use any information from Alarm and Event objects to interfere with the safety function. This applies, for example to control a safety function in an 1131 SIL application based on the state of an Alarm and Event object.

Control Builder M Professional - Settings and Restrictions

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

The user shall always connect the EN input to true when used on SFC and ST Code Blocks in FD.

Controller Settings and Restrictions

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.

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 12. Safety Related Settings of AI880A.

It is the user's responsibility to handle warnings (related to under range, 0-4mA, see Signal Range in Table 12. Safety Related Settings of AI880A) and errors from IO.Status as well as errors related to the soft error indication (if Device Malfunction Low (DML) < 1.6mA, see Figure 9) according to plant requirements.

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 13. Safety Related Settings of AI880A as DI - Loop Supervised.

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 14. Safety Related Settings of DI880.

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 15. Safety Related Settings of DO880.

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 16. Response times for safety components.

When the $\text{FDRT}_{\text{Controller}}$ is required to be less than the configured FDRT(Diag.Cycle.), the user must connect the channel error from the I/O within the application code such that it affects a SIL3 output signal, i.e. in such a way that the affected loop is brought to a safe state.

During Warm Download and Hot Insert of SM811/SM812 the calculated shorter $\text{FDRT}_{\text{Controller SIL3}}$ is superseded by the configured FDRT (Diag.Cycle.). It is the responsibility of the end user, via organizational measures, ensuring that this can be done in a safe way.

Formulas for FDRT are only valid if Modulebus scan time is less than half the Application Interval Time such that all I/Os are scanned before the application is executed.

The ModuleBus timeout shall be less than half the configured FDRT(Diag.Cycle.) timeout to fulfill the FDRT calculations.

The Application Interval Time shall be less than half the configured FDRT(Diag.Cycle.) to fulfill the FDRT calculations.

When using an FDRT shorter than 1500ms the Modulebus Timeout must be shorter than or equal to 128ms.

Force Control

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

SIL Access Control

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

Multisystem Integration - Confirmed Write Support

The Provider Name shall be a unique identifier that the user has to enter manually, both on the Subscriber System and on the Provider System. For user friendliness, the Provider Name shall be an easily distinguishable string with a length of 2 - 16 characters, assuming 16 bit characters. It is the operators’ responsibility to initially select and to subsequently verify the Provider Name when performing a Confirmed Write Support from the subscriber.

User Defined Diagnostics

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

Difference Report

Difference Report Viewer is not for review verification and acknowledge at download. All changes must be reviewed and acknowledged in the Control Builder M Professional Difference Report.

It is the user's responsibility to verify that there are no postponed difference report items in the HI controller before commissioning. All mandatory items must be reviewed and acknowledged before the controller is put into production.

Software Verification

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

Regression Testing

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

Mechanical Completion

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

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* and S800 I/O Getting Started, 3BSE020923* shall be followed. If all the recommendations given in these manuals are not strictly followed, the responsibility lies with the user to demonstrate an equivalent safe and reliable assembly and installation of the equipment.

Electrical Completion

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

Program Download and Startup

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

Program Download

To ensure a safe download and startup of applications to the AC 800M HI, the steps described in Table 19. Program Download Procedure shall be performed.

Program Download with LEG

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

To ensure a safe program Download with LEG to the AC 800M HI, the steps described in Table 20. Program Download with LEG Procedure shall be performed.

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

Operation Procedures

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

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.

Remote Operation Procedure

The VPN connection for Remote Operation shall be configured as described in System 800xA 6.0 Network Configuration, 3BSE034463*.

Fault Finding and Repair

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

Online Replacement of SM811/SM812 (Hot Insert)

Online replacement (Hot Insert) of the SM811/SM812 will lead to a short stop of the SIL3 applications. The stop time is limited by the configured FDRT.

Application Modifications

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).

Upgrade of stopped controllers

To ensure a safe Firmware Upgrade of a stopped AC 800M HI, the steps described in Table 21. Firmware Upgrade Procedure shall be performed.

Online Upgrade

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 SIF includes IAC or MMS, the extended communication time-out during OLU needs to be considered as well.

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 22. Online Upgrade Procedure shall be performed.

System 800xA Network Configuration, 3BSE034463*

There are no safety warnings in this manual.

System 800xA Administration and Security, 3BSE037410*

There are no safety warnings in this manual.

System 800xA Technical Data and Configuration, 3BSE041434*

There are no safety warnings in this manual.

System 800xA Operator Manual, 2PAA111131*

There are no safety warnings in this manual.

System 800xA Multisystem Integration, 3BSE037076*

This section lists the warnings mentioned in the System 800xA Multisystem Integration manual.

Warnings

Transfer of Responsibility

The responsibility is kept in the subscriber system when the connection is broken. The provider must use the grab responsibility to take the responsibility from a disconnected subscriber.

AC 800M Controller Hardware, 3BSE036351*

This section lists the warnings mentioned in the AC 800M Controller Hardware manual.

Warnings

Electrostatic Sensitive Device

ESD

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

Equipment Environment

All components, whether in transportation, operation or storage, must be in a noncorrosive environment.

Electrical Shock Hazard During Maintenance

Disconnect power or take precautions to insure that contact with energized parts is avoided when servicing.

Prefabricated aluminum profile

The AC 800M Controller and associated units must be unpowered and disconnected when being mounted onto a DIN-rail!

It is not allowed to manipulate CEX bus baseplates in a powered and running system. Before changing or removing a baseplate, all CEX modules on that segment must be removed.

AC 800M units must be disconnected from the power source before removing them from a DIN-rail!

It is not allowed to manipulate CEX bus baseplates in a powered and running system. Before changing or removing a baseplate, all CEX modules on that segment must be removed.

Installing the PM86x/TP830 Processor Unit in Single Configuration

For PM858/PM861/PM864/PM865/PM866/PM866A insert the RCU Link Termination plug TB852, at the RCU Link connector. The termination plug must always be used when running in single configuration.

When a redundant processor is running in a single configuration use the RCU Link Cable TK851, if the RCU Link Termination plug TB852 is not available.

Unit to Baseplate Alpha Code Lock

The CI862 baseplate has no locking device. Insert only the CI862 unit into this baseplate. Insertion of other unit types may cause damage to the equipment.

Maintenance

Before attempting maintenance or troubleshooting, read the Safety Summary on page 13. Failure to do so could lead to personal injury or damage to equipment.

Online Replacement of Unit

It is not allowed to manipulate CEX bus baseplates in a powered and running system. Before changing or removing a baseplate, all CEX modules on that segment must be removed.

Hazardous Location Approval

Explosion hazard - Substitution of components may impair suitability for Class I, Zone 2.

Explosion hazard - Do not replace batteries unless the power has been switched off or the area is known to be non-hazardous.

Explosion hazard - Do not disconnect equipment unless the power has been switched off or the area is known to be non-hazardous.

S800 I/O Getting Started, 3BSE020923*

This section lists the warnings mentioned in the S800 I/O Getting Started manual.

Warnings

Electrostatic Sensitive Device

ESD

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

Equipment Environment

All components, whether in transportation, operation or storage, must be in a noncorrosive environment.

Electrical Shock Hazard During Maintenance

Disconnect power or take precautions to insure that contact with energized parts is avoided when servicing.

Hazardous Location - North American Approval (cULus)

Explosion hazard! Do not disconnect equipment unless power has been removed or the area is known to be non-hazardous.

Explosion hazard! Substitution of components may impair suitability for Class 1 Zone 2 and Class 1 Division 2.

Explosion hazard! Do not replace batteries unless power has been switched off or the area is known to be non-hazardous.

Explosion hazard! Do not remove fuses unless the area is known to be non-hazardous.

Explosion hazard! Do not remove fuses unless the area is known to be non-hazardous

Safety Regulations - Personnel Safety

Work with care when supply voltage is applied to the system. Voltages within the cabinet can cause serious injury or death.

Start-up Procedures

Work with care when supply voltage is applied in the system. The voltage in the cabinet can cause serious injury or death.

Shut-down Procedures

Work with care when supply voltage is applied in the system. The voltage in the cabinet can cause serious injury or death.

List of General Fault Finding Procedures and Hints

A restart of the I/O system or controller can have very serious consequences. It is important to be aware of the local requirements for safety when starting and stopping the I/O system or controller.

User Repair

Switch off the process voltage before removal of the module, if the plastic cover for the I/O modules DI802, DI803, DI820, DI821, DO802, DO820 or DO821 is damaged, and there is risk for contact with live parts.

S800 I/O Modules and Termination Units, 3BSE020924*

This section lists the warnings mentioned in the S800 I/O Modules and Termination Units manual.

Warnings

Electrostatic Sensitive Device

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

Equipment Environment

All components, whether in transportation, operation or storage, must be in a noncorrosive environment.

Electrical Shock Hazard During Maintenance

Disconnect power or take precautions to insure that contact with energized parts is avoided when servicing.

System 800xA Safety 6.0 AC 800M High Integrity Reliability and Availability, 3BSE034876

There are no safety warnings in this manual.

System 800xA Control 6.0 AC 800M Configuration, 3BSE035980*

This section lists the warnings mentioned in the System 800xA Control 6.0 AC 800M Configuration manual.

Warnings

Entities and Reservation (Multi-User Engineering)

Reservations do not protect any runtime data or prevent download of modified applications to a controller. For example, if a controller is reserved by user A, and an application is reserved by user B, it is still possible for user C to download the application. However, reservations are indicated in the Download dialog. A single user who has logged on to more than one client, and several users who use the same user account, can unintentionally overwrite configuration data.

Task Connections

Do not re-connect tasks to applications unless it is necessary, as this might disrupt the task execution during reconfiguration. Else change the parameters of the connected task (to fit the needs). A SIL3 task reconnection might lead to a shutdown of the controller.

Non-Cyclic Execution in Debug Mode

Functions based on the real-time clock (PID controllers, timers, etc.) cannot be properly debugged in Debug mode. Timer functions will take into account the actual time elapsed since started, regardless if, for example, the task is halted in Debug mode.

Tasks

If debug mode is used in a running plant, task execution will be stopped.

Upgrading Controller Firmware using Backup Media

The firmware upgrade function in PM85x-PM86x controllers uses a low level function to locate a special “boot” file on the CompactFlash card which does not depend on the normal file system. Hence it may find this file even if it has been deleted unless a thorough reformatting has been done. See chapter Remove Files Completely from a CompactFlash Card.

System 800xA Control 6.0 AC 800M Planning, 3BSE043732*

There are no safety warnings in this manual.

System 800xA Control 6.0 AC 800M Binary and Analog Handling, 3BSE035981*

There are no safety warnings in this manual.

AC 800M 6.0 Communication Protocols, 3BSE035982*

This section lists the warnings mentioned in the AC 800M 6.0 Communication Protocols manual.

Warnings

Explicit and Implicit Addressing

In order to obtain supervision of the Network connection, and the PPP connection done with explicit addressing, RNRP must be configured (enabled at all time).

System 800xA Release Notes New Functions and Known Problems, 2PAA111899-600

This section list the safety warnings mentioned in this manual

Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

Safety

In order to get the formal status of the safety certification of a 800xA Safety product (safety documentation, hardware and software components), refer to the latest version of the TÜV Certification Report, Annex A, ABB SolutionsBank or ABB Library (3BSE074100).

System 800xA Release Notes Fixed Problems, 2PAA112277-600

This section list the safety warnings mentioned in this manual

Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

System 800xA Release Notes New Functions and Known Problems, 2PAA111899-601

This section list the safety warnings mentioned in this manual

Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

Safety

In order to get the formal status of the safety certification of a 800xA Safety product (safety documentation, hardware and software components), refer to the latest version of the TÜV Certification Report, Annex A, ABB SolutionsBank or ABB Library (3BSE074100).

System 800xA Release Notes Fixed Problems, 2PAA112277-601

This section list the safety warnings mentioned in this manual

Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

System 800xA Release Notes New Functions and Known Problems, 2PAA111899-602

This section list the safety warnings mentioned in this manual

⚠ Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

Safety

In order to get the formal status of the safety certification of a 800xA Safety product (safety documentation, hardware and software components), refer to the latest version of the TÜV Certification Report, Annex A, ABB SolutionsBank or ABB Library (3BSE074100).

System 800xA Release Notes Fixed Problems, 2PAA112277-602

This section list the safety warnings mentioned in this manual

⚠ Warnings

Release Notes Safety Notices

Failure to follow all Warnings and Instructions may lead to loss of process, fire, or death.

Section 2 Safety Operator Warnings - BurnerLib

This section provides a list of all the safety operator warnings in BurnerLib.

The references in this manual pertaining to page numbers, section names, section numbers, tables, and figures correspond to the references in the original user manuals.

AC 800M Burner Library Safety and User Manual, 3BSE079156-600

This section lists the warnings mentioned in the *AC 800M Burner Library Safety and User Manual (3BSE079156-600)*.

Warnings

Electrostatic Sensitive Device

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

Equipment Environment

All components, whether in transportation, operation or storage, must be in a noncorrosive environment.

Electrical Shock Hazard During Maintenance

Disconnect power or take precautions to insure that contact with energized parts is avoided when servicing.

About This User Manual

The End-User shall comply with all restrictions and conditions for the safety system that is provided by the Safety Manuals or by other mandatory documents referred to by the Safety Manual. This includes all aspects of installation, configuration, operation and maintenance.

System and Software Requirements

The development process for the Burner application/management application shall comply with the requirements of the related standards and regulations, e.g. with IEC 61508 2nd edition SIL3. The correct implementation shall be subject of a functional validation.

All persons involved in the use of the Burner Library shall have sufficient competence in their associated activity and shall have enough safety knowledge about the AC 800M HI safety system.

It is assumed that the application software is subject to safety analysis to determine the level of reliance of the Burner Lib Function Blocks. Safety measures might be required to ensure the safety integrity of the application software. For security reasons an additional thread analysis might be required.

Never use AC 800M High Integrity software- or hardware components, that are not covered by the TÜV SÜD certificate/TÜV SÜD letter of conformance or the DGC certificate covering the Burner related safety standards, within the safety system used in Burner applications. The construction of any additional functions included in the system, programming unit or flame detector device for which no provisions exist, shall be such that they do not degrade the safe and correct operation of the system, programming unit or flame detector device.

The hints and warnings for recommended use of the Safety and User Manual shall be considered for parametrization and for integration of the function blocks into the user program, as well as for installation, commissioning, operation and validation.

The Burner Library is capable for the use in SIL3 (or lower) applications. The Burner Library makes use of "SIL restricted" functionality for the alarm and event functionalites, which may not be used to be part of any safety related control loop.

Burner Recommended use

Always set the Fault Detection and Reaction diagnostics cycle to <2 seconds for burner applications. This will lead to an allowed warning (FDRT time below default value) in the Task Analysis tool. FDRT (Fault Detection and Reaction Time) is the maximum time from an internal error occur in the controller, to the defined action is taken.

The Start-up sequence may only occur if the potential source for the cause of the safety-shut-down conditions disappears. Connect the safety shut-down conditions to PriorityCmdStop.

Always make the interval between safety-shutdown and the next start attempt to >30 seconds for oil burner control systems which are not provided with a pre-purge function.

The start flame proving period shall be no less than that declared by the manufacturer. Configure the pilot flame proving period to Config.PilotFlameProvingTime. Configure the main flame proving period to Config.MainFlameProvingTime.

If the lock-out function is used it shall be checked for proper operation during each start-up sequence. The capability of the burner control system to store the non-volatile lock-out status shall be checked at least during each main power restoration. Connect the lock-out function to StartCond.

The application shall implement the Start Condition for the burner start in accordance with EN 12952-8, EN 746-2 and EN 12953-7. In case of an abnormal situation the application shall interrupt the 'Burner' function block by use of the Priority Stop command.

The application shall implement the shutdown of a burner in accordance with EN12952-9, EN 746-2 and EN 12953-7 using the Start Condition, stop and priority stop command of the 'Burner' function block.

External flame detector devices shall conform to EN 298 for permanent operation. Their flame failure response time shall not exceed 1 second.

The function block ‘Burner’ shall be configured such that reaction on loss of flame during start or during operation conforms to the applicable functional requirements of the individual application.

During online download (normal application update or Load Evaluate Go), the user shall take appropriate precautions dependent on the properties and the time demands of the process under control.

The parameter Config.FlamePresentBeforeStart needs to be set to true always, except when a specific standard can be pointed out to state the contrary.

The supervision of the success of closing the FuelValve1 (at the beginning of the Cleaning sequence) is in the users responsibility.

It is not allowed to connect the same flame guard to the parameters FlameGuardPilot and FlameGuardMain as the function block expects separate flame guards. If only one flame guard is used it is necessary to add logic to at least one of the parameters. This logic is the users responsibility.

Tightness Test Recommended use

Always set the Fault Detection and Reaction diagnostics cycle to <3 seconds for Tightness Test applications. FDRT (Fault Detection and Reaction Time) is the maximum time from an internal error occur in the controller, to the defined action is taken.

Set the parameter Config.TestTime to the leakage testing time as declared by the manufacturer.

The response time to achieve safety shutdown, whenever this is required, shall not exceed 1 second after a functional failure has been detected. Connect the functional failure conditions to PriorityCmdStop.

After a fault is detected the valve proving system shall execute safety actions according to EN1643.

It is the responsibility of the application engineer and implementation of the burner management system to set the correct pressure limits and reaction time for the Tightness Test.

Depending on the volume between the main gas valves, the gas pressure and the set points of the gas pressure monitoring device, the leakage testing time must be adjusted in a way that a leakage rate of 0,1 % of the burner heat input, at least 50 dm^3/h, will be safely detected.

A leak gas flow rate of 0,1 % of the nominal volume flow at maximum firing rate, but at least 50 dm^3/h, shall be safely detected.

The application shall implement diagnostics of the pressure switches.

It is the responsibility of the application engineer to define the amount of Gas used during the tightness test. Limits are defined for discharging into the combustion chamber according to EN1643.

Lambda Recommended use

All the input values must be of the right unit for the calculation to be correct. For example, all gas flows are in Nm3. If the measured values are of different units, the values must be corrected to the right measure units before connected to the function block.

There is one high limit and three low limits; low, lowlow and lowlowlow for the lambda value, which are all configurable. If the calculated lambda value is outside of these limits, the function block will set the LambdaError signal and generate an alarm for the condition.

To enable the supervision and the calculation it is necessary to set the parameter Enable to true. When the input Enable is set to false the supervision will be disabled and the output value set to the Config.PredeterminedValue.

RealIn2003 Recommended use

The setting of both the Config.DeviationLimit and the Config.DelayTime shall be in accordance with the requirements for the specific application.

The discrepancy timer shall be taken into account for the Fault Detection and Reaction time of the related safety loop.

ComplementIn Recommended use

The Config.DiscrepancyTime shall be taken into account for the Fault Detection and Reaction time of the related safety loop.

Safety precautions

The application shall be in accordance with the details provided by the manufacturer's instructions.

The application shall implement the Lock Out function and the process to restart the system. This includes for instance the mandatory use of manual reset devices for a restart.

The application shall implement functionality in accordance with EN 267: “In the case of permanent loss of the actuating energy the burner shall proceed to a safe condition. If an on/off control, switch or limiter operates, the fuel oil supply shall be automatically cut off immediately.”

As far as practicable the application design shall minimize the safety-related part of the software. This means that the End User shall as far as possible, split safety and non-safety functions in different applications.

If external safety devices are used, the application shall be able to process a requested shutdown independent from the actions of the Burner Library elements.

The sum of the safety times and the closing time of the shut off valve/final element shall be less than the fault tolerance time of the relevant process function. This fault tolerance time shall be defined by the End User and in compliance with the relevant application standard, the configurable safety times according to applicable standards and the application cycle times have to be adjusted accordingly.

Reset from lock-out shall be implemented in the external safety logic such that static or dynamic failures of the reset device do not cause the system to operate outside the requirements of the applicable standards or regulations (e.g. by evaluating the logical and temporal properties of the reset signal).

All safety functions of the individual application which are not covered by the function blocks (such as purging, protection of the heat generator, flue gas discharge, fuel system, etc.) shall be implemented in the external safety logic according to the requirements of the applicable standards or regulations.

It is the users responsibility to check the ParError outputs of each function block and make appropriate and necessary actions in case an error is indicated by these outputs.

The configuration parameters of all function blocks shall be confirmed (including the default values) by the users.

The error output from any function blocks shall be treated by the safety application to react on the detected error appropriately.

System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP004865*

Refer to System 800xA Safety AC 800M High Integrity Safety Manual, 3BNP004865-601 on page 9

System 800xA Control 6.0 AC 800M Getting Started, 3BSE041880*

There are no safety warnings mentioned in this manual.

System 800xA Operations 6.0, 3BSE036904*

There are no safety warnings mentioned in this manual.

Revision History

Introduction

This section provides information on the revision history of this User Manual.

The revision index of this User Manual is not related to the 800xA 6.0 System Revision.

Revision History

The following table lists the revision history of this User Manual.

Revision Index	Description	Date
-	First release, based on 3BNP004865-601 and 3BSE079156-600	September 2016

Contact us

www.abb.com/800xA
www.abb.com/controlsystems
www.abb.com/highintegritysafety

Power and productivity
for a better world™