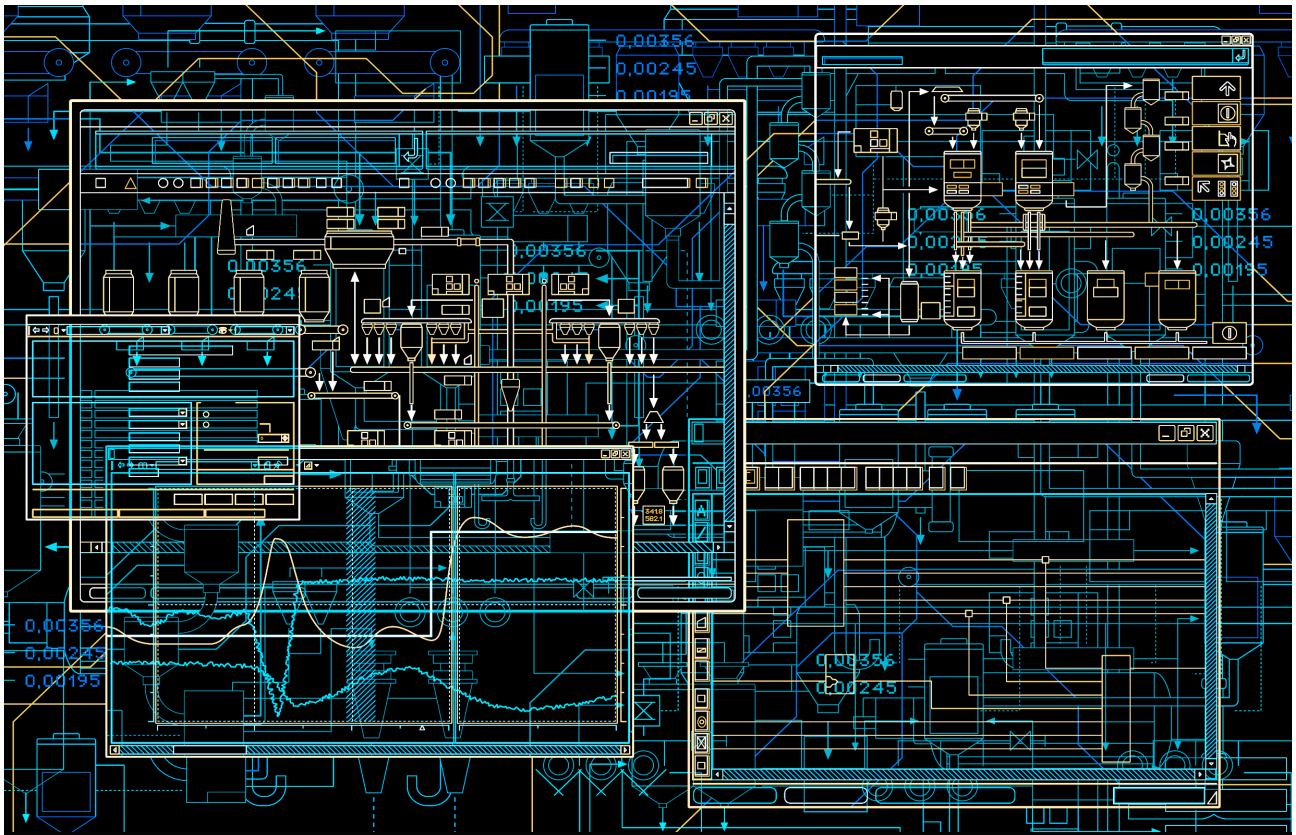

800xA for Safeguard

Operation

System Version 6.0

Power and productivity
for a better world™

800xA for Safeguard

Operation

System Version 6.0

NOTICE

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

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

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

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

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

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

TRADEMARKS

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

Release: August 2014
Document number: 3BNP004849-600

Table of Contents

Section 3 - Operator Messages

Index

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.

The 800xA for Safeguard is used for connecting operator workplaces to a MasterBus 300 control network with connected Safeguard controllers.

This user manual is intended for the operators controlling and monitoring a Safeguard system (including tuning of control parameters and calibration).

The user should have knowledge on distributed automated process control and the hardware and software functionality of Operator Workplace.

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.

Feature Pack

The Feature Pack content (including text, tables, and figures) included in this User Manual is distinguished from the existing content using the following two separators:

Feature Pack Functionality _____

<Feature Pack Content>

_____

Feature Pack functionality included in an existing table is indicated using a table footnote (*) :
*Feature Pack Functionality

Feature Pack functionality in an existing figure is indicated using callouts.

Unless noted, all other information in this User Manual applies to 800xA Systems with or without a Feature Pack installed.

Warning, Caution, Information, and Tip Icons

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

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

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

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

Information icon alerts the reader to pertinent facts and conditions.

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

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

Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018*)*. The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as Webster's Dictionary of Computer Terms. Terms that uniquely apply to this User Manual are listed in the following table.

Term/Acronym	Description
MB300	MasterBus 300 - the control network communication protocol that is used by the AC 400 controllers.
Safeguard	Safeguard 400 Series, ABB's safety controller based on the AC400 Series. Also refers to the previous model, Safeguard 3000.
SCS	Safety Control System / Safety Control Station, the dual safety system configuration of SG 3000 / Safeguard 400 Series consisting of two equally configured safety controllers.
SC	Safety Controller, refers to one of the nodes in a SCS.
SCA	The safety controller with the lowest node number in a SCS.
SCB	The safety controller with the highest node number in a SCS.

Term/Acronym	Description
ESD system	Emergency Shut-Down system.
PSD system	Process Shut-Down system.

Released User Manuals and Release Notes

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 ABB SolutionsBank when released as part of a major or minor release, Service Pack, Feature Pack, or System Revision.
- Published to ABB SolutionsBank 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 ABB SolutionsBank.

Section 1 Introduction

Product Overview

The Operator Workplace is used for process monitoring and control. It has a generic design and can be used for different process control systems.

The 800xA for Safeguard is a software product that enables you to connect an Operator Workplace to Safeguard Controllers in a MasterBus 300 network.

Product Scope

The 800xA for Safeguard is built on the 800xA for Advant Master. This is integrated in the Operator Workplace and provides the following features:

- support for single and dual Safeguard controllers.
- handling of dual controllers as one object in the operator's workplace.
- execution of operator commands in both controllers.
- status and diagnostic display for both single and dual controllers.
- faceplates, object displays and alarm/event handling consistent with AC 400 Controllers.
- signal filtering.

The supported Safeguard functions and functional units are:

- FI (Fire Input), loop monitored digital inputs.
- FD (Fire Detector), for addressable detectors.
- GI (Gas Input), loop monitored analog inputs.
- Fireguard central, control and monitoring.

- C&E shutdown level.
- Safeguard system status and control

What you can do with 800xA for Safeguard

The following are various configuratios which can be done using 800xA for Safeguard.

- Configure the connection of the workplace to Safeguard controllers on MasterBus 300 control network.
- Setup the workplace for handling the process data defined in the database of Safeguard controller. The database is uploaded from the controllers through network.
- Setup the event handling for the process events that are reported from the Safeguard controllers.
- Collect and present System status for the Safeguard controllers.
- Apply filter to suppress display of events arising from a specified controller.

Prerequisites and Requirements

The general hardware and software requirements for the 800xA system is described in Industrial^{IT} 800xA, System, System Installation (3BSE034678*).

Section 2 Operation

Operating Overview

The operation of Safeguard controllers and implementation of safety applications described in this section are:

- Start-up and dual system synchronization
- Safeguard system status monitoring
- Bypass Management and exception handling (blocking, inhibit)
- Calibration of Gas detectors
- Signal Filtering

Start-up Sequence

During start-up of Safeguard controllers, the system software initiates several safety-related functions:

1. Base system start-up test.
2. Initialization of process communication.
3. Start of AMPL-programs exempted from normal safety start up.
4. Dual start up database synchronization.
5. Start of AMPL-programs with normal safety start-up.
6. Start of AMPL-programs with delayed safety start-up.

The start-up progress can be monitored in the Safeguard system status display. For more information, refer to Safeguard Status Monitoring on page 14.

The system errors that occur during the start-up, are displayed in the status display and alarms are generated.

Safeguard Status Monitoring

Status Object

The Safeguard Status Object is an MMCX object with configured reftype = 38 in the Safeguard controllers. In the Control structure of Plant Explorer this object type is named MMCX3.

When a Safeguard system is created in the Control Structure and an upload is performed, all objects are included in **Extended Process Object** and **Local IO** (as for AC400 controller types).

The Safeguard Status Object (MMCX3) is located beneath each of the branches of a Safeguard controller (see Figure 2). This is the only object that is not uploaded beneath the virtual Safeguard controller object. Each branch of a dual system has its own status object which can be viewed and displayed individually. The operator can obtain the status of ‘Side A’ and ‘Side B’ independently.

The Safeguard Status object can also be added to the Functional Structure. This is done when a Status object presentation is used in process displays (see Figure 1) because it is easier to find it in the Object Browser of the Graphic Builder.

Figure 1. Safeguard Status Presentation (Side A and B)

A fixed display of an operator workplace can be customized to include a Safeguard Status object presentation or an object shortcut can be added to the application bar.

The other presentation elements are the Faceplate and the Object display.

The safety critical applications that are subject to certification by authorities require diagnostic capabilities and status visualization available to the operators during the system degraded mode time.

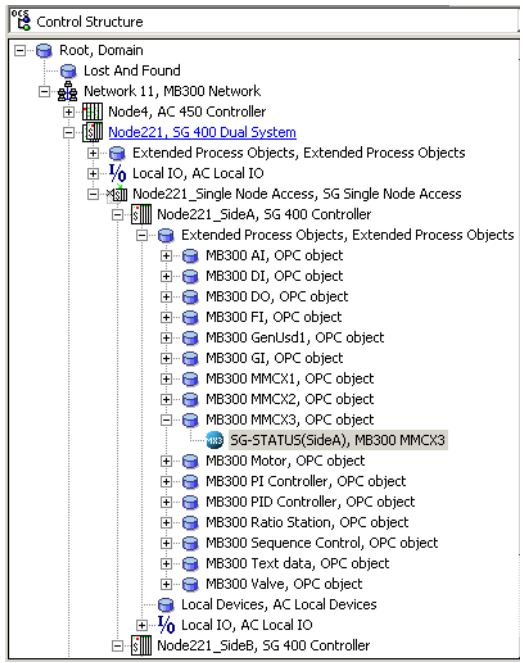

Figure 2. A Safeguard Status Object (SG-STATUS) in the Control Structure

Faceplate

The Safeguard status faceplates presents the following:

- Name and description of the individual controllers.
- Status of the controllers.
- Operator messages and warnings with scrolling facilities.
- Status of the output units.
- Group error indication.

- C&E communication status.

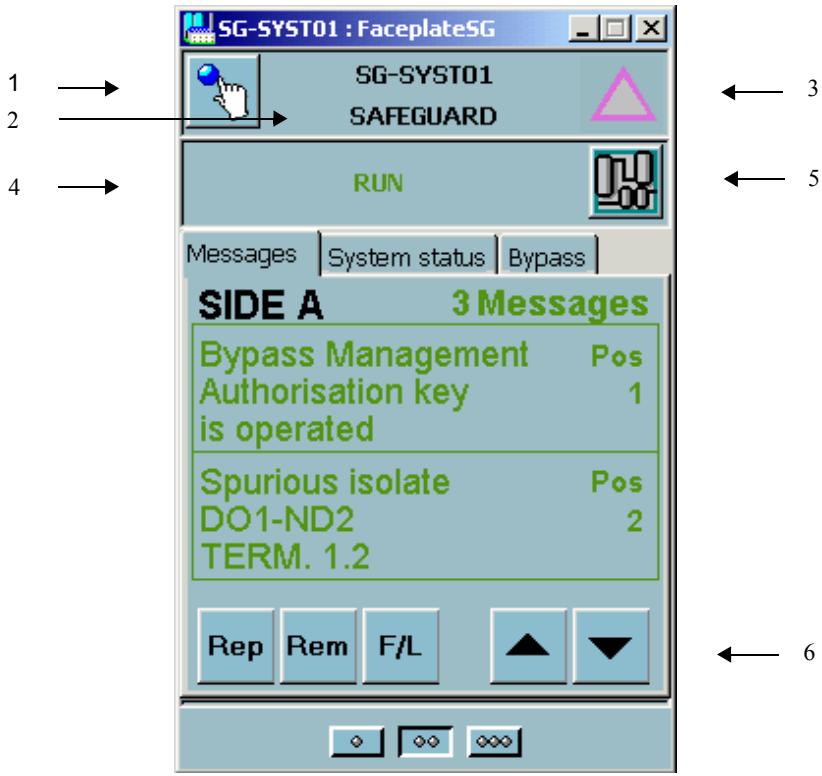

Figure 3. Safeguard Status Faceplate

Table 1 shows the item designations for the Faceplate are:

Table 1. Faceplate Items

No	Description
1	Lock button
2	Name and description
3	Warning and alarm indication

Table 1. Faceplate Items (Continued)

No	Description
4	Status indication:
4.1	Isolate commanded
4.2	Local control
4.3	Programs running
4.4	I/O Error
4.5	Print Blk
4.6	Local net request
4.7	Local net block out
4.8	Dual net request
4.9	Dual net block out
5	Aspect links:
5.1	Event list
5.2	Alarm list
5.3	Object display
5.4	Object trend display
5.5	Help
6	Buttons for scrolling the message window and for reporting and removing the detailed messages.

In a faceplate, the user can activate a lock mode for an object to prevent other operators to view and control that object. This object may appear to be locked in only one of the two sides of a dual Safeguard system. This condition terminates automatically. The user can also create an additional lock on the faceplate.

Object Display

The Object Display is similar to the faceplate and presents Safeguard system status messages in a larger, full screen frame as shown in Figure 4. This displays:

- Name and description of the individual controllers.
- Status of the controllers.
- Operator messages and warnings.
- Status of the output units.
- Group error indication.
- C&E communication status.
- Isolate control of the Master Vote 3000 outputs.
- Alarm and print blocking.
- C&E matrix communication blocking.

For maintenance purpose, a local panel is often installed in the control rooms with the following facilities:

- Activation of local control.
- Request for local Safeguard controller isolation.
- Request for On-Line Builder communication.

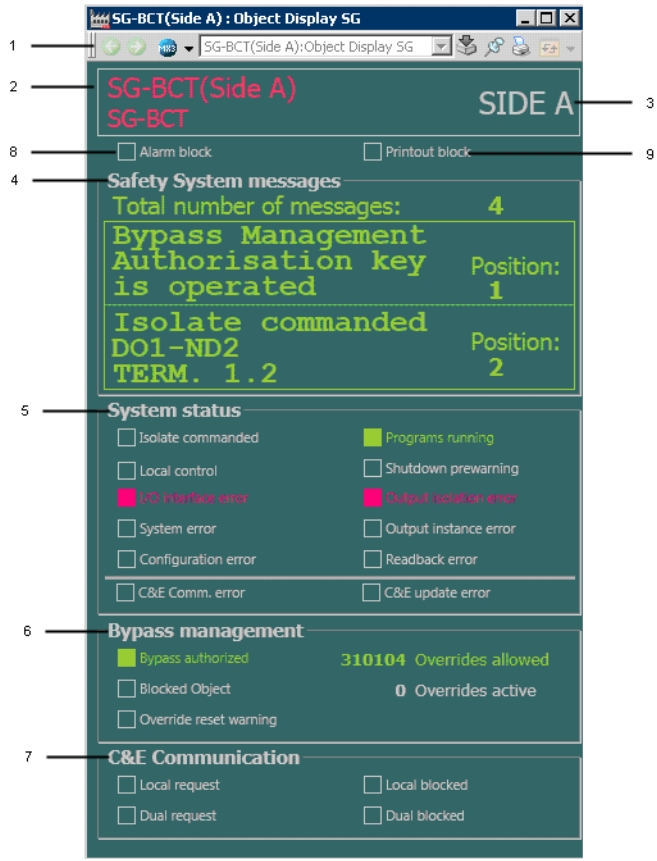

Figure 4. Safeguard Status Object Display

Table 2 shows the item designations for the Object Display are:

Table 2. Item Designation Object Display

No	Description
1	Lock frame
2	Header
3	Side A/B
4	Safety system messages
4.1	Total / Position / Position
4.2	Total No. of Messages
4.3	Acknowledge mark
4.4	Message position
4.5	Message text line 1
4.6	Message text line 2
4.7	Message text line 3
4.8	Message position
4.9	Message text line 4
4.10	Message text line 5
4.11	Message text line 6
5	System Status
5.1	Programs running
5.2	Isolate commanded
5.3	Local control
5.4	Shutdown prewarning
5.5	System error
5.6	Configuration error

Table 2. Item Designation Object Display (Continued)

No	Description
5.7	I/O Interface error
5.8	Output instance error
5.9	Output isolation error
5.10	Readback error
5.11	C&E comm. error
5.12	C&E update error
6	Bypass Management
6.1	Overrides allowed
6.2	Overrides active
6.3	Bypass authorized
6.4	Blocked object
6.5	Override reset warning
7	C&E Communication
7.1	Local request
7.2	Local blocked
7.3	Dual request
7.4	Dual blocked
8	Alarm block
9	Printout block

Local Panel

An alternate way of interacting with the Safeguard 400 Series controller is the local panel. The controller has a local panel switch (**ISOLATE**), which has three positions (**0**, **SCA**, **SCB**):

- The middle position (**0**) is normal where both SCA and SCB control the outputs unless isolated for other reasons.
- The two other position are marked **SCA** and **SCB**. Turning the switch to these positions sets the related safety controller in local mode. When the safety controller is in local mode the safety dialog is disabled except for the message buffer scrolling keys.

Status Presentation in Process Displays

To insert the Safeguard Status object in a process display:

1. Create and upload a Safeguard dual system in the Control Structure.
2. Insert the two MMCX3 objects in the Functional Structure where appropriate.
3. Create and edit a Graphic Display.
4. In the Graphic Builder, open the Object Browser.
   a. Browse to the first of two Safeguard Status objects (MMCX3) in the Functional structure and select the graphic element aspect NameSG02.
   b. Select the other Safeguard Status object and insert the same graphic element for this as well.
5. Position the two graphic elements as convenient, save and deploy the display.
6. Exit the Display Builder.

System Status

The **System Status Viewer** aspect follows the basic principles of status presentation for Safeguard Dual systems, that is, displaying combined status of SCA and SCB in the **Dual Object** structure and displaying the individual status of SCA and SCB in the **Single Node Access** structure.

However, there is a deviation from this behavior. The Process Graphics (PG) aspect **Local Devices** shows individual Program Card indications, that is, the status of SCA and SCB are displayed.

It is recommended to use the **System Status Viewer** from **Single Node Access** structure because this provides clarity on the actual status in each node.

Operating Instructions

Command Propagation

When an object is selected in a dual Safeguard system, the orders are issued to both control branches. The selection process consumes up to three seconds depending on the load situation. It is recommended to wait at least this amount of time before an order is given to ensure that both control branches receive the order.

System Synchronization

A prerequisite for the dual concept is synchronized application software in the operation mode.

The dual controllers will not be synchronized if one of the controller is disconnected from the operator workplace. In this case, the operator should to initiate a restart of the disconnected controller to synchronize the dual controllers.

Bypass Management

Bypass Management functions are controlled by configuration parameters in the system. Refer to Safeguard 400 Series Safety Manual (3BNP000432*) for more information on this feature.

If one of the controller in a dual Safeguard system is connected to the MB300 network is restarted, trend logging stops progressing for a short period of time.

Exception Handling

Inhibit of Inputs

The gas detector inputs and the fire inputs have the possibility for setting inhibit (**Set/Reset Inhibit)** on individual signals from the operator dialog. The function is used to disable actions from the signals while the alarm and event reporting is retained. Inhibit is most commonly used in fire and gas systems but is also utilized in ESD systems for special applications.

In Cause & Effect matrices implemented with Safety Builder it is also possible to specify an inhibit function for DIS[1]/DIC and AIS/AIC. The property **Tested** is used for emulating the inhibit function. Control and indication of the **Tested** property is included in the Faceplate by configuring attributes in the Function Selector aspect, see figure Figure 5. To use **Tested** for the inhibit function, select the checkbox corresponding to **Boolean** and click **Apply** to save the changes.

A special dialog with inhibit function for these signals is available for use with display elements (dcDiInhibitDialog and dcAiInhibitDialog). When these objects are selected by name the standard dialog is used.

1. DIS can not be used for safety critical signals.

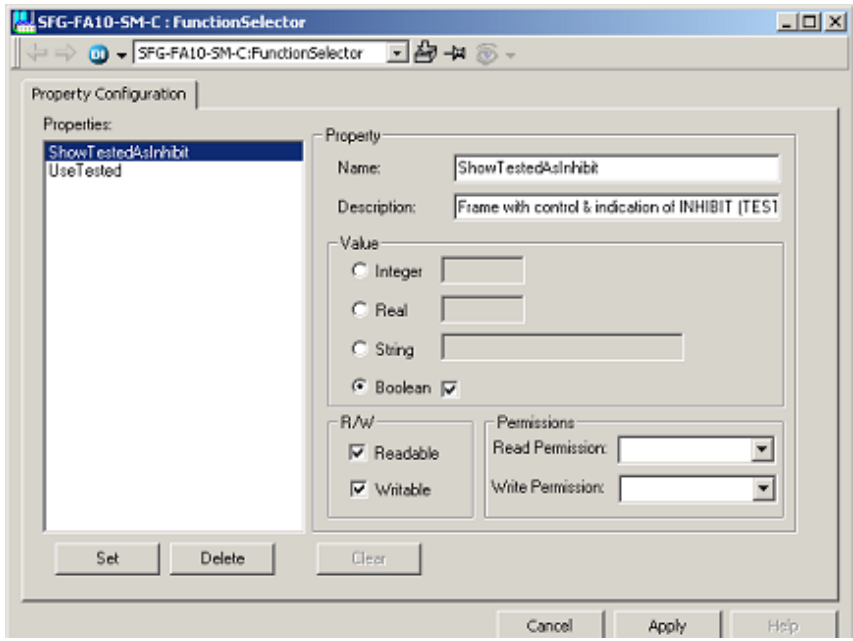

Figure 5. Function Selector Aspect

The dialog is also used with AMPL logic when inhibit function is implemented as part of the logic.

Do not use inhibited signals for prolonged periods of time as this will jeopardize the safety functions. This should preferably be controlled by the Bypass Management function.

Block Update of Inputs

Blocking of inputs and outputs should never be used for safety critical signals as this will jeopardize the safety system function. Safety outputs in blocked mode are reported in the Safeguard System status display

Outputs in Manual Mode

If the outputs are accessible for operator control under normal operation, the use of manual mode should be given special consideration.

The manual mode state of objects is included in the dual start-up synchronization to ensure that the database contents of the two nodes are equal at start-up.

To notify the operator about objects in manual mode, the Quick List aspect can be used occasionally to search for such objects and print or display them on screen.

Safety outputs should not be set in manual mode as this will jeopardize the safety system function. Safety outputs in manual mode are reported in the Safeguard System status display but are not covered by the channel test

Blocking of Outputs

The blocked state of output signals is included in the dual start-up synchronization to ensure that the database contents of the two nodes are equal at start-up.

To notify the operator about blocked outputs, the Quick List aspect could be used occasionally to search for such objects and print or display them on screen.

Blocking of outputs must never be used in safety applications as this will reduce the availability of the system. If the property OUTP_BLK=1 at dual start -up synchronization, the concerned DO-board channel is not updated with VALUE from the database. This could lead to a discrepancy between the physical outputs in the two controllers.

Latched Alarms

The gas detector inputs and the loop monitored digital inputs have a latched alarm in the data base. The latched alarm can be reset (**Reset Latch**) for individual signals from the operator dialog.

Calibration of Gas Detectors

The calibration of pellistor gas detectors connected to DSAI 165/DSTA 191 is performed from the operator workplace.

Check that the loop current (adjustable 170-350 mA) is according to the detector specifications. The procedure is as follows:

1. Select the GI object, bring up the Object Display.
2. Select the Extended Faceplate, tabulator ‘Calibration’.
3. Press the ‘Enter’ command button in the Test mode frame. The test mode (OK) shall be indicated (filled square).

   The loop and hardware are verified by a system test program and all event handling and actions are blocked.
4. Select the calibration value, and enter the value 0 (%) for zero calibration.
5. Ensure that the detector is supplied with clean air and press the ‘Cal’ command button.
   Calibration 0 shall be indicated (filled square).
6. Select the calibration value, and enter the value, e.g. 50, (%) for the test gas you are using.
7. Ensure that the detector is supplied with the test gas and press the ‘Cal’ command button.
   Calibration X shall be indicated (filled square).
8. The detector is now calibrated. Press the ‘Leave’ command button in the Test mode frame. The test mode (off) shall be indicated (unfilled square). Event handling and actions are activated now.

This has changed values in the database. Perform a backup of the controllers (DUAP or DUTDB) to save the changes after the calibration.

Section 3 Operator Messages

Fault Finding and User Repair

For details on fault finding and error messages, refer to Industrial^{IT} 800xA, System, 800xA for Advant Master, Configuration (3BSE030340*).

Operator Messages

If incorrect parameters are specified, or if other communication problems occur, an operator message is issued. The message is included in the event list. The event list must be of type ‘Operator Messages List’ set up at the time of system configuration.

The following additional operational messages specific to Safeguard 400 Series controllers apply.

Dual: Command executed in one of the dual nodes only

The command given from the operator station has only been executed by one of the controllers in the Safeguard system. Check if both controllers are available on the network or if one of them is in configuration mode.

Dual: Command not executed. Nodes currently not available

The command given from the operator station has not been executed by any of the controllers in the Safeguard system. Try to give the command once more, if no improvement, check whether the controllers are overloaded.

Dual: No response from the dual system

Check if both controllers are available on the network. They might be in configuration mode.

Dual: Object selected in one of the dual nodes only

Check if both controllers are available on the network or if one of the controllers are in configuration mode.

Dual: Object selection failed in one of the dual nodes

There is a discrepancy between the database contents of the two controllers. Check that both controllers have the same database contents, i.e. the objects exist and are implemented.

Dual: Single operation or configuration is not allowed

Single operation/configuration is not enabled. This can be done by setting the relevant SNG_DIAL property in the NODE_DESCR database element. Used for test purposes only.

Bypass Management: This OS is not accepted for system operation

The operator workplace is not granted access to the Safeguard system and the desired operation can not be performed.

The function is controlled by a Safeguard configuration parameter.

Bypass Management: Bypass Authorize Key is not activated

The access control input to a Safeguard system is not activated. This input must be activated to perform changes in the Safeguard database.

The function is controlled by a Safeguard configuration parameter.

Bypass Management: Maximum number of overrides in the system is exceeded

The Safeguard system controls the number of simultaneously occurring overrides (inhibit, block, manual mode).

The function is controlled by a Safeguard configuration parameter.

Bypass Management: Block commands are not allowed in the system

The Safeguard system controls the possibility of using the block commands in the dialogs.

This function is controlled by a Safeguard configuration parameter.

Index

Contact us

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

3BNP004849-600

Power and productivity
for a better world™