

# Triggering Fail-safe Actions on the Basis of Non-safety HMI

Distributed Safety

Application Description • March 2012

## Applications & Tools

Answers for industry.

**SIEMENS**

## Siemens Industry Online Support

This entry originates from the Siemens Industry Online Support. The following link takes you directly to the download page of this document:

<http://support.automation.siemens.com/WW/view/en/59012254>

### Caution:

The functions and solutions described in this entry are mainly limited to the realization of the automation task. In addition, please note that suitable security measures in compliance with the applicable Industrial Security standards must be taken if your system is interconnected with other parts of the plant, the company's network or the Internet. For further information on this issue, please refer to Entry ID 50203404.

<http://support.automation.siemens.com/WW/view/en/50203404>.

If you have any questions regarding this document, please send us an e-mail to the following address:

<mailto:online-support.industry@siemens.com>

For further information on this topic you may also actively use our Technical Forum in the Service & Support Portal. Add your questions, suggestions and problems and discuss them in our large forum community:

<http://www.siemens.de/forum-applikationen>

**SIEMENS**

**SIMATIC**

**Safety with non safety HMI**

**Task**

**1**

**Solution**

**2**

**Functional Mechanisms  
of this Example**

**3**

**Configuration and  
Settings**

**4**

**Installation**

**5**

**Operation of the Example  
Project**

**6**

**Standards Consideration  
in Accordance with IEC  
62061**

**7**

**References**

**8**

**History**

**9**

## Warranty and Liability

### Note

The application examples are not binding and do not claim to be complete regarding configuration, equipment and any eventuality. The application examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not discharge you from the obligation of safe handling during application, installation, operation and maintenance. By using these application examples, you acknowledge that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these application examples at any time and without prior notice. If there are any deviations between the recommendations provided in this application example and other Siemens publications – e.g. catalogs – the contents of the other documents have priority.

We do not accept any liability for information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, setting and performance data etc. described in this application example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency, or breach of fundamental contractual obligations. However, claims for damages arising from a breach of fundamental contractual obligations shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions do not imply a change in the burden of proof to your detriment.

These application examples or excerpts thereof must not be handed on or copied without express authorization by Siemens Industry Sector.

# Table of Contents

<b>Warranty and Liability .....</b>	<b>4</b>
<b>1 Task.....</b>	<b>7</b>
1.1 Overview .....	7
1.2 Requirements for this safety function example .....	9
<b>2 Solution.....</b>	<b>10</b>
2.1 Overview of the overall solution .....	10
2.2 Description of the core functionality .....	11
2.2.1 Core functionality of the example .....	11
2.2.2 The applied safety concept .....	12
2.2.3 Overview and description of the visualization user interface .....	13
2.3 Hardware and software components used.....	16
<b>3 Functional Mechanisms of this Example .....</b>	<b>18</b>
3.1 State machine and program structure of the control station .....	18
3.1.1 State machine of the control station.....	18
3.1.2 Program structure of the control station .....	20
3.2 State machine and program structure of the substation .....	21
3.2.1 State machine of the substation .....	21
3.2.2 Program structure of the substations .....	22
3.3 Error detection via path 1 and path 2 .....	23
3.3.1 Error detection via path 1 .....	23
3.3.2 Error detection via path 2 .....	26
3.3.3 Joining of paths 1 and 2 .....	30
3.4 Acknowledgement concept .....	31
3.5 Behavior in the event of communication errors.....	32
3.6 Life bit in the "Coordination" area pointer.....	33
3.6.1 Context .....	33
3.6.2 Implementation in the F-program .....	35
<b>4 Configuration and Settings .....</b>	<b>37</b>
4.1 Address overview .....	37
4.2 Hardware configuration of STEP 7.....	39
4.2.1 Settings of the F-CPU .....	39
4.2.2 Settings of the F-DI .....	40
4.2.3 Collective signatures of the safety programs .....	40
4.3 Fail-safe communication .....	41
4.3.1 Configuration overview.....	41
4.3.2 Exchanging the user data .....	43
4.3.3 Integrating the F-communication DBs in the STEP 7 program.....	44
4.3.4 Data structure of the used F-communication DBs .....	45
4.4 Messages configuration .....	48
4.5 Indication of the state of the substation on the HMI of the control station .....	49
4.6 Creating the "Coordination" area pointer .....	50
<b>5 Installation.....</b>	<b>52</b>
5.1 Hardware installation.....	52
5.2 Software installation .....	52
5.3 Setting the PG/PC interface .....	52
5.4 Installation of the example project.....	53
<b>6 Operation of the Example Project.....</b>	<b>55</b>
6.1 Variables table (VAT).....	55
6.2 Scenario A: Switching to another substation .....	56

## Table of Contents

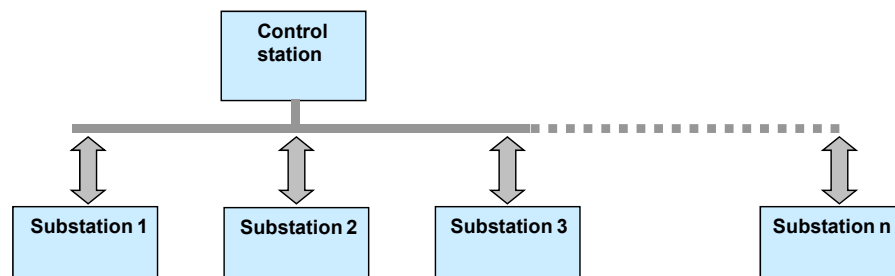
6.2.1	Correct switching .....	56
6.2.2	Incorrect switching .....	56
6.3	Scenario B: Triggering an emergency stop in the control station .....	57
6.4	Scenario C: Triggering an emergency stop in the substation .....	57
6.5	Scenario D: Creating a communication error .....	58
6.5.1	F-CPU of substation 1 cut off from communication .....	58
6.5.2	HMI of the control station cut off from communication .....	60
6.5.3	HMI of substation 1 cut off from communication .....	61
<b>7</b>	<b>Standards Consideration in Accordance with IEC 62061 .....</b>	<b>62</b>
7.1	Definition of safety function and SRCF .....	62
7.2	SRECS and SRCF .....	63
7.2.1	SRECS executes SRCF 1 .....	64
7.2.2	SRECS executes SRCF 2 .....	66
7.2.3	SRECS executes SRCF 3 .....	68
7.3	SIL of the safety function for SRCF 1 .....	70
7.3.1	SIL CL and PFH <sub>D</sub> of subsystem 1 .....	70
7.3.2	SIL CL and PFH <sub>D</sub> of subsystem 2 .....	72
7.3.3	SIL CL and PFH <sub>D</sub> of subsystem 3 .....	72
7.3.4	Result for SRCF 1 .....	75
7.4	SIL of the safety function for SRCF 2 .....	75
7.4.1	SIL CL and PFH <sub>D</sub> of subsystem 4 .....	75
7.4.2	SIL CL and PFH <sub>D</sub> of subsystem 5 .....	75
7.4.3	SIL CL and PFH <sub>D</sub> of subsystem 6 .....	76
7.4.4	Result for SRCF 2 .....	76
7.5	SIL of the safety function for SRCF 3 .....	77
7.5.1	SIL CL and PFH <sub>D</sub> of subsystem 7 .....	77
7.5.2	SIL CL and PFH <sub>D</sub> of subsystem 8 .....	78
7.5.3	SIL CL and PFH <sub>D</sub> of subsystem 9 .....	78
7.5.4	Result for SRCF 3 .....	79
7.6	Summary .....	79
<b>8</b>	<b>References .....</b>	<b>80</b>
8.1	Bibliographic references .....	80
8.2	Internet links .....	80
<b>9</b>	<b>History .....</b>	<b>80</b>

# 1 Task

## 1.1 Overview

### Introduction

Many industrial automation solutions comprise data structures in which a control station communicates with various substations.



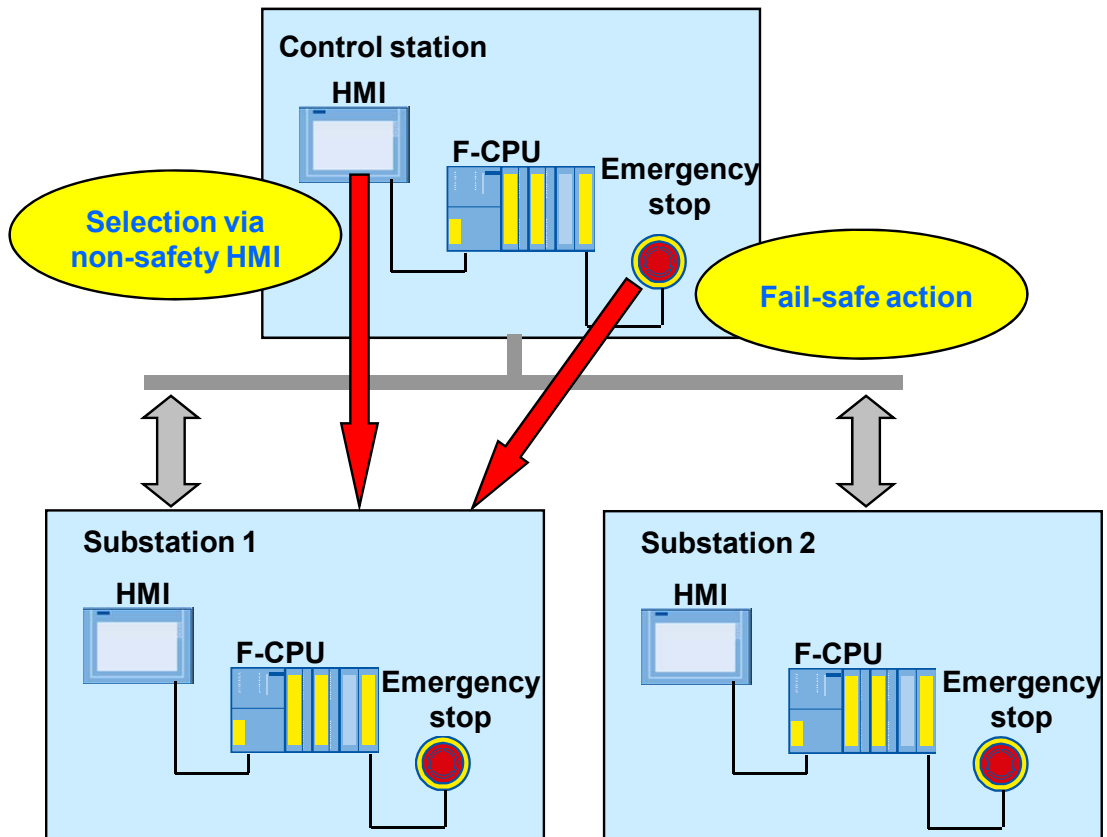
The control station can select one or several substations to execute various actions there (specify setpoints, request actual values, etc.). The selection of these substations is often made via an HMI (panel).

Transferring this principle to a task definition in the safety system can lead to the following requirements:

- A substation is to be selected via an HMI (panel) of the control station.
- An emergency stop triggered in the control station is to affect the selected substation only.

Thus, a **fail-safe** action (triggering of an emergency stop) is required, which is based on a **not safe** action (selection of the substation via a non-safety HMI). It is therefore obvious that additional measures have to be integrated in this concept for safety requirements.

## Overview of the automation task



The figure above shows the task definition for the present safety function example:

A substation (here: 1 or 2) is selected via an HMI of the control station. If, for example, (as shown in the figure) substation 1 is selected and an emergency stop is triggered in the control station, the emergency stop is to affect substation 1 only.

The requested concept of allowing a fail-safe action on the basis of a non-safety HMI can be applied in various applications, e.g.:

- Ship locks and weirs
  - The requirements of the European Machinery Directive also apply to locks and weirs.
  - Fail-safe actions (e.g. emergency stop) can be triggered from a spatially far off (several kilometers) control station, affecting solely the selected substation (e.g. lock on a dam).
- Selection of various (container) cranes from the driver's cab



## 1.2 Requirements for this safety function example

### Requirements due to the automation task

Requirement	Explanation
<ul style="list-style-type: none"> <li>One of two substations is to be selected via the HIM of the control station.</li> <li>At any time, always exactly one substation is to be selected.</li> <li>An emergency stop triggered in the control station is to affect solely the actively selected substation.</li> <li>This concept is to meet the safety requirements.</li> <li>If an error occurs (signature error, communication error, emergency stop), a corresponding error bit is to be provided to the user.</li> </ul>	<b>Core requirements</b> of the example to show how a non-safety HMI can be integrated in a fail-safe action.
<ul style="list-style-type: none"> <li>An acknowledgement is to be performed at the place where the error occurred. Example:             <ul style="list-style-type: none"> <li>An emergency stop triggered in the control station requires an acknowledgement in the control station.</li> <li>An emergency stop triggered in a substation (local emergency stop) requires an acknowledgement in this substation.</li> </ul> </li> <li><b>Exception:</b> Signature errors in a substation are sent to the control station and need to be acknowledged there (see "Note").</li> <li>The substations do not communicate with each other.</li> <li>Control station and substations have the same structure:             <ul style="list-style-type: none"> <li>HMI</li> <li>F-CPU</li> <li>Emergency stop control device</li> </ul> </li> </ul>	<b>Conventions</b> which are already prepared in this example as described on the left but can be varied depending on the individual requirements.

### "Signature" and "signature error"

The terms "signature" and "signature error" are frequently mentioned in this document. In the following it is explained what is to be understood by that.

Term	Explanation
Signature	Numerical value of the INTEGER type. Depending on the selected substation, a certain signature is sent from the control station to this substation. In the corresponding substation, this signature is stored as setpoint (in the F-program), where it is compared for equality with the received signature. In the case of inequality...
Signature error	...this is referred to as signature error.

#### NOTICE

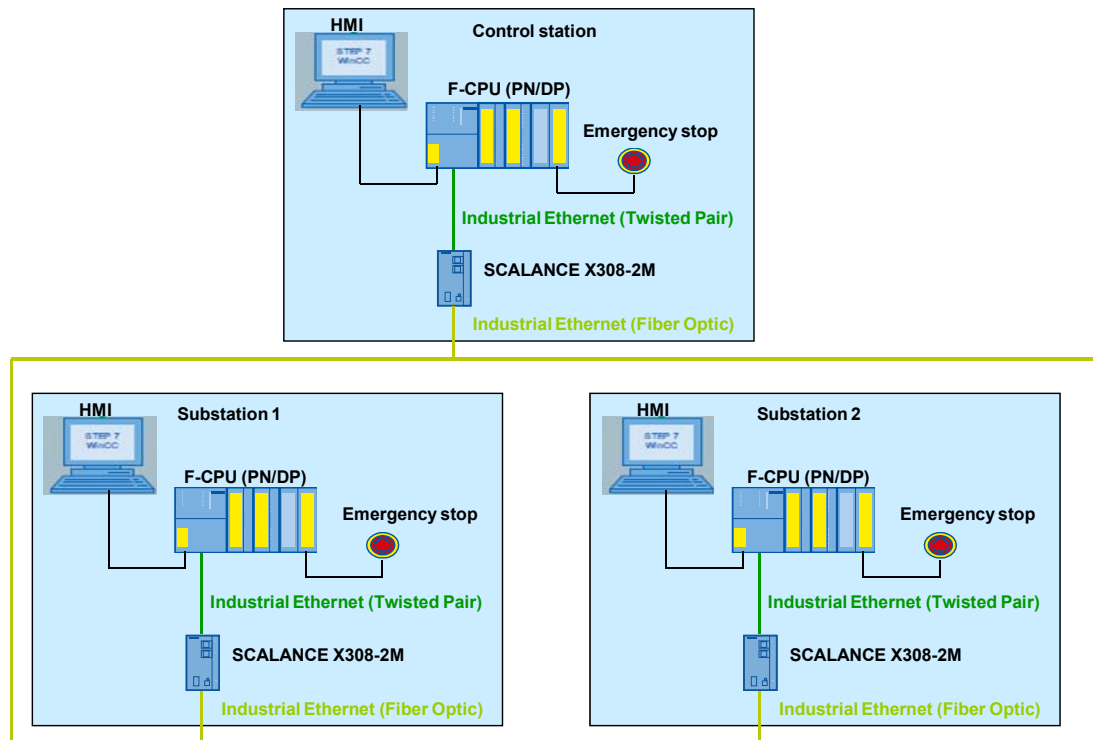
In this example, some fail-safe actions are only triggered after configured delay times. You have to assess this aspect individually for your application and requirements.

## 2 Solution

### 2.1 Overview of the overall solution

#### Schematic view

The following figure gives a schematic overview of the most important components of the solution:



#### Note

In our test setup we refrained from using fiber-optic cables.

#### Advantages

This safety function example offers you the following advantages:

- Integration of the functionality of a non-safety HMI in a workable safety concept
- Fail-safe communication via standard bus cables
- Runnable STEP 7 and WinCC flexible project

#### Required knowledge

The following knowledge is required:

- Basic experience with STEP 7 and Distributed Safety
- Basic experience with WinCC flexible
- Basic knowledge of the standards IEC 62061 and ISO 13849-1

## 2.2 Description of the core functionality

### 2.2.1 Core functionality of the example

The core functionality of this safety function example is the demonstration of a safety concept in which a non-safety HMI forms the basis for triggering fail-safe actions (here: emergency stop).

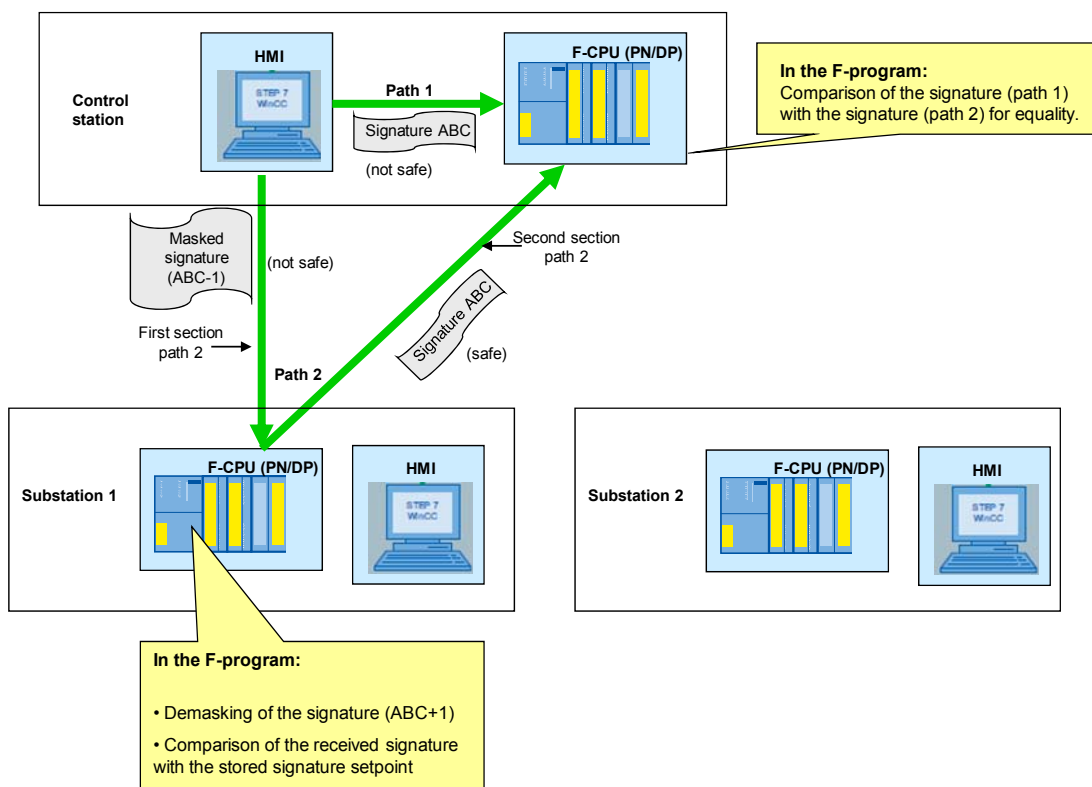
This safety concept is explained in this chapter. In the subsequent chapter "Functional mechanisms", this explanation is deepened, e.g. with notes on the programming solution.

#### Note

The core functionalities described here are already implemented in the provided STEP 7 project.

The following figure of the overall solution serves for explaining the safety concept. The figure is described in the following section 2.2.2. For reasons of clarity,

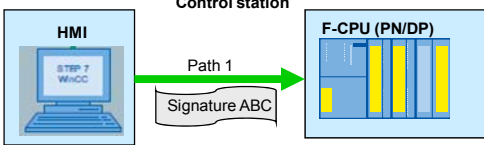
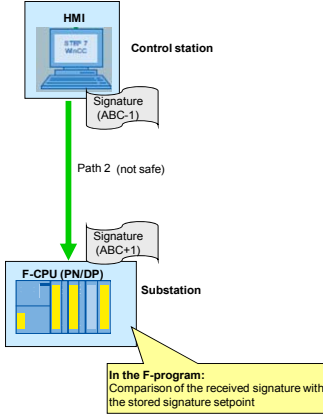
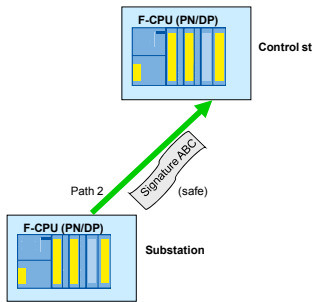
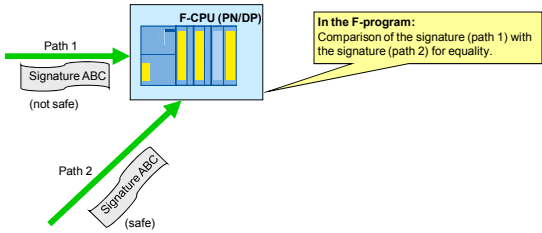
- the cabling is not shown,
- it is assumed that substation 1 has been selected by the control station.



### 2.2.2 The applied safety concept

#### Description of the safety concept

The description of the safety concept is based on the figure used in section 2.2.1.

No.	Description	Explanation / Figure
1	From the HMI of the control station, the substation (here: 1) is selected via a button.	All statements made here apply analogously for a selection of substation 2.
2	After substation 1 has been selected, a signature ABC is transmitted to the F-CPU of the control station ( <b>path 1</b> ).	 <ul style="list-style-type: none"> <li>The signature ABC is a numerical value of the INTEGER data type stored in the HMI.</li> <li>The transmission via path 1 is not safe (configured connection in WinCC flexible).</li> </ul>
3	From the HMI of the control station, a masked signature (ABC-1) is transmitted to the F-CPU of the selected substation via a second button ( <b>path 2</b> ). In the F-CPU of the substation, the transmitted signature is demasked again (ABC+1) and compared for equality with a signature setpoint placed in the substation.	 <ul style="list-style-type: none"> <li>The signature ABC is a numerical value of the INTEGER data type stored in the HMI.</li> <li>The transmission via this section of path 2 is not safe (configured connection in WinCC flexible).</li> </ul>
4	The receiving substation of No. 3 sends the received signature to the F-CPU of the control station ( <b>path 2</b> ).	 <p>The transmission via this section of path 2 is safe (fail-safe communication via S7 connections).</p>
5	In the F-CPU of the control station, the signatures received via path 1 and path 2 are compared for equality. In the case of equality: the correct substation is selected.	 <p>In the F-program: Comparison of the signature (path 1) with the signature (path 2) for equality.</p>

**Why is this concept safe?**

Although the selection of the substation from the control station is made via a non-safety HMI, the stored signature (numerical value of the INTEGER data type) reaches the F-CPU of the control station on two independent paths. The F-CPU of the selected substation also takes on tasks for error detection.

Not safe is first of all path 1 and the first section of path 2. There, data corruptions of the signature can theoretically occur. In this example, however, this is safely revealed through the following proprietary mechanisms:

**Error detection in the substation**

In the F-CPU of each substation, an individual setpoint is stored (safely) for the signature. This is compared with the signature received from the F-CPU control station (first section of path 2).

The comparison takes place in the F-program of the F-CPU of the substation. If the received signature does not correspond to the setpoint, this is detected as an error in the substation. This error information is sent to the F-CPU of the control station by fail-safe communication via S7 connections (second section of path 2).

An additional reasonable measure is to send the masked signature via the not safe section 1 of path 2, i.e. with a different signature than via path 1 (here: signature is subtracted by 1). In the F-CPU of the substation, the incoming masked signature is demasked again, i.e. the incoming signature is added by 1 (in the F-program), so that in the case of absence of errors the signature via section 1 of path 2 equals the signature setpoint fixedly stored in the F-CPU of the substation.

**Error detection in the control station**

The correctness of the signature received in the F-CPU of the control station via path 2 is ensured with the measure described above. The signature transmitted not safely via path 1 is now compared with the signature via path 2. If the signatures are not equal, this is interpreted as an error and a corresponding error bit is set.

**NOTICE**

**If you want to add further substations to the example, make sure that the signature setpoints of the individual substations are different.**

**2.2.3 Overview and description of the visualization user interface****General**

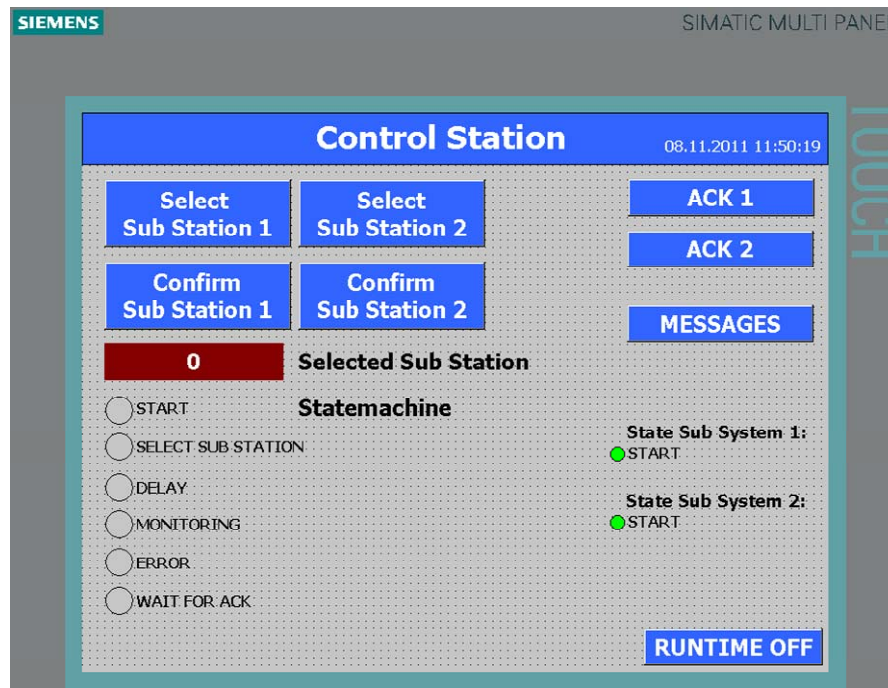
The control station and the two substations each have an HMI. The visualization user interfaces of the HMIs of the substations are structured identically.

In the following, the visualization user interfaces of the HMIs of the control station and substations are described.

## 2 Solution

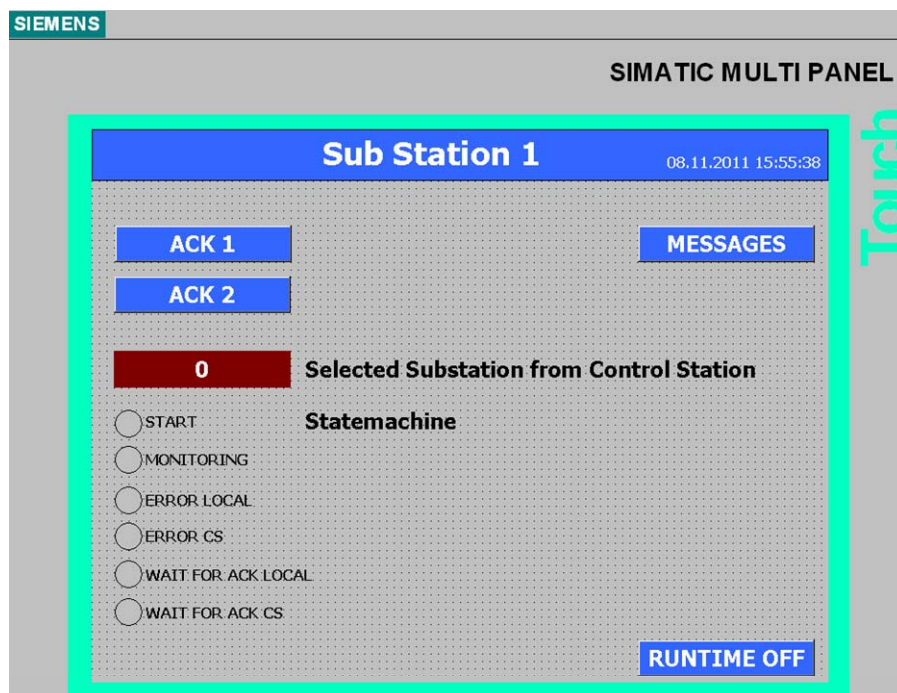
### 2.2 Description of the core functionality

#### HMI of the control station



Selection button	Function	Explanation
Select Sub Station 1	Selection of the substation (path 1)	Two buttons required for safe error detection
Confirm Sub Station 1	Confirmation of the substation (path 2)	
ACK 1 ACK 2	<ul style="list-style-type: none"> <li>Fail-safe acknowledgement via standard panel</li> <li>Also for the reintegration of passivated F-I/O</li> </ul>	See also section 3.4 "Acknowledgement concept"
MESSAGES	Switching to a new screen on which configured messages are displayed.	
RUNTIME OFF	Termination of the runtime on the HMI	
Indications	Function	Explanation
0 Selected Sub Station	Indication of the currently selected substation.	In operation always 1 or 2.
Statemachine <input type="radio"/> START <input type="radio"/> SELECT SUB STATION <input type="radio"/> DELAY <input type="radio"/> MONITORING <input type="radio"/> ERROR <input type="radio"/> WAIT FOR ACK	State machine: At any time in operation, the control station is in exactly one of six possible states.	The state machine with the respective six states is explained in detail in chapter 3 "Functional Mechanisms of this Example".
State Sub System 1: <input checked="" type="radio"/> START State Sub System 2: <input checked="" type="radio"/> START	The processes in the substations are also realized according to a state machine. The current state of each substation is indicated on the HMI of the control station (see screenshot to the left).	

## HMI of the substation

**Note**

The figure above shows the visualization user interface of substation 1. The visualization user interface of station 2 has an identical structure with regard to the selection buttons and indications.

Selection buttons	Function	Explanation
<div>ACK 1</div> <div>ACK 2</div>	<ul style="list-style-type: none"> <li>Fail-safe acknowledgement via standard panel</li> <li>Also for the reintegration of passivated F-I/O</li> </ul>	See also section 3.4 "Acknowledgement concept"
MESSAGES	Switching to a new screen on which configured messages are displayed.	
RUNTIME OFF	Termination of the runtime on the HMI	
Indications	Function	Explanation
<div>0 Selected Sub Station</div> <div> <div>START</div> <div>MONITORING</div> <div>ERROR LOCAL</div> <div>ERROR CS</div> <div>WAIT FOR ACK LOCAL</div> <div>WAIT FOR ACK CS</div> </div>	Indication of the substation currently selected by the control station.  State machine: At any time in operation, the substation is in exactly one of six possible states.	In operation always 1 or 2.  The state machine with the respective six states is explained in detail in chapter 3 "Functional Mechanisms of this Example".



## 2.3 Hardware and software components used

The following components were used to reproduce the safety function example.

**Note**

It is possible to use similar products deviating from the list.  
In such a case, please mind that changes in the example code might be required (e.g. other addresses) and that a changed PFH<sub>D</sub> value might also change the SIL.

### Hardware components

#### Control station

Component	Qty.	order number	Note
Power supply	1	6S7307-1EA00-0AA0	
CPU 317F-2 PN/DP	1	6ES7317-2FK14-0AB0	
SM 326 DI	1	6ES7326-1BK02-0AB0	
Emergency stop mushroom pushbutton	1	3SB3801-0EG3	
MULTI PANEL MP 277 10" Touch	1	6AV6643-0CD01-1AX0	

#### Substation 1

Component	Qty.	order number	Note
Power supply	1	6S7307-1EA00-0AA0	
CPU 315F-2 PN/DP	1	6ES7315-2FH13-0AB0	
SM 326	1	6ES7326-1BK02-0AB0	
Emergency stop mushroom pushbutton	1	3SB3 801-0EG3	
MULTI PANEL MP 370 Touch-12 TFT	1	6AV6545-0DA10-0AX0	

#### Substation 2

Component	Qty.	order number	Note
Power supply	1	6S7307-1EA00-0AA0	
CPU 315F-2 PN/DP	1	6ES7315-2FH13-0AB0	
SM 326	1	6ES7326-1BK02-0AB0	
Emergency stop mushroom pushbutton	1	3SB3 801-0EG3	
MULTI PANEL MP 370 Touch-12 Z	1	6AV6545-0DA10-0AX0	

#### Further hardware

Component	Qty.	order number	Note
SCALANCE X208	1	6GK5208-0BA00-2AA3	



**Software components**

Component	Qty.	order number	Note
SIMATIC STEP 7 V5.5	1	6ES7810-4CC10-0YA5	Floating license for 1 user
SIMATIC Distributed Safety V5.4 + SP5	1	6ES7833-1FC02-0YA5	Floating license for 1 user
SIMATIC WinCC flexible 2008 SP2	1	6AV6613-0AA51-3CA5	Floating license For the configuration of SIMATIC panels and WinCC flexible 2008 Runtime

**Example files and projects**

The following list comprises all files and projects used in this example.

Component	Note
59012254_non_safety_hmi_v10.zip	This zip file contains the STEP 7 and WinCC flexible project.
59012254_non_safety_hmi_v10_de.pdf	This document

## 3 Functional Mechanisms of this Example

### General overview

The functionalities for the control station and substations are each represented in a state machine (also referred to as state graph). The STEP 7 program is structured according to this state machine. For that reason, the functional mechanisms are explained as follows in this chapter:

- State machine and program structure
  - of the control station (section 3.1)
  - of the substation (section 3.2)
- From section 3.3 on, the described functionalities are explained in more detail down to the program level.

### Note

The terms SIGNATURE or SIG refer to numerical values of the INTEGER data type (except chapter 4.2.3), which are part of the safety concept presented here. In this context, they have nothing to do with the collective signature of all F-blocks or the signature of individual F-blocks resulting from the generation of the F-program.

## 3.1 State machine and program structure of the control station

### 3.1.1 State machine of the control station

#### General information on the state machine

The state machine is a representation of all possible states (e.g. error, waiting for acknowledgement, etc.) which might occur in an application. Only one state can be active at a time.

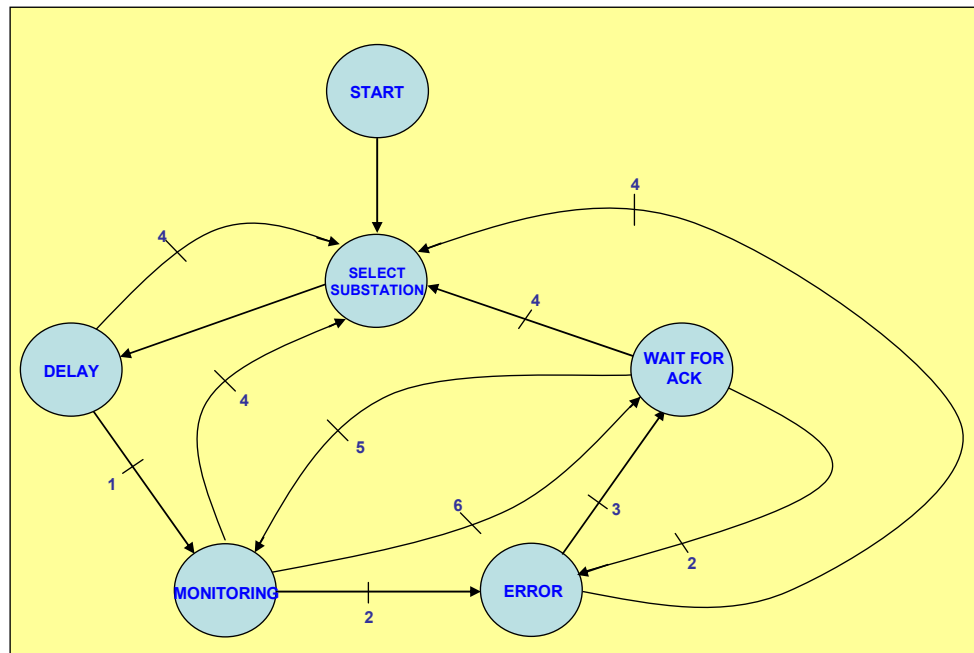
A state is left (i.e. a new state becomes active) when a transition (or also a switching condition) is fulfilled.

The advantages of a state machine are the following:

- All states which might occur are known before the implementation in a program
- Simple implementation of the state machine in a program
- Facilitated troubleshooting
- Simple expandability of the program

The state machine is implemented in the F-block F\_STATEMACHINE (FB4).

## State machine



## States of the state machine

State	Description of the state
	After switch-on, START is reached automatically. Without transition, SELECT_SUBSTATION is reached automatically.
	Is jumped at when a substation is selected on the HMI of the control station.
	Start of a switch-on delay procedure. This is required after the selection of a substation. Otherwise, a signature error would occur (will be explained later in detail).
	Normal operation (no error, a substation is selected).
	Error pending (e.g. incorrect signature detected) or emergency stop triggered.
	Error has been fixed; acknowledgement possible.

## Note

A state can only reach another state via the indicated transition. For example, it is never possible to get from the DELAY state directly to the ERROR state.

### 3 Functional Mechanisms of this Example

#### 3.1 State machine and program structure of the control station

##### Transitions of the state machine

Transition	Description of the transition
1	Switch-on delay procedure
2	At least one of the following errors occurred: <ul style="list-style-type: none"> <li>Signature error</li> <li>Communication error</li> </ul> Or the emergency stop of the control station was triggered.
3	Error fixed or emergency stop unlocked.
4	On the HMI of the control station, the button for selecting a substation is pressed.
5	Acknowledgement: On the HMI of the control station, the buttons ACK1 and ACK2 are pressed in succession (and within one minute).
6	Selected substation awaits acknowledgement by the control station.

#### 3.1.2 Program structure of the control station

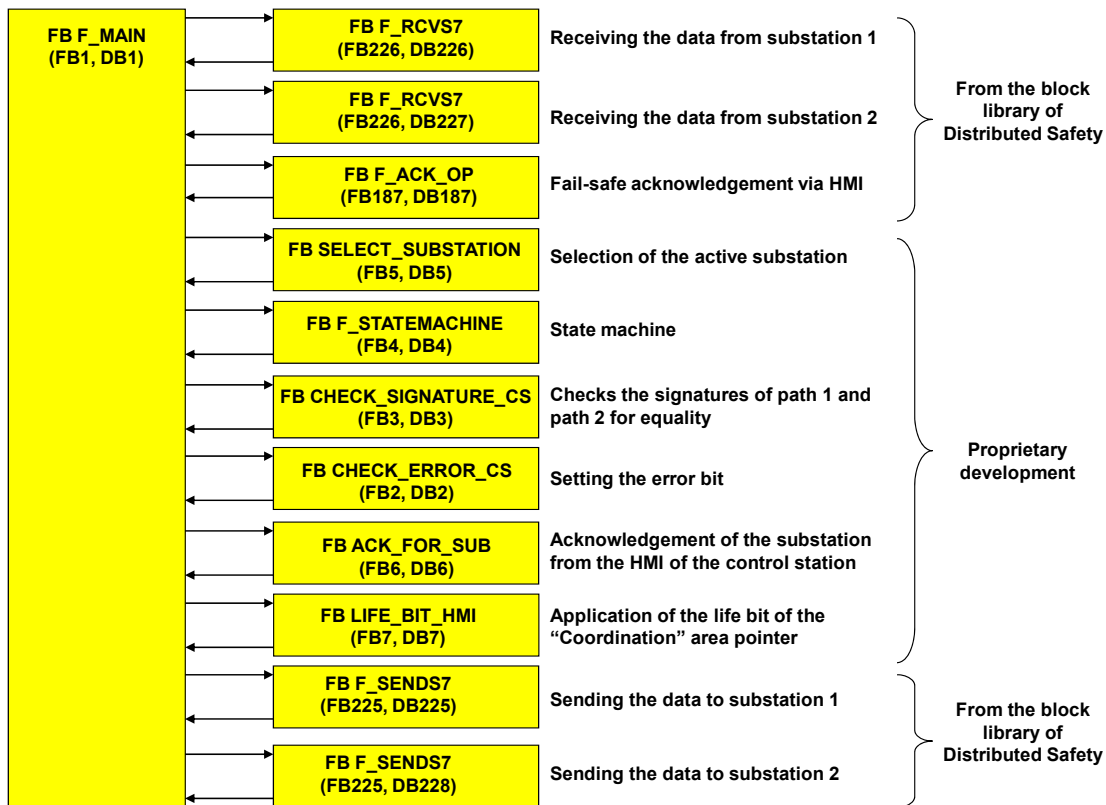
##### Standard program

The standard program basically consists of the following blocks:

- OB100: Preconfigured so that substation 1 is active after startup.
- FB MESSAGES\_HMI\_CS (FB9, DB9): Configured message texts for the HMI.

##### F-program

The following is the call sequence of the F-runtime group with brief explanations:



## 3.2 State machine and program structure of the substation

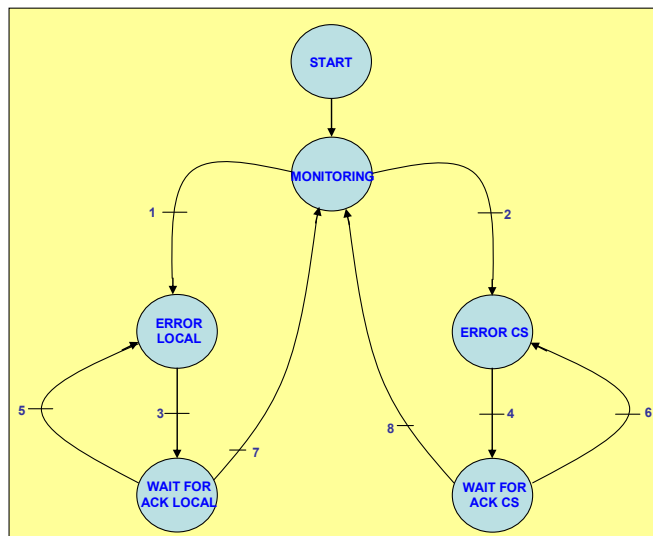
### 3.2.1 State machine of the substation

#### General information on the state machine

The same statements as in section 3.1.1 "State machine of the control station" apply.

Since the substations 1 and 2 are structured identically, they have the same state machine as well as the same program structure. Therefore, the following statements apply to substation 1 as well as to substation 2.

#### State machine



#### States of the state machine

State	Description of the state
	After switch-on, START is reached automatically. Without transition, MONITORING is reached automatically.
	Normal operation (no errors).
	Local emergency stop triggered.
	Error triggered and pending in the control station, which affects the substation, or emergency stop triggered in the control station, which affects the substation currently selected by the control station.
	Local error in the substation has been fixed. Acknowledgement in the substation possible. <b>Note:</b> An acknowledgement from the control station does not leave the WAIT_FOR_ACK_LOCAL state.
	Error so far pending in the control station has been fixed. Acknowledgement in the control station possible. <b>Note:</b> A local acknowledgement in the substation does not leave the WAIT_FOR_ACK_CS state.

### 3 Functional Mechanisms of this Example

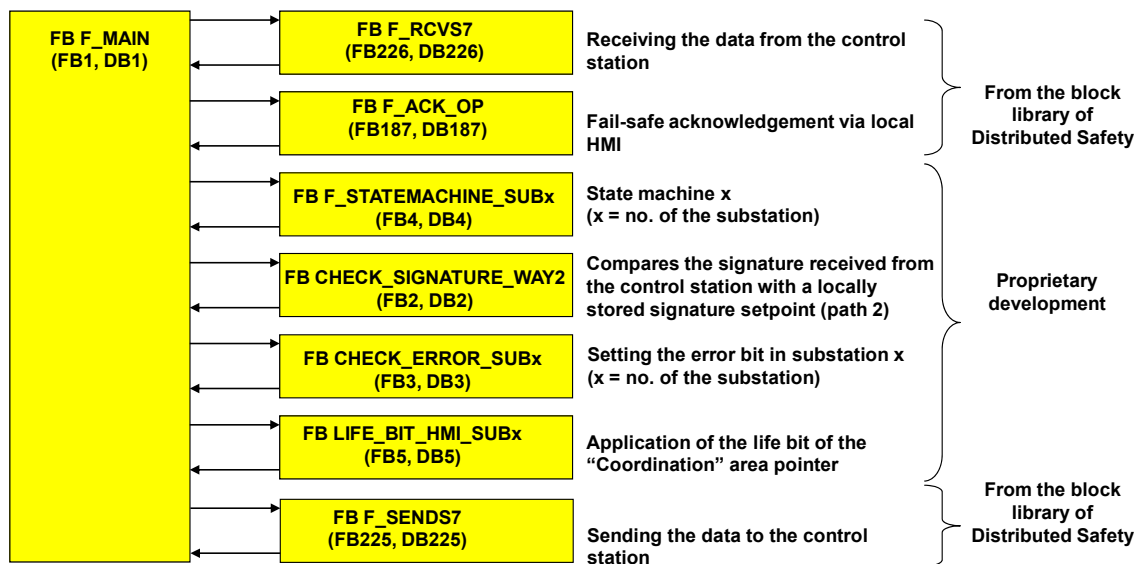
#### 3.2 State machine and program structure of the substation

##### Transitions of the state machine

Transition	Description of the transition
1	At least one of the following local situations has arisen: <ul style="list-style-type: none"> <li>Emergency stop triggered in the substation</li> <li>Communication error</li> </ul>
2	At least one of the following situations has arisen: <ul style="list-style-type: none"> <li>Emergency stop triggered in the control station</li> <li>Signature error</li> <li>Communication error</li> </ul>
3	Local error fixed or emergency stop of the substation unlocked again
4	Error in the control station fixed or emergency stop in the control station unlocked again
5	Before the possible local acknowledgement, another local error occurs or the local emergency stop is triggered.
6	Before the possible acknowledgement by the control station, another error occurs in the control station or the emergency stop is triggered there.
7	Local error fixed or local emergency stop unlocked and an acknowledgement is issued locally in the substation.
8	Error in the control station fixed or emergency stop unlocked there and an acknowledgement is issued in the control station.

#### 3.2.2 Program structure of the substations

The following is the call sequence of the F-runtime group with brief explanations:



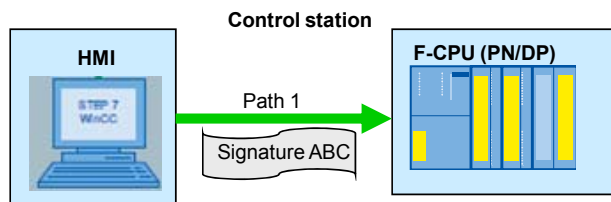
### 3.3 Error detection via path 1 and path 2

Although the selection of the substation from the control station is made via a non-safety HMI, the signature stored there reaches the F-CPU of the control station on two independent paths. These two paths are closely looked at in the following.

#### 3.3.1 Error detection via path 1

##### Definition "path 1"

Path 1 indicates the not safe connection from the HMI of the control station to the F-CPU of the control station.

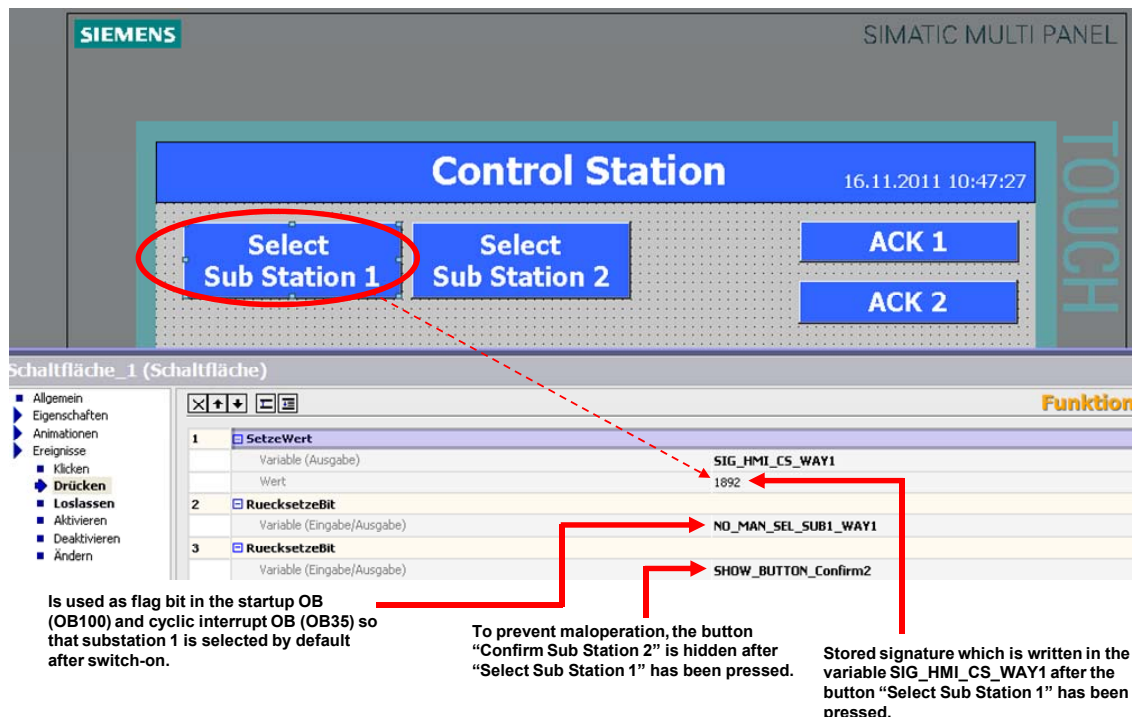


The signature ABC is an arbitrary numerical value of the INTEGER data type. In this STEP 7 project, the following decimal values were used for the signature:

- For the selection of substation 1: **1892**
- For the selection of substation 2: **2474**

##### Selection of the substation on the HMI

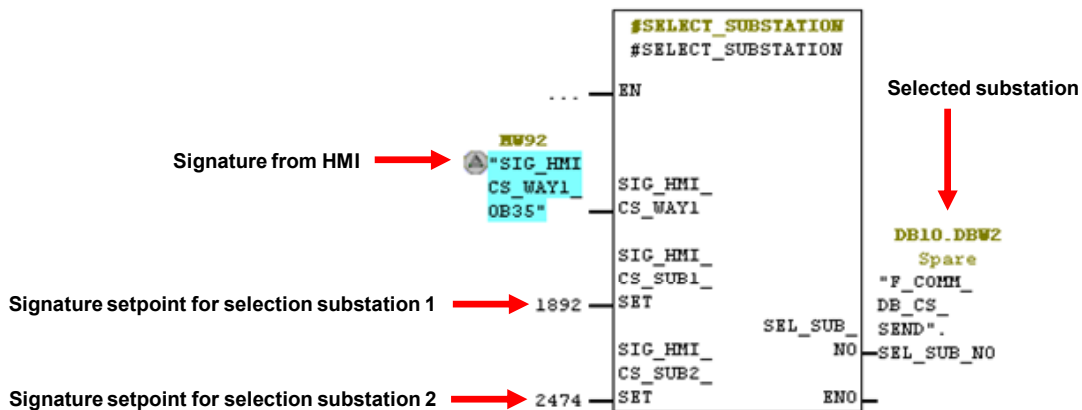
The corresponding signature is transmitted by pressing the assigned button "Select Sub Station x" on the HMI of the control station. The following figure shows this for the selection of substation 1:



##### Selection of the substation in the STEP 7 program

The selection of the substation is made via path 1; via path 2, a corresponding plausibility check is performed. All checks for plausibility take place in the F-program.

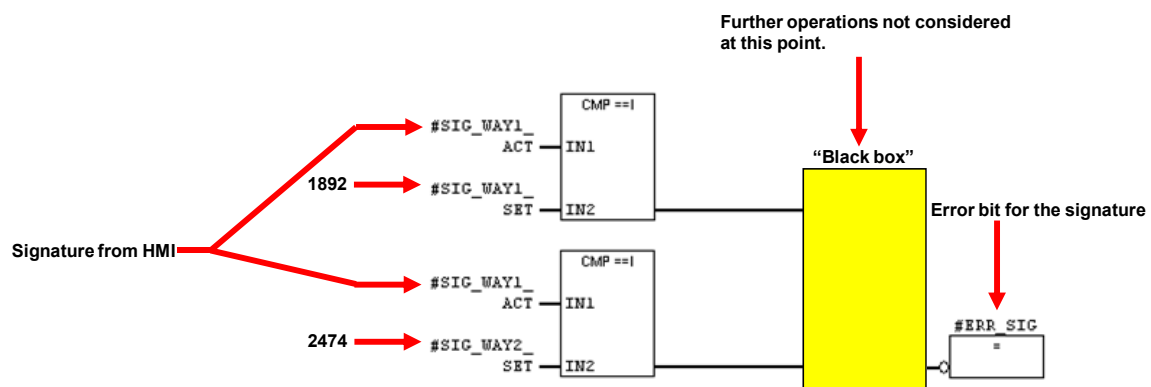
The selection of the substation is made by comparing the signature from the HMI of the control station with the fixedly stored signature setpoints 1892 (for substation 1) and 2474 (for substation 2) in **FB SELECT\_SUBSTATION (FB5, DB5)**:



FB SELECT\_SUBSTATION (FB5, DB5) is called from the F-program block FB F\_MAIN (FB1, DB1).

##### Error detection via path 1

The check whether the selected substation correlates with the signature from the HMI is performed in **FB CHECK\_SIGNATURE\_CS (FB3, DB3)**. This check is one of several checks with regard to the signature performed in this FB. These other checks are described in section 3.3.3 and are represented as "black box" here, which is not to be considered further for the moment:



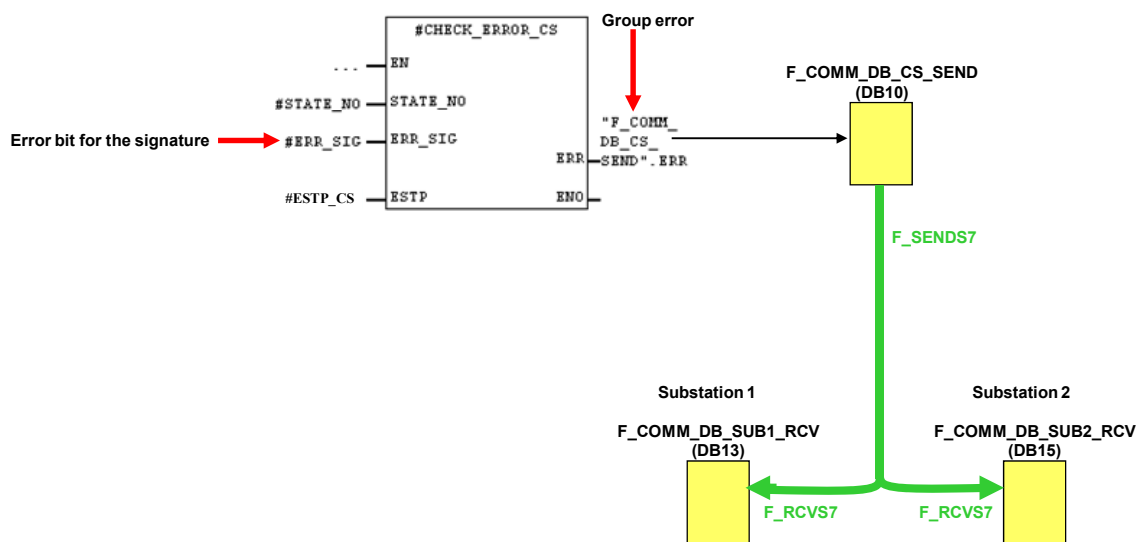
FB CHECK\_SIGNATURE\_CS (FB3, DB3) is called from the F-program block FB F\_MAIN (FB1, DB1).



### Error processing in the F-program

The error processing in the F-program looks as follows:

- If the selected substation does not correlate with the stored signature, the error bit ERR\_SIG is set (see figure above).
- If the state machine FB F\_STAEMACHINE\_CS (FB4) is in the MONITORING or WAIT\_FOR\_ACK state (queried via STATE\_NO), the error bit (group error) is set to 1 (see figure below). The state machine changes to the ERROR state.
- The ERROR state is queried in **FB CHECK\_ERROR\_CS (FB2, DB2)**.
  - State machine in the ERROR state: group error bit ERR=1
  - Otherwise: ERR=0



With the help of the F-communication DBs, the error information reaches the substation in a fail-safe manner via F\_SENDS7. With this information, the currently selected substation is set to the ERROR\_CS state.

FB CHECK\_ERROR\_CS (FB2, DB2) is called from the F-program block FB F\_MAIN (FB1, DB1).

### Error response

This example transmits this error information (group error bit ERR) as interface. The response to this error information (e.g. fail-safe breaking of actuators) is to be realized depending on the individual application.

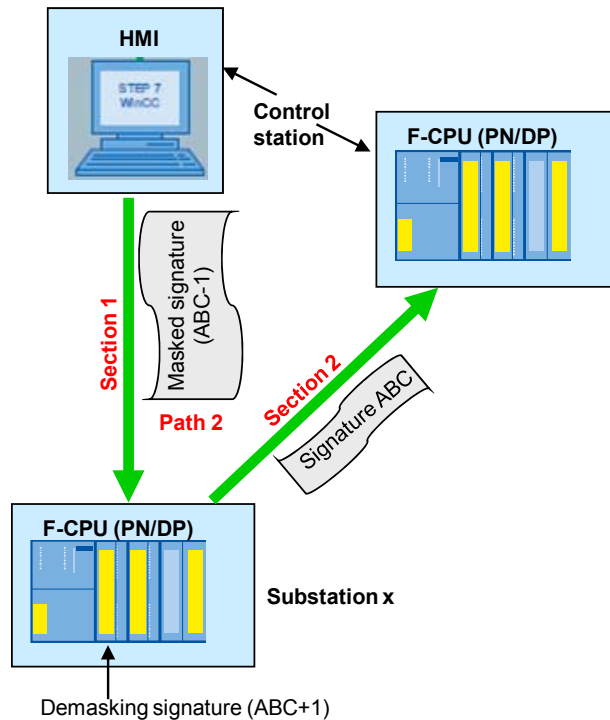
##### 3.3.2 Error detection via path 2

###### Definition "path 2"

Path 2 consists of two sections:

Section 1: HMI of the control station to the F-CPU of the selected substation.

Section 2: F-CPU of the selected substation to the F-CPU of the control station.



The signature ABC as described for path 1 in section 3.3.1 is subtracted by 1 (masked) for section 1 of path 2:

- For the selection of substation 1: **1891** (section 1 path 2) instead of 1892 (path 1)
- For the selection of substation 2: **2473** (section 1 path 2) instead of 2474 (path 1)

###### Selection of the substation on the HMI (section 1)

The corresponding (masked) signature is transmitted via section 1 to the F-CPU of substation x by pressing the button "Confirm Sub Station x". As before via the button "Select Sub Station x" for path 1, the numerical value is sent as signature, but subtracted by 1.

The masking is undone in the F-program of the substation by adding 1 to the masked signature. Then, this signature can be compared for equality with the signature setpoint stored in the F-CPU.

Masking and demasking are additional stabilizing measures for error detection via the not safe section 1 of path 2 in case the value stored for the button "Select Sub Station x" is also written on the value stored for the button "Confirm Sub Station x". This case is extremely unlikely, but it would be safely detected with the masking and demasking described here.

The next figure shows this situation for the confirmation of the selection of substation 1:

### 3 Functional Mechanisms of this Example

#### 3.3 Error detection via path 1 and path 2

**Control Station** 17.11.2011 11:34:41

Select Sub Station 1 Select Sub Station 2

**Confirm Sub Station 1** Confirm Sub Station 2

ACK 1 ACK 2

MESSAGES

**Funktionslist**

Id	Variable (Ausgabe)	Wert
1	SIG_FROM_HMI_CS_WAY2	1891
2	SIG_FROM_HMI_CS_WAY2_0	0
3	NO_MAN_SEL_SUB1_WAY2	

Is used as flag bit in the startup OB (OB100) and cyclic interrupt OB (OB35) of the selected substation so that substation 1 is selected by default after switch-on.

Stored (masked) signature which is written in the variable SIG\_HMI\_CS\_WAY2 after the button "Confirm Sub Station 1" has been pressed.

For the not selected substation (here: 2), the value 0 is written in the variable for the signature (MW96 in F-CPU for substation 2).

#### Note

Via the button "Confirm Sub Station x", the value zero is written in the variable of the signature via path 2 in the not selected substation. This is required to perform the error analyses and plausibility consideration in FB CHECK\_SIGNATURE\_CS (FB3, DB3) of the F-CPU of the control station.

#### Note

With regard to the values configured in WinCC flexible, always consider which connection the variables refer to. In the figure above, for example, all three displayed variables refer to the F-CPU of a substation. The assignment between variable and connection is shown in the figure below.

The next figure shows the assignment between the used variables and the configured connection. This is found in the "Variables" tab of WinCC flexible (see also previous note).

Name	Anzeigename	Verbindung
F_COMM_DB_RCV_FROM_SUB1.ERR_SIG_SUB1		HMI_CS_TO_FCPU_CS
NO_MAN_SEL_SUB1_WAY1		HMI_CS_TO_FCPU_CS
SHOW_BUTTON_Confirm2		HMI_CS_TO_FCPU_CS
IDB_F_STATEMACHINE_CS.ESTP		HMI_CS_TO_FCPU_CS
F_ACK_OP_6_9		HMI_CS_TO_FCPU_CS
F_COMM_DB_CS_SEND_SEL_SUB_NO		HMI_CS_TO_FCPU_CS
SIG_HMI_CS_WAY1		HMI_CS_TO_FCPU_CS
IDB_F_STATEMACHINE_CS.STATE_NO		HMI_CS_TO_FCPU_CS
F_COMM_DB_RCV_FROM_SUB2.STATE_NO_SUB2		HMI_CS_TO_FCPU_CS
NO_MAN_SEL_SUB2_WAY1_0		HMI_CS_TO_FCPU_CS
NO_MAN_SEL_SUB2_WAY1		HMI_CS_TO_FCPU_CS
F_COMM_DB_RCV_FROM_SUB1.STATE_NO_SUB1		HMI_CS_TO_FCPU_CS
SIG_FROM_HMI_CS_WAY2		HMI_CS_TO_FCPU_SUB1
NO_MAN_SEL_SUB1_WAY2		HMI_CS_TO_FCPU_SUB1
NO_MAN_SEL_SUB2_WAY2		HMI_CS_TO_FCPU_SUB1
SIG_FROM_HMI_CS_WAY2_0		HMI_CS_TO_FCPU_SUB2

**F-CPU control station**

**F-CPU substation 1**

**F-CPU substation 2**

##### Selection of the substation on the HMI (section 2)

While the transmission of the signature via section 1 takes place via a not safe connection, the transmission of the signature via section 2 is safe due to the use of the fail-safe S7 communication.

For a plausibility check this means the following: The occurrence of an error (e.g. falsified numerical value of the signature) has to be detected via section 1. Via section 2, corresponding plausibility considerations are not required because this section is of a fail-safe design.

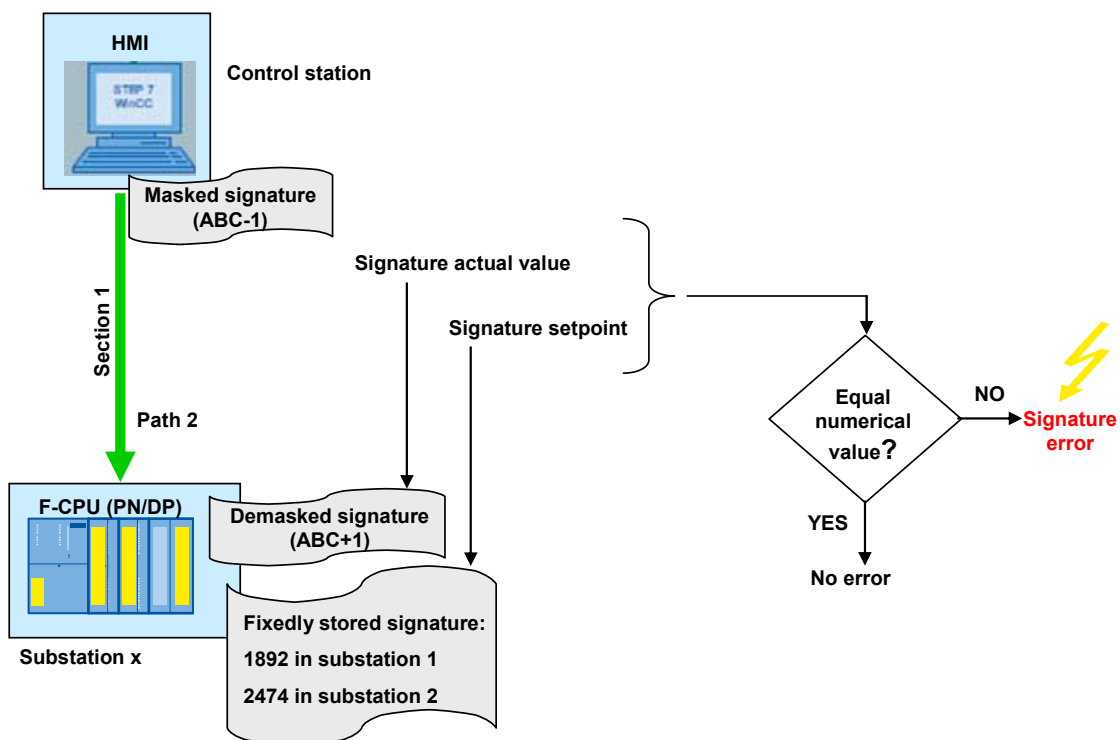
The detection of this error is described in the following.

##### Error detection via section 1 of path 2

A signature setpoint is fixedly stored in the F-CPU of the substation. The masked signature coming in via section 1, which is demasked again in the F-CPU of the substation, has to equal this setpoint.

An error (the two signatures are unequal) is safely detected by comparing this signature actual value and the signature setpoint in the F-program of the substation.

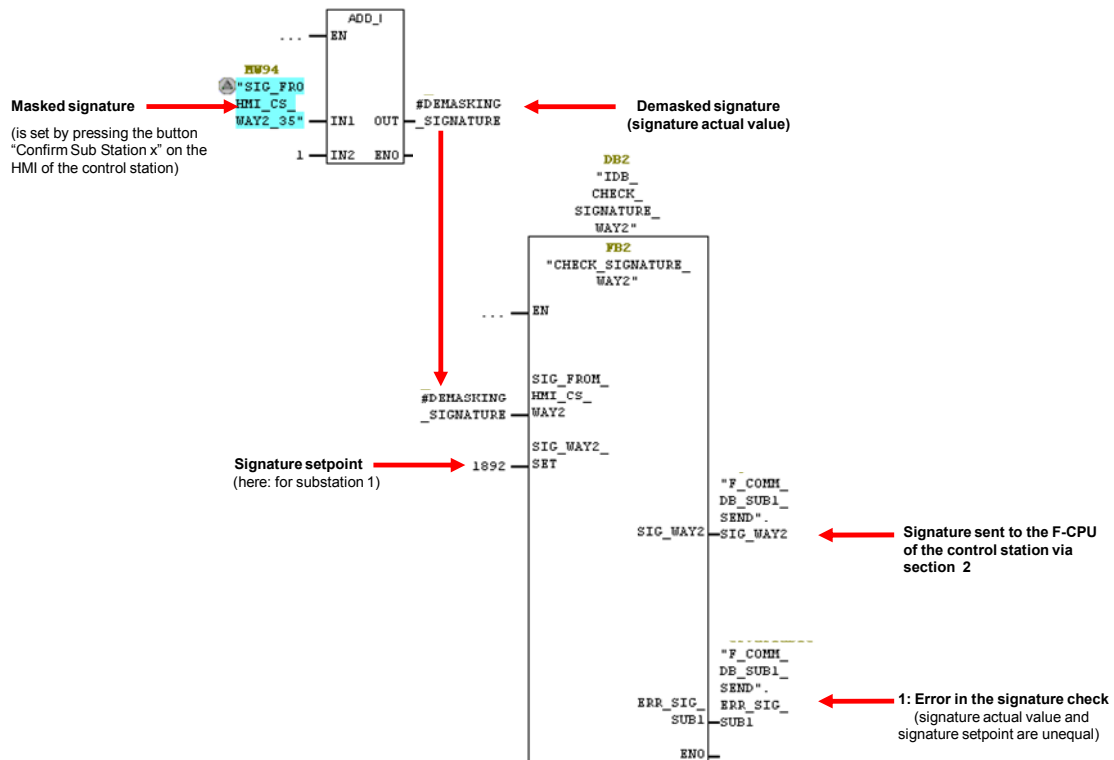
The following figure shows this connection:



The information about an error safely reaches the F-CPU of the control station via section 2.

**Realization in the F-program of the substation:**

The principle presented above is realized as follows in the F-program of the substation (using the example of substation 1 here):

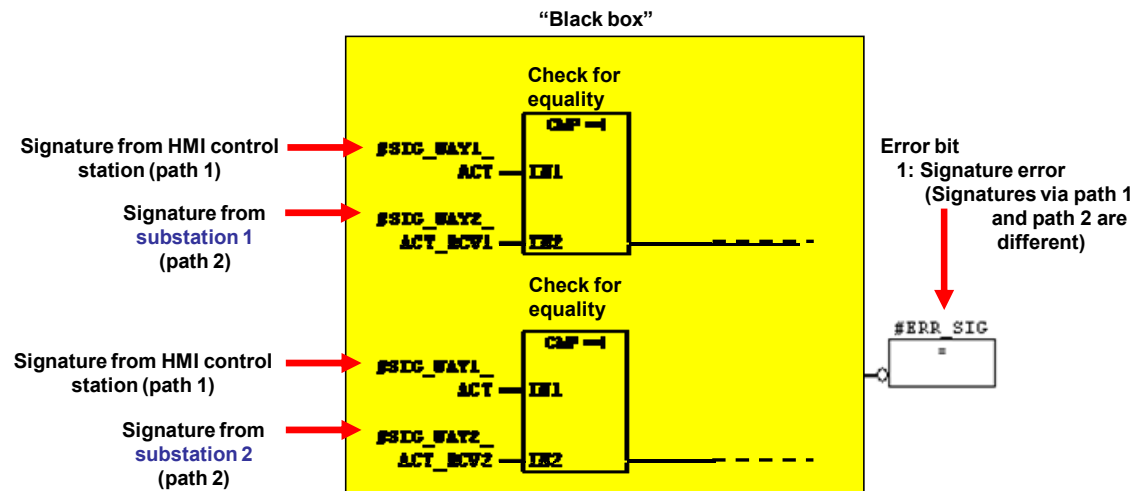


**FB CHECK\_SIGNATURE\_WAY2 (FB2, DB2)** is called from the F-program block **FB F\_MAIN (FB1, DB1)**.

##### 3.3.3 Joining of paths 1 and 2

###### Comparison of the signatures

The signature via path 1 and the signature via path 2 both reach the F-CPU of the control station and are checked for equality there in the F-program. The operations used for that are executed in **FB CHECK\_SIGNATURE\_CS (FB3, DB3)** and are exactly those which were not considered in the "black box" in section 3.3.1 ("Error detection via path 1") for reasons of clarity. This is made up for at this point:



Furthermore, the same statements as under "Error processing in the F-program" in section 3.3.1 apply.

## 3.4 Acknowledgement concept

### Convention

The acknowledgement has to be issued where the error occurred, i.e.:

- Error in the control station: the acknowledgement has to be issued in the control station after the error has been fixed.
- Error in a substation: the acknowledgement has to be issued locally in the respective substation after the error has been fixed.

### Acknowledgement via HMI

In all cases (control station or substation), the acknowledgement is issued by pressing the two buttons ACK1 and ACK2 of the respective HMI. The following has to be considered for the pressing of the buttons:

- ACK1 has to be pressed first, then ACK2.
- After having pressed ACK1, it has to be waited for at least one second (but not longer than one minute) before pressing ACK2. If this is not observed, the acknowledgement is not accepted.

This acknowledgement via the HMI is fail-safe.

### Why is this acknowledgement fail-safe?

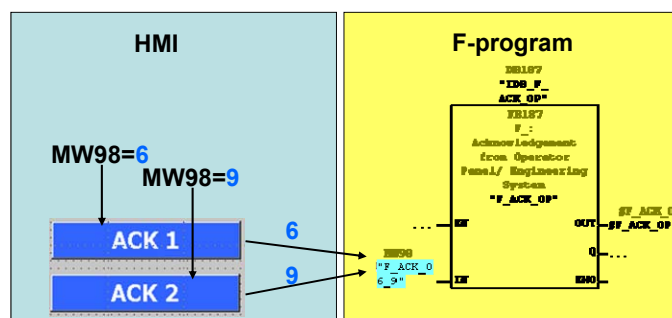
The next figure shows why this is a fail-safe acknowledgement:

Via the buttons ACK1 and ACK2, first a 6 and then a 9 is written in the F-block FB F\_ACK\_OP. If FB F\_ACK\_OP detects these numbers within the time specified above (longer than one second but shorter than one minute), the acknowledgement is evaluated as safe and the output signal F\_ACK\_OP (see formal parameter OUT in the figure) is set to logic 1 for one program cycle.

The F-block FB F\_ACK\_OP

- is part of the block library of Distributed Safety
- is called within FB F\_MAIN (FB1), namely in the F-program
  - of the control station
  - of the substations 1 and 2

Figure



### Reintegration of passivated I/O

The reintegration of passivated F-I/O is identical with that for acknowledgement described above.

### 3.5 Behavior in the event of communication errors

#### Acknowledgement if an error is pending?

The usual convention that an acknowledgement is only accepted when the pending error has been fixed also applies here. However, in this safety function example a situation might arise in which

- the state machine of the control station is in the ERROR state and
- the ERROR state is left via the acknowledgement buttons ACK1 and ACK2.

In the following it is described why even this situation is in consistence with the usual convention (error fixing first, then acknowledgement).

#### When does this situation arise?

This situation arises in the event of a communication error, e.g. when the F-CPU of substation 1 no longer has a connection to the other communication nodes.

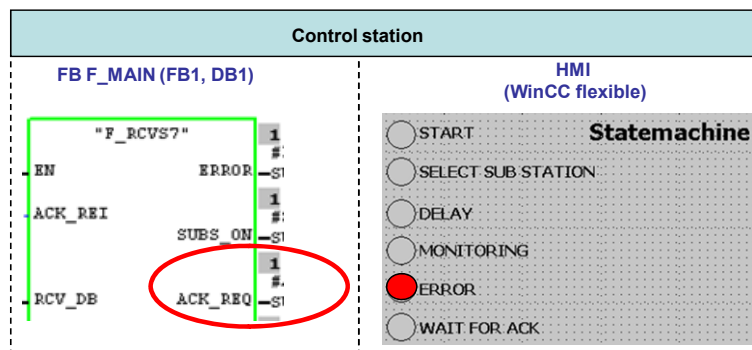
#### What does the HMI of the control station indicate?

After the communication error has been fixed, the behavior described above arises. The HMI of the control station indicates the following:

- The state machine of the control station is in the ERROR state and
- the acknowledgement buttons ACK1 and ACK2 are flashing.

#### Background

After a going communication error, the corresponding receive blocks FB F\_RCVS7 indicate that they require an acknowledgement (ACK\_REQ=1), and the state machine of the control station is in the ERROR state:



By acknowledging via ACK1 and ACK2 on the HMI of the control station, the request by ACK\_REQ=1 on FB F\_MAIN (FB1, DB 1) is complied with. If there are currently no more errors pending, the state machine changes to the WAIT\_FOR\_ACK state. By acknowledging via ACK1 and ACK2 again, the change to the MONITORING state is initiated.

#### Indication on the HMI

The case described here is indicated by the flashing buttons ACK1 and ACK2 on the HMI of the control station. For this purpose, the buttons are linked with the bit DB9.DBX0.0 from the block for signal configuration in WinCC flexible (see FB9, NW9).



## 3.6 Life bit in the "Coordination" area pointer

### 3.6.1 Context

#### What is this about?

Imagine the following situation as an example:

The connection to the HMI of the control station is interrupted. This state is indicated optically on the HMI:



**NOTICE** Please bear in mind that in the event of an interrupted connection of the HMI, the state machine on this HMI might indicate a not current state.

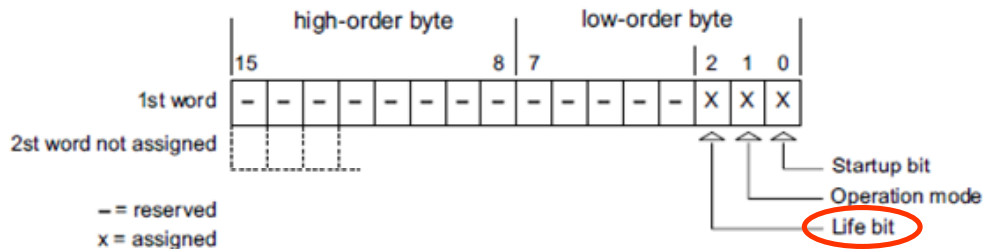
Switching to a different substation is no longer possible now. For this reason, the F-CPU requires evaluable information about the fact that the HMI does not communicate any longer.

For this case, it is possible to create a "Coordination" area pointer in WinCC flexible.

**Note** How to create the "Coordination" area pointer in WinCC flexible and how to link it with the STEP 7 program is described in section 4.6 "Creating the "Coordination" area pointer".

#### Assignment of the bits in the "Coordination" area pointer

The following figure shows the assignment of the "Coordination" area pointer which has a length of one double word. The information whether the HMI still participates in the communication is determined from the life bit.



##### **Life bit**

The life bit is inverted by the operator panel with a time lag of approx. one second. In the control program, this bit can be queried in order to check whether the connection to the operator panel still exists.

In the following it is described how this state is determined in the STEP 7 program and how this information is processed.

##### **Safety consideration with regard to the HMI failure**

The "Coordination" area pointer which provides the continuously inverting bit (life bit) is located in the standard program of the S7-CPU. In the following it is explained why the evaluation of the life bit yet provides sufficient safety functionality:

- The word in which the life bit is included is completely transmitted to the F-program. The selection and monitoring of the continuous inversion of the life bit is safely realized there.
- An error (no longer continuous inversion of the life bit) is transmitted to the selected substation via safe communication (F-SENDS7/F-RCVS7) and can be safely processed there. The state of the state machine in the respective substation changes to ERROR CS.
- The information about a no longer communicating HMI is optically perceivable for the operator. Irrespective of that,
  - the emergency stop functionality is still available
  - an error response is triggered automatically (see previous point)
- The (unlikely) flipping of a bit in the standard program has to be considered in a safety-related application. However, in the application on hand, this consideration is not about a one-time bit flip. In the case that the HMI no longer communicates, the life bit would have to continuously flip erroneously. This case can virtually be excluded, in particular when considering that the life bit is provided by the system explicitly for the monitoring of the communication of the HMI.

### 3.6.2 Implementation in the F-program

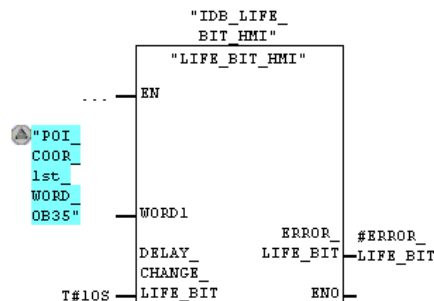
**Note** In the following, the implementation in the F-program of the control station is shown. The implementation for the substations is similar.

#### What does the HMI provide?

In WinCC flexible, an address area from the controller is to be stated for the "Coordination" area pointer. This address area is of the WORD data type; the area pointer itself is of the DWORD data type (see previous figure). The life bit is located in bit 2 of the first word of the area pointer.

#### Calling FB LIFE\_BIT\_HMI (FB7, DB7)

FB LIFE\_BIT\_HMI (FB7, DB7) is called from FB F\_MAIN (FB1, DB1):



#### Input parameters:

Formal parameter	Data type	Description
WORD1	WORD	The first word of the double word of the "Coordination" area pointer. Bit 2 of this word is the life bit.
DELAY_CHANGE_LIFE_BIT	TIME	If the life bit does not flip within the time configured (exemplarily) here, the error bit ERROR_LIFE_BIT is set.

**Note** The time to be configured DELAY\_CHANGE\_LIFE\_BIT is to be defined individually depending on the requirements of the application.

#### Output parameter:

Formal parameter	Data type	Description
ERROR_LIFE_BIT	BOOL	1: HMI has no connection any longer.

**Note** The first word of the double word of the "Coordination" area pointer is stored in the memory word POI\_COOR\_1st\_WORD (MW86) and transferred to the memory word POI\_COOR\_1st\_WORD\_OB35 (MW90) in OB35. In the F-program, then only the memory word POI\_COOR\_1st\_WORD\_OB35 (MW90) is accessed.

### 3 Functional Mechanisms of this Example

#### 3.6 Life bit in the "Coordination" area pointer

##### Description of the functionality of FB LIFE\_BIT\_HMI (FB7, DB7)

Upon each flipping of the life bit, one timer is reset and another one is started. If the life bit does not flip any longer, a timer runs through until the end, which is interpreted as an error.

NW	Figure	Description
1		Masking of the first word of the "Coordination" area pointer. The life bit (bit 2) is filtered out. Life bit=0.....LIFE_BIT=0 Life bit=1.....LIFE_BIT=4
2		For comparative operations in NW3 and NW4, the LIFE_BIT has to be of the INT data type: With MOVE, the LIFE_BIT of the WORD data type changes into the variable LIFE_BIT_INT of the INT data type.
3		Life bit=0..>.LIFE_BIT_INT=0..>..TRIGGER_TIMER_A=1 Life bit=1..>.LIFE_BIT_INT=4..>..TRIGGER_TIMER_B=0
4		Life bit=0..>.LIFE_BIT_INT=0..>..TRIGGER_TIMER_A=0 Life bit=1..>.LIFE_BIT_INT=4..>..TRIGGER_TIMER_B=1
5		Life bit=0 and does not flip any longer: Upon expiry of the time configured at PT: Q_TIMER_A=1.
6		Life bit=1 and does not flip any longer: Upon expiry of the time configured at PT: Q_TIMER_B=1.
7		If one of the two timers runs through, this is interpreted as an error (ERROR_LIFE_BIT=1).

##### What does the processing with the ERROR\_LIFE\_BIT look like?

The LIFE\_BIT is processed within the state machine FB F\_STATEMACHINE\_CS(FB4, DB4):

- LIFE\_BIT=1 changes the state machine in the ERROR state.
- LIFE\_BIT=0 is the prerequisite for leaving the ERROR state again.

## 4 Configuration and Settings

### 4.1 Address overview

#### IP addresses

Hardware	IP address	Subnet mask
F-CPU control station	192.168.0.1	255.255.255.0
F-CPU substation 1	192.168.0.2	255.255.255.0
F-CPU substation 2	192.168.0.3	255.255.255.0
HMI control station	192.168.0.4	255.255.255.0
HMI substation 1	192.168.0.5	255.255.255.0
HMI substation 2	192.168.0.6	255.255.255.0

#### ID

##### F-CPU control station

Local ID	Partner ID	Partner	Type	Active connection establishment
1	2	F-CPU substation 1	S7 connection	Yes
2	3	F-CPU substation 2	S7 connection	Yes

##### F-CPU substation 1

Local ID	Partner ID	Partner	Type	Active connection establishment
2	1	F-CPU control station	S7 connection	No

##### F-CPU substation 2

Local ID	Partner ID	Partner	Type	Active connection establishment
3	2	F-CPU control station	S7 connection	No

#### R\_ID

Sender	Receiver	R-ID
F-CPU control station	F-CPU substation 1	D hex
F-CPU control station	F-CPU substation 2	F hex
F-CPU substation 1	F-CPU control station	B hex
F-CPU substation 2	F-CPU control station	11 hex

#### Note

The numerical value of R\_ID has to be odd.

#### Address areas already used in the example

##### F-CPU control station

△	7	6	5	4	3	2	1	0	B	W	D
EB 0											
AB 0											
MB86									↓		↓
MB87									↓		
MB88											
MB89											↓
MB90									↓		
MB91									↓		
MB92									↓		
MB93									↓		
MB94									↓		
MB95									↓		
MB96	X	X	X	X							
MB97											
MB98									↓		
MB99									↓		

##### F-CPU substation 1

△	7	6	5	4	3	2	1	0	B	W	D
EB 0								X			
AB 0											
MB86									↓		↓
MB87									↓		
MB88											
MB89											↓
MB90									↓		
MB91									↓		
MB92											
MB93								X			
MB94									↓		
MB95									↓		
MB96									↓		
MB97									↓		
MB98									↓		
MB99									↓		

##### F-CPU substation 2

△	7	6	5	4	3	2	1	0	B	W	D
EB 8								X			
AB 0											
MB88									↓		↓
MB89									↓		
MB90											↓
MB91									↓		
MB92									↓		
MB93									↓		
MB94									↓		
MB95									↓		
MB96									↓		
MB97									↓		
MB98									↓		
MB99									↓		

4.2 Hardware configuration of STEP 7

The STEP 7 project supplied for the safety function example on hand contains the hardware configuration and example code.

In the following, some important settings from the hardware configuration of STEP 7 are presented for gaining an overview. Changing these settings (e.g. due to individual specifications) is generally possible; however, please consider the following note:

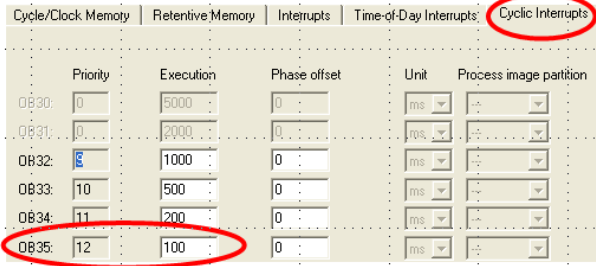
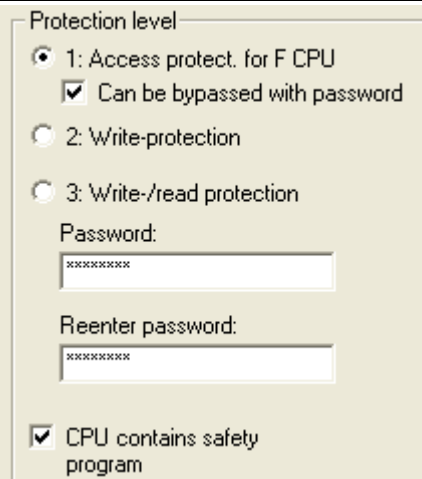
**NOTICE**

The settings presented in the following are preset. If these settings are changed, this might result in loss of the safety function.

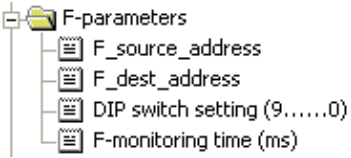
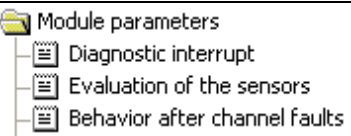
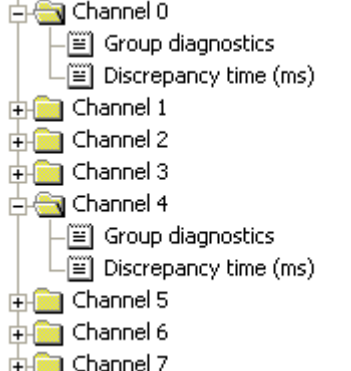
**Note**

The following screenshots show parts of the HW Config from the F-CPU of the control station. The statements made in the "Note" column apply analogously to the F-CPU's of the substations.

4.2.1 Settings of the F-CPU

Figure	Note
	<p>For OB35, the default value (100 ms) is kept.</p> <p>It has to be considered that the F-monitoring time has to be larger than the call time of OB35 (see "Settings of the fail-safe F-DI").</p>
	<p>A password needs to be assigned so that the parameter "CPU contains safety program" can be set. Only in this case are all F-blocks required for the safe operation of the F-blocks generated when the hardware configuration of STEP 7 is compiled.</p> <p>Password used here: <b>siemens</b></p>

## 4.2.2 Settings of the F-DI

Figure	Note
	<p><b>Parameters / F-parameters:</b></p> <p><u>DIP switch setting (9...0)</u> This value has to be set on the F-module (F-DI).</p> <p><b>Note:</b> The screenshot to the left shows the setting for the F-CPU of the control station. Please refer to HW Config for the settings of the F-CPU's of the substations.</p> <p><u>F-monitoring time (ms)</u> The F-monitoring time has to be larger than the call time of OB35.</p>
	<p><b>Parameters / Module parameters:</b></p> <p><u>Evaluation of the sensors</u> 1 of 2 evaluation</p> <p><u>Behavior after channel faults</u> In the case of a channel fault, the respective channel is passivated.</p>
	<p><b>Parameters / Module parameters:</b></p> <p>Assignment of the channels: <u>Channel 0, 4</u> Channel 0: emergency stop Channel 4: emergency stop</p> <p>In the case of a 1 of 2 evaluation, the second channel (here: channel 4) is used automatically and can no longer be edited.</p>

## 4.2.3 Collective signatures of the safety programs

After download of the STEP 7-Project the F-programs have the following collective signature:

- F-CPU Control Station
  - 27026962
- F-CPU Sub Station 1
  - 8CD2F5CA
- F-CPU Sub Station 2
  - 8B730595



## 4.3 Fail-safe communication

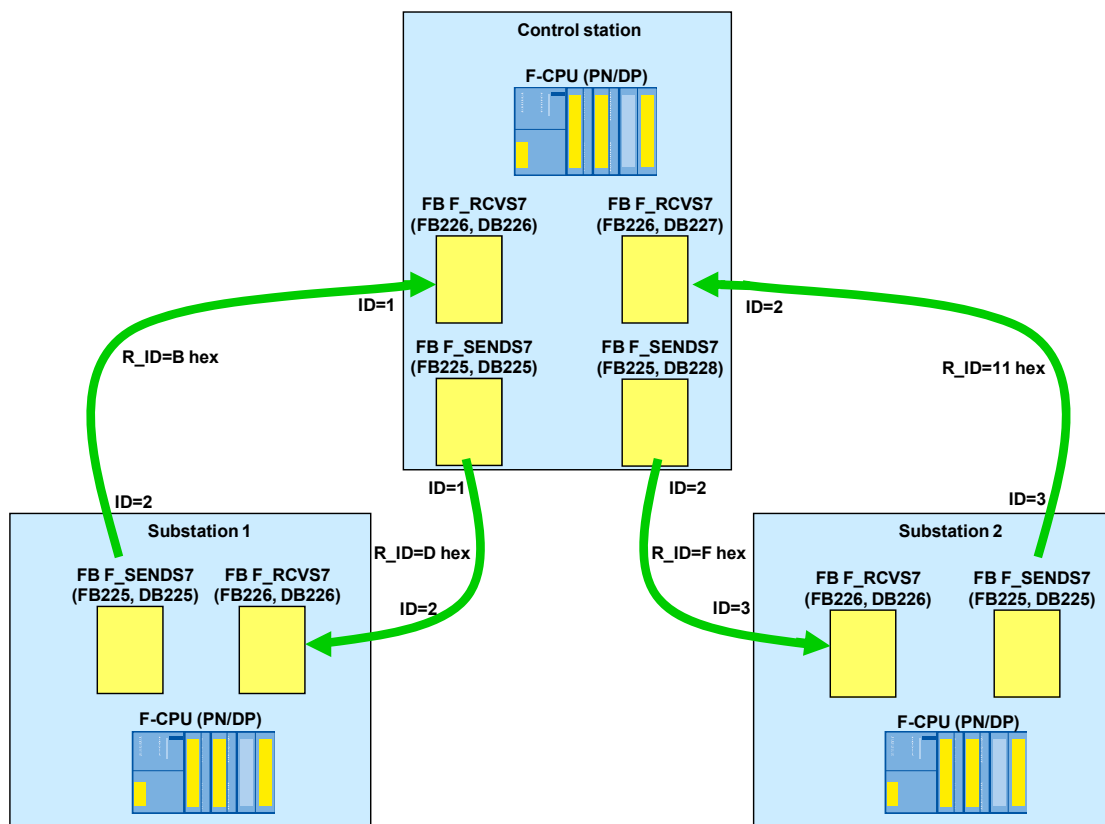
### 4.3.1 Configuration overview

#### General

This overview is of an informing character. It is not mandatory to change the configured values, but this information is required if the structure is to be changed or expanded.

#### Figure

The following figure shows the address relationships between the fail-safe communication blocks F\_SENDS7 and F\_RCVS7.



## 4 Configuration and Settings

### 4.3 Fail-safe communication

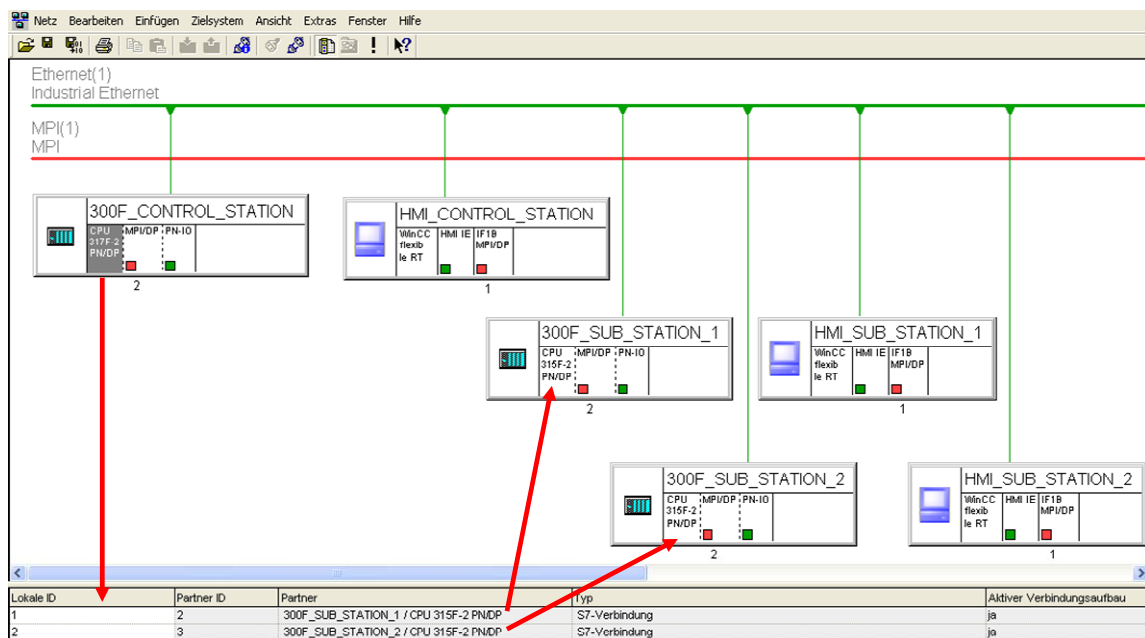
#### R\_ID

The R\_ID indicates a value which is unique throughout the network for an address relationship between an F\_SENDS7 and an F\_RCVS7. Therefore, always make sure that the R\_ID

- between the two communicating F-communication blocks is equal (see figure above) and
- has an odd numerical value.

#### ID

The ID is defined in NetPro. This is the local ID of the S7 connection. The next figure shows the configuration in NetPro.



### 4.3.2 Exchanging the user data

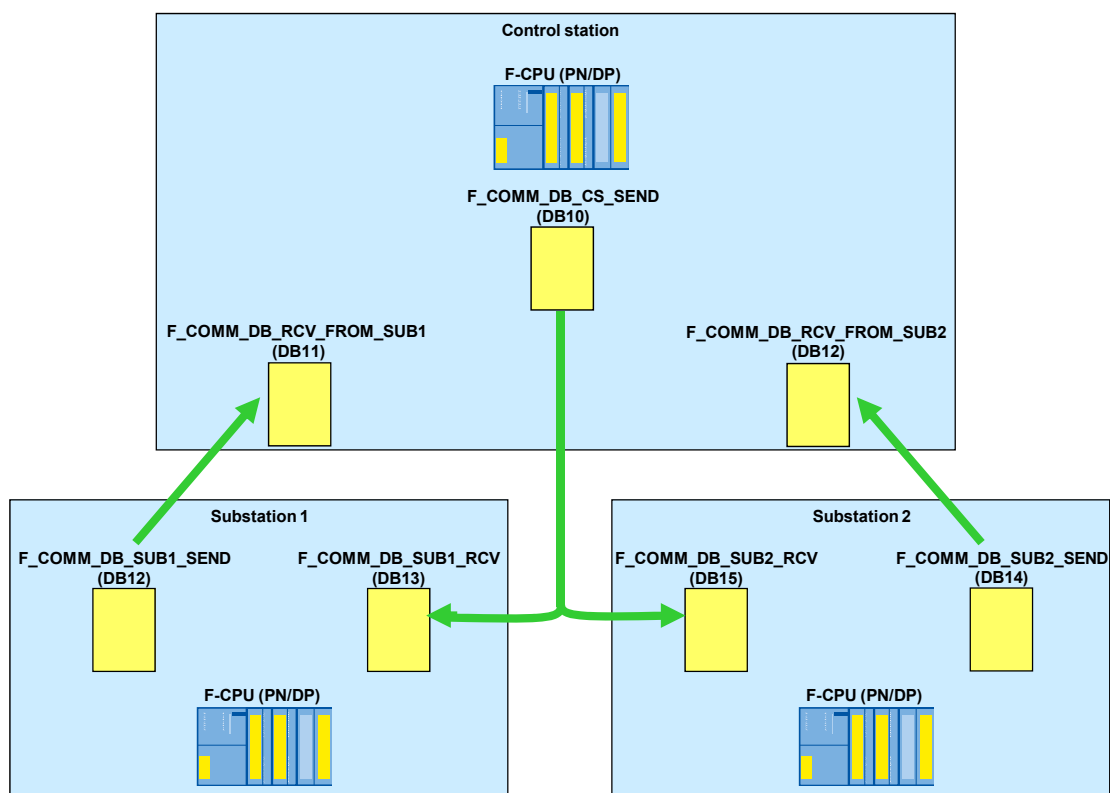
#### Via which blocks are the user data sent / received?

The data exchanged via the fail-safe communication between the control station and substations (section 2 of path 2) are referred to as user data in this example.

User data includes the following:

- Error information
- Acknowledgement signals
- Currently selected substation (1 or 2)
- Current state of the state machine
- Signature via path 2

The user data are stored in the F-communication DBs. The following figure shows which F-communication DBs receive or send user data.



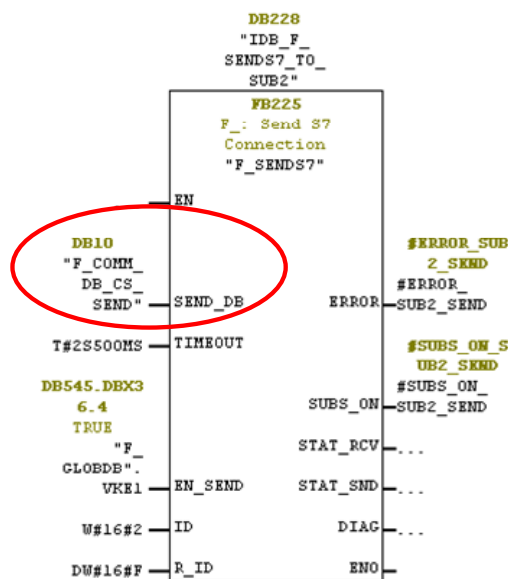
### 4.3.3 Integrating the F-communication DBs in the STEP 7 program

#### Configuration on F\_SENDS7 / F\_RCVS7

The information in which communication DB the user data for the fail-safe communication are stored is created at the input of FB F\_SEND or FB F\_RCV. For that, the address of the F-communication DB is created as actual parameter at the formal parameter SEND\_DB (for FB F\_SEND) or RCV\_DB (for FB F\_RCV).

Example:

The following figure shows FB F\_SENDS7 of the control station, which is responsible for the safe sending to substation 2. The user data sent from the control station to substation 2 are located in DB F\_COMM\_DB\_CS\_SEND (DB10).



#### Inserting a new F-communication DB in SIMATIC Manager

If you want to expand the application and create new F-communication DBs, please consider the following note:

#### Note

When creating the F-DB, assign in its object properties the signature "COM\_DBS7" in the "Family" input field in the "General – Part 2" tab. This signature indicates that the F-DB is an F-communication DB. Only F-DBs with this signature can be transmitted as F-communication DBs to F\_SENDS7 or F\_RCVS7. Assign a symbolic name to the F-communication DB.

#### 4.3.4 Data structure of the used F-communication DBs

##### F-communication DBs in the F-CPU of the control station

Control station DB F_COMM_DB_CS_SEND (DB10)			
Variable	Data type	Explanation	Sends / Receives
ERR	BOOL	Error of the control station is sent to the substations.	<b>Sends to:</b> <ul style="list-style-type: none"> <li>Substation 1               <ul style="list-style-type: none"> <li>- DB13</li> </ul> </li> <li>Substation 2               <ul style="list-style-type: none"> <li>- DB15</li> </ul> </li> </ul>
ACK_CS	BOOL	Acknowledgement signal (buttons ACK1 and ACK2 on the HMI of the control station) to change the state machine of the corresponding substation to the MONITORING state.	
SEL_SUB_NO	INT	Information which substation is currently selected by the control station (1 or 2). The selection is made via the buttons on the HMI of the control station. Substation 1 is selected by default.	

Control station DB F_COMM_DB_RCV_FROM_SUB1 (DB11)			
Variable	Data type	Explanation	Sends / Receives
ERR_SIG_SUB1	BOOL	Signature error in substation 1. Acknowledgement in control station required.	<b>Receives from:</b> <ul style="list-style-type: none"> <li>Substation 1               <ul style="list-style-type: none"> <li>- DB12</li> </ul> </li> </ul>
STATE_NO_SUB1	INT	State of the state machine of substation 1	
SIG_WAY2	INT	Current signature of substation 1: If selected: 1892 Otherwise: 0	

Control station DB F_COMM_DB_RCV_FROM_SUB2 (DB12)			
Variable	Data type	Explanation	Sends / Receives
ERR_SIG_SUB2	BOOL	Signature error in substation 2. Acknowledgement in control station required.	<b>Receives from:</b> <ul style="list-style-type: none"> <li>Substation 2               <ul style="list-style-type: none"> <li>- DB14</li> </ul> </li> </ul>
STATE_NO_SUB2	INT	State of the state machine of substation 2	
SIG_WAY2	INT	Current signature of substation 2: If selected: 2474 Otherwise: 0	

## F-communication DBs in the F-CPU of substation 1

Substation 1 DB F_COMM_DB_SUB1_SEND (DB12)			
Variable	Data type	Explanation	Sends / Receives
ERR_SIG_SUB1	BOOL	Signature error in substation 1. Acknowledgement in control station required.	<b>Sends to:</b> <ul style="list-style-type: none"> <li>Control station               <ul style="list-style-type: none"> <li>- DB11</li> </ul> </li> </ul>
STATE_NO_SUB_1	INT	State of the state machine of substation 1: 1: START 2: MONITORING 3: ERROR_LOCAL 4: ERROR_CS 5: WAIT_FOR_ACK_LOCAL 6: WAIT_FOR_ACK_CS	
SIG_WAY2	INT	Current signature of substation 1: If selected: 1892 Otherwise: 0	

Substation 1 DB F_COMM_DB_SUB1_RCV (DB13)			
Variable	Data type	Explanation	Sends / Receives
ERR_CS	BOOL	<ul style="list-style-type: none"> <li>Signature error or</li> <li>Emergency stop control station or</li> <li>Communication error</li> </ul>	<b>Receives from:</b> <ul style="list-style-type: none"> <li>Control station               <ul style="list-style-type: none"> <li>- DB10</li> </ul> </li> </ul>
ACK_CS	BOOL	Acknowledgement signal from the control station (buttons ACK1 and ACK2 on the HMI of the control station) to change the state machine of substation 1 to the MONITORING state.	
SEL_SUB_NO_FROM_CS	INT	Information which substation is currently selected by the control station (1 or 2).	

**F-communication DBs in the F-CPU of substation 2**

Substation 2 DB F_COMM_DB_SUB2_SEND (DB14)			
Variable	Data type	Explanation	Sends / Receives
ERR_SIG_SUB2	BOOL	Signature error in substation 2. Acknowledgement in control station required.	<b>Sends to:</b> <ul style="list-style-type: none"> <li>Control station               <ul style="list-style-type: none"> <li>- DB12</li> </ul> </li> </ul>
STATE_NO_SUB_2	INT	State of the state machine of substation 2: 1: START 2: MONITORING 3: ERROR_LOCAL 4: ERROR_CS 5: WAIT_FOR_ACK_LOCAL 6: WAIT_FOR_ACK_CS	
SIG_WAY2	INT	Current signature of substation 2: If selected: 2474 Otherwise: 0	

Substation 2 DB F_COMM_DB_SUB2_RCV (DB15)			
Variable	Data type	Explanation	Sends / Receives
ERR_CS	BOOL	<ul style="list-style-type: none"> <li>Signature error or</li> <li>Emergency stop control station or</li> <li>Communication error</li> </ul>	<b>Receives from:</b> <ul style="list-style-type: none"> <li>Control station               <ul style="list-style-type: none"> <li>- DB10</li> </ul> </li> </ul>
ACK_CS	BOOL	Acknowledgement signal from the control station (buttons ACK1 and ACK2 on the HMI of the control station) to change the state machine of substation 2 to the MONITORING state.	
SEL_SUB_NO_FROM_CS	INT	Information which substation is currently selected by the control station (1 or 2).	

## 4.4 Messages configuration

### What is that?

Depending on the events (here: occurring errors), supportive help texts appear on the HMI of the control station and the HMIs of the substations.

### How can the texts be read?

On each HMI, an own message window has been configured for the message texts. The message window has to be called to read any pending texts. On each HMI, the message window is called by pressing the following button:

**MESSAGES**

### Which texts are stored?

The texts are bit messages stored in WinCC flexible:

Text
Emergency Button Control Station is active
Signature Error
Passivation of F-DI
Communication Error (F-SENDS7 / F-RCVS7)
Receiver outputs fail-safe values
Fail-safe values are output RCV
Signature Error checked in Sub System 1
Signature Error checked in Sub System 2

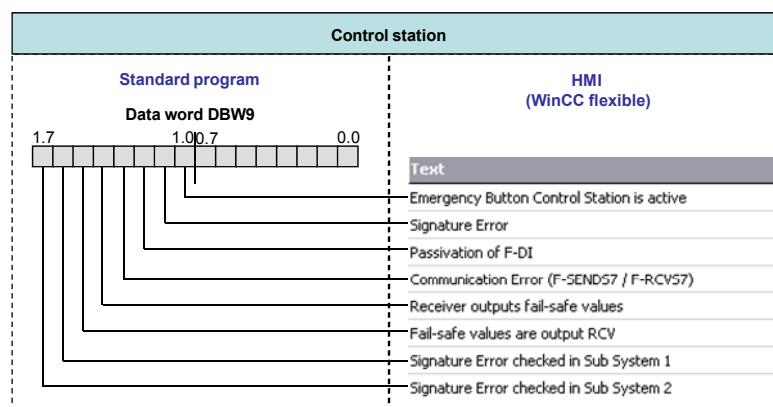
### How are occurring events linked with the text display?

Each text is assigned to a bit in the STEP 7 (standard) program:  
bit=0: text is not displayed; bit=1: text is displayed.

These bits are located in the instance DB of FB9:

- Control station: FB MESSAGES\_HMI\_CS (FB9, DB9)
- Substation x: FB MESSAGES\_HMI\_SUBx (FB9, DB9)

In FB9, the bits are compiled in a data word. In WinCC flexible, the stored texts are linked with the bits of this data word.

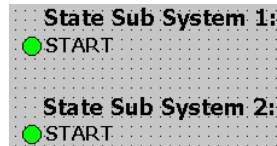




## 4.5 Indication of the state of the substation on the HMI of the control station

### Introduction

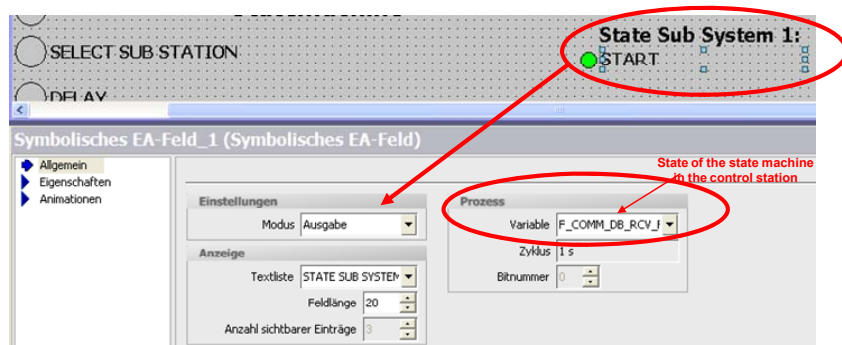
The current states of the state machines of the substations are indicated on the HMI of the control station (for reasons of clarity) (see following figure):



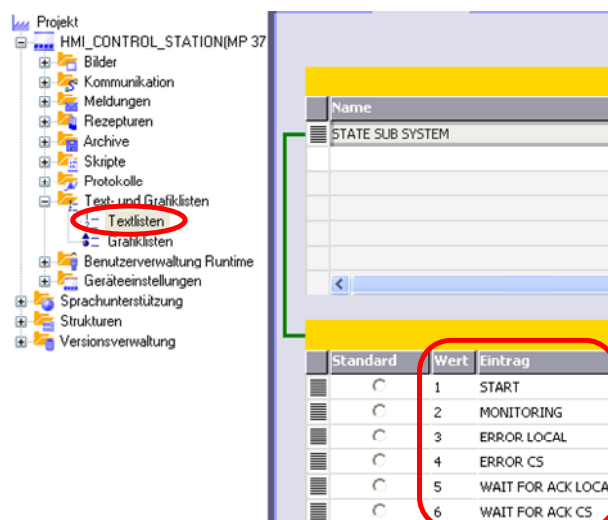
In the following, the realization of this indication is explained by taking the example of substation 1. All statements apply analogously also to substation 2.

### Realization

In WinCC flexible, a symbolic I/O output field is created and linked with the variable STATE\_NO\_SUB1 (see following figure). This variable displays the status of the state machine of the substation and is located in the F-communication DB F\_COMM\_DB\_RCV\_FROM\_SUB1 (DB11) of the control station.



The assignment which state is displayed as text for which value of STATE\_NO\_SUB1 results from the text list created in WinCC flexible:



## 4.6 Creating the "Coordination" area pointer

### What will you learn here?

This section is of an informing character only. It is only supposed to illustrate the steps required to use an area pointer created in WinCC flexible in the STEP7 program.

#### Note

How to use the "Coordination" area pointer and for which purpose is described in section 3.6 "Life bit in the "Coordination" area pointer".

#### Note

The following statements on the WinCC flexible and STEP 7 project use the example of the control station. They apply analogously also to the WinCC flexible and STEP7 projects of the substations.

### Creating the area pointer in WinCC flexible

Area pointer is created for the connection HMI (control station) to F-CPU (control station).

Creation of the "Coordination" area pointer

Name	Aktiv	Kommunikationstreiber
HMI_CS_TO_FCPU_CS	Ein	SIMATIC S7 300/400
HMI_CS_TO_FCPU_SUB1	Ein	SIMATIC S7 300/400
HMI_CS_TO_FCPU_SUB2	Ein	SIMATIC S7 300/400

Für alle Verbindungen			
Verbindung	Name	Symbol	Adresse
<undefiniert>	Bildnummer	<undefiniert>	
<undefiniert>	Datum/Uhrzeit Steuerung	<undefiniert>	
<undefiniert>	Projektkennung	<undefiniert>	

Für jede Verbindung getrennt			
Aktiv	Name	Symbol	Adresse
Aus	Datensatz	<undefiniert>	
Aus	Datum/Uhrzeit	<undefiniert>	
Ein	Koordinierung	POI_COOR_1st_WORD	MW 86

Variable in STEP 7      Address in STEP 7

**Transfer to the F-program**

POI\_COOR\_1st\_WORD (MW86) is a variable in the standard program. In OB35, this variable is transferred to the variable POI\_COOR\_1st\_WORD\_OB35 before F-CALL is called. In the F-program, then only POI\_COOR\_1st\_WORD\_OB35 is accessed. This is for the following reason:

If you want to read data from the standard program (flags or PII of the standard I/O) (here: POI\_COOR\_1st\_WORD) that can be changed by the standard program or an operator control and monitoring system during the runtime of an F-runtime group in the safety program, you have to use separate flags (here: POI\_COOR\_1st\_WORD\_OB35). Otherwise, the F-CPU might change to STOP.

In OB35, the program sequence looks as follows:

```

L      "POINTER_COORDINATION"      MD86
L      "POI_COOR_1st_WORD"         HW86
T      "POI_COOR_1st_WORD_OB35"    HW90

```

**POINTER\_COORDINATION**

This is the "Coordination" area pointer with a length of 1 double word. This is loaded at this point for reasons of clarity only or to prevent unintended overwriting of this address.

**POI\_COOR\_1st\_WORD**

This is the first word of the double word POINTER\_COORDINATION. It is created in WinCC flexible.

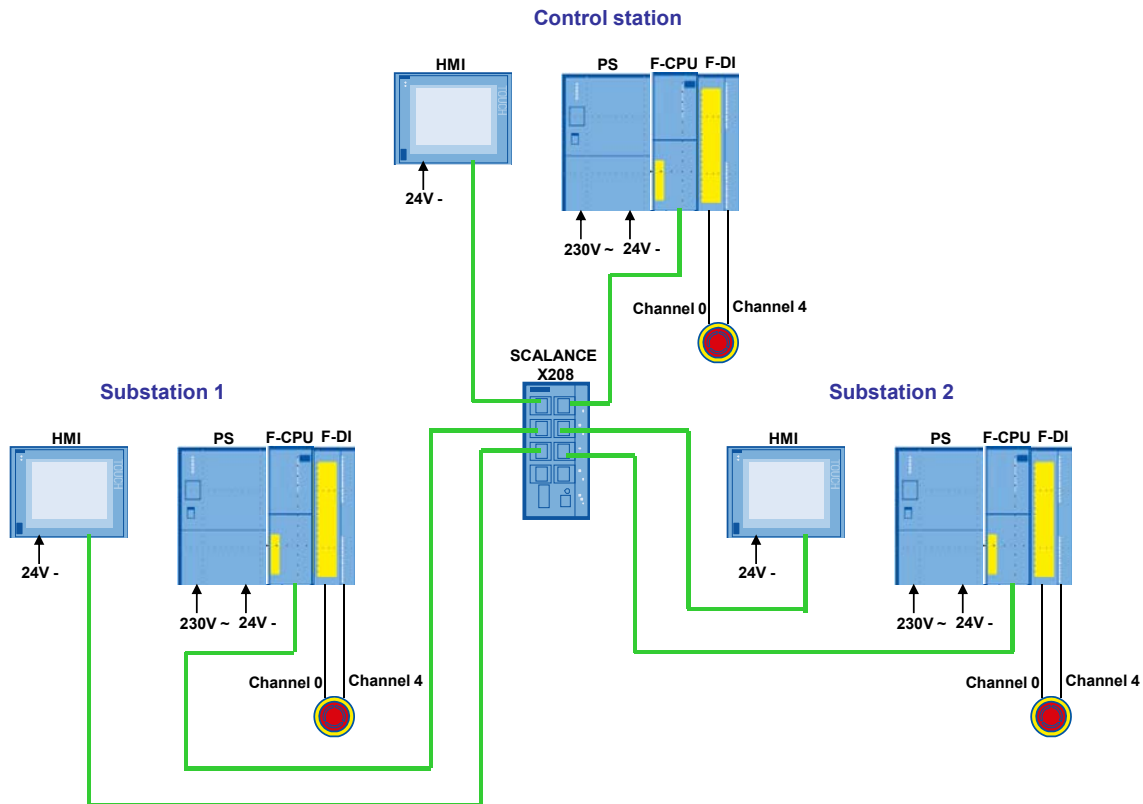
**POI\_COOR\_1st\_WORD\_OB35**

This is a copy of POI\_COOR\_1st\_WORD. In the F-program, only POI\_COOR\_1st\_WORD\_OB35 is accessed.

## 5 Installation

### 5.1 Hardware installation

The figure below shows the hardware configuration of the application.



### 5.2 Software installation

No.	Action
1	Install STEP 7
2	Install Distributed Safety
3	Install WinCC flexible

### 5.3 Setting the PG/PC interface

No.	Action	Note
1	In SIMATIC Manager: "Options > Set PG/PC Interface"	
2	Select the TCP IP interface	Setting according to the communication card used

## 5.4 Installation of the example project

### Retrieval

No.	Action
1	Load the zip file provided on the HTML page to a local directory of the Window Explorer.
2	In the SIMATIC Manager menu, go to "File -> Retrieve" and select the zip file. Follow the instructions.

### Password

In all cases, the required safety password is: **siemens**

### Ethernet nodes

To operate the example project, each F-CPU and each HMI has to contain the corresponding example project. So that this can reach the F-CPU and HMIs via a download, these have to be known as Ethernet nodes.

To check whether this is the case, proceed as follows:

No.	Action	Note																														
1	In SIMATIC Manager: "PLC > Edit Ethernet Node"																															
2	Click "Browse..."	The search starts after some seconds. Please wait for that.																														
3	In the "normal case", the three F-CPU and the HMI of the control station are displayed with the associated IP addresses.	<table><tr><th>!</th><th>IP address</th><th>MAC address</th><th>Device type</th><th>Name</th></tr><tr><td></td><td>192.168.0.1</td><td>00-0E-8C-F7-D4-C5</td><td>S7-300</td><td>pn-io</td></tr><tr><td></td><td>192.168.0.2</td><td>00-0E-8C-87-5E-5A</td><td>S7-300</td><td>pn-io-1</td></tr><tr><td></td><td>192.168.0.3</td><td>08-00-06-99-23-A2</td><td>S7-300</td><td>pn-io-2</td></tr><tr><td></td><td>192.168.0.4</td><td>00-0E-8C-84-1F-87</td><td>SIMATIC HMI</td><td>mp377</td></tr><tr><td></td><td>192.168.0.12</td><td>08-00-06-96-A9-A5</td><td>SCALANCE X-200</td><td>SCALANCE X208</td></tr></table>	!	IP address	MAC address	Device type	Name		192.168.0.1	00-0E-8C-F7-D4-C5	S7-300	pn-io		192.168.0.2	00-0E-8C-87-5E-5A	S7-300	pn-io-1		192.168.0.3	08-00-06-99-23-A2	S7-300	pn-io-2		192.168.0.4	00-0E-8C-84-1F-87	SIMATIC HMI	mp377		192.168.0.12	08-00-06-96-A9-A5	SCALANCE X-200	SCALANCE X208
!	IP address	MAC address	Device type	Name																												
	192.168.0.1	00-0E-8C-F7-D4-C5	S7-300	pn-io																												
	192.168.0.2	00-0E-8C-87-5E-5A	S7-300	pn-io-1																												
	192.168.0.3	08-00-06-99-23-A2	S7-300	pn-io-2																												
	192.168.0.4	00-0E-8C-84-1F-87	SIMATIC HMI	mp377																												
	192.168.0.12	08-00-06-96-A9-A5	SCALANCE X-200	SCALANCE X208																												

If the Ethernet nodes are not known, proceed as follows:

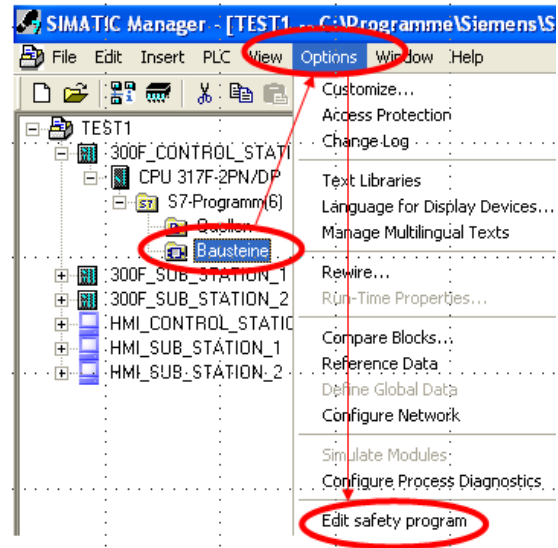
No.	Action	Note
1	Select a node from the list and click "OK".	
2	Assign the IP address and subnet mask. <b>Note:</b> The addresses used in this example can be found in section 4.1 "Address overview". Confirm your entry by clicking "Assign IP Configuration".	
3	Assign a device name to the node and confirm your entry by clicking "Assign Name".	

## 5 Installation

### 5.4 Installation of the example project

#### Download

Proceed as follows for the download:

Nr.	Aktion	Anmerkung
1	Switch all 3 F-CPU's to STOP	
2	Load successive the <b>HW Config</b> in the corresponding F-CPU.	
3	Load successive the net configuration of <b>NetPro</b> in the corresponding F-CPU.	Loading of HW Config is not sufficient!
4	Load the STEP 7 program from SIMATIC Manager to the corresponding F-CPU: <ul style="list-style-type: none"> <li>Select the block container</li> <li>Menu: "Options &gt; Edit safety program"</li> </ul>	 <p>The screenshot shows the SIMATIC Manager interface. The 'Options' menu is open, and the 'Edit safety program' option is highlighted. The project tree on the left shows the 'Bausteine' (Blocks) folder selected.</p>
5	Open WinCC flexible and load the projects in the corresponding panels.	
6	Switch all 3 F-CPU's to RUN.	

## 6 Operation of the Example Project

### Requirements

The following requirements have to be met to operate the example project:

- Each F-CPU contains the corresponding STEP 7 project
- Each HMI contains the corresponding WinCC flexible project

When all emergency stop buttons are unlocked and the communication is undisturbed, the HMIs of the substations indicate the state WAIT FOR ACK LOCAL and the HMI of the control station indicates the state WAIT FOR ACK.

By acknowledging via the buttons ACK1 and ACK2 on the HMI, the MONITORING state is reached in the control station and in the substations.

#### Note

All of the following scenarios (A to D) assume

- the MONITORING state in the control station and substations,
- that substation 1 is currently selected by the control station.

#### Note

In those cases in which you are requested to acknowledge with the buttons ACK1 and ACK2, please think of the procedure described in section 3.4 "Acknowledgement concept" for fail-safe acknowledgement via panels:

- ACK1 has to be pressed first, then ACK2.
- After having pressed ACK1, it has to be waited for at least one second (but not longer than one minute) before pressing ACK2. If this is not observed, the acknowledgement is not accepted.

### 6.1 Variables table (VAT)

Each block container of SIMATIC Manager contains a variables table:

- Control station: STATEMACHINE\_CS (CS = **C**ontrol **S**tation)
- Substation 1: STATEMACHINE\_SUB1
- Substation 2: STATEMACHINE\_SUB2

The structure of all three state machines is the same. The following is the VAT of the control station:

	Address	Symbol	Display format	Status value
1	DB4.DBX 14.0	"IDB_F_STATEMACHINE_CS".START	BOOL	false
2	DB4.DBX 14.1	"IDB_F_STATEMACHINE_CS".SELECT_SUBSTATION	BOOL	false
3	DB4.DBX 14.2	"IDB_F_STATEMACHINE_CS".DELAY	BOOL	false
4	DB4.DBX 14.3	"IDB_F_STATEMACHINE_CS".MONITORING	BOOL	true
5	DB4.DBX 14.4	"IDB_F_STATEMACHINE_CS".ERROR	BOOL	false
6	DB4.DBX 14.5	"IDB_F_STATEMACHINE_CS".WAIT_FOR_ACK	BOOL	false
7				
8	DB1.DBW 0	"IDB_F_MAIN".STATE_NO	HEX	VW#16#0004
9	DB10.DBW 2	"F_COMM_DB_CS_SEND".SEL_SUB_NO	HEX	VW#16#0001
10				
11	I 0.0	"ESTP_CS"	BOOL	true
12				
13	DB7.DBX 12.0	"IDB_LIFE_BIT_HMI".TRIGGER_TIMER_A	BOOL	false
14	DB7.DBX 12.1	"IDB_LIFE_BIT_HMI".TRIGGER_TIMER_B	BOOL	true

## 6.2 Scenario A: Switching to another substation

### 6.2.1 Correct switching

#### Actions on the HMI of the control station

No.	Action	Note
1	Press the button "Select Sub Station 2".	<ul style="list-style-type: none"> <li>The button "Confirm Sub Station 2" appears.</li> <li>The state machine changes to the DELAY state.</li> <li>The indication "Selected Sub Station" changes from 1 to 2.</li> </ul>
2	Press the button "Confirm Sub Station 2" while the state machine is yet in the DELAY state.	If an emergency stop is triggered, this affects substation 2.

### 6.2.2 Incorrect switching

#### Actions on the HMI of the control station

No.	Action	Note
1	Press the button "Select Sub Station 2".	<ul style="list-style-type: none"> <li>The button "Confirm Sub Station 2" appears.</li> <li>The state machine changes to the DELAY state.</li> <li>The indication "Selected Sub Station" changes from 1 to 2.</li> </ul>
2	Wait for the expiry of the DELAY time (i.e. do <b>not</b> press the button "Confirm Sub Station 2").	<p>Upon expiry of the switch-on delay, a signature error is detected because the signatures via path 1 and path 2 are different:</p> <ul style="list-style-type: none"> <li>Via path 1, the signature 2474 is transmitted (button "Select Sub Station 2" pressed).</li> <li>Via path 2, there is still the signature 1892 transmitted to the F-CPU of the control station because the button "Confirm Sub Station 2" has not been pressed.</li> </ul> <p>State of the state machine: ERROR</p>
3	Press the button "Confirm Sub Station 2" now.	<ul style="list-style-type: none"> <li>The correct signature 2474 is now transmitted via path 2. The signatures via path 1 and 2 are equal.</li> <li>There is no longer an error, the state machine changes to the WAIT FOR ACK state.</li> </ul>
4	Acknowledge by successively pressing ACK1 and ACK2.	The state machine changes to the MONITORING state and substation 2 is selected.



## 6.3 Scenario B: Triggering an emergency stop in the control station

## 6.3 Scenario B: Triggering an emergency stop in the control station

### Actions in the control station and substations

No.	Action	Note
1	Press the emergency stop button in the control station.	<u>State of the state machines:</u> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- ERROR</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- ERROR CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>
2	Unlock the emergency stop in the control station.	<u>State of the state machines:</u> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>
3	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of the control station.	<u>State of the state machines:</u> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p>An acknowledgement on the HMI of the substation would not have any effect because of the convention that an acknowledgement is only possible where the error occurred.</p>

## 6.4 Scenario C: Triggering an emergency stop in the substation

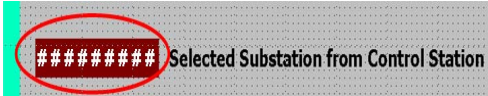
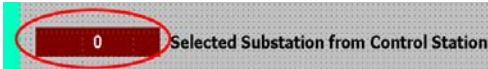
### Actions in the control station and substations

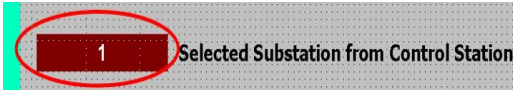
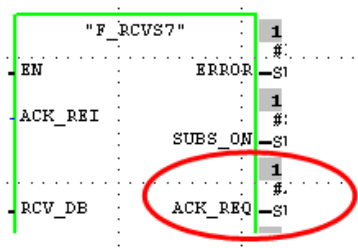
No.	Action	Note
1	Press the emergency stop button in substation 2.	<u>State of the state machines:</u> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- ERROR LOCAL</li> </ul> </li> </ul>
2	Unlock the emergency stop in substation 2.	<u>State of the state machines:</u> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK LOCAL</li> </ul> </li> </ul>

No.	Action	Note
3	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of substation 2.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p>An acknowledgement on the HMI of the control station would not have any effect because of the convention that an acknowledgement is only possible where the error occurred.</p>


## 6.5 Scenario D: Creating a communication error

### 6.5.1 F-CPU of substation 1 cut off from communication

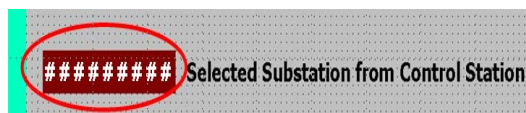
No.	Action	Note
1	Disconnect the Ethernet cable from the F-CPU of substation 1.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- ERROR</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p><u>Further indications on the HMI:</u></p> <ul style="list-style-type: none"> <li>• Substation 1</li> </ul> <p>The field "Selected Sub Station from Control Station" indicates that the connection is disturbed:</p> 
2	Reconnect the Ethernet cable to the F-CPU of substation 1.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- ERROR</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK LOCAL</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p><u>Further indications on the HMI:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- The buttons ACK1 and ACK2 are flashing</li> </ul> </li> <li>• <b>Substation 1</b></li> </ul>  <p><u>Flashing buttons ACK1 and ACK2</u></p> <p>For background information on these indications, please refer to section 3.5 "Behavior in the event of communication errors".</p>

No.	Action	Note
3	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of <b>substation 1</b> .	<p>On the HMI of substation 1, the substation currently selected by the control station is indicated:</p>  <p>The state machine remains in the WAIT FOR ACK LOCAL state.</p>
4	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of <b>substation 1</b> .	<p>State of the state machines:</p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- ERROR</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- ERROR CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>
5	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of the <b>control station</b> .	<p>State of the state machines:</p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p>Further indications on the HMI:</p> <ul style="list-style-type: none"> <li>• <b>Control station</b> The buttons ACK1 and ACK2 are no longer flashing</li> </ul> <p>By acknowledging via ACK1 and ACK2 on the HMI of the control station, the request by ACK_REQ=1 on FB F_MAIN (FB1, DB 1) is complied with:</p> 
6	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of the <b>control station</b> .	<p>State of the state machines:</p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>

**6.5.2 HMI of the control station cut off from communication**

No.	Action	Note
1	<p>Disconnect the Ethernet cable from the HMI of the control station and wait for the configured time created at parameter DELAY_CHANGE_LIFE_BIT of FB LIFE_BIT_HMI (FB7, DB7) (in this example, 10s are preconfigured).</p> <p><b>Note:</b> Further information is available in section 3.6 "Life bit in the "Coordination" area pointer".</p>	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- ERROR, but MONITORING indication remains because there is no connection to the HMI</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- ERROR_CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p><u>Further indications on the HMI:</u></p> <ul style="list-style-type: none"> <li>• Control station</li> </ul> <p>The field "Selected Substation" indicates that the connection is disturbed:</p> 
2	Reconnect the Ethernet cable to the HMI of the control station.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK CS</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>
3	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of the control station.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>

### 6.5.3 HMI of substation 1 cut off from communication

No.	Action	Note
1	<p>Disconnect the Ethernet cable from the HMI of substation 1 and wait for the configured time created at parameter DELAY_CHANGE_LIFE_BIT of FB LIFE_BIT_HMI_SUB1 (FB5, DB5).</p> <p><b>Note:</b> Further information is available in section 3.6 "Life bit in the "Coordination" area pointer".</p>	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- ERROR LOCAL, but MONITORING indication remains because there is no connection to the HMI</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul> <p><u>Further indications on the HMI:</u></p> <ul style="list-style-type: none"> <li>• Substation 1</li> </ul> <p>The field "Selected Sub Station from Control Station" indicates that the connection is disturbed:</p> 
2	Reconnect the Ethernet cable to the HMI of substation 1.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- WAIT FOR ACK LOCAL</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>
3	Acknowledge by successively pressing ACK1 and ACK2 on the HMI of substation 1.	<p><u>State of the state machines:</u></p> <ul style="list-style-type: none"> <li>• <b>Control station</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 1</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> <li>• <b>Substation 2</b> <ul style="list-style-type: none"> <li>- MONITORING</li> </ul> </li> </ul>

## 7 Standards Consideration in Accordance with IEC 62061

### 7.1 Definition of safety function and SRCF

#### Safety function and SRCF

For the example on hand, we formulate the following three safety functions with the associated SRCF (**S**afety **R**elated **C**ontrol **F**unction):

No.	Safety function	SRCF
1	In the event of an erroneous transmission of data (signature for the selection of a substation), from the non-safety HMI (of the control station) to the F-CPU ( <b>of the control station</b> ), the currently selected substation has to trigger actions.	Stopping of the actuators in the selected substation.
2	In the event of an erroneous transmission of data (signature for the selection of a substation), from the non-safety HMI (of the control station) to the F-CPU ( <b>of the substation</b> ), the currently selected substation has to trigger actions.	Stopping of the actuators in the selected substation.
3	In the event that the emergency stop in the control station is triggered, the currently selected substation has to trigger actions.	Stopping of the actuators in the selected substation.

#### Note

If an error occurs here (incorrect signature or emergency stop in the control station), a corresponding bit is safely transmitted to the substation; any actuators are not considered. However, for the standards calculation in this section, corresponding actuators have to be assumed. Otherwise, the standards consideration could not be performed appropriately.

#### Note

The Machinery Directive 2006 / 42 / EC generally requests stopping in the event of an emergency (emergency stop). However, an emergency stop is not described as a risk-reducing measure but as an additional measure:

"Emergency stop devices must be a back-up to other safeguarding measures and not a substitute for them." (Machinery Directive, 1.2.4.3).

The emergency stop as an additional measure is adopted in the standards consideration in accordance with IEC 62061.

#### Note

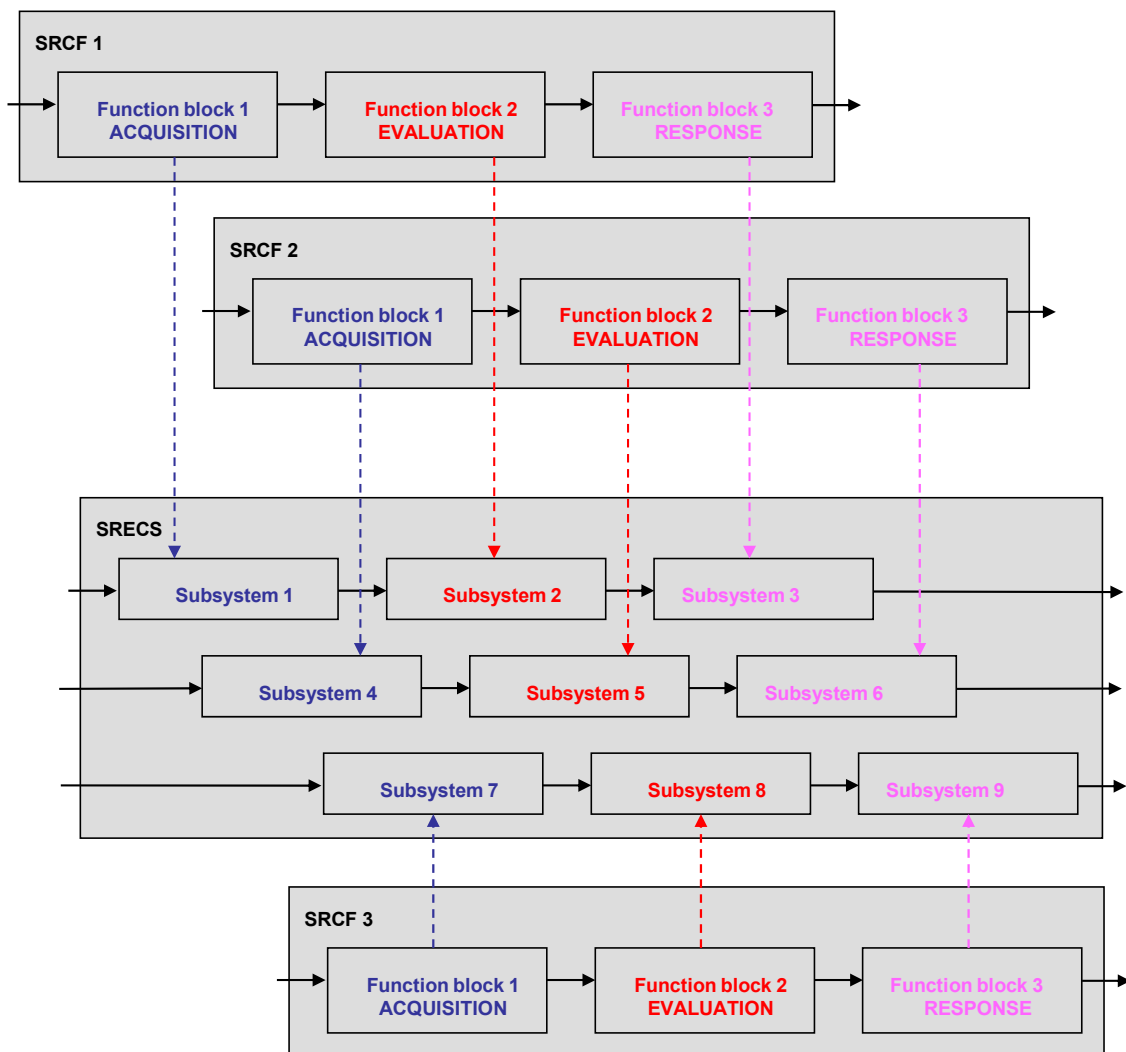
The local emergency stop in the substations is not considered in this context.

## 7.2 SRECS and SRCF

### Connection and division

For the realization of the safety function, a SRECS (Safety Related Electrical Control Systems) is used. The SRECS executes the SRCF (Safety Related Control Function).

Thus, in this example, an SRECS executes SRCF 1, SRCF 2, and SRCF 3 described in section 7.1:

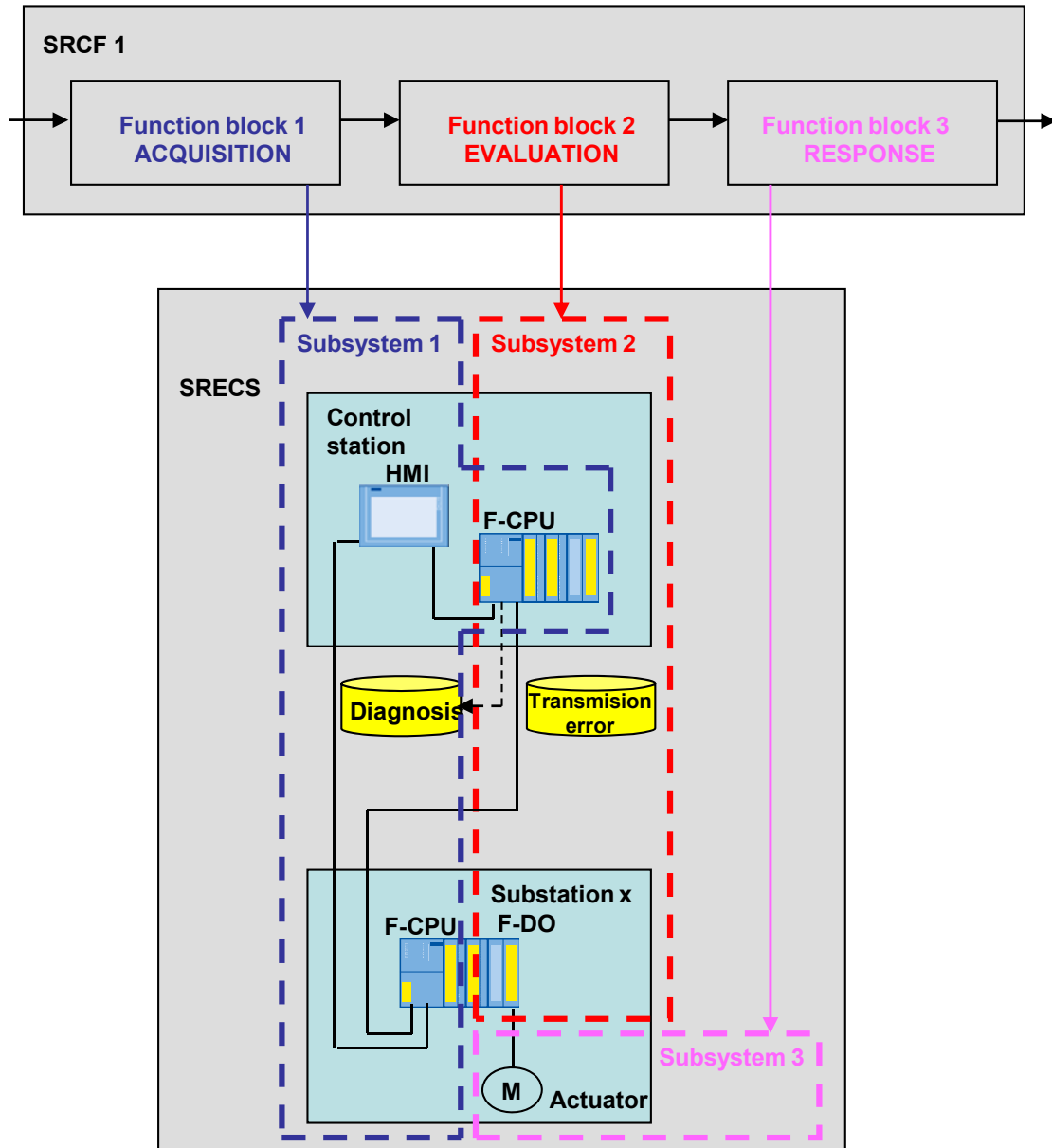


For reasons of clarity, these are not represented in one central but in three individual figures in the following. The associated explanation is given after the respective figure.

- Section 7.2.1: SRECS executes SRCF 1
- Section 7.2.2: SRECS executes SRCF 2
- Section 7.2.3: SRECS executes SRCF 3

### 7.2.1 SRECS executes SRCF 1

Figure





**Explanation of the figure****Subsystem 1 executes function block 1 ACQUISITION**

This subsystem consists of the components

- HMI of the control station
  - Transmits the signature to the F-CPU of the control station (path 1)
- F-CPU of the control station
  - Receives the signature from the HMI of the control station (path 1)
- F-CPU of the substation
  - Transmits the signature to the F-CPU of the control station (section 2, path 2)

**Subsystem 2 executes function block 2 EVALUATION**

This subsystem consists of the components

- F-CPU of the control station
- Assumption: F-DO of the substation

Therefore, subsystem 2 consists of certified safety components only.

In accordance with IEC 62061, the probability of dangerous transmission errors has to be considered for digital communication processes, in this case the data transmission via Industrial Ethernet. This consideration takes effect once in a (freely selectable) subsystem of the communication. In this example, we select subsystem 2 for that.

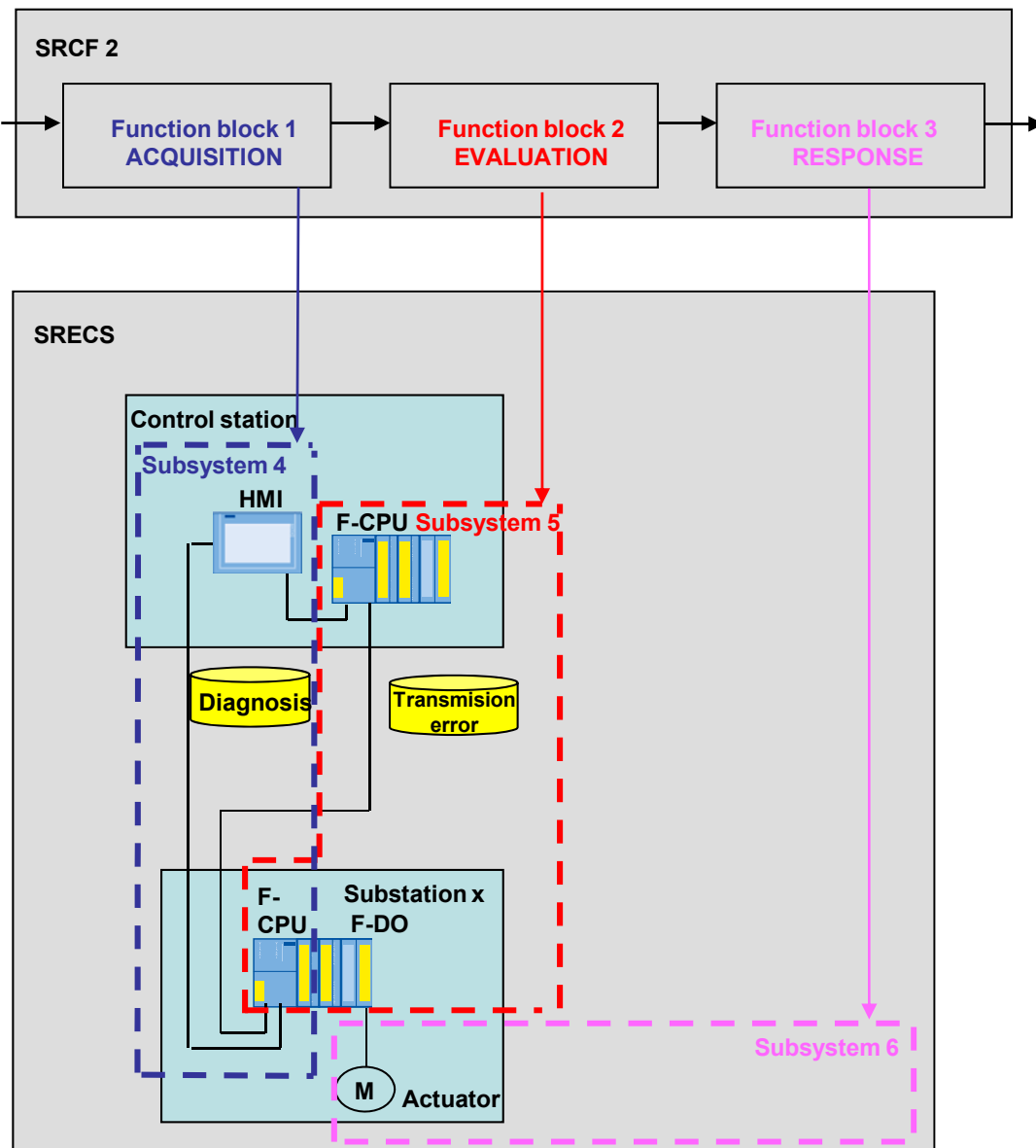
**Subsystem 3 executes function block 3 RESPONSE**

This subsystem consists of the components

- Assumption: Contactors  $K_1$  and  $K_2$

## 7.2.2 SRECS executes SRCF 2

Figure



**Explanation of the figure****Subsystem 4 executes function block 1 ACQUISITION**

This subsystem comprises the following:

- HMI of the control station
  - Transmits the signature to the F-CPU of the substation
- F-CPU of the substation
  - Safely detects signature errors

**Subsystem 5 executes function block 2 EVALUATION**

This subsystem comprises the following:

- F-CPU of the control station
- F-CPU of the substation
- Assumption: F-DO of the substation

The transmission errors for digital communication processes are considered in this subsystem 5.

If a signature error is detected in the F-CPU of the substation, this error information is transmitted to the control station. The F-CPU of the control station sets the error bit, which makes the substation change to the ERROR\_CS state.

Due to this convention that signature errors are assigned to the control station, all components except for the HMIs are involved in this subsystem.

**NOTICE**

**The convention made here was made on condition that it is not a time-critical application.**

Of course, the signature error detected in the substation can also be interpreted as local error (ERROR LOCAL). The respective STEP 7 program has to be changed correspondingly for that.

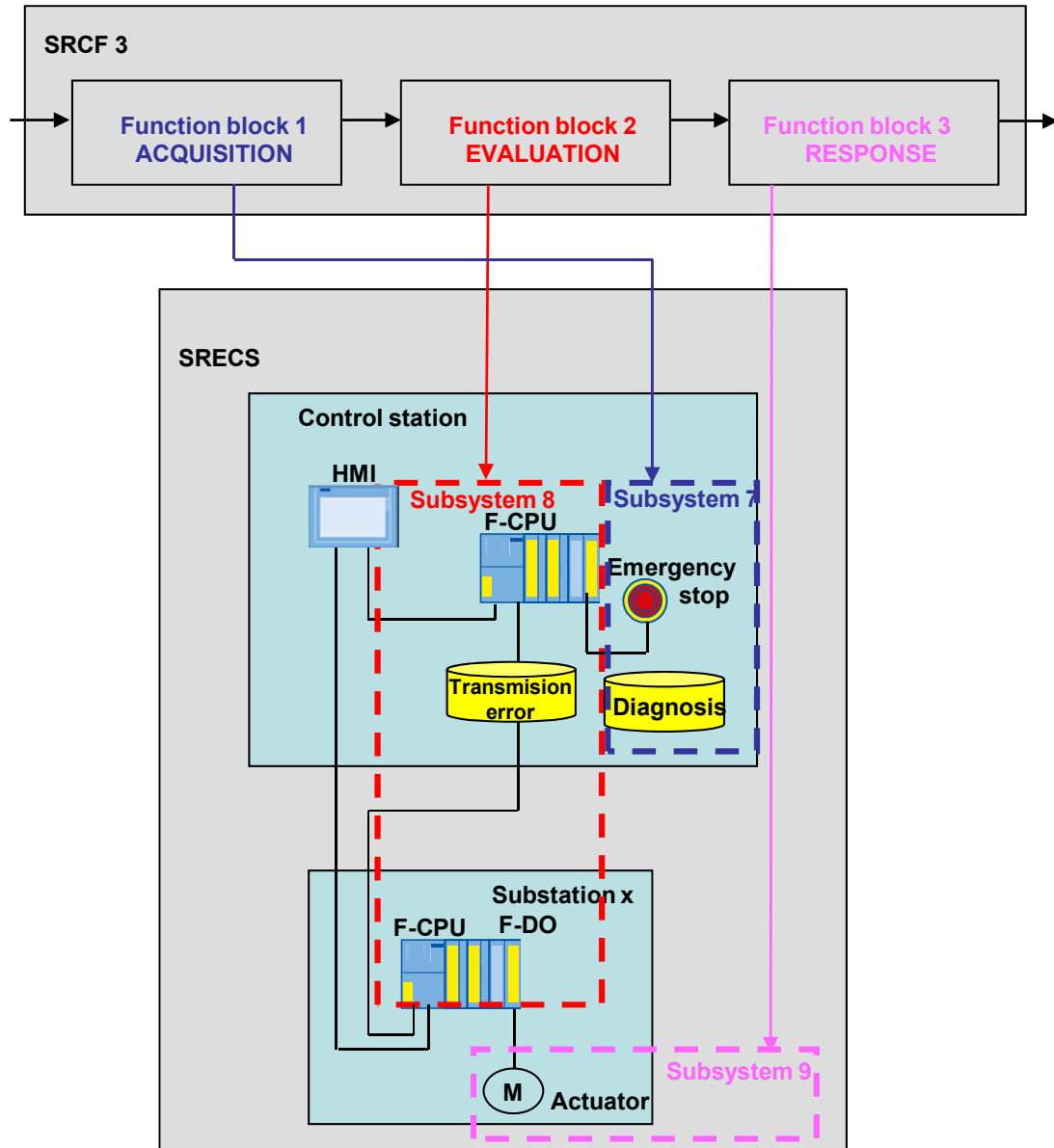
**Subsystem 6 executes function block 3 RESPONSE**

This subsystem consists of the components

- Assumption: Contactors  $K_1$  and  $K_2$

### 7.2.3 SRECS executes SRCF 3

Figure



### Explanation of the figure

#### **Subsystem 7 executes function block 1 ACQUISITION**

This subsystem comprises the following:

- Emergency stop button of the control station

#### **Subsystem 8 executes function block 2 EVALUATION**

This subsystem comprises the following:

- F-CPU of the control station
- F-DI of the control station
- F-CPU of the substation
- Assumption: F-DO of the substation

The transmission errors for digital communication processes are considered in this subsystem 8.

#### **Subsystem 9 executes function block 3 RESPONSE**

This subsystem consists of the components

- Assumption: Contactors  $K_1$  and  $K_2$

## 7.3 SIL of the safety function for SRCF 1

### Assumptions

In this example, the F-program safely provides an error bit. The error response is individual and is not considered in the functionality of this example. For the standards consideration, we have to assume concretely used components to be able to make the calculations. For this reason, the standard consideration is based on the following assumptions for the substation:

#### Assumption:

F-DO in the central rack, which activates and deactivates two contactors in parallel (as actuator) via a (safe) output.

The read back contacts of both contactors are connected to a standard DI.

Data of the assumed components:

Component	Qty.	Order number	Value
Electronic module 4F-DO DC24V/2A	1	6ES7138-4FB03-0AB0	$PFH_{D(F-DO\_SUBx)} = 10^{-10}$
Contactors AC-3, 3KW/400V, 1NC, DC 24V	2	3RT1015-2BB42	See following table

### 7.3.1 SIL CL and $PFH_D$ of subsystem 1

#### Hardware fault tolerance (HFT)

The signature reaches the F-CPU of the control station via two independent paths. The starting point of both paths is the HMI of the control station. Although the transmission of the signature is triggered via two independent buttons on the HMI, the hardware (panel) is the same so that **HFT=0** is assumed.

#### Safe failure fraction (SFF)

All dangerous failures are detected through diagnosis: **SFF=99%**.

#### SIL CL

According to Table 5 of IEC 62061, the following results from HFT=0 and SFF=99%: **SIL CL 3**

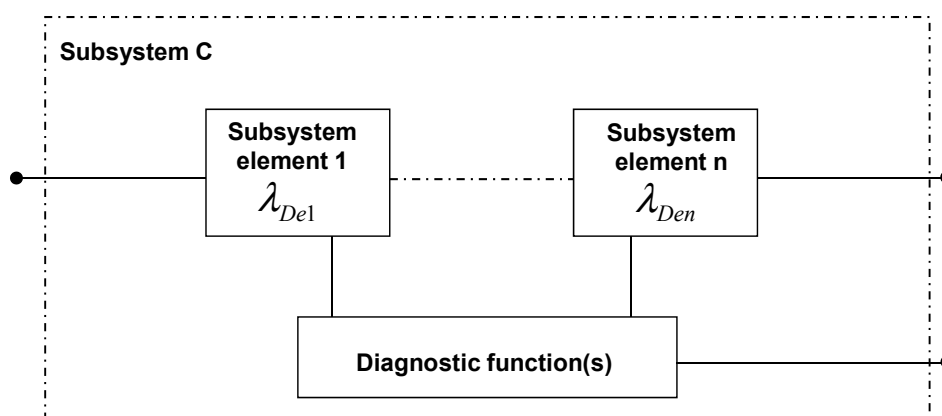
#### $PFH_D$

The following values can be calculated or apply:

Value of the subsystem element	Component	Calculation	Result / Specification
$\lambda_{De(HMI\_CS)}$	HMI control station	MTBF=8.7a $\lambda_{DeHMI\_CS} = \frac{1}{2 \cdot MTBF}$	$65.61 \cdot 10^{-7} h^{-1}$
$PFH_{D(F-CPU\_CS)}$	F-CPU control station	See section 8.2 "Internet links" under /5/	$10^{-9}$
$PFH_{D(F-CPU\_SUBx)}$	F-CPU substation	See section 8.2 "Internet links" under /5/	$1.09 \cdot 10^{-9}$

In this subsystem it is the case that apart from the certified safety components (F-CPU) also a non-safety component (HMI) is involved. For this reason, the basic subsystem architecture C "Zero fault tolerance with diagnostic function" of IEC 62061 is considered:

#### Basic subsystem architecture C



Related formulas:

$$PFH_{DssC} = \lambda_{DssC} \cdot 1h$$

and

$$\lambda_{DssC} = \lambda_{De1} \cdot (1 - DC_1) + \dots + \lambda_{Den} \cdot (1 - DC_n)$$

Therefore, we assume the following for the HMI:

$$\lambda_{DssC} = \lambda_{De(HMI\_CS)} \cdot (1 - DC_1) = 65.61 \cdot 10^{-7} h^{-1} \cdot 0.01 = 0.66 \cdot 10^{-7} h^{-1}$$

or

$$PFH_{DssC} = PFH_{D(HMI\_CS)} = 0.66 \cdot 10^{-7}$$

For the diagnostic coverage  $DC_1$  of the respective function, we assume 99% and refer to Table E1 of ISO 13849-1:2006, which allows this value for plausibility considerations. In this example, the plausibility consideration is the evaluation in the F-program of the F-CPU of the control station (diagnosis).

The PFH values of the two certified safety components (F-CPU) are known. In these, the diagnostic characteristics are already considered. For this reason, the formula of the basic subsystem architecture is not applied to the two F-CPU.

Therefore, the following results for subsystem 1:

$$PFH_{D(subsystem1)} = PFH_{D(HMI\_CS)} + PFH_{D(F-CPU\_CS)} + PFH_{D(F-CPU\_SUBx)}$$

$$PFH_{D(subsystem1)} = 0.68 \cdot 10^{-7}$$

### 7.3.2 SIL CL and PFH<sub>D</sub> of subsystem 2

#### SIL CL

Subsystem 2 consists of certified safety components only, which achieve SIL CL 3. For this reason, there are no further diagnostics-related considerations by the user required. The safety-related data of the components are specified by the manufacturer (here: SIEMENS). All diagnostics-related considerations are already considered in the manufacturer data on SIL CL or PFH<sub>D</sub>.

The same statements apply analogously to the SIL CL.

#### PFH<sub>D</sub>

Besides the PFHD value of F-CPU (control station) and F-DO (substation), the transmission error is assumed with the following defined value:

$$P_{TE} = 10^{-9} \text{ (considered once per SRCF in one subsystem).}$$

Therefore, the following results for subsystem 2:

$$PFH_{D(subsystem2)} = PFH_{D(F-CPU\_CS)} + PFH_{D(F-DO\_SUBx)} + P_{TE} = 10^{-9} + 10^{-10} + 10^{-9}$$

$$PFH_{D(subsystem2)} = 2.1 \cdot 10^{-9}$$

### 7.3.3 SIL CL and PFH<sub>D</sub> of subsystem 3

#### Determining the HFT

The reading back of the auxiliary contacts of the contactors would be realized with the certified FB F\_FDBACK from the block library of Distributed Safety. A read back error would be safely detected and lead to a safe shutdown of the actuators (contactors).

Therefore, subsystem 3 achieves a **HFT = 1**.

#### Determining the SFF

All dangerous failures are detected through diagnosis: **SFF=99%**.

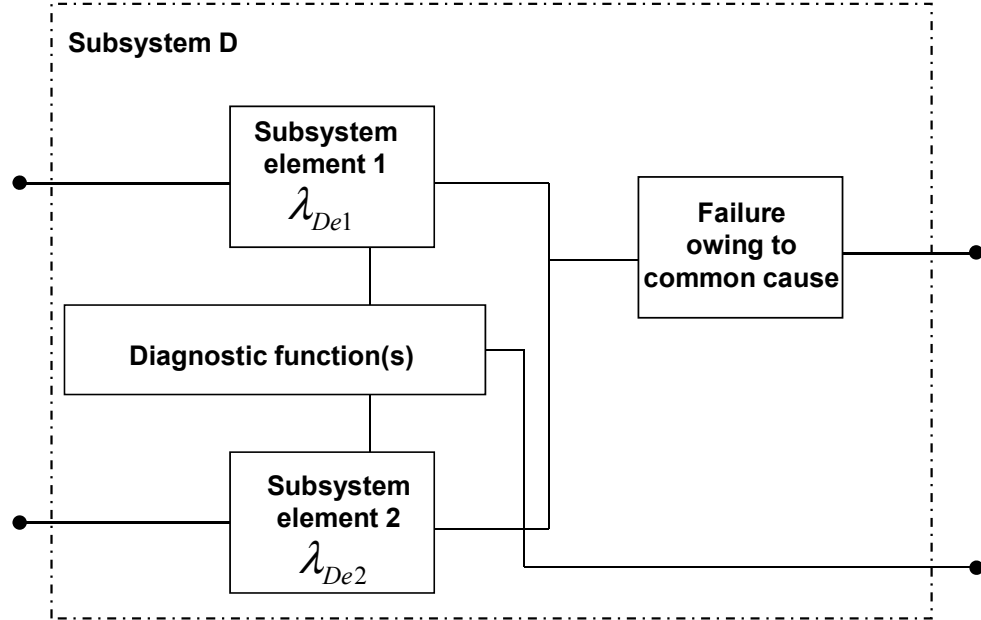
#### Determining the SIL CL

According to Table 5 of IEC 62061, the following results from HFT=1 and SFF=99%: **SIL CL 3**



**Determining the PFH<sub>D</sub>**

For the determination of the PFH<sub>D</sub> value, the basic subsystem architecture D of IEC 62061 is used (single fault tolerance with diagnostic function).

**Basic subsystem architecture D**

Related formulas:

$$PFH_D = \lambda_D \cdot 1h$$

and

$$\lambda_{DSSD} = (1 - \beta)^2 \cdot \left\{ \left[ \lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2) \cdot \frac{1}{2} \cdot T_2 \right] + \left[ \lambda_{De1} \cdot \lambda_{De2} \cdot \frac{1}{2} \cdot T_1 \cdot (2 - DC_1 - DC_2) \right] \right\} + \frac{1}{2} \cdot \beta \cdot (\lambda_{De1} + \lambda_{De2})$$

The following values can be calculated or apply:

Variable	Value	Reason
$\beta$	0.1 (conservative)	Appendix F of IEC 62061 provides an estimate for $\beta$ .
$\lambda_{De1}$	$1.13 \cdot 10^{-7} h^{-1}$	<p>The subsystem element consists of contactor K1 or K2.</p> $\lambda = 0.1 \cdot \frac{C}{B_{10}}$ <p>The rate of dangerous failures is 75%: <math>\lambda_{De1} = 0.75 \cdot \lambda</math></p> <p><u>Determining C</u> C is the amount of contactor operations. We assume that the contactor switches 12 times per shift. In three-shift operation, this would be 36 switching cycles per day or: C = 1.5/h</p> <p><u>Determining the <math>B_{10}</math> value</u> Manufacturer data: <math>B_{10} = 1 \cdot 10^6</math></p> $\lambda_{De1} = 0.1 \cdot 1.5 \cdot h^{-1} \cdot 10^{-6} \cdot 0.75 = 1.13 \cdot 10^{-7} h^{-1}$
$\lambda_{De2}$		<p>For the consideration, we assume identical components:</p> $\lambda_{De1} = \lambda_{De2}$
$DC_1$	0,99	Mathematically, we have a DC = 1 because of $\lambda_{DU} = 0$ . Since the table assumes DC = 99% max. for the estimation of the DC (Appendix E of ISO 13849-1:2006), we select DC = 0.99.
$DC_2$	0,99	$DC_1 = DC_2$ applies.
$T_1$	20a	Typical value for a contactor
$T_2$	0.67h	Assumption: 12 switching cycles per shift (every 0.67 hours).

Through  $\lambda_{De} = \lambda_{De1} = \lambda_{De2}$  and  $DC = DC_1 = DC_2$ , the formula is simplified as:

$$\lambda_{DssD} = (1 - \beta)^2 \cdot \lambda_{De}^2 \cdot [T_2 \cdot DC + T_1 \cdot (1 - DC)] + \beta \cdot \lambda_{De}$$

With the assumed values, the following results:

$$\lambda_{DssD} = 0.81 \cdot (1.13 \cdot 10^{-7})^2 \cdot \frac{1}{h^2} \cdot [0.67h \cdot 0.99 + 20 \cdot 365 \cdot 24h \cdot 0.01] + 0.1 \cdot 1.13 \cdot 10^{-7} \frac{1}{h}$$

$$\lambda_{DssD} = 0.11 \cdot 10^{-7} h^{-1}$$

or

$$PFH_{D(subsystem3)} = 0.11 \cdot 10^{-7}$$

### 7.3.4 Result for SRCF 1

The  $PFH_D$  value for SRCF1 results from the sum of the  $PFH_D$  values of subsystems 1 to 3:

$$PFH_{D(SRCF1)} = PFH_{D(subsystem1)} + PFH_{D(subsystem2)} + PFH_{D(subsystem3)}$$

$$PFH_{D(SRCF1)} = 0.81 \cdot 10^{-7}$$

**SRCF 1 meets SIL 3 in accordance with IEC 62061** because:

- the subsystems 1 to 3 each achieve SIL CL 3
- $PFH_{D(SRCF1)} < 10^{-7}$

## 7.4 SIL of the safety function for SRCF 2

### 7.4.1 SIL CL and $PFH_D$ of subsystem 4

#### SIL CL and $PFH_D$

Except for the F-CPU of the control station, the same components are involved in this subsystem as in subsystem 1 (for the execution of the ACQUISITION function block of SRCF 1). The statements on SIL CL and  $PFH_D$  can be applied analogously.

Therefore, the following can be applied directly from section 7.3.1:

- HFT = 0
- SFF = 99%
- SIL CL 3

$$PFH_{D(subsystem4)} = PFH_{D(HMI\_CS)} + PFH_{D(F-CPU\_SUBx)}$$

$$PFH_{D(subsystem4)} = 0.67 \cdot 10^{-7}$$

### 7.4.2 SIL CL and $PFH_D$ of subsystem 5

#### SIL CL

Subsystem 2 consists of certified safety components only. For this reason, there are no further diagnostics-related considerations by the user required. The safety-related data of the components are specified by the manufacturer (here: SIEMENS). All diagnostics-related considerations are already considered in the manufacturer data on SIL CL or  $PFH_D$ .

The same statements apply analogously to the SIL CL.

#### $PFH_D$

Besides the  $PFH_D$  values of the F-CPU and F-DO (substation), the transmission error is assumed with the following defined value:  $P_{TE} = 10^{-9}$  (considered once per SRCF in one subsystem). Therefore, the following results for subsystem 5:

$$PFH_{D(subsystem5)} = PFH_{D(F-CPU\_CS)} + PFH_{D(F-CPU\_SUBx)} + PFH_{D(F-DO\_SUBx)} + P_{TE}$$

$$PFH_{D(subsystem5)} = 10^{-9} + 1.09 \cdot 10^{-9} + 10^{-10} + 10^{-9}$$

$$PFH_{D(subsystem5)} = 3.19 \cdot 10^{-9}$$

### 7.4.3 SIL CL and PFH<sub>D</sub> of subsystem 6

#### SIL CL

For the actuators, the statements in section 7.3.3 (**HFT = 1**; **SFF = 99%**) apply so that **SIL CL 3** can also be assumed here.

#### PFH<sub>D</sub>

The statements in section 7.3.3 apply. Therefore, the following applies:

$$PFH_{D(subsystem6)} = 0.11 \cdot 10^{-7}$$

### 7.4.4 Result for SRCF 2

The PFH<sub>D</sub> value for SRC2 results from the sum of the PFH<sub>D</sub> values of subsystems 4 to 6:

$$PFH_{D(SRCF2)} = PFH_{D(subsystem4)} + PFH_{D(subsystem5)} + PFH_{D(subsystem6)}$$

$$PFH_{D(SRCF2)} = 0.81 \cdot 10^{-7}$$

**SRCF 2 meets SIL 3 in accordance with IEC 62061** because:

- the subsystems 4 to 6 each achieve SIL CL 3
- $PFH_{D(SRCF1)} < 10^{-7}$

## 7.5 SIL of the safety function for SRCF 3

### 7.5.1 SIL CL and PFH<sub>D</sub> of subsystem 7

#### Hardware fault tolerance (HFT)

Due to the dual-channel design, the following applies: **HFT = 1**

#### Safe failure fraction (SFF)

All dangerous failures are detected through diagnosis: **SFF=99%**.

#### SIL CL

According to Table 5 of IEC 62061, the following results from HFT=1 and SFF=99%: **SIL CL 3**

#### PFH<sub>D</sub>

Basic subsystem architecture D is applied for the calculation (see section 7.3.3). The following values are assumed:

Variable	Value	Reason
$\beta$	0.1 (conservative)	Appendix F of IEC 62061 provides an estimate for $\beta$ .
$\lambda_{De1}$	$0.84 \cdot 10^{-7} h^{-1}$	<p>The subsystem element consists of two positively opening contacts (NC/NC)</p> $\lambda_{De1} = 0.1 \cdot \frac{C}{B_{10}}$ <p>The rate of dangerous failures is 20%: <math>\lambda_{De1} = 0.2 \cdot \lambda</math></p> <p><u>Determining C</u> C is the amount of emergency stop actuations. It is assumed that the emergency stop is actuated 10 times a day. C = 0.42/h</p> <p><u>Determining the B<sub>10</sub> value</u> Manufacturer data: <math>B_{10} = 1 \cdot 10^5</math></p> $\lambda_{De1} = 0.1 \cdot 0.42 \cdot h^{-1} \cdot 10^{-5} \cdot 0.2 = 0.84 \cdot 10^{-7} h^{-1}$
$\lambda_{De2}$		<p>For the consideration, we assume identical components: <math>\lambda_{De1} = \lambda_{De2}</math></p>
$DC_1$	0,99	Mathematically, we have a DC = 1 because of $\lambda_{DU} = 0$ . Since the table assumes DC = 99% max. for the estimation of the DC (Appendix E of ISO 13849-1:2006), we select DC = 0.99.
$DC_2$		$DC_1 = DC_2$ applies.
$T_1$	20a	Life expectancy
$T_2$	2.4h	Assumption: 10 actuations a day (= every 2.4h)

The following applies:

$$\lambda_{DSSD} = 0.81 \cdot (0.84 \cdot 10^{-7})^2 h^{-2} [2.4h \cdot 0.99 + 20 \cdot 365 \cdot 24h \cdot 0.01] + 0.1 \cdot 0.84 \cdot 10^{-7} h^{-1}$$

$$\lambda_{DSSD} = 0.084 \cdot 10^{-7} h^{-1}$$

or

$$PFH_{D(subsystem7)} = 0.084 \cdot 10^{-7}$$

## 7.5.2 SIL CL and PFH<sub>D</sub> of subsystem 8

### SIL CL

Subsystem 8 consists of certified safety components only. For this reason, there are no further diagnostics-related considerations by the user required. The safety-related data of the components are specified by the manufacturer (here: SIEMENS). All diagnostics-related considerations are already considered in the manufacturer data on SIL CL or PFH<sub>D</sub>.

The same statements apply analogously to the SIL CL.

### PFH<sub>D</sub>

Besides the PFH<sub>D</sub> values of the F-CPU, F-DI (control station) and F-DO (substation), the transmission error is assumed with the following defined value:

$$P_{TE} = 10^{-9} \text{ (considered once per SRCF in one subsystem).}$$

Therefore, the following results for subsystem 2:

$$PFH_{D(subsystem8)} = PFH_{D(F-CPU\_CS)} + PFH_{D(F-DI\_CS)} + PFH_{D(F-CPU\_SUBx)} + PFH_{D(F-DO\_SUBx)} + P_{TE}$$

$$PFH_{D(subsystem8)} = 10^{-9} + 10^{-8} + 1.09 \cdot 10^{-9} + 10^{-10} + 10^{-9}$$

$$PFH_{D(subsystem8)} = 0.13 \cdot 10^{-7}$$

## 7.5.3 SIL CL and PFH<sub>D</sub> of subsystem 9

### SIL CL

For the actuators, the statements in section 7.3.3 (**HFT = 1**; **SFF = 99%**) apply so that **SIL CL 3** can also be assumed here.

### PFH<sub>D</sub>

The statements in section 7.3.3 apply. Therefore, the following applies:

$$PFH_{D(subsystem9)} = 0.11 \cdot 10^{-7}$$

### 7.5.4 Result for SRCF 3

The  $PFH_D$  value for SRC2 results from the sum of the  $PFH_D$  values of subsystems 7 to 9:

$$PFH_{D(SRCF2)} = PFH_{D(subsystem7)} + PFH_{D(subsystem8)} + PFH_{D(subsystem9)}$$

$$PFH_{D(SRCF2)} = 0.32 \cdot 10^{-7}$$

**SRCF 3 meets SIL 3 in accordance with IEC 62061** because:

- the subsystems 7 to 9 each achieve SIL CL 3
- $PFH_{D(SRCF1)} < 10^{-7}$

## 7.6 Summary

The calculations made prove that SIL 3 in accordance with IEC 62061 can be achieved by applying the safety concept described herein.

The achievement of SIL 3 depends in particular on the used hardware. In particular the MTBF of the HMI of the control station influences the  $PFH_D$  value of the subsystem. The better (higher) the MTBF of the used HMI of the control station, the better (lower) becomes the  $PFH_D$  value of the subsystem.

## 8 References

### 8.1 Bibliographic references

The following list is by no means complete and only provides a selection of appropriate sources.

	Topic	Title
/1/	STEP7	Automating with STEP7 in STL and SCL Hans Berger Publicis Publishing ISBN 3895782955
/2/	Standards for safety technology	Funktionale Sicherheit von Maschinen und Anlagen: Umsetzung der Europäischen Maschinenrichtlinie in der Praxis [Functional safety of machines and systems: Practical implementation of the European Machinery Directive] Patrick Gehlen Publicis Publishing ISBN 3895783668

### 8.2 Internet links

The following list is by no means complete and only provides a selection of appropriate sources.

	Topic	Title
\1\	Reference to the entry	<a href="http://support.automation.siemens.com/WW/view/en/EntryID">http://support.automation.siemens.com/WW/view/en/EntryID</a>
\2\	Siemens I CS Customer Support	<a href="http://support.automation.siemens.com">http://support.automation.siemens.com</a>
\3\	Distributed Safety	Distributed Safety - configuring and programming <a href="http://support.automation.siemens.com/WW/view/en/22099875">http://support.automation.siemens.com/WW/view/en/22099875</a>
\4\	WinCC flexible 2008	WinCC flexible 2008 Communication Part 1 <a href="http://support.automation.siemens.com/WW/view/en/18797552">http://support.automation.siemens.com/WW/view/en/18797552</a>
\5\	PFH values	FAQ: Which values can you use with F-CPU's and products of the ET 200 family for PFD, PFH and the proof test interval? <a href="http://support.automation.siemens.com/WW/view/en/27832836">http://support.automation.siemens.com/WW/view/en/27832836</a>
\6\	MTBF list for SIMATIC products	Download: MTBF list for SIMATIC products <a href="http://support.automation.siemens.com/WW/view/en/16818490">http://support.automation.siemens.com/WW/view/en/16818490</a>

## 9 History

Version	Date	Revision
V1.0	03/2012	First issue