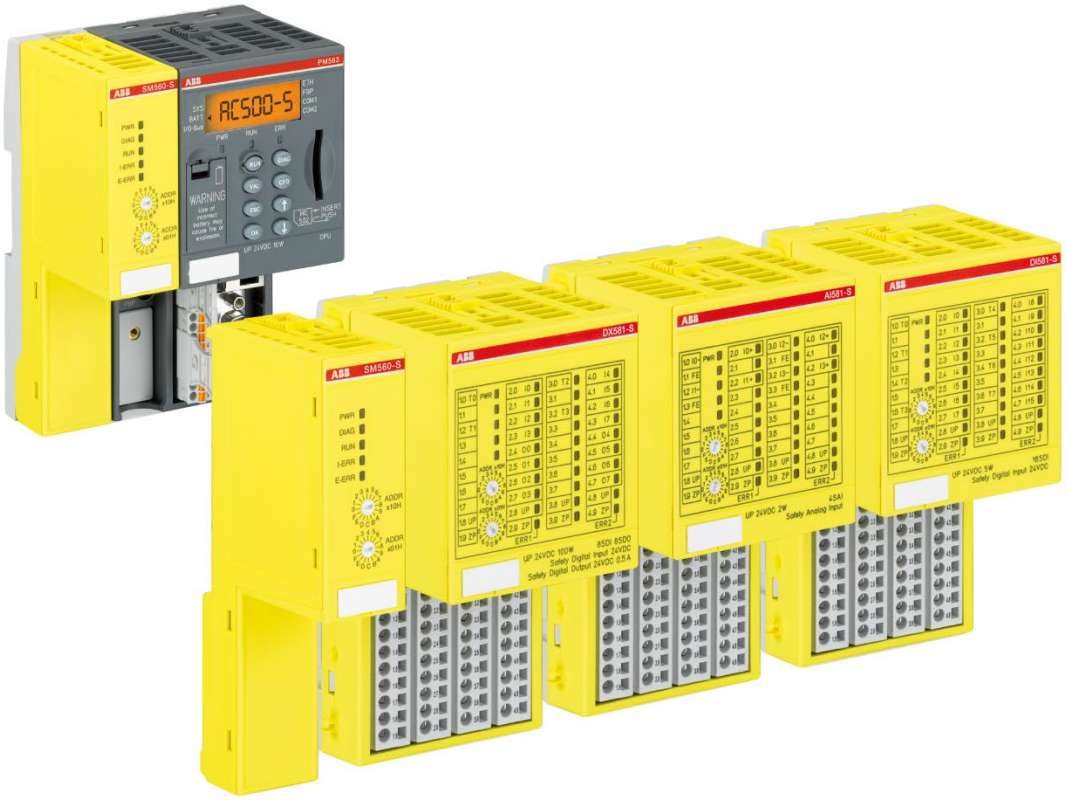
APPLICATION NOTE

AC500-S safety PLC

Triggering safety actions using standard HMI



Contents

1. Introduction **3**
1.1. Purpose 3
1.2. Document history 3
1.3. Validity 3
1.4. Important user information 4
1.5. Definitions, expressions, abbreviations 4
1.6. References / related documents 5

2. Triggering safety actions using standard HMI **6**
2.1. Overview 6
2.2. Task 9
2.3. Solution 10

3. Example **20**
3.1. General 20
3.2. Safety function 21
3.3. Functional description 21
3.4. Design features 22
3.4.1. Implementation details 22
3.4.2. Common cause failures 34
3.4.3. Systematic failures 35
3.4.4. Safety function response time 36
3.5. Calculation of the probability of failure and correspondence to PL (ISO 13849-1) 36

4. Conclusion **39**

1. Introduction

1.1. Purpose

There are industrial applications like those in harbors, logistic centers, airport and mining applications in which safety actions for selection of substations, machines or pre-defined safely limited values are required to re-configure implemented safety control functions. Such safety actions are further validated in machines on the application level by responsible qualified personal to make sure that performed safety actions to re-configure the safety function control were successfully executed.

In practice, one or more mechanical or electro-mechanical mode selector switches connected to digital safety inputs of the safety PLC are often used to perform safety actions for selection of substations, machines or pre-defined safely limited values. However, this approach with mechanical or electro-mechanical mode selector switches has significant drawbacks because of its limited user-friendliness, low flexibility if modifications are required, limited number of selection options and relatively high additional controls cost (both for mode selector switches and required digital safety input channels).

In this application note, we present a method and an example with AC500-S safety PLC on how safety actions for selection of substations, machines or pre-defined safely limited values can be performed using standard (non-safety) HMI (Human Machine Interface) with the satisfaction of PL d (ISO 13849-1) requirements. The functional safety calculation according to ISO 13849-1 is used as an example to show the compliance of the proposed approach with the relevant functional safety requirements for PL d (ISO 13849-1).

The functional safety calculation and analysis according to IEC 62061 or IEC 61511 standards can be similarly done.

1.2. Document history

Rev.	Description of version / changes	Who	Date
C	Programming environment for safety devices was restyled and renamed to "AC500-S Programming Tool".	ABB	26.04.2023
B	Company name was changed. Various typos were corrected and various improvements in the texts and illustrations were made.	ABB	15.09.2021
A (V1.0.0)	First release	ABB	15.12.2016

1.3. Validity

The data and illustrations found in this documentation are not binding. ABB reserves the right to modify its products in line with its policy of continuous product development.

ABB assumes no liability or responsibility for any consequences arising from the use of this document information. ABB is in particular in no way liable for missed profits, loss of income, loss of life, loss of use, loss of production, capital costs or costs associated with an interruption of operation, the loss of expected savings or for indirect or follow up damages or losses no matter of what kind.

1.4. Important user information

This documentation is intended for qualified personnel familiar with functional safety. You must read and understand the safety concepts and requirements presented in AC500-S Safety User Manual [1.] as well as further referenced documents prior to operating AC500-S safety PLC system.

The following special notices may appear throughout this documentation to warn of potential hazards or to call attention to specific information.

⚠ DANGER

The notices referring to your personal safety are highlighted in the manual by this safety alert symbol, which indicates that death or severe personal injury may result if proper precautions are not taken.

NOTICE

This symbol of importance identifies information that is critical for successful application and understanding of the product. It indicates that an unintended result can occur if the corresponding information is not taken into account.

1.5. Definitions, expressions, abbreviations

AC500	ABB PLC, refer also to www.abb.com/PLC for further details
AC500-S	ABB Safety PLC for applications up to SIL3 (IEC 61508:2010 and IEC 62061) and PL e (ISO 13849-1), refer also to www.abb.com/PLC for further details
AB	Automation Builder (ABB Automation Builder is the integrated software suite for machine builders and system integrators which covers the engineering of ABB AC500 PLC, AC500-S safety PLC, control panels, drives, motion and robots)
CCF	Common Cause Failure
CPU	Central Processing Unit
DC	Diagnostic Coverage
DCavg	Diagnostic Coverage – average (ISO 13849-1)
DPRAM	Dual-ported Random Access Memory
EMC	Electromagnetic compatibility
FB	Function Block
FSDT	Functional Safety Design Tool (ABB tool for functional safety calculation according to ISO 13849-1 and/or IEC 62061)
GUI	Graphical User Interface
HFT	Hardware Fault Tolerance (IEC 61508:2010)
HMI	Human Machine Interface

IEC	International Electro-technical Commission Standard
I/O	Input/Output
MTBF	Mean Time Between Failures
MTTFd	Mean Time To Failure dangerous
PC	Personal Computer
PFHavg	Probability of Failure per Hour (1/h) average (ISO 13849-1)
PL	Performance Level according to ISO 13849-1
PLC	Programmable Logic Controller
PM	Processing Module
SFRT	Safety Function Response Time
SIL	Safety Integrity Level (IEC 61508)
TÜV	Technischer Überwachungs-Verein (Technical Inspection Association)

1.6. References / related documents

[1.] AC500-S Safety User Manual, 3ADR025091M0204

[2.] Cyclic Non-safe Data Exchange between SM560-S Safety CPU and PM5xx Non-Safety CPU, 3ADR025195M0201

[3.] AC500 Documentation, refer to www.abb.com/PLC and then navigate to “Downloads” area

[4.] BGIA Report 2/2008e, Functional safety of machine controls - Application of EN ISO 13849

[5.] HVBG Hauptverband der gewerblichen Berufsgenossenschaften: Prüfgrundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten. HVBG, Sankt Augustin, 2002.

2. Triggering safety actions using standard HMI

2.1. Overview

In this document, we discuss the usage of standard HMI for safety actions to select substations, machines or pre-defined safely limited values. AC500-S safety PLC is used for safety control (refer to [1.] for more details about AC500-S safety PLC).

The following principles, which can be also found in examples with hard-wired switches to safety digital inputs of AC500-S safety PLC, are similarly used in this application note with standard HMI and AC500-S safety PLC:

1. **2-channel input functionality** (see Figure 1 with an example of 2-channel input using hard-wired approach);
2. **Mode selector switch functionality** (see Figure 2 with an example, in which 1-channel inputs instead of 2-channel inputs are used for simplicity in the hard-wired approach).

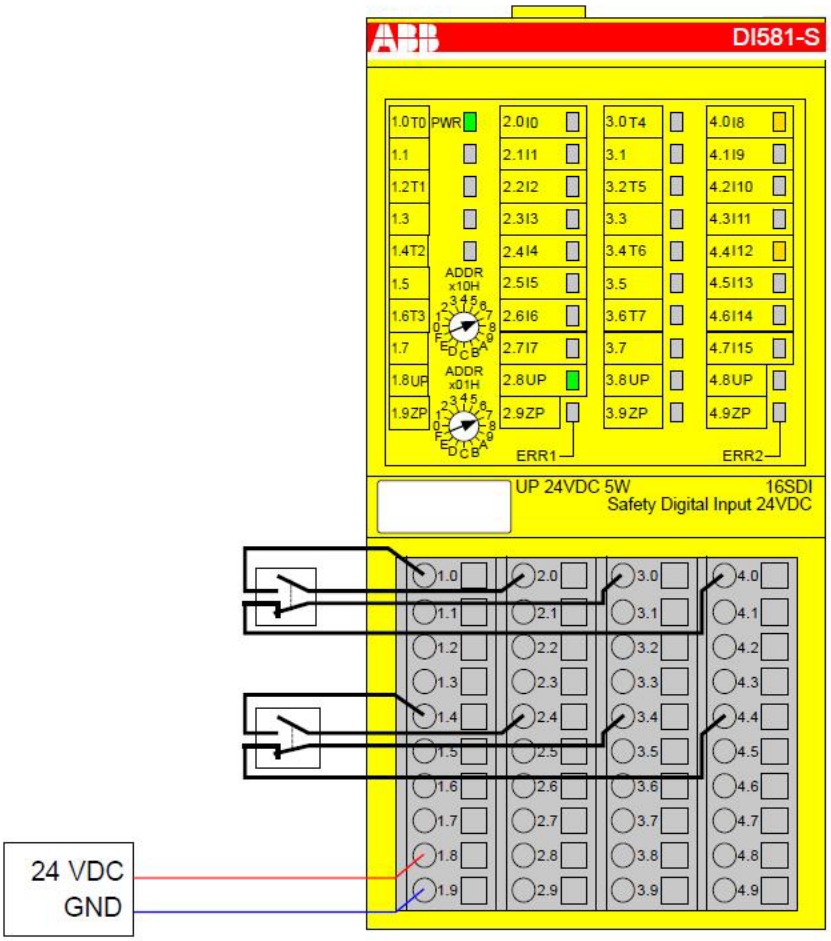


Figure 1. 2-channel inputs using AC500-S safety I/O modules

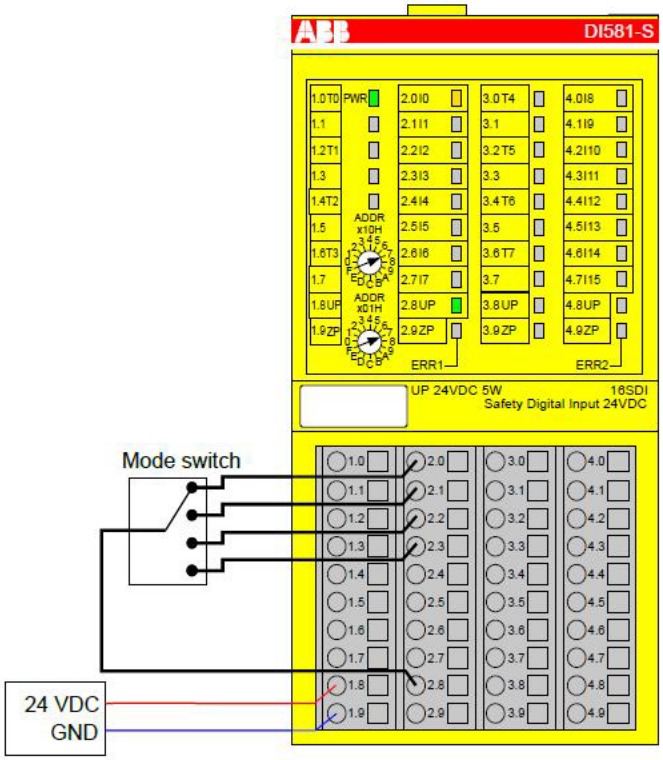


Figure 2. Mode selector switch functionality using AC500-S safety I/O modules

Figure 3 provides an overview of an exemplary minimal AC500-S configuration with a connected standard HMI through Ethernet interface. This system setup will be used to demonstrate the proposed method and perform functional safety analysis to confirm that PL d (ISO 13849-1) functional safety requirements for selection of substations, machines or pre-defined safely limited values are satisfied.

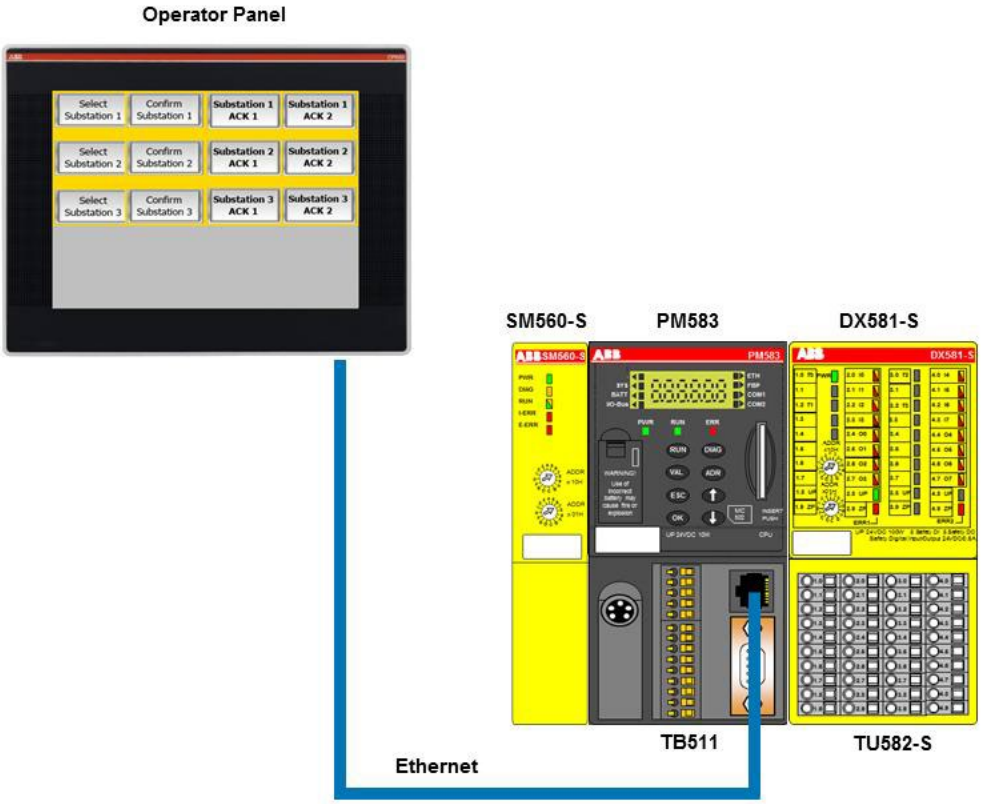


Figure 3. Exemplary setup with standard HMI and AC500/AC500-S modules

Any standard HMI, which satisfies the following prerequisites and features, can be suitable for triggering safety actions in combination with AC500-S safety PLC. The following key requirement for standard HMI (Operator panel, industrial PC, etc.) shall be fulfilled to pre-qualify for triggering safety actions:

- Support of at least 2 different Ethernet based communication protocols (see Figure 4). These protocols shall be also supported by AC500 PLC. In this application note, we recommend usage of Modbus/TCP and CODESYS ETH communication protocols (see [3.] for more details) for communication to PM5xx standard CPU from standard HMI and then acyclic DPRAM based data exchange (DPRAM_SM5XX_SEND and DPRAM_SM5XX_REC FBs) [1.] and "Cyclic non-safe data exchange" [2.] for communication between PM5xx and SM560-S safety CPU (see Figure 4); ·
- MTBF value (≥ 22.5 years) which shall be suitable to reach PL d (ISO 13849- 1), as one can see from the functional safety calculation in chapter 3.5. If MTBF value is < 22.5 years, then only PL c (ISO 13849-1) can be reached.

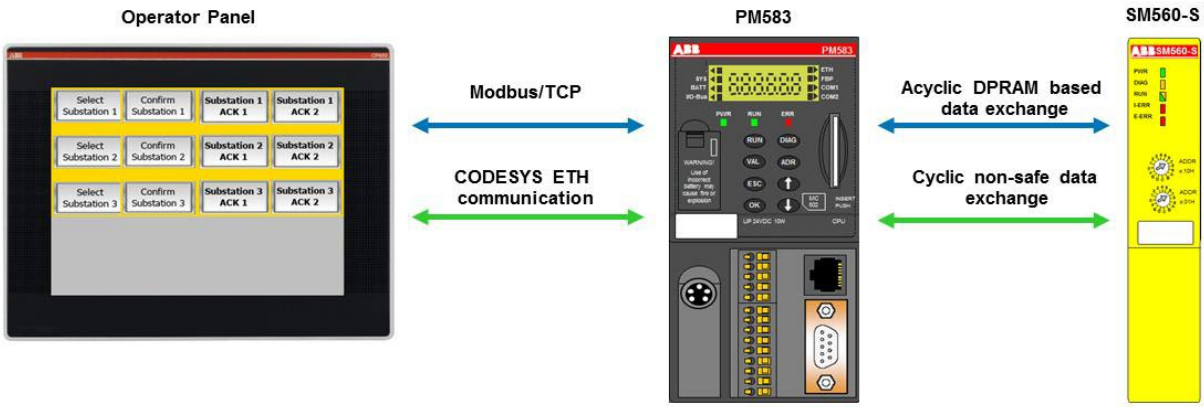


Figure 4. Two communication paths between standard HMI and SM560-S safety CPU through PM583-ETH CPU (example only)

Additional information related to AC500 PLC, engineering, operator panels and communication options can be found in [3.].

2.2. Task

In this application note, we describe a method how safety actions up to PL d (ISO 13849-1) can be triggered using standard HMI and AC500-S safety PLC.

NOTICE

The safety action term is defined in this application note as a user configuration activity to change the internal safety state of the given safety application in safety CPU module and NOT as a safety function. Even though the functional safety analysis for the safety action is performed using requirements listed for safety functions in ISO 13849-1, the consequences of possible faults in safety action execution are different to those found in safety functions, for example:

- **There are no SFRT requirements on a safety action, because if a safety action is not executed then previous state of the safety function configuration would remain valid and there shall be no dangerous situation (special organizational procedures have to be defined in the application to handle this situation, e.g., temporary safe stop of involved machines with a restart after successful reconfiguration). It is different to the safety function which has SFRT requirements on it.**
- **Since there are no SFRT requirements on safety actions, then even if no safety action can be executed at all, then no dangerous situation is expected, as it was described in the previous item.**
- **The following dangerous cases in safety actions on the application level are similar to those, which can be found with mode selector switches, for example:**
  - **More than one mode is active;**
  - **Wrong mode is selected.**

These potential dangerous cases shall be avoided using proper safety integrity measures, as described in chapter 2.3

NOTICE

The safety action to select substations, machines or pre-defined safely limited values shall comply also with the following generic mode selection requirements:

- **2006/42/EC: "… It must be possible to start machinery only by voluntary actuation of a control provided for the purpose." · EN ISO 12100-2: 2003: "… shall be fitted with a mode selector which can be locked in each position. Each position of the selector shall be clearly identifiable and shall exclusively enable one control or operating mode to be selected …"**
- **IEC 60204-1, Ed. 5.0: 2003: "... When a hazardous condition can result from a mode selection, unauthorized and/or inadvertent selection shall be prevented by suitable means (e.g., key operated switch, access code). Mode selection by itself shall not initiate machine operation. A separate action by the operator shall be required. ... Indication of the selected operating mode shall be provided ..."**
- **ISO 12100-2: 2003: Restart following power failure/spontaneous restart; Manual reset.**

Customer benefits from using standard HMI for triggering safety actions for functional safety applications up to PL d (ISO 13849-1) are:

- Ability to use standard HMIs for triggering safety functions up to PL d (ISO 13849-1) because the number of available off-the-shelf safety HMIs is very limited and usage of hard-wired mode selector switches may be not an option because of limitations described in chapter 1.1;
- Reuse of existing standard HMI for both standard control and functional safety control functions results in cost savings on additional HMIs and potentially user-friendlier interface to operators.

⚠ DANGER

It is the responsibility of the project administrator to setup proper user management (e.g., user roles, password protection, limited access, etc.) on the standard HMI for the given safety application at the end-customer site to avoid unauthorized access to safety-relevant controls on the standard HMI.

Before any deployment of a safety application with standard HMI for triggering safety actions, an assessment of dangerous threats such as eavesdropping or data manipulation shall be executed. In case of threats, appropriate security measures shall be implemented.

NOTICE

It is always highly recommended to use PL (ISO 13849-1) certified HMI for functional safety applications up to PL d (ISO 13849-1). Thus, the presented approach with the usage of standard HMI is only an option if no suitable PL (ISO 13849-1) certified HMI is available.

2.3. Solution

The proposed solution is based on the design analysis and additional diagnostic safety measures which can be implemented using AC500-S setup (see Figure 3) to enable usage of standard HMI in functional safety applications up to PL d (ISO 13849-1).

Figure 5 shows an overview on reachable Performance Levels depending on Category, DCavg and MTTFd values, as defined in ISO 13849-1. As one can see from Figure 5 (see a selection in blue), one of the possible approaches to satisfy PL d requirements is the usage of Category 2, DCavg = Medium and MTTFd = High.

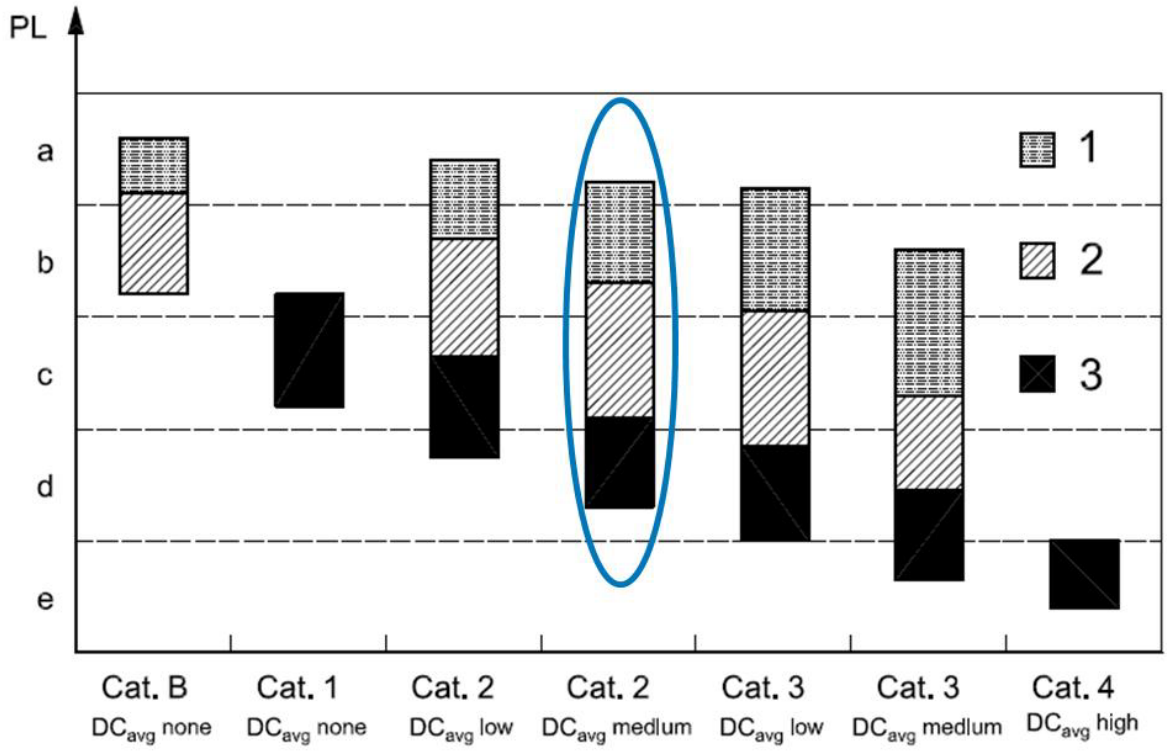


Figure 5. Relationship between Categories, DCavg, MTTFd (1 = Low, 2 = Medium and 3 = High) of each channel and PL from ISO 13849-1

Category 2 architecture based on ISO 13849-1 is shown in Figure 6.

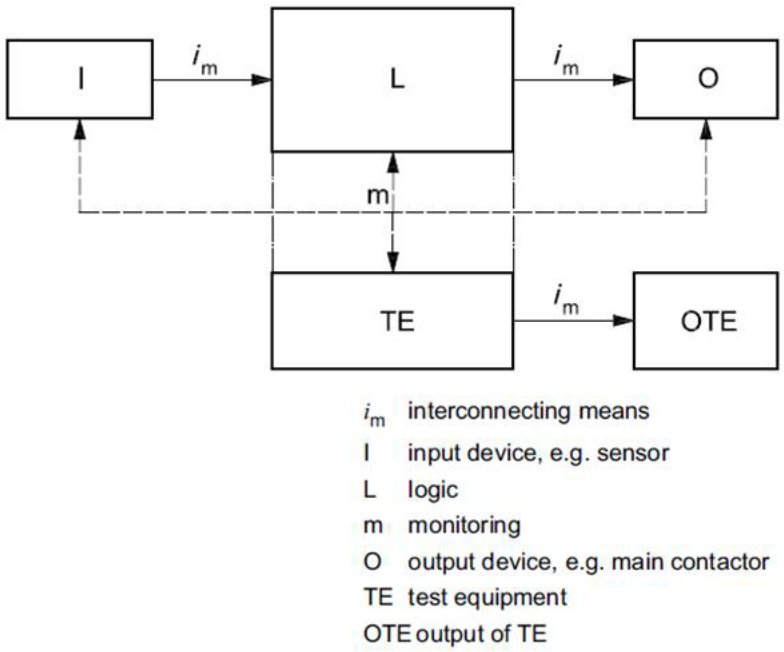


Figure 6. Category 2 architecture from ISO 13849-1

Key requirements for Category 2 (ISO 13849-1) are:

- Requirements of Category B (refer to ISO 13849-1 for details) and the use of well-tried safety principles shall apply;

- Safety function shall be checked at suitable intervals by the machine control system;
- The occurrence of a fault can lead to the loss of the safety function between the checks;
- The loss of safety function is detected by the check.

Category 2 architecture realization using standard HMI and AC500/AC500-S modules is shown in Figure 7 (refer also to Figure 3).

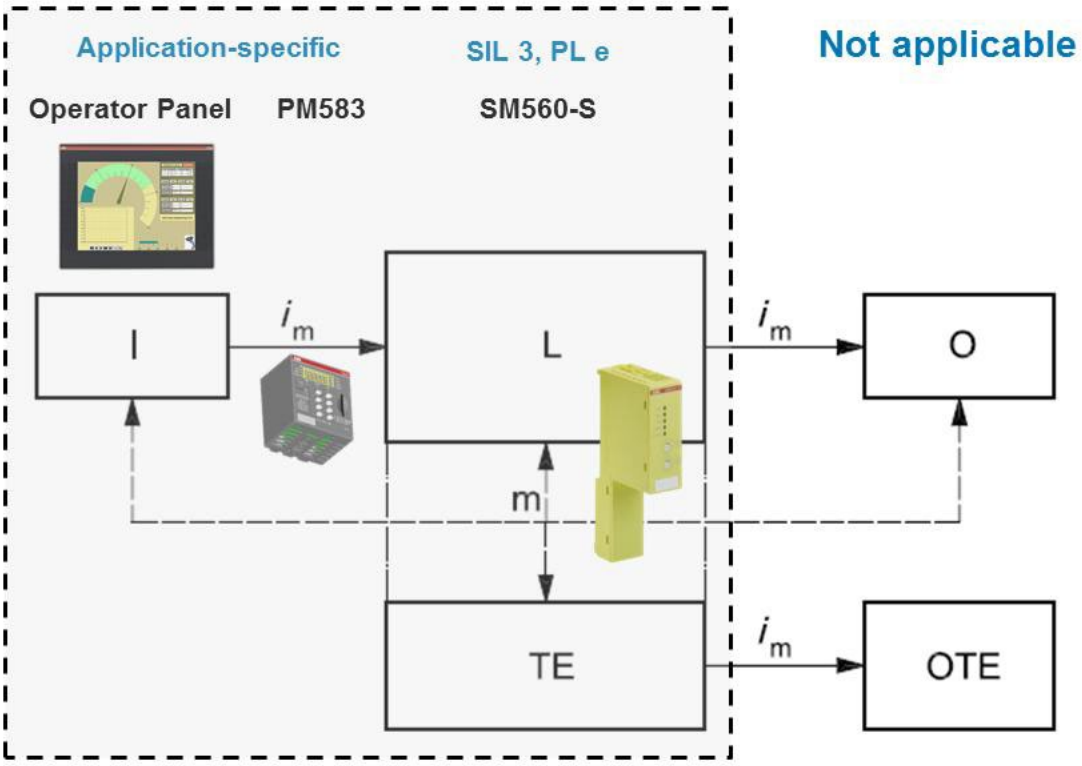


Figure 7. Category 2 equivalent architecture using standard HMI and AC500/AC500- S modules for triggering safety actions

As one can see from Figure 7, safety logic processing is fully covered by SM560-S safety CPU (SIL3, PL e) and the output functionality is not applicable in the given application because only re-configuration of SM560-S safety CPU (SIL3, PL e) program execution is done on the logic part. However, we need an additional analysis for the input part in which standard (non-safety) HMI can be used. This input part will be always application-specific and will require additional measures to satisfy PL d requirements, as described below.

To fulfill PL d (ISO 13849-1) requirements for input part, special DC (Diagnostic Coverage) measures shall be implemented according to ISO 13849-1. The following measure was selected for the input part with standard HMI and PM5xx standard CPU:

- Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements), which provides DC = 99% (see Annex E, ISO 13849-1). SM560-S safety CPU will take over the function of direct monitoring for input part with standard HMI.

The exemplary realization of this measure using standard HMI and AC500/AC500-S setup is presented in Figure 8 and is based on the setup in Figure 3 with the following assumptions, which are later described in more details in chapter 3:

- Two standard communication paths (diverse principle) for data exchange in both directions shall be established for standard HMI and SM560-S safety CPU:
  - **Path 1** (see normal lines in Figure 8): As an example, usage of Modbus/ TCP communication protocol to PM5xx standard CPU, then storage in a dedicated array (Data array 1) in the application program of PM5xx standard CPU and transfer to SM560-S safety CPU using acyclic DPRAM based data exchange (DPRAM_SM5XX_SEND and DPRAM_SM5XX_REC FBs).
  - **Path 2** (see dashed lines in Figure 8): As an example, usage of CODESYS ETH communication protocol to PM5xx standard CPU, then storage in a dedicated array (Data array 2) in the application program of PM5xx standard CPU and transfer to SM560-S safety CPU using “Cyclic non-safe data exchange” (see [2.] for more details).
- 4 different types of push buttons shall be created on the standard HMI. These push buttons shall be triggered one after another (“disable” or “hidden” features for buttons on the standard HMI can be used to support users in the selection procedure):
  - “Select …” buttons with unique integer signatures (e.g., 2784, 5362, 8493, etc.) defined for each button, which will form the first channel of 2-channel architecture with “Confirm …” buttons as a second channel. If “Select …” button is triggered, the relevant stored integer signature value will be transferred to the SM560-S safety CPU using communication **path 1** (normal lines in Figure 8).
  - “Confirm …” buttons with a negated integer value of the signature from relevant “Select …” buttons, which will form the second channel of 2- channel architecture with “Select …” buttons. This negated integer signature value (62751, 60173, 57042, etc.) are defined for each “Confirm …” button. If “Confirm …” button is triggered, then the stored negated signature will be transferred to the SM560-S safety CPU using communication **path 2** (dashed lines in Figure 8).
  - “… ACK1” buttons with unique integer signatures (e.g., 35552, 38130 and 41261, etc.) defined for each buttons, which will form the first channel of 2-channel architecture with “… ACK2” buttons as a second channel. If “… ACK1” button is triggered, the relevant stored signature will be transferred to the SM560-S safety CPU using communication **path 1** (normal lines in Figure 8).
  - “… ACK2” buttons with a negated integer value of the signature from relevant “… ACK1” buttons, which will form the second channel of 2-channel architecture with “… ACK1” buttons. This negated integer signature value (29983, 27405, 24274, etc.) is defined for each “… ACK2” button. If “… ACK2” button is triggered, the relevant stored negated signature will be transferred to the SM560-S safety CPU using communication **path 2** (dashed lines in Figure 8).

⚠ DANGER

The selection of signature values from the list of values from 0x0001 to 0xFFFE, the uniqueness of signature values and later handling including assignment to relevant buttons on the standard HMI is the responsibility of safety application engineers. These activities shall be performed according to ISO 13849 or IEC 62061 functional safety requirements for the given application safety integrity level.

0x0000 and 0xFFFF values shall not be used for signatures to avoid usage of 0 values in the selection procedure. 0 values have a special status in functional safety applications and, thus, shall be avoided.

In this application note, the selection range from 0x0001 to 0xFFFE for signature values also defines the maximum number of selection options to 32767 (65534 / 2 = 32767). It means that there are 32767 unique signature values for selection buttons and 32767 unique signature values for acknowledgement buttons, respectively.

The responsibility for correct implementation, verification and validation of the proposed approach is fully within the endcustomer responsibility.

- All unique integer signature values shall be pre-defined and stored in SM560- S safety CPU (SIL 3, PL e), for example, in memory flash during commissioning. This allows direct supervision of 2-channel input (transferred signature and negated signature values) coming from respectively “Select …” and “Confirm …” as well as “… ACK1” and “… ACK2” buttons on the standard HMI. This approach implements a direct monitoring of the user selection on the standard HMI from SM560-S safety CPU as defined by ISO 13849-1. Both integer signature and negated integer signature values from respectively “Select …” and “Confirm …” as well as “… ACK1” and “… ACK2” buttons after transfer to SM560-S safety CPU and appropriate transformations shall be evaluated in the safety application program against stored in SM560-S safety CPU signature values for push buttons. This includes the usage of SF_Equivalent FBs [1.], in which DiscrepancyTime input is also included to define maximum allowed discrepancy time between 2 channels (refer to chapter 3 for more details). This 2-channel evaluation against pre-defined and stored in SM560-S safety CPU signature values allows confirming DC = 99% for direct monitoring of user selection on standard HMI to detect such errors as “Wrong mode is selected”.

⚠ DANGER

The responsibility for the correct storage of signature values in SM560-S safety CPU flash memory is fully within the end-customer responsibility. It means that appropriate verification and validation steps (e.g., the use of SF_FLASH_READ FB on SM560-S safety CPU to read back stored signature values and verify them) shall be defined in the safety application development to make sure that correct signature values were stored in the pre-defined SM560-S flash memory cells. These activities shall be performed according to ISO 13849 or IEC 62061 functional safety requirements for the given application safety integrity level.

- After 2-channel evaluation for both “Select …” and “Confirm …” as well as “… ACK1” and “… ACK2” buttons one can use SF_ModeSelector FB in SM560-S safety CPU to evaluate selection options similar to mechanical or electromechanical mode selector switches, as mentioned in chapter 2.1, to detect such errors as “More than one mode is active”.
- Reset, lock, readback, diagnostics and other functions can be also added to the standard HMI using a similar approach. Reset, readback and diagnostics function implementation is shown in details in the example in chapter 3.

⚠ DANGER

Depending on the selection mode and its defined PL and SIL levels, one may have to define additional access rights for selection and acknowledgement buttons to be able to differentiate various user groups for a limited or full access to selection options.

It is the responsibility of the project administrator to setup proper user management (e.g., user roles, password protection, limited access, etc.) on the standard HMI for the given safety application at the end-customer site to avoid unauthorized access to safety-relevant controls on the standard HMI.

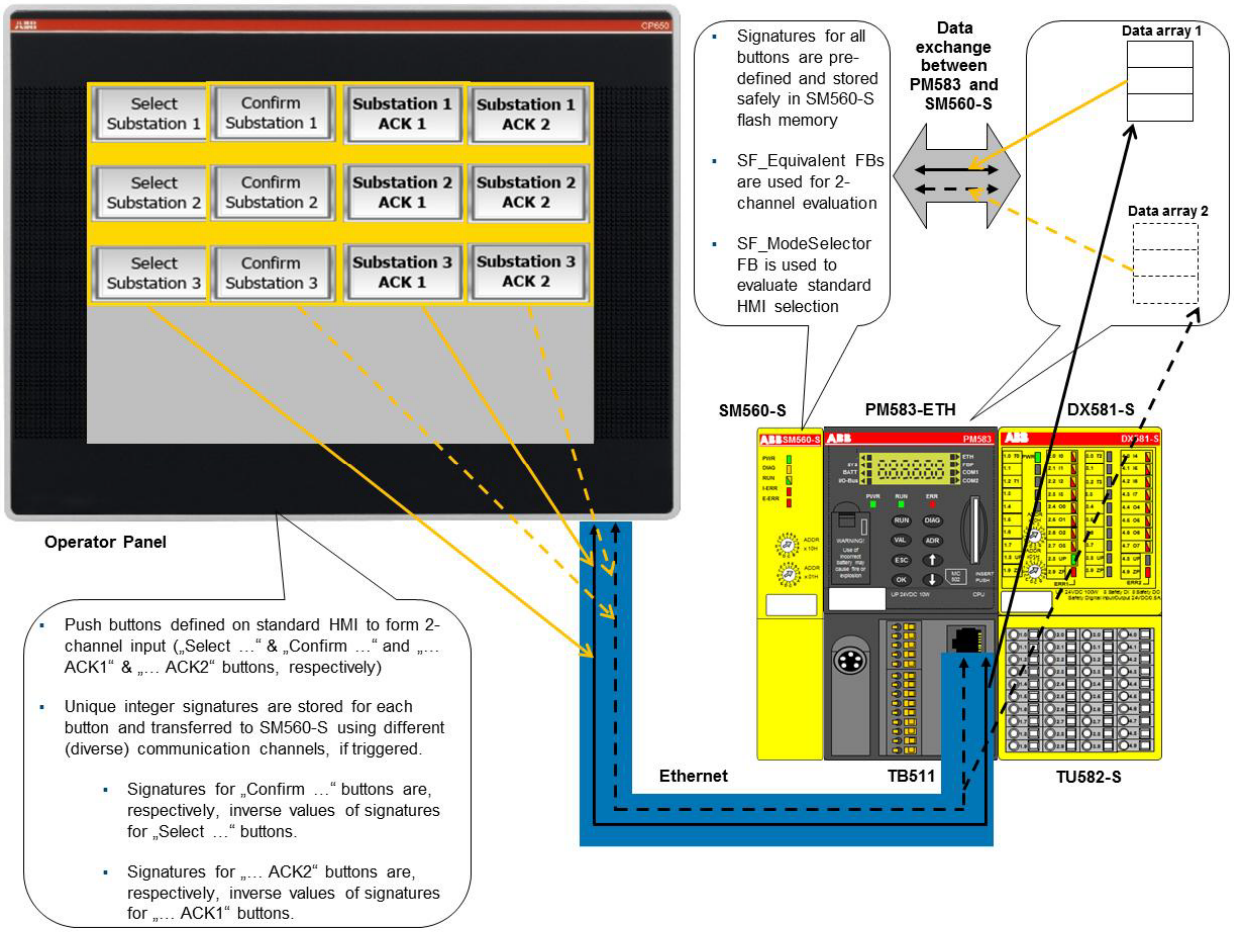


Figure 8. Exemplary realization of triggering safety actions using standard HMI with AC500-S safety PLC

The sequence chart in Figure 9 shows data flows using two pre-defined diverse communication paths (see Figure 8, normal and dashed lines, respectively) between standard HMI and SM560-S safety CPU. The data flow is triggered when “Select …” push buttons on the standard HMI are activated by the user. If 2-channel evaluation in SM560-S safety CPU is successful, the selection result from SM560-S safety CPU is transferred back to the standard HMI (see Figure 9) to enable “… ACK1” and “… ACK2” push buttons on the standard HMI and to acknowledge the selection by the user.

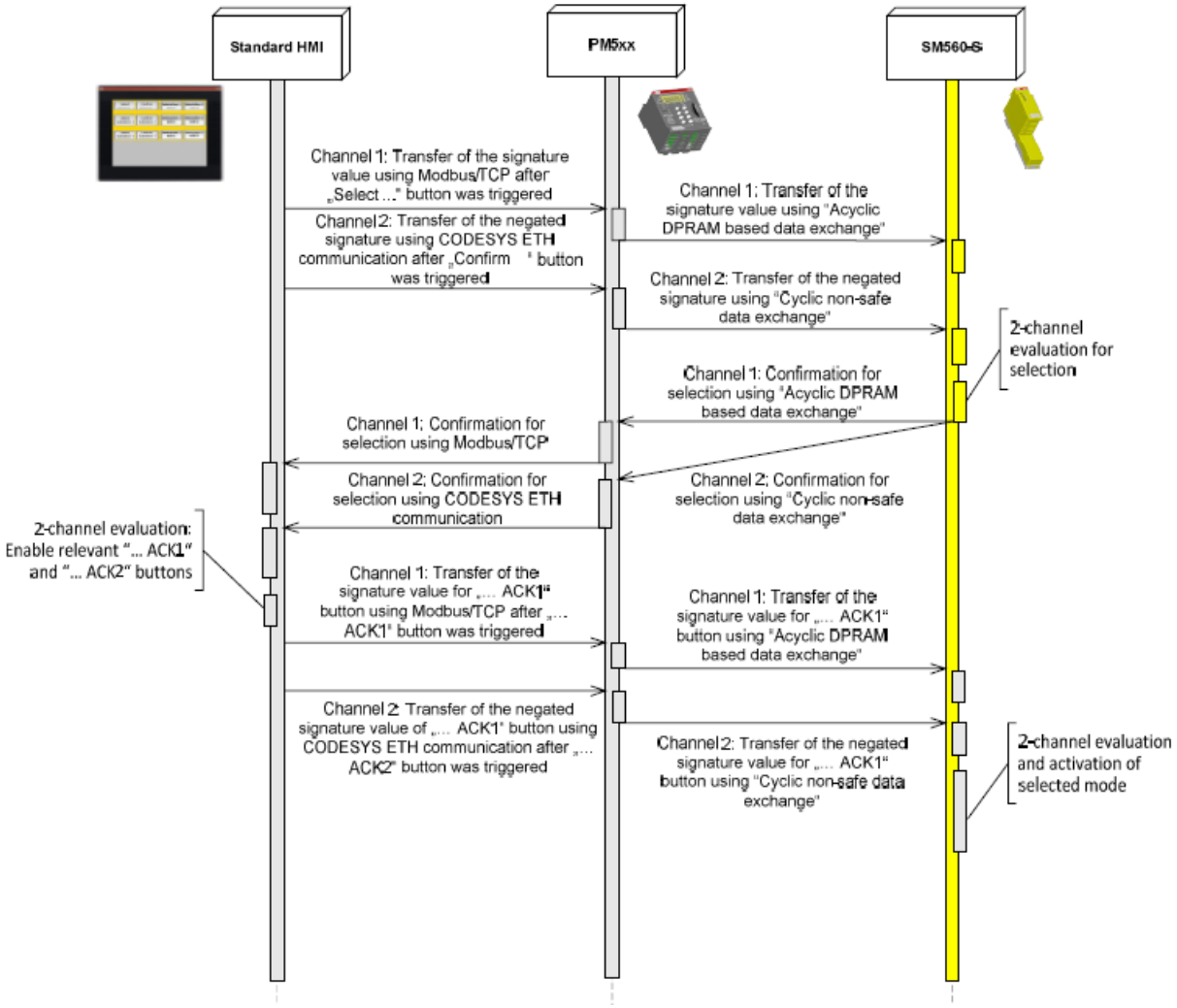


Figure 9. Sequence diagram for triggering safety actions using standard HMI and SM560-S safety CPU

The control flow diagram in Figure 10 and 11 describes typical actions which have to be performed to realize the method of triggering safety actions using standard HMI.

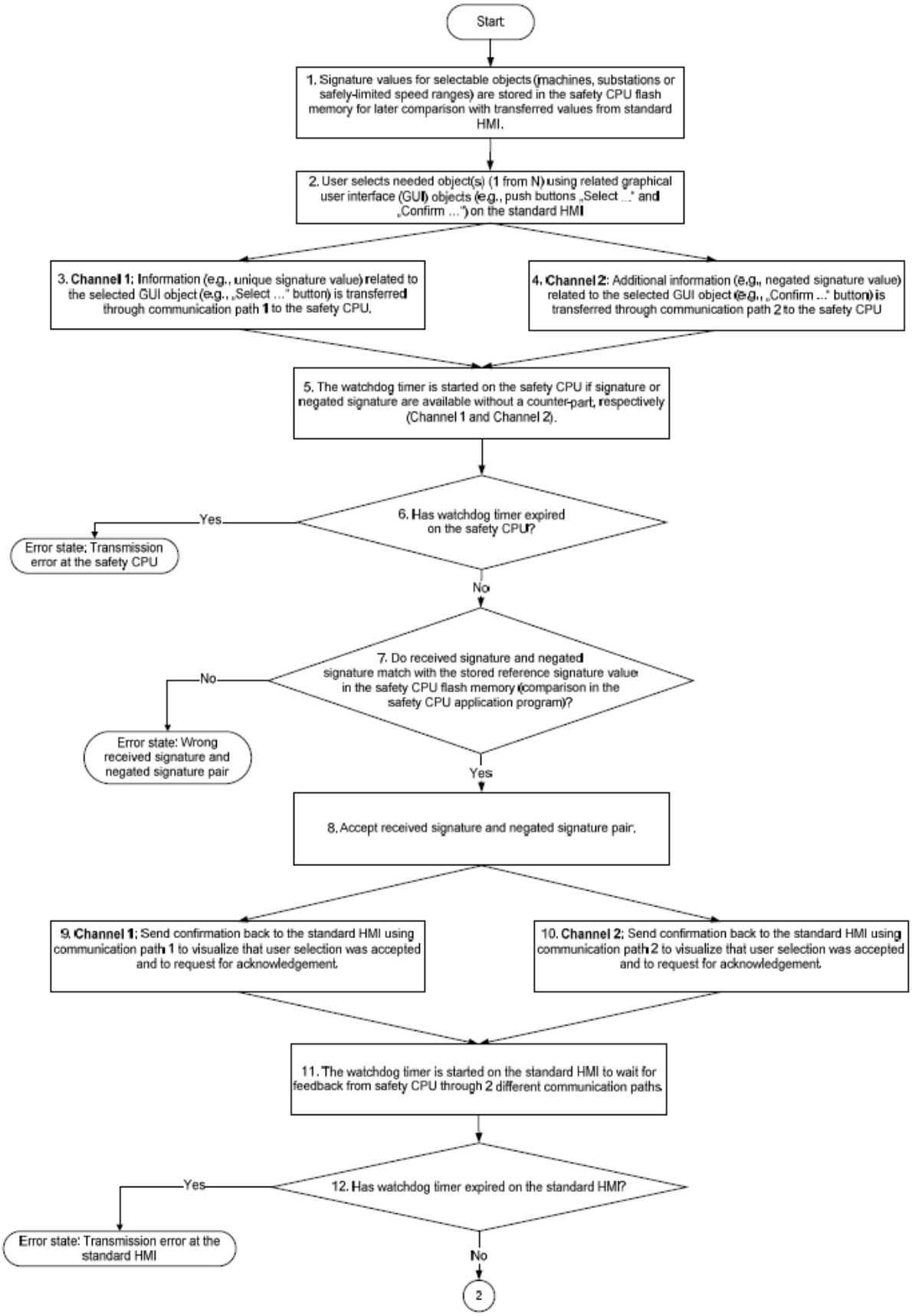


Figure 10. Control flow diagram (Part 1) for triggering safety actions using standard HMI and safety CPU

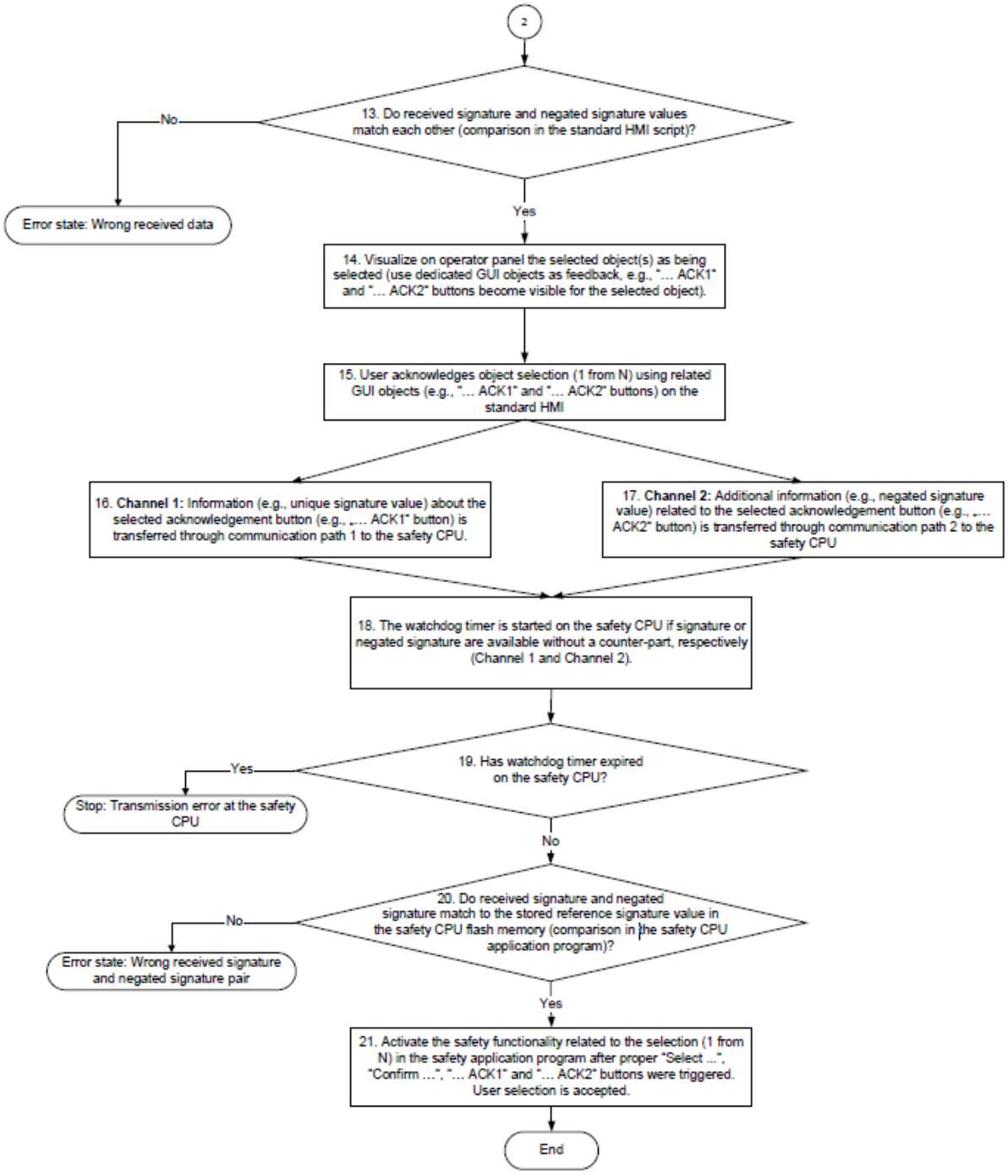


Figure 11. Control flow diagram (Part 2) for triggering safety actions using standard HMI and safety CPU

NOTICE

There are various options (e.g., usage of pre-defined GUI elements, etc.) to visualize the fact that user selection using “Select …” and “Confirm …” push buttons was accepted and the acknowledge action using “… ACK1” and “… ACK2” push buttons is required.

In this application note, we used an approach of default hidden “… ACK1” and “… ACK2” push buttons. It means that only if the feedback from the SM560-S safety CPU for triggered selection using “Select …” and “Confirm …” push buttons is received on the standard HMI using two separate communication paths, the related “… ACK1” and “… ACK2” become visible and accessible for operator actions.

In the safety application program on SM560-S safety CPU, the user can define the watchdog time for the follow-up acknowledgement actions with “… ACK1” and “… ACK2” push buttons. If acknowledgement actions are not registered on SM560-S safety CPU in the pre-defined time interval (it is always application specific), then the error state shall be triggered in the SM560-S safety CPU application program. This error state can be left using a reset operation, e.g., ”Reset” push button on the standard HMI.

The proposed method of triggering safety actions using standard HMI in functional safety applications up to PL d (ISO 13849-1) is described with more details in the example in chapter 3.

3. Example

The following example describes the safety analysis and implementation needed for selection of substations, machines or pre-defined safely limited values in functional safety applications up to PL d (ISO 13849-1).

3.1. General

In our example, we refer to the system setup in harbor crane applications with standard HMI and AC500-S safety PLC (see Figure 12). Figure 12 presents an exemplary control setup with three harbor cranes (we will call them substations in our example), which are able to work in both automatic and remote control mode and include their own standard and safety control parts.

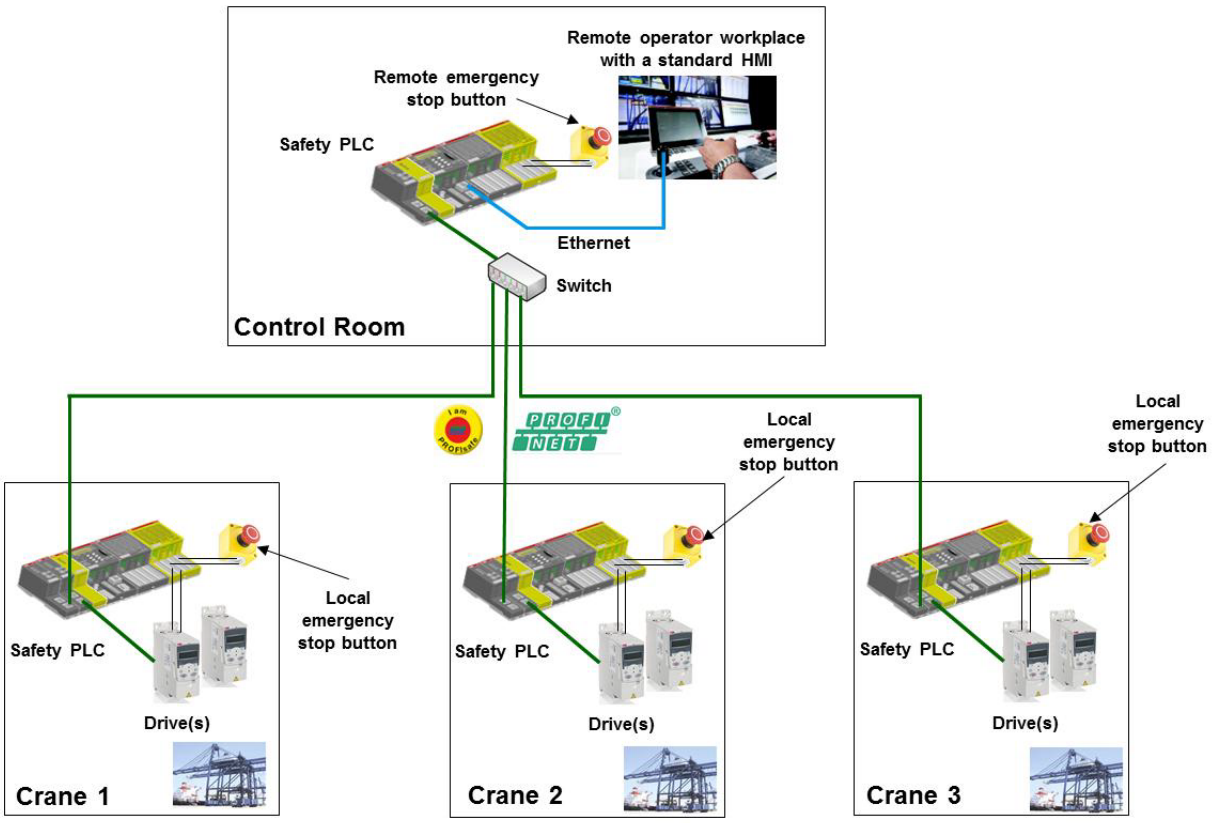


Figure 12. Exemplary harbor crane application for triggering safety actions using standard HMI and safety CPU

To enable the remote control mode, the control part of each crane (both standard and safety) is connected using PROFINET/PROFIsafe [1] to the remote control room with an operator control workplace with a standard HMI and safety PLC. Local emergency stop buttons are always available to stop the crane and are not further discussed in this example. In addition to local emergency stop buttons, remote emergency stop button is available at the operator workplace in the remote control room (see Figure 12). This remote emergency stop button (using standard HMI selection means described below) can be enabled to stop the selected crane.

The operator from the remote control room is able to control only one crane at a time. Depending on which crane has to be currently controlled, the operator shall be able to safely (up to PL d (ISO 13849-1))

select one of cranes (e.g., crane 1, crane 2 or crane 3) using the standard HMI on his control desk. When selected, the crane can be safely stopped using the emergency stop button located in the operator control room. If another crane is selected, then emergency stop button will stop that crane only. As a result, the emergency stop safety function becomes reconfigurable.

NOTICE

Locking of selected substations, machines or pre-defined safely limited values is not covered in this application note, but can be implemented in a similar way as it was done in the example for selection of substations, machines, etc.

We will provide a safety analysis with the supporting calculation for all parts of the safety control loop (sensor and logic processing, refer to Figure 7). We aim to reach PFHavg ≤ 9.39E-7 1/h (see Table K1 from ISO 13849-1), as it is required for PL d.

⚠ DANGER

Triggering of safety actions on the standard HMI is safety-relevant but the visualization of selected substations, machines or pre-defined safely limited values is not considered as safety-relevant in the application note (visualization of selected substation on the standard HMI can be used only as diagnostics). To have safety-relevant visualization of user selection, additional measures shall be implemented, e.g., usage of safety-related lights (integrated in the user control panel) connected to DX581- S safety digital outputs and activated depending on the selection in the safety CPU program.

3.2. Safety function

The safety function in this example is the actuation of the emergency stop button (see Figure 12) on the remote control station by an operator to safely stop the selected crane (substation) using, e.g., SS1 (Safe Stop 1) with a controlled stop of the motor within a maximum permissible time and SBC (Safe Break Control) implemented locally on the crane using the safety control equipment (safety PLC, safety option in drives and safe break control). This safety function is not further analysed in this example because it represents the state-of-the-art (see [4.] for more details on emergency stop implementation and analysis).

In this application note, we evaluate only safety action and not a safety function described above. The safety action is the selection of the crane (substation) up to PL d (ISO 13849-1). If, for any reasons, the selection of the next crane is not possible then there is no dangerous situation, because cranes in automatic mode would be still safely controlled by their local safety PLC and rely on their local safety function implementation. It is, however, dangerous if a wrong crane could be selected by the operator or more than one cranes are selected at a time.

3.3. Functional description

- The user is able to select a crane (1 of 3 in the given example) for their remote control using standard HMI connected to the SM560-S safety CPU, as it is shown in Figure 8 and 12. The successful selection of a crane enables remote emergency stop safety function for this selected crane from the remote emergency stop button on the operator remote control desk.
- The selection of a crane is done by triggering four buttons allocated to the given crane in a row (see Figure 8) in a sequence (one after another). “…ACK1” and “…ACK2” buttons become visible for the selected crane only after “Select …” and “Confirm …” buttons for the given crane were selected, successfully transferred to the safety CPU program, passed 2-channel evaluation and the feedback was received about the successful pre-selection. This has to be followed by the operator acknowledgement using “…ACK1” and “…ACK2” buttons.

- After successful user selection (see Figure 10 and 11 for exemplary control flow), the selected crane can be controlled using emergency stop button on the remote operator control desk.
- The fault control for such cases as “More than one mode is active” and “Wrong mode is selected” is done using application-specific implementation, as further described in details in chapter 3.4.1.

3.4. Design features

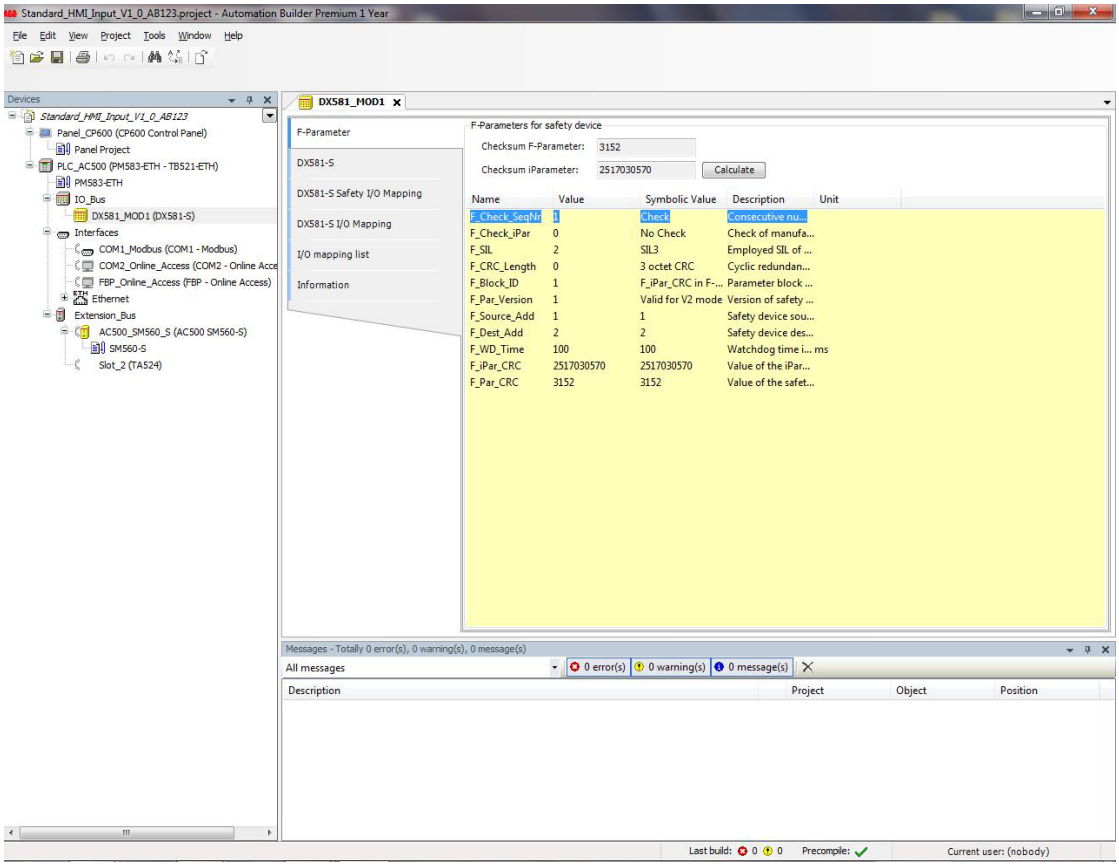
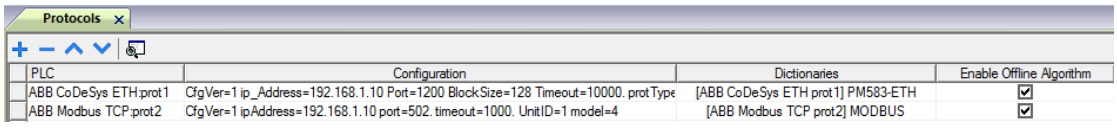
3.4.1. Implementation details

The following steps (1 to 11) shall be considered during the implementation of the proposed approach for the selection of cranes (cranes are called substations in this example to be generic) for remote control in functional safety applications up to PL d (ISO 13849-1) using standard HMI and AC500-S safety PLC:

NOTICE

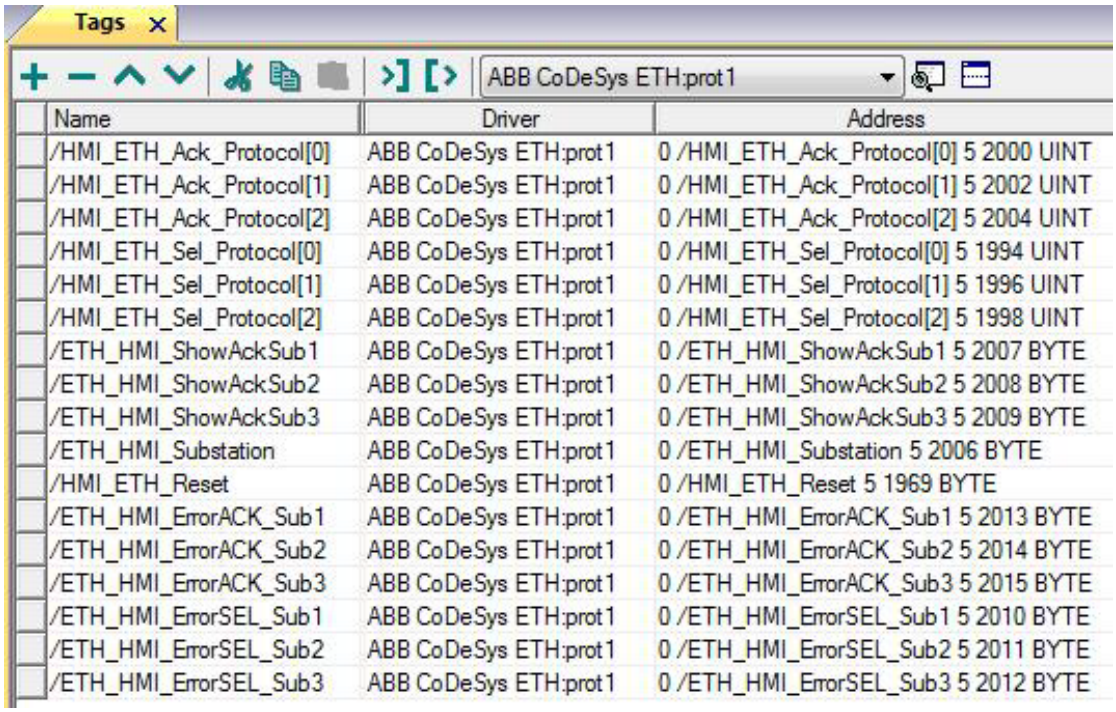
In the table below, only major steps are listed and it provides a general overview on the required actions. Depending on the application needs and selected standard HMI, additional implementation steps or modifications of presented steps may be required.

Contact ABB technical support for more details.

Step	Description
1	Create a new Automation Builder project (refer to [3.] for details), which will have to include AC500 components listed in Figure 3 with a standard HMI connected using Ethernet to PM583-ETH standard CPU. Configure all modules to create ready-to-use boot projects for PM583-ETH, SM560-S and standard HMI (refer to [1.] and [3.] to get more details on how to configure and use AC500 modules). Example of Automation Builder project: 
2	Create a project for standard HMI using the vendor-specific engineering tool (we use Panel Builder 600 from ABB in this example) and configure two independent / diverse communication protocols, e.g., CODESYS ETH communication and Modbus/TCP, to communicate with PM583-ETH standard CPU. Example with a protocol configuration for CODESYS ETH communication and Modbus/TCP in Panel Builder 600: 

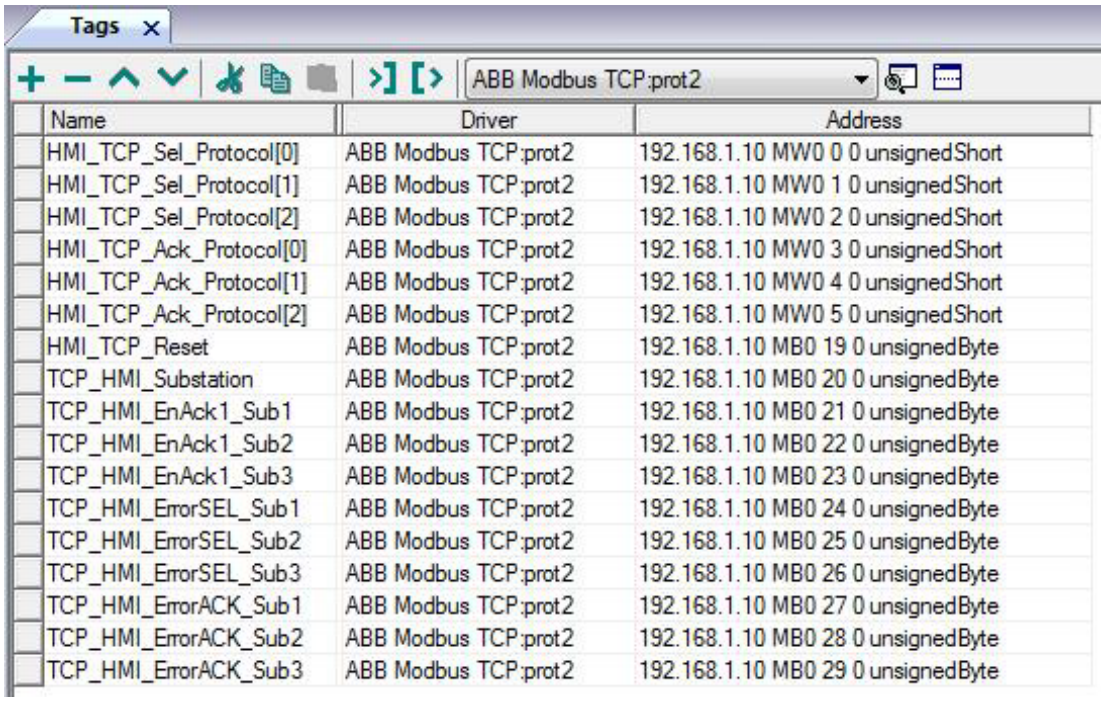
3 Define tags for communication with PM583-ETH.

Example for CODESYS ETH communication:



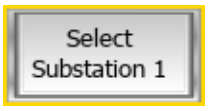
Name	Driver	Address
/HMI_ETH_Ack_Protocol[0]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Ack_Protocol[0] 5 2000 UINT
/HMI_ETH_Ack_Protocol[1]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Ack_Protocol[1] 5 2002 UINT
/HMI_ETH_Ack_Protocol[2]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Ack_Protocol[2] 5 2004 UINT
/HMI_ETH_Sel_Protocol[0]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Sel_Protocol[0] 5 1994 UINT
/HMI_ETH_Sel_Protocol[1]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Sel_Protocol[1] 5 1996 UINT
/HMI_ETH_Sel_Protocol[2]	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Sel_Protocol[2] 5 1998 UINT
/ETH_HMI_ShowAckSub1	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ShowAckSub1 5 2007 BYTE
/ETH_HMI_ShowAckSub2	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ShowAckSub2 5 2008 BYTE
/ETH_HMI_ShowAckSub3	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ShowAckSub3 5 2009 BYTE
/ETH_HMI_Substation	ABB CoDeSys ETH:prot1	0 /ETH_HMI_Substation 5 2006 BYTE
/HMI_ETH_Reset	ABB CoDeSys ETH:prot1	0 /HMI_ETH_Reset 5 1969 BYTE
/ETH_HMI_ErrorACK_Sub1	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorACK_Sub1 5 2013 BYTE
/ETH_HMI_ErrorACK_Sub2	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorACK_Sub2 5 2014 BYTE
/ETH_HMI_ErrorACK_Sub3	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorACK_Sub3 5 2015 BYTE
/ETH_HMI_ErrorSEL_Sub1	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorSEL_Sub1 5 2010 BYTE
/ETH_HMI_ErrorSEL_Sub2	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorSEL_Sub2 5 2011 BYTE
/ETH_HMI_ErrorSEL_Sub3	ABB CoDeSys ETH:prot1	0 /ETH_HMI_ErrorSEL_Sub3 5 2012 BYTE

Example for Modbus/TCP communication:

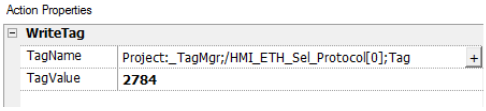
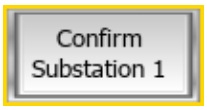


Name	Driver	Address
HMI_TCP_Sel_Protocol[0]	ABB Modbus TCP:prot2	192.168.1.10 MW0 0 0 unsignedShort
HMI_TCP_Sel_Protocol[1]	ABB Modbus TCP:prot2	192.168.1.10 MW0 1 0 unsignedShort
HMI_TCP_Sel_Protocol[2]	ABB Modbus TCP:prot2	192.168.1.10 MW0 2 0 unsignedShort
HMI_TCP_Ack_Protocol[0]	ABB Modbus TCP:prot2	192.168.1.10 MW0 3 0 unsignedShort
HMI_TCP_Ack_Protocol[1]	ABB Modbus TCP:prot2	192.168.1.10 MW0 4 0 unsignedShort
HMI_TCP_Ack_Protocol[2]	ABB Modbus TCP:prot2	192.168.1.10 MW0 5 0 unsignedShort
HMI_TCP_Reset	ABB Modbus TCP:prot2	192.168.1.10 MB0 19 0 unsignedByte
TCP_HMI_Substation	ABB Modbus TCP:prot2	192.168.1.10 MB0 20 0 unsignedByte
TCP_HMI_EnAck1_Sub1	ABB Modbus TCP:prot2	192.168.1.10 MB0 21 0 unsignedByte
TCP_HMI_EnAck1_Sub2	ABB Modbus TCP:prot2	192.168.1.10 MB0 22 0 unsignedByte
TCP_HMI_EnAck1_Sub3	ABB Modbus TCP:prot2	192.168.1.10 MB0 23 0 unsignedByte
TCP_HMI_ErrorSEL_Sub1	ABB Modbus TCP:prot2	192.168.1.10 MB0 24 0 unsignedByte
TCP_HMI_ErrorSEL_Sub2	ABB Modbus TCP:prot2	192.168.1.10 MB0 25 0 unsignedByte
TCP_HMI_ErrorSEL_Sub3	ABB Modbus TCP:prot2	192.168.1.10 MB0 26 0 unsignedByte
TCP_HMI_ErrorACK_Sub1	ABB Modbus TCP:prot2	192.168.1.10 MB0 27 0 unsignedByte
TCP_HMI_ErrorACK_Sub2	ABB Modbus TCP:prot2	192.168.1.10 MB0 28 0 unsignedByte
TCP_HMI_ErrorACK_Sub3	ABB Modbus TCP:prot2	192.168.1.10 MB0 29 0 unsignedByte

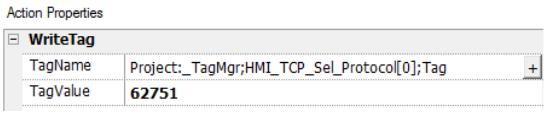
4 Create a GUI for the selection of cranes (substations), which shall include at least four buttons in a row for each selectable substation (Substation 1 is used here as an example):

<table>
<tr><th>Button</th><th>Function</th><th>Explanation</th></tr>
<tr><td> 
</td><td>Selection of the substation e.g., using CODESYS ETH communication or Modbus/TCP depending on the selected communication protocol for “Confirm Substation 1” button (these protocols have to be different for “Select Substation 1” and “Confirm Substation 1” buttons).

After selection, the unique pre-defined signature value 0x0AE0 has to be transferred to PM583-ETH.

Example (Decimal value 2784 = Hexadecimal value 0x0AE0):
 
</td><td rowspan="2">Two buttons are required for safe error detection. The buttons form a 2- channel path with a discrepancy time supervision on the SM560-S safety CPU.</td></tr>
<tr><td> 
</td><td>Confirmation of the substation selection e.g., using Modbus/TCP or CODESYS ETH communication depending on the selected communication protocol for “Select Substation 1” button (these protocols have to be different for “Confirm Substation 1” and “Select Substation 1” buttons).

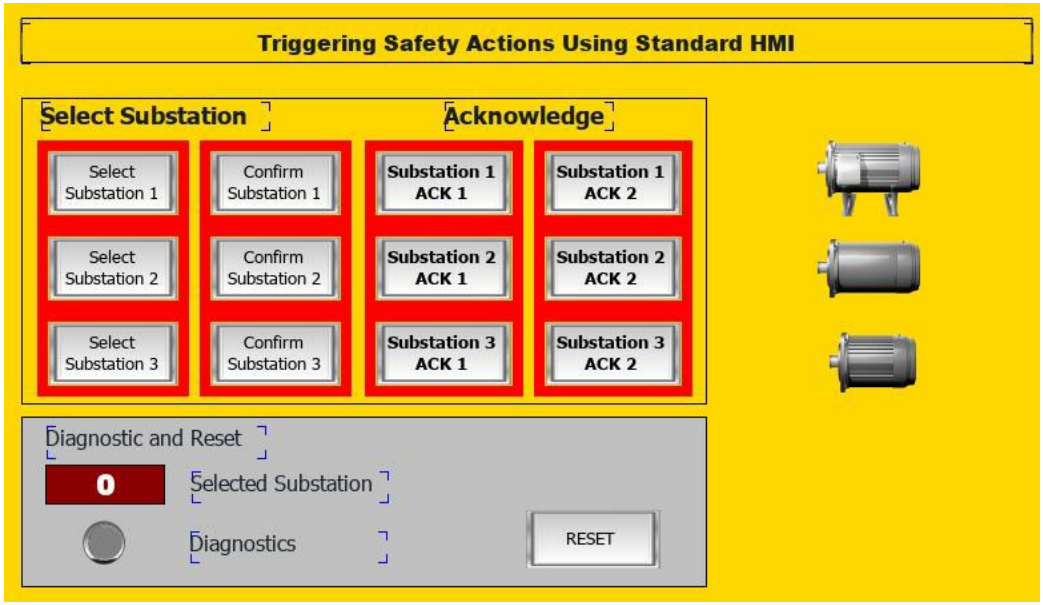
After confirmation, the negated unique pre-defined signature value (0xF51F is the negated value of 0x0AE0 from “Select Substation 1” button) defined for “Confirm Substation 1” button has to be transferred to PM583-ETH.

Example (Decimal value 62751 = Hexadecimal value 0xF51F):
 
</td></tr>
<tr><td> 
</td><td>Two buttons “Substation 1 ACK1” and “Substation 1 ACK2” shall be used for acknowledgement via standard HMI (the 2-channel principle used for “Select Substation 1” and “Confirm Substation 1” buttons is reused for the acknowledgement with other unique signature value):

• After pressing “Substation 1 ACK 1”, the unique pre-defined signature value 0x8AE0 has to be transferred to PM583-ETH using CODESYS ETH communication</td><td></td></tr>
</table>

	or Modbus/TCP depending on the selected communication protocol for “Substation 1 ACK 2” button (these protocols have to be different for “Substation 1 ACK 1” and “Substation 1 ACK 2” buttons). • After pressing “Substation 1 ACK 2”, the negated unique pre-defined signature value 0x751F (0x751F is the negated value of 0x8AE0 from “Substation 1 ACK1” button) has to be transferred to PM583-ETH using Modbus/TCP or CODESYS ETH communication depending on the selected communication protocol for “Substation 1 ACK 1” button (these protocols have to be different for “Substation 1 ACK 2” and “Substation 1 ACK 1” buttons). Implement such a behavior on the standard HMI using scripting engine so that only after the successful selection using “Select …” and “Confirm …” buttons, acknowledgement buttons “… ACK1” and “… ACK2” related to the selected substation will become visible. This will improve user-friendliness of the given application and limit potential wrong user selections.	The buttons form a 2-channel path with a discrepancy time supervision on SM560-S safety CPU.
	Reset occurred errors	After pressing the button “RESET”, the value 0 is sent for all signatures defined for “Select …”, “Confirm …”, “…ACK1” and “…ACK2” buttons to enable a restart for the user selection.

Example of GUI (the red background can be used to visualize error situations in case of discrepancy time errors):



⚠ DANGER

Note that the grey part in the HMI presents non-safe information which includes:

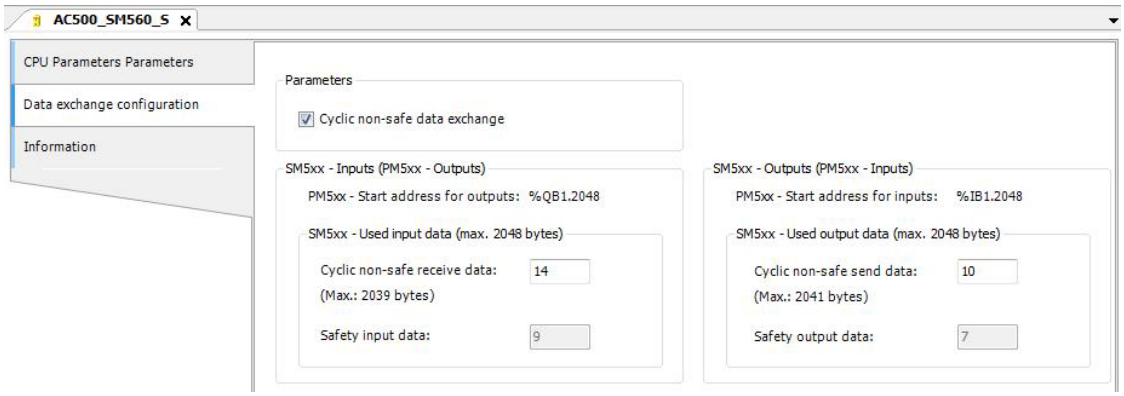
- **Indication of the currently selected substation;**
- **Indication if an error has occurred during the selection.**

Depending on the given application needs, various additional implementations on the standard HMI part can be implemented (these implementations are not presented in this application note) to improve user-friendliness of the given application. Some of these additional features are listed here:

- Visualisation of error states in case of wrong sequence of events;
- Usage of standard HMI Javascript procedures to handle events coming from SM560-S safety CPU through PM583-ETH;
- Usage of enable/disable or visible/invisible properties of buttons depending on the application event.

NOTICE

In case of a wrong option selection using “Select …”, “Confirm …” or “… ACK1” push buttons, the user can always use „Reset“ push button to re-start the selection procedure from the beginning.

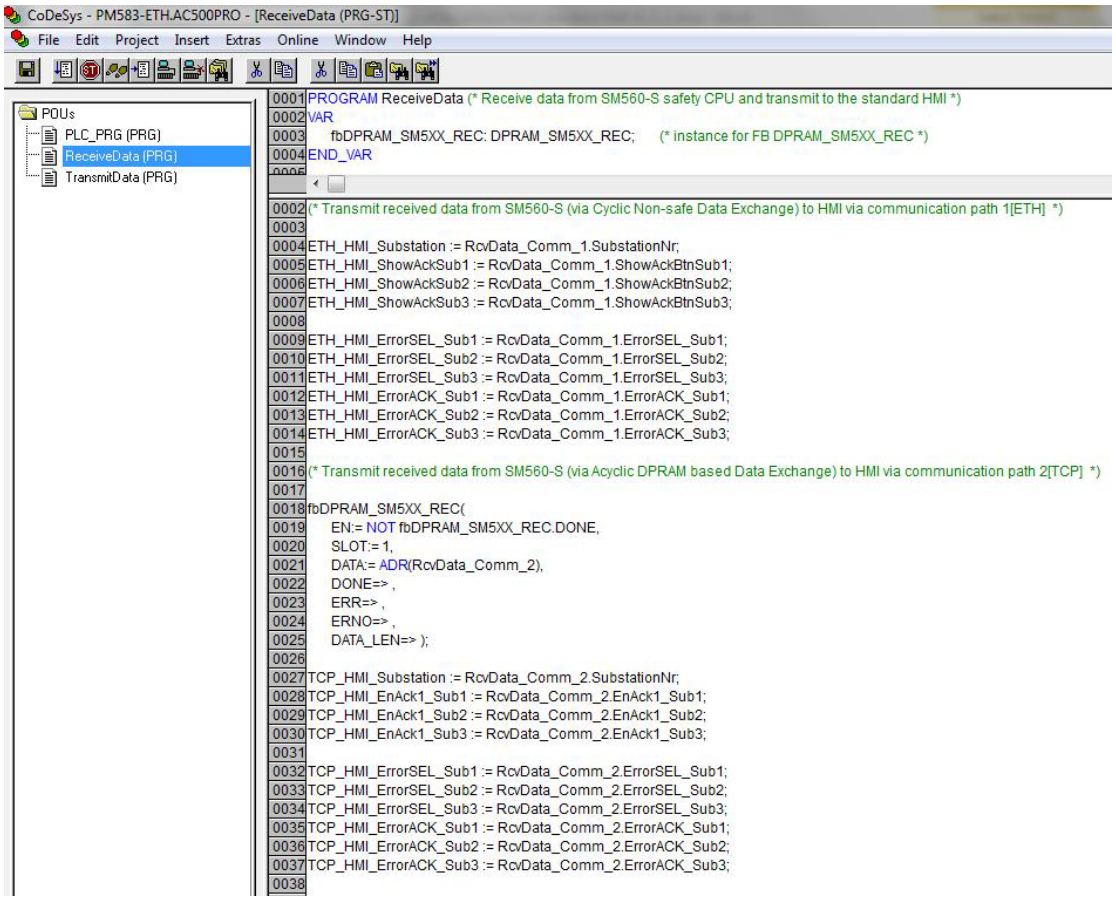
5	Enable and configure “Cyclic non-safe data exchange” for SM560-S safety CPU (refer to [2.] for more details). Example of “Cyclic non-safe data exchange” configuration: 

6 Create a high-priority task on PM583-ETH and implement data exchange (CODESYS ETH communication and Modbus/TCP communication) between PM583-ETH and standard HMI as well as PM583-ETH and SM560- S (“Acyclic DPRAM based data exchange” [1.] using DPRAM_SM5XX_SEND and DPRAM_SM5XX_REC FBs and “Cyclic nonsafe data exchange” [2]).

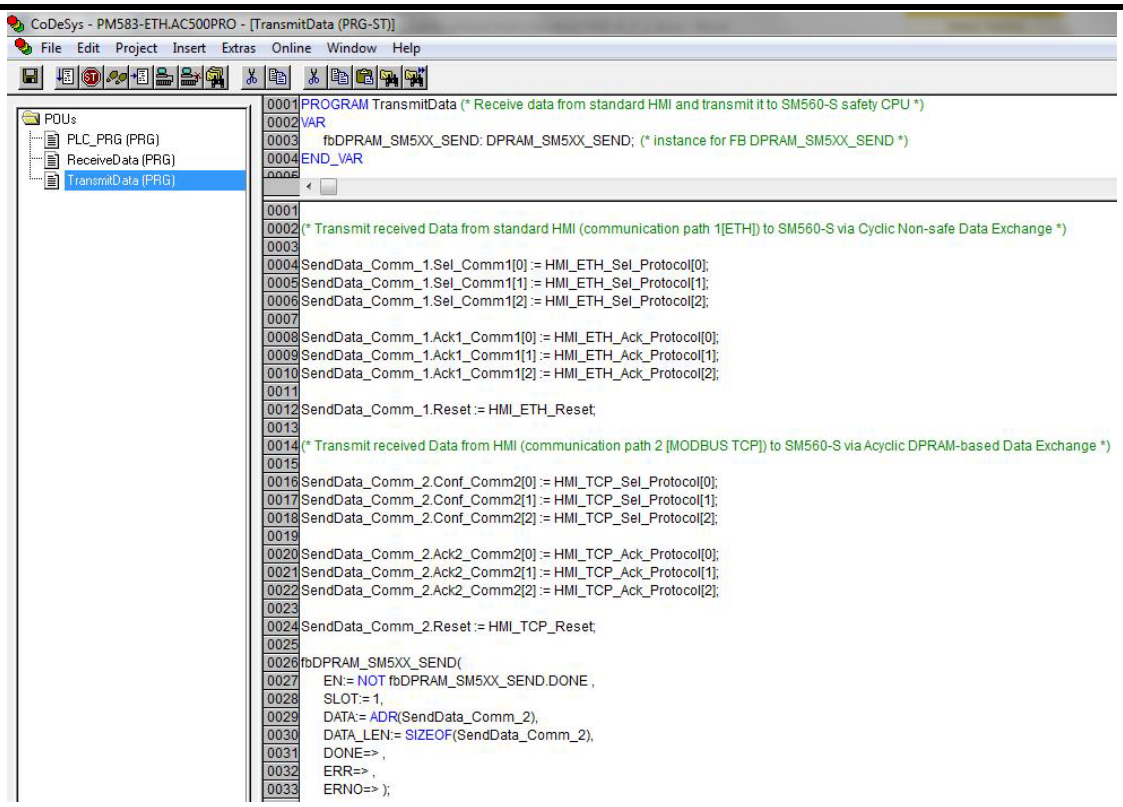
NOTICE

Note that the data related to the selection shall not be modified in PM583-ETH program. The data shall be only mapped and then copied from one communication channel to another to enable 2-channel data exchange between the standard HMI and SM560-S safety CPU.

Example of received data on PM583-ETH from SM560-S safety CPU and its transfer to the standard HMI:



Example of received data on PM583-ETH from the standard HMI and its data transfer to the SM560-S safety CPU:



7

Store predefined signatures for selection buttons in SM560-S safety CPU flash memory using SF_FLASH_WRITE FB, as described in [1.], or simply store them as global variable constants.

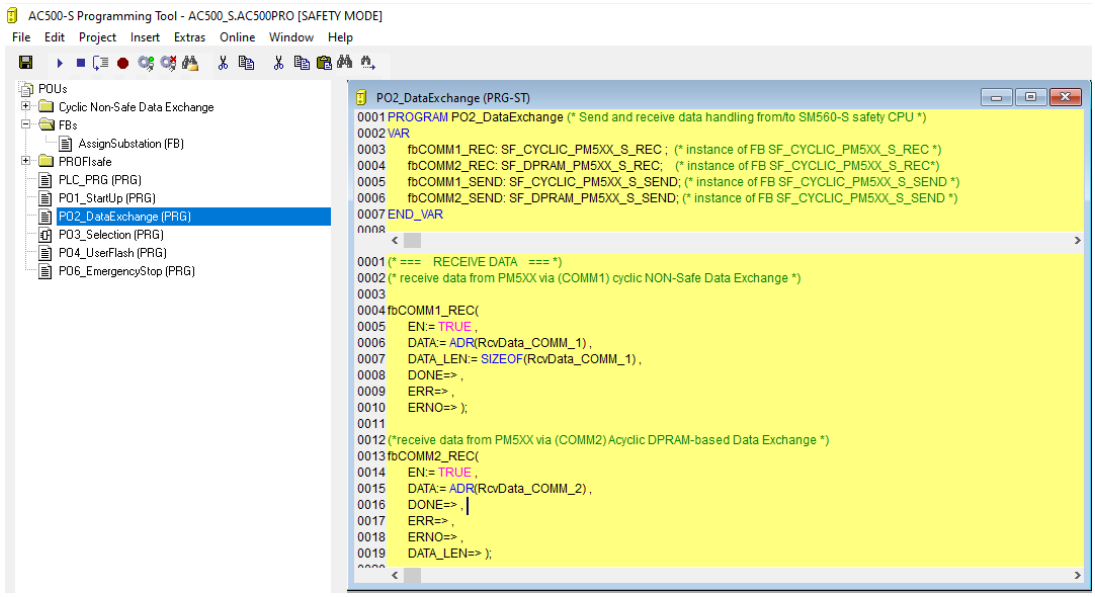
Example with signatures for 3 “Select …” and “… ACK1” buttons stored as global variable constants:

```
(* Signatures used for comparison. The signatures can be also located in the SM560-S User Flash. *)

    Signature_Sub1_Sel: WORD := 16#0AE0;   (* Signature *)
    Signature_Sub2_Sel: WORD := 16#14F2;   (* Signature *)
    Signature_Sub3_Sel: WORD := 16#212D;   (* Signature *)

    Signature_Sub1_Ack: WORD := 16#8AE0;   (* Signature *)
    Signature_Sub2_Ack: WORD := 16#94F2;   (* Signature *)
    Signature_Sub3_Ack: WORD := 16#A12D;   (* Signature *)
```

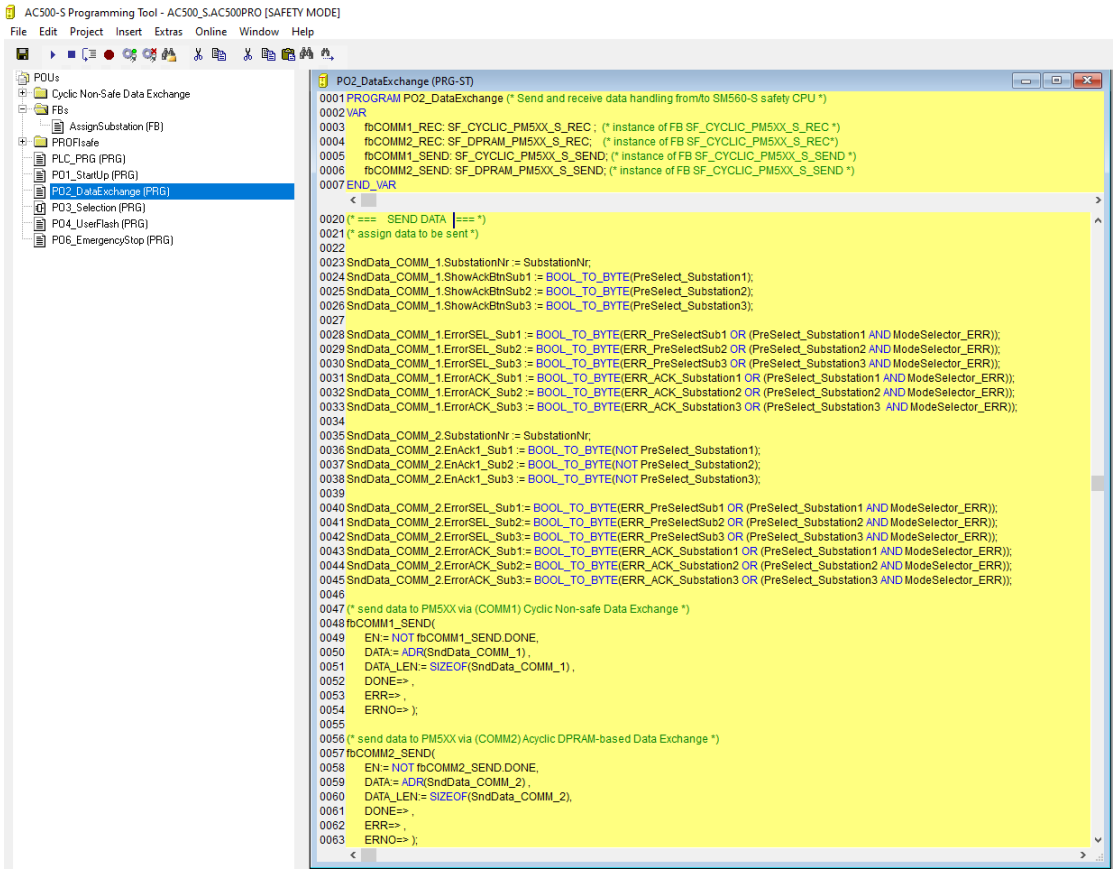
8 Implement data exchange (both “Acyclic DPRAM based data exchange” and “Cyclic non-safe data exchange”) between SM560-S and PM583-ETH to be able to handle user actions from standard HMI on SM560-S safety CPU.

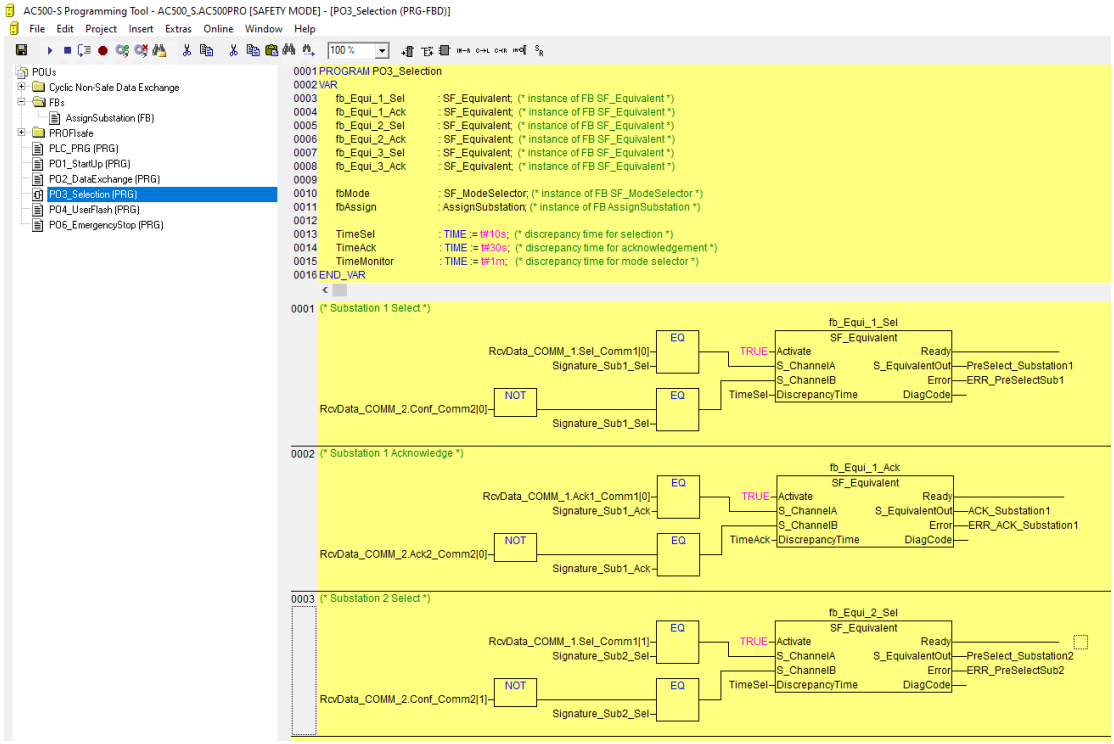
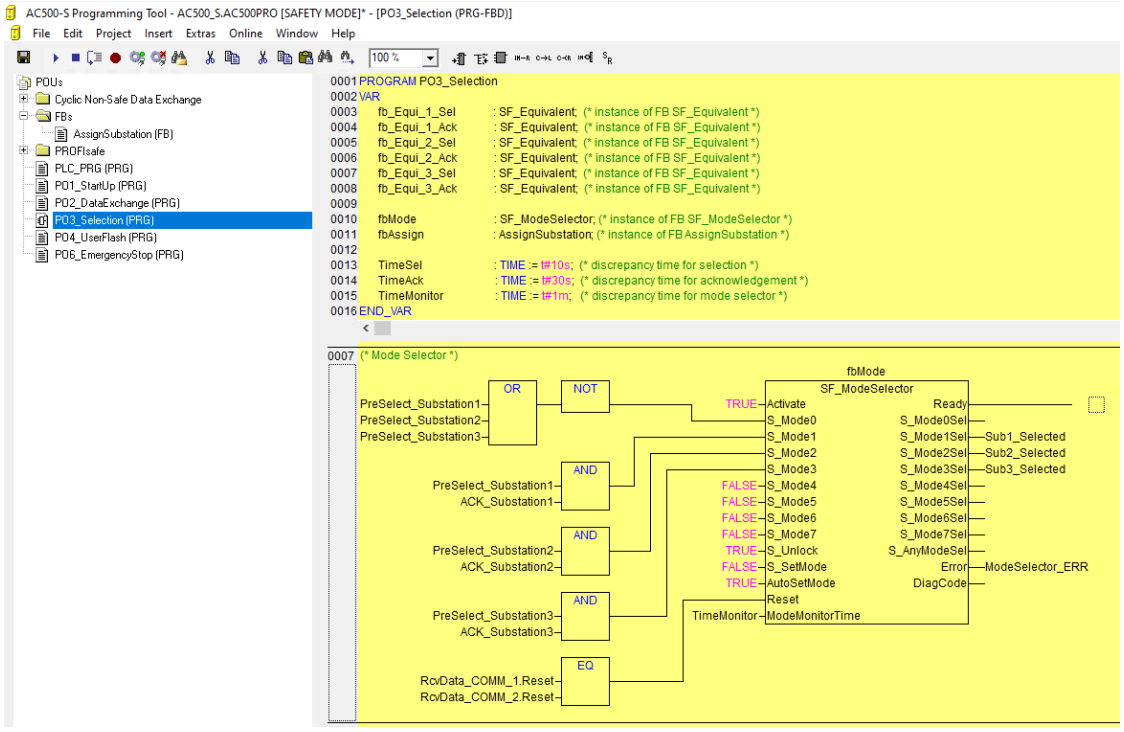
Example of data exchange implementation between SM560-S safety CPU and PM583-ETH:

- Receive data from PM583-ETH



- Send data to PM583-ETH

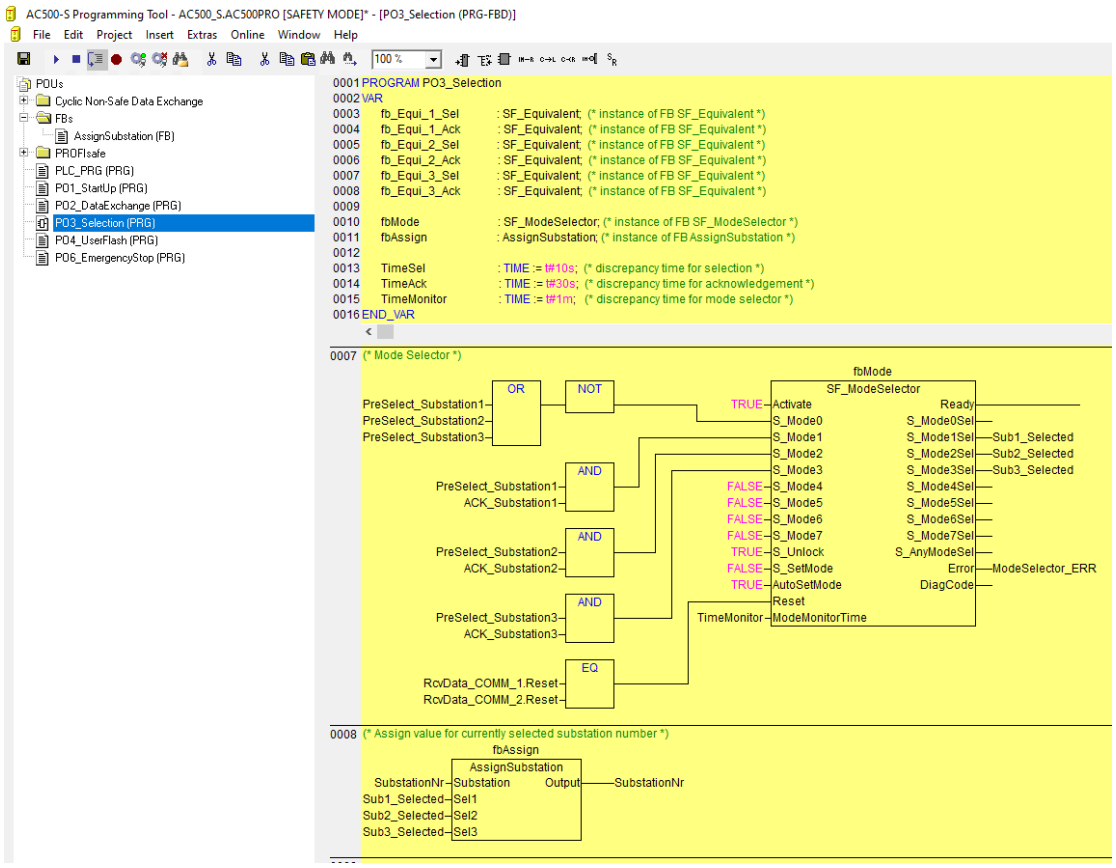


9	Implement 2-channel handling for “Select …” and “Confirm …” buttons as well as “…ACK1” and “…ACK2” buttons using SF_Equivalent FBs [1.] (the negation of received signatures from the second communication path shall be also taken into account). Example of 2-channel handling for buttons from standard HMI: 
10	Implement crane (substation) selection after 2-channel evaluation using SF_ModeSelector FB [1.]. Example of substation selection implementation: 

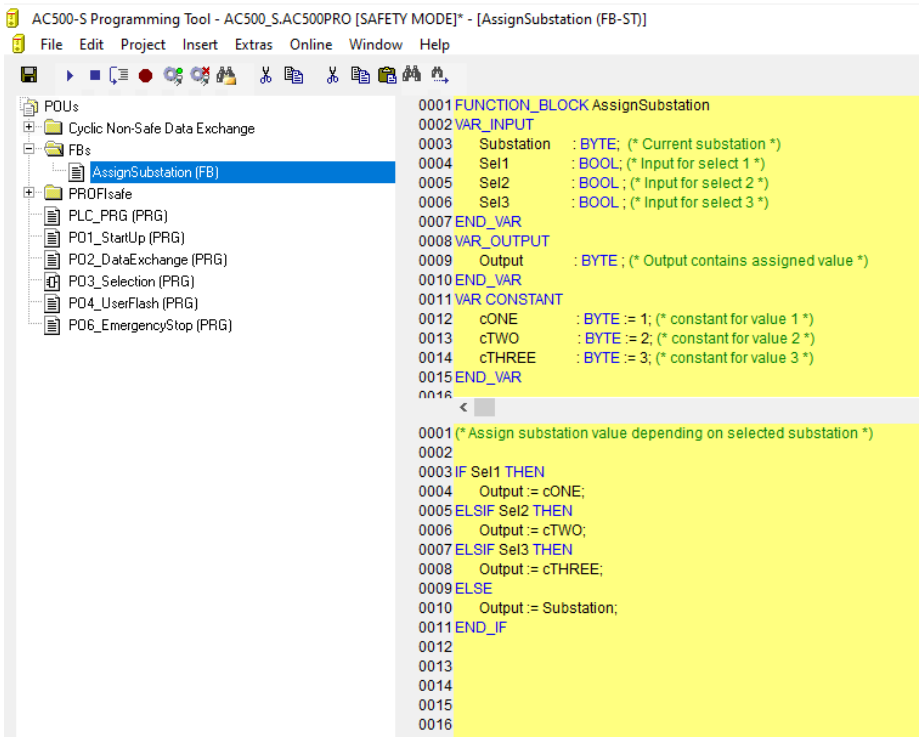
11 Store selected crane (substation) in SM560-S safety CPU flash to be able to keep the selected value after system restart or power failure.

Example of substation selection storage in SM560-S safety CPU flash memory:

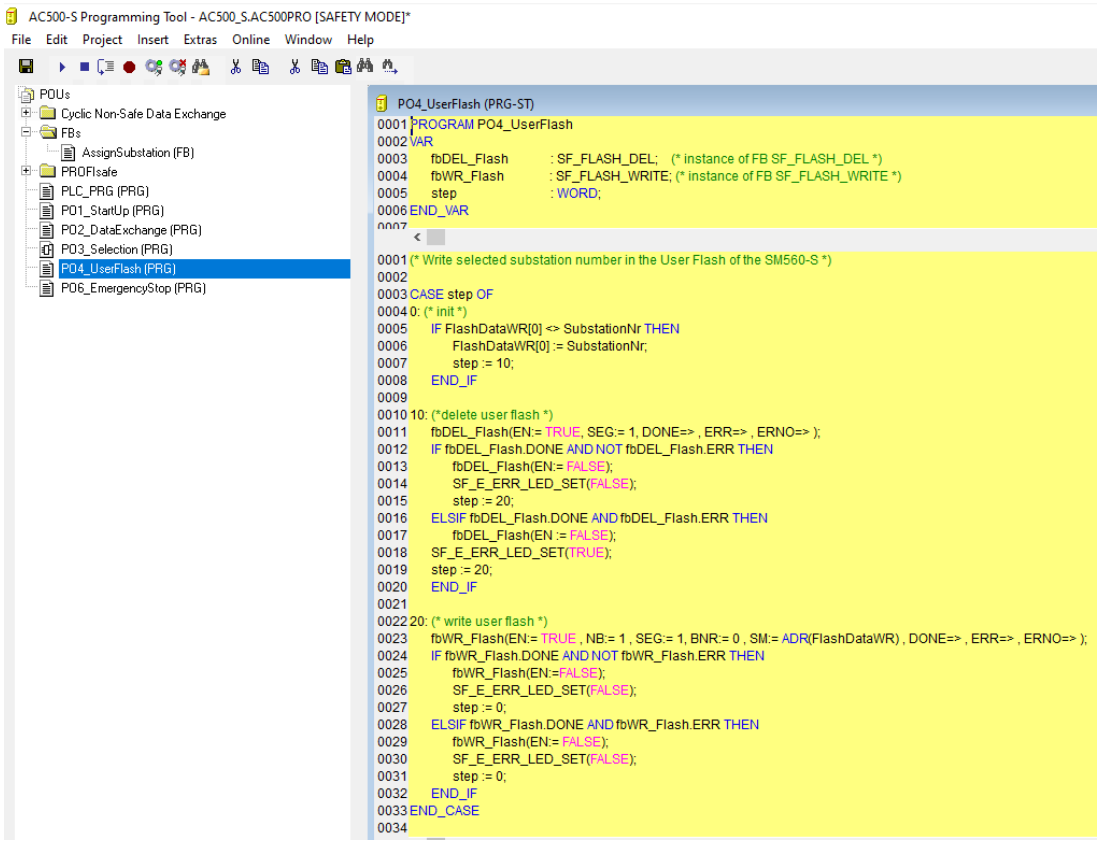
- Prepare selected substation for saving in SM560-S safety CPU flash memory



- Auxiliary FB for selection handling



- Writing of selected substation number in SM560-S flash memory



Depending on the selected standard HMI, the implementation steps may slightly differ.

When the emergency stop button is triggered from the remote control room, the emergency stop signal is transferred using PROFINET/PROFIsafe communication from the safety CPU on the control station to the currently selected crane (substation) only and trigger, e.g., SS1 (Safe Stop 1) with a controlled stop of the motor within a maximum permissible time and SBC (Safe Break Control) implemented locally on the crane using the safety control equipment (safety PLC, safety option in drives and safe break control). This will safely stop this particular machine only. Other not selected machines will not be influenced by this remote emergency stop activation.

3.4.2. Common cause failures

All measures for CCF are already covered for AC500-S safety PLC modules like SM560-S and DX581-S, which are certified for up to PL e (ISO 13849-1) and SIL CL 3 (IEC 62061) safety applications. However, for all AC500 standard (non-safety) modules, like PM583-ETH and standard HMI, the estimation of CCF effect shall be performed using Annex F, ISO 13849-1.

We use below the scoring process and quantification of measures against CCF based on Annex F, ISO 13849-1 for all AC500 PM CPU modules (e.g., PM583-ETH, etc.):

1. Physical separation between signal paths, refer to AC500 design process (see chapter 3.4.3) – **15 points** - Sufficient clearances and creepage distances on printed-circuit

boards

2. Design/application/experience (Protection against overvoltage), refer to AC500 design process (see Chapter 3.4.3) – **15 points**

3. Environmental conditions (EMC, etc.), refer to CE declaration type test report for a given AC500 product – **25 points**

⚠ DANGER

The environmental (EMC, etc.) conditions which are applied for standard PLCs and extreme condition versions (-XC) of PLCs with extended temperature range, shock and vibrations, etc. are fulfilled by relevant AC500 modules in accordance with CE requirements for PLC products. However, depending on the application type and requirements, more detailed analysis of environmental (EMC, etc.) conditions can be required to be able to confirm the assigned points for CCF.

4. Environmental (Other influences - shock, vibration and temperature), refer to CE declaration type test report for a given AC500 product – **10 points**

Total sum of points: **65 points**

As a result, according to ISO 13849-1, CCF requirements for usage of AC500 standard CPU modules are fulfilled because 65 points are needed for this based on Annex F, ISO 13849-1.

⚠ DANGER

The same CCF effect analysis shall be performed for the standard HMI. CCF data shall be obtained from the vendor of the standard HMI with a written statement to confirm the fulfillment of CCF requirements for ISO 13849-1 or any other relevant functional safety standard valid for the given application.

3.4.3. Systematic failures

Measures for the control and avoidance of systematic failures from Annex G, ISO 13849-1 shall be considered for standard (non-safety) HMI and AC500 components separately:

- All these measures are already covered for AC500-S safety PLC modules like SM560-S and DX581-S, which are certified for up to PL e (ISO 13849-1) and SIL CL 3 (IEC 62061) safety applications).

The AC500 product requirements for the control and avoidance of systematic failure in PL d (ISO 13849-1) applications are satisfactorily covered in the proposed implementation through ABB AC500 product development model:

- Usage of Integrated Management System which is ISO 9001 certified by external certification body
- Quality guidelines for software development
- Hardware development process including hardware quality statistics for at least last 3 years
- Continuous analysis of all critical bug entries in the bug tracking system

All used AC500 modules have CE declaration (European Conformity) available which means that they satisfy Low Voltage Directive 2006/95/EG, EMC Directive 2004/108/EG and IEC 61131-2:2007 standard requirements in addition to various other standards (refer to www.abb.com/PLC for details).

⚠ DANGER

The same analysis for the control and avoidance of systematic failure in PL d (ISO 13849-1) applications shall be performed for the standard HMI. The data shall be obtained from the vendor of the standard HMI with a written statement to confirm the fulfillment of relevant ISO 13849-1 requirements.

⚠ DANGER

If standard (non-safety) AC500 or HMI modules are used for safety functions, one still have to perform a systematic failure analysis (refer to Annex G, ISO 13849-1) on the application level for the application part in which these standard (non-safety) modules are used.

3.4.4. Safety function response time

There is no need for safety function response time calculation in the given example, because only safety re-configuration action is considered and not a safety function. For example, if, for any reasons, the selection of the next crane is not possible then there is no dangerous situation, because cranes in automatic mode would be still safely controlled by their local safety PLC and rely on their local safety function implementation.

Despite the fact that safety function response time calculation is not needed for triggering safety actions using standard HMI, one still has to implement appropriate application-specific watchdogs (discrepancy time monitoring) for 2-channel evaluation, mode selector switch and feedback time for standard HMI – safety CPU communication in the application program to have reasonable error reaction times, as it is explained in chapter 3.4.1.

NOTICE

The settings for various watchdogs (discrepancy time monitoring) for 2-channel evaluation, mode selector switch and feedback time for standard HMI – safety CPU communication are application-specific and, thus, shall be defined by responsible safety application developers during the design process and implemented as part of their application program.

3.5. Calculation of the probability of failure and correspondence to PL (ISO 13849-1)

For calculation of the probability of failure for Safety PLC part, we will use ABB FSDT (Functional Safety Design Tool) software (see www.abb.com). Our goal is to confirm that PFHavg for the safety action is below or equal to **1E-6 1/h** (see Table K1 from ISO 13849-1), as it is required for PL d.

NOTICE

MTTFd values for standard HMI and AC500 standard (non-safety) modules were obtained based on MTBF values (contact AC500 technical support at www.abb.com/PLC to obtain MTBF values for selected AC500 modules). The following relation, which complies with ISO 13849-1, was used:

MTTFd = 2 * MTBF

This relationship is based on the following assumptions:

- **It is assumed that statistically only every second failure is a potentially dangerous failure**
- **The permissible ambient conditions are met**
- **Mean Time to Repair (MTTR) is significantly less than the MTBF**

The following MTTFd values were used in the calculation for standard HMI and AC500 standard modules (all AC500 modules which are involved in the communication between the standard HMI and SM560-S safety CPU):

- PM583-ETH → 2 * 170 years = 340 years
- TB511-ETH → 2 * 292 years = 584 years
- Standard HMI → 2 * 22.5 years = 45 years

NOTICE

Typical MTBF values for standard HMIs are ~10 years, which are well below the needed MTBF of ~ 23 years to meet PL d (ISO 13849-1) requirements (as it is further shown in the calculation example). However, one can satisfy SIL CL 2 (IEC 62061) or SIL 2 (IEC 61511) requirements even with standard HMIs, which have MTBF values of ~10 years. The related calculation is not included in this application note.

Using formula D.1 from Annex D, ISO 13849-1, MTTFd value for the input part, which is composed of all hardware components contributing to the safety function and listed above, was calculated:

- MTTFd for input part (without communication) is **37 years**

DC = 99% was used for standard modules because SM560-S safety CPU will take over the function of direct monitoring for input part with standard HMI (2-channel evaluation for selection, evaluation of transferred signature and negated signature values against pre-defined and stored signature values in the SM560-S safety CPU (SIL 3, PL e) memory flash and later mode selector switch evaluation).

All safety values for SM560-S safety CPU are available from the TUV certification process and are a part of the ABB FSDT library.

In addition to MTTFd values for hardware components, one has to include also two communications parts (see Figure 4), which have diverse (signature and negated signature) data transmission using different communication protocols:

- Standard HMI → PM583-ETH (2 times: 1 for “Select …” and “Confirm …” buttons on the standard HMI and 1 for “… ACK1” and “… ACK2” buttons on the standard HMI)
- PM583-ETH → SM560-S (2 times: 1 for “Select …” and “Confirm …” buttons on the standard HMI and 1 for “… ACK1” and “… ACK2” buttons on the standard HMI)

We assume the bit error probability of 1E-2 1/h for standard communication based on [5]. It means that due to the redundant data transfer (signature and negated signature are separately transferred) and two separate groups of actions (1 for “Select …” and “Confirm …” buttons on the standard HMI and 1 for “… ACK1” and “… ACK2” buttons on the standard HMI), the probability of a dangerous failure per hour is the multiplication of 1E-2 1/h four times which results in PFHavg = 1E-8 1/h for communication (Standard HMI → PM583-ETH → SM560-S).

Figure 13 shows a screenshot from ABB FSDT safety calculation with all related data from the presented example.

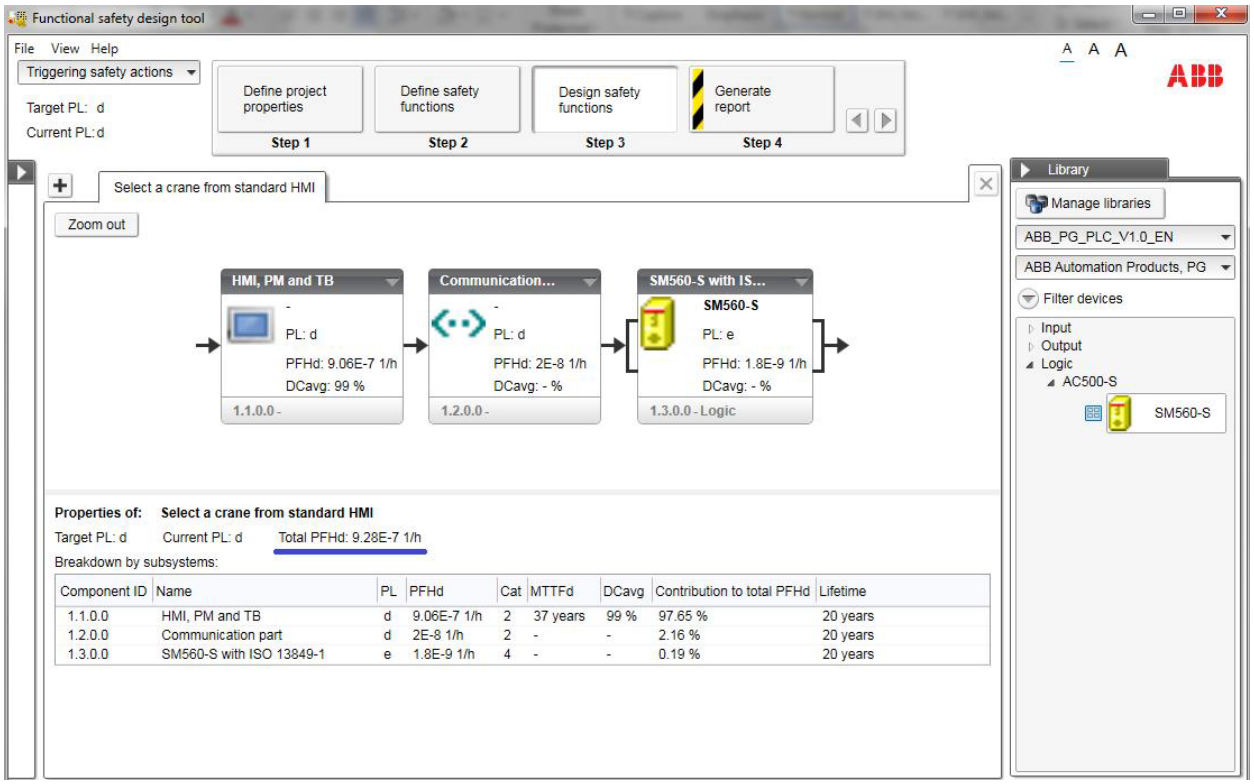


Figure 13. FSDT safety calculation for the example with triggering safety actions from standard HMI

The safety calculation result (see Figure 13) is the PFHavg value of **9.28E-7 1/h** for triggering safety actions from standard HMI.

NOTICE

The mission time for the presented example is 20 years and cannot be extended because standard components are used in the input part of the safety function.

This value is smaller than the required limit value PFHavg **1E-6 1/h** for PL d (ISO 13849-1), which means that the proposed approach is suitable for usage in safety application up to PL d (ISO 13849-1).

NOTICE

ISO 13849-1 functional safety standard sets the highest requirements (Category 2) to standard HMIs and requires MTBF values of 22.5 years and above.

However, one can satisfy SIL CL 2 (IEC 62061) or SIL 2 (IEC 61511) requirements even with standard HMIs, which have MTBF values of ~10 years. The related calculation is not included in this application note.

4. Conclusion

The results of our safety analysis confirm that standard HMI (provided that safety analysis similar to ours in this example is satisfactory) with AC500-S safety PLC can be used for the selection of substations, machines or pre-defined safely limited values in functional safety applications up to PL d (ISO 13849-1).

⚠ DANGER

The presented approach enables the usage of standard HMI with AC500-S safety PLC in functional safety applications up to PL d (ISO 13849-1). However, the implementation, verification and validation of the approach in practice according to ISO 13849-1 or any other functional safety standard will remain always application specific because standard (non-safety) modules (HMI and standard CPU) becomes involved in the execution of functional safety functions. Thus, the responsibility for correct implementation, verification and validation of the proposed approach is fully within the end-customer responsibility.

The functional safety calculation and analysis according to IEC 62061 or IEC 61511 standards can be similarly done, if required.

3ADR020158K0201, REV C, en_US, 2023/04/26

ABB AG
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444
Fax: +49 62 21 701 1382
Mail: plc.support@de.abb.com
www.abb.com/plc