Fail-safe Controllers

SIMATIC Safety Integrated

Passivation and Reintegration of F-I/O considering as example the ET 200S

Functional Example no. AS-FE-I-011-V10-EN

safety INTEGRATED

SIEMENS

Preliminary Remarks

The functional examples dealing with “Safety Integrated” are fully functional and tested automation configurations based on A&D standard products for simple, fast and inexpensive implementation of automation tasks in safety engineering. Each of these function examples covers a frequently occurring subtask of a typical customer problem in safety engineering.

Apart from a list of all required hardware and software components and a description of the way they are connected to each other, the function examples include the tested and commented code. This ensures that the functionalities described here can be reset in a short period of time and thus also be used as basis for individual expansions.

Important Note

The Safety Functional Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Safety Functional 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 Safety Functional Examples do not relieve you of the responsibility in safely and professionally using, installing, operating and servicing equipment. When using these Safety Functional Examples, you recognize that Siemens cannot be made liable for any damage/claims beyond the liability clause described above. We reserve the right to make changes to these Safety Functional Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Safety Function Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

Conventions in the document on hand

Terms used in the text

Table 1-1

Term	Explanations
”Safety engineering“ ”F-technology“	Both terms have the same meaning.
“fail-safe“ ”F-“	Both terms have the same meaning. Example: “F-DI" means “Fail-safe Digital Input module".
User program Safety program Standard program	The three terms refer to the STEP7 program of the F-CPU. The overall STEP7 program is the “user program”. It consists of the “safety program“ and the “standard program”.
F-system	In this document, the term “F-system“ is used as a general term for “operating system of the F-CPU“ and “operating system of the F-I/O-module“. The term is necessary to be able to distinguish between the following in the text: • Action by the **user** (e.g. pressing an acknowledge button) • Action by the **operating system** of the F-CPU or the F-I/O-module (e.g. passivation of an F-I/O-module)

Color code for background shades

Table 1-2

Background color	Meaning
light blue	Standard application, standard program
light yellow	Fail-safe application, safety program

Names of process signals

Process signals are named with capital letters in this document and in the example code.

Example: “ACTUATOR“ refers to a process signal

Table of Contents

1 Warranty, Liability and Support

We accept no 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, engineering and performance data etc., described in this Safety Function 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 a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). However, claims arising from a breach of a condition which goes to the root of the contract 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.

For questions about this document please use the following e-mail-address:

csweb@ad.siemens.de

2 Automation Function

2.1 Scope of validity of the functional example

The functional example applies for the following framework conditions:

Hardware:

- CPU 315F-2 DP, with PROFIsafe I/O modules ET 200S

Software:

- STEP 7 V5.3 + SP3
- S7 Distributed Safety V5.4, and S7 F Configuration Pack V5.4 + SP1

2.2 Functionality of the functional example

Task

The fail-safe system “S7 Distributed Safety“ enables realizing safety functions at machines. Proper functioning of the “S7 Distributed Safety“ system is necessary as human health depends on it and it avoids damage to machines.

In case of an error, the “S7 Distributed Safety“ system must behave so that the machine remains fail-safe or will be turned fail-safe. An error at the F-I/O-module for example (e.g. wire break at actuator or sensor) turns the affected F-I/O-module fail-safe, i.e. it is “passivated“.

This functional example demonstrates “passivation“ and “reintegration“ of fail-safe I/O modules in the “S7 Distributed Safety“ system.

Solution

A concrete example from practice illustrates the behavior of “S7 Distributed Safety“ in case of errors at the F-I/O-module:

- Passivation *channels* due to wire-break at an F-DO.
  Manual reintegration after error has been removed.
- Passivation *entire module* due to wire-break at an F-DI.
  Automatic reintegration after error has been removed.
- Passivation of the F-I/O-module due to disconnecting F-CPU and distributed station.
  Reintegration after error has been removed.

Apart from the practical application, the functional example provides extensive background knowledge on the topic of “passivation“ and ”reintegration“.

Note In this functional example, the combination of type of passivation (channels, entire module), type of F-module (F-DO, F-DI), and type of reintegration (manual, automatic) is exemplary. Other combinations can also be realized.

2.3 Advantage / Customer benefits

The “passivation“ and “reintegration“ functions of “S7 Distributed Safety“ have the following function:

- Errors at the F-I/O-module are turned fail-safe.
- F-modules can be passivated entirely or by channels.
- If an F-module passivates, passivation of further F-modules can be “forced“.
- After the error has been removed, the reintegration occurs only after acknowledgement by the user. In cases where an automatic startup of the plant is not possible, reintegration can also occur automatically.

3 Required Components

In this chapter you find an overview of hardware and software components required for the functional example.

Hardware components

Table 3-1

Component	Type	MLFB / Order information	No.	Manufacturer
Power supply	PS307 5A	6ES73071EA00-0AA0	1	SIEMENS
S7-CPU, can be used for safety applications	CPU 315F-2 DP	6ES7315-6FF01-0AB0	1	
Micro Memory Card	MMC 512 KByte	6ES7953-8LJ10-0AA0	1	
Interface module for ET 200S	IM 151 High Feature	6ES7151-1BA01-0AB0	1	
Power module for ET 200S	PM-E DC24..48V AC24..230V	6ES7138-4CB10-0AB0	2	
Electronic module for ET 200S	4 DI, DC 24V, Standard	6ES7131-4BD01-0AA0	1	
Electronic module for ET 200S	4 DO, DC 24V/0,5A, Standard	6ES7132-4BD01-0AA0	1	
Electronic module for ET 200S	4/8 F-DI, DC 24V, PROFIsafe	6ES7138-4FA02-0AB0	1	
Electronic module for ET 200S	4 F-DO, DC24V/2A, PROFIsafe	6ES7138-4FB02-0AB0	1	
Terminal module for ET 200S	TM-P15C22-01	6ES7193-4CE10-0AA0	2	
Terminal module for ET 200S	TM-E15C23-01	6ES7193-4CB10-0AA0	2	
Terminal module for ET 200S	TM-E30C44-01	6ES7193-4CG30-0AA0	2	
S7-300, mounting rail	Length 482.6 mm	6ES7390-1AE80-0AA0	1	
Standard mounting rail for ET 200S	35 mm, length:483 mm	6ES5710-8MA11	1	
Indicator light including incandescent lamp	yellow	3SB3217-6AA30	2	
Indicator light including incandescent lamp	green	3SB3217-6AA40	1	
Indicator light including incandescent lamp	white	3SB3217-6AA60	2	
Push button	green, 1NO	3SB3801-0DA3	3	
Emergency stop	Push button, 2NC	3SB3801-0DG3	1	

Note The functionality was tested with the listed hardware components. Similar products not included in the above list can also be used. Please note that in such a case changes in the sample code (e.g. setting different addresses) may become necessary.

Software components

Table 3-2

Component	Type	MLFB / Order information	No.	Manufacturer
STEP 7	V5.3 + SP3	6ES7810-4CC07-0YA5	1	SIEMENS
S7 Distributed Safety	V5.4	6ES7833-1FC02-0YA5	1	
S7 F Configuration Pack + SP1	V5.4	---	1	

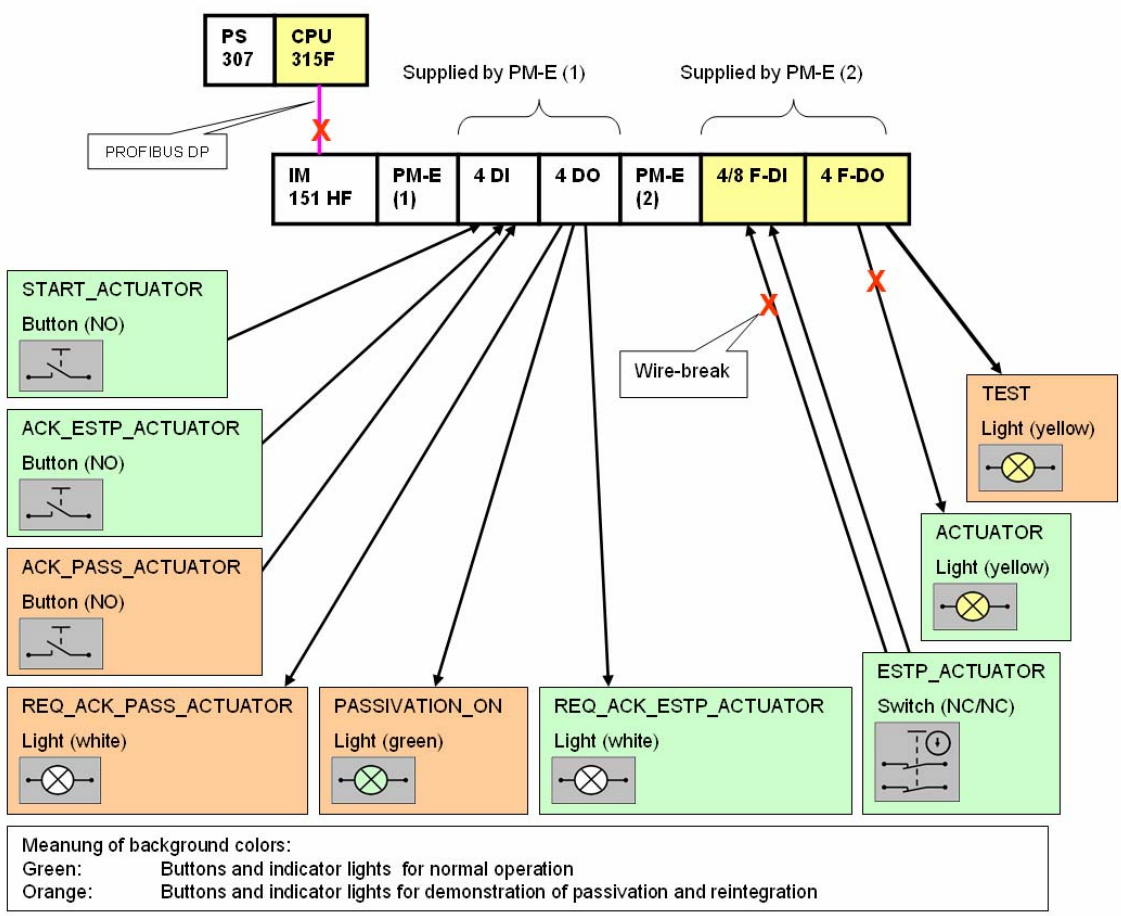
4 Setup and Wiring

This chapter describes hardware setup and wiring of the functional example.

4.1 Overview of hardware configuration

The arrangement used to demonstrate passivation and reintegration consists of a PROFIBUS configuration. A fail-safe S7-CPU is used as DP master, an ET 200S as DP slave. Passivation is triggered by means of disconnections (simulated wire-break) at F-DI, F-DO or DP interface.

Figure 4-1



4.2 Wiring of hardware components

This chapter contains information on the setup of hardware components. It contains the required address settings and the wiring plan.

Address settings

The following addresses must be set at the DIL-switches of the hardware components.

Table 4-1

Hardware component	Address to be set at the DIL switch	Note
IM 151 HIGHFEATURE	3 (PROFIBUS address)	You can change the PROFIBUS address.
4/8 F-DI	0011001000 (PROFIsafe address)	The PROFIsafe addresses are automatically assigned when configuring the fail-safe modules in STEP 7. Please ensure that the setting at the address switch of the F-I/O-module (DIP switch) on the module side corresponds to the PROFIsafe address in the hardware configuration of STEP7.
4 F-DO	0011000111 (PROFIsafe-Address)	

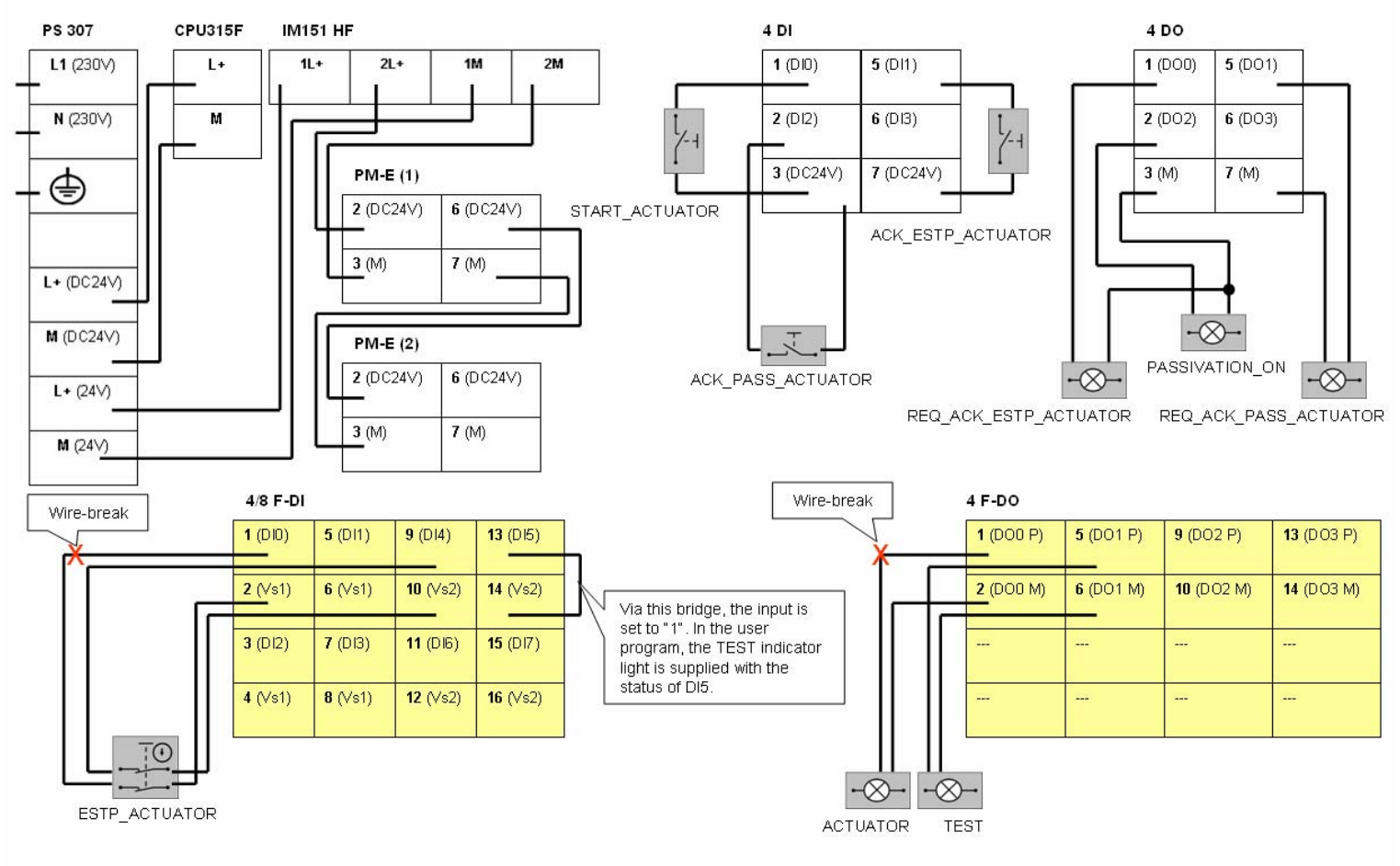
Wiring plan

Please wire the hardware components according to the wiring plan on the next page (Figure 4-2)

Please include the following **additional** wiring settings:

- Power supply “PS 307“ with 230V AC
- Connect the DP interface of the CPU 315F-2 DP with the DP interface of the IM 151 HF.

Figure 4-2


PS 307
CPU315F
IM151 HF
L1 (230V)
N (230V)
L+ (DC24V)
M (DC24V)
L+ (24V)
M (24V)
L+
M
1L+
2L+
1M
2M
PM-E (1)
2 (DC24V)
6 (DC24V)
3 (M)
7 (M)
PM-E (2)
2 (DC24V)
6 (DC24V)
3 (M)
7 (M)
4 DI
1 (DI0)
5 (DI1)
2 (DI2)
6 (DI3)
3 (DC24V)
7 (DC24V)
START_ACTUATOR
ACK_ESTP_ACTUATOR
ACK_PASS_ACTUATOR
4 DO
1 (DO0)
5 (DO1)
2 (DO2)
6 (DO3)
3 (M)
7 (M)
PASSIVATION_ON
REQ_ACK_ESTP_ACTUATOR
REQ_ACK_PASS_ACTUATOR
Wire-break
4/8 F-DI
1 (DI0)
5 (DI1)
9 (DI4)
13 (DI5)
2 (Vs1)
6 (Vs1)
10 (Vs2)
14 (Vs2)
3 (DI2)
7 (DI3)
11 (DI6)
15 (DI7)
4 (Vs1)
8 (Vs1)
12 (Vs2)
16 (Vs2)
Via this bridge, the input is set to "1". In the user program, the TEST indicator light is supplied with the status of DI5.
ESTP_ACTUATOR
Wire-break
4 F-DO
1 (DO0 P)
5 (DO1 P)
9 (DO2 P)
13 (DO3 P)
2 (DO0 M)
6 (DO1 M)
10 (DO2 M)
14 (DO3 M)
ACTUATOR
TEST

4.3 Overview of inputs and outputs

Overview of connected push buttons:

Table 4-2

No.	HW component (type)	Address	Symbolic address	Default	Function
1	Push button (NO)	E 0.0	START_ACTUATOR	0	This button switches on the ACTUATOR indicator light .
2	Push button (NO)	E 0.1	ACK_ESTP_ACTUATOR	0	This button acknowledges the emergency stop circuit.
3	Push button (NO)	E 0.2	ACK_PASS_ACTUATOR	0	This button acknowledges the manual reintegration of the ACTUATOR indicator light.
4	Emergency stop push button at F-DI (NC/NC)	E 1.0	ESTP_ACTUATOR	1	This button switches off the ACTUATOR indicator light .

Overview of connected indicator light:

Table 4-3

No.	HW component (color)	Address	Symbolic address	After startup	Meaning
5	Indicator light (white)	A 0.0	REQ_ACK_ESTP_ACTUATOR	1	The switched on indicator light indicates, that the emergency stop circuit requires acknowledgement.
6	Indicator light (white)	A 0.1	REQ_ACK_PASS_ACTUATOR	0	The switched on indicator light indicates, that acknowledgement for manual reintegration of the ACTUATOR indicator light is necessary.
7	Indicator light (green)	A 0.2	PASSIVATION_ON	0	The switched on indicator light indicates the current passivation.
8	Indicator light at F-DO (gelb)	A 7.0	ACTUATOR	0	The indicator light simulates the “hazardous loads”. The switched on indicator light indicates the “hazardous loads” being switched on.
9	Indicator light at F-DO (yellow)	A 7.1	TEST	1	The indicator light is only used to demonstrate the passivation of the entire module. The indicator light has no other function. Normally, TEST is always switched on. TEST is only switched off if F-DI is passivated.

4.4 Function test

After wiring the hardware components and loading the STEP 7 project into the S7-CPU (see chapter 6.2), please test the inputs (buttons) and the outputs (indicator lights) for correct functioning.

Note

A connection between the MPI interface of your PG/PC and the MPI interface of the CPU 315F-2DP (MPI cable) is required to download the STEP7 project to the CPU 315F-2DP.

Please perform the steps of the table below successively. For each step check whether the indicator light is switched on or off.

Table 4-4

Step	Action	Indicator light (*2) A: PASSIVATION_ON B: REQ_ACK_PASS_ACTUATOR C: REQ_ACK_ESTP-ACTUATOR D: AKTUATOR E: TEST				
		A	B	C	D	E (*3)
1	Mode switch of the S7-CPU: Switch from STOP to RUN (startup)	0 (*1)	0	1	0	1
2	Press: ACK_ESTP_ACTUATOR	0	0	0	0	1
3	Press: START_ACTUATOR	0	0	0	1	1
4	Press: ESTP_ACTUATOR	0	0	0	0	1
5	Press: ESTP_ACTUATOR	0	0	1	0	1
6	Press: ACK_ESTP_ACTUATOR	0	0	0	0	1

Explanations on the table:

(*1): The PASSIVATION_ON indicator light briefly lights up in step 1, as during startup the F-I/O-modules are passivated shortly.

(*2): Switched on indicators are marked with “1“. To recognize more clearly which bits change during a mode transition, they are shaded in gray: If a bit is shaded gray, it has changed compared with its previous state.

(*3): One channel of F-DI is constantly set to ”1“. In the user program this channel is read in, and it is output at the TEST indicator light.

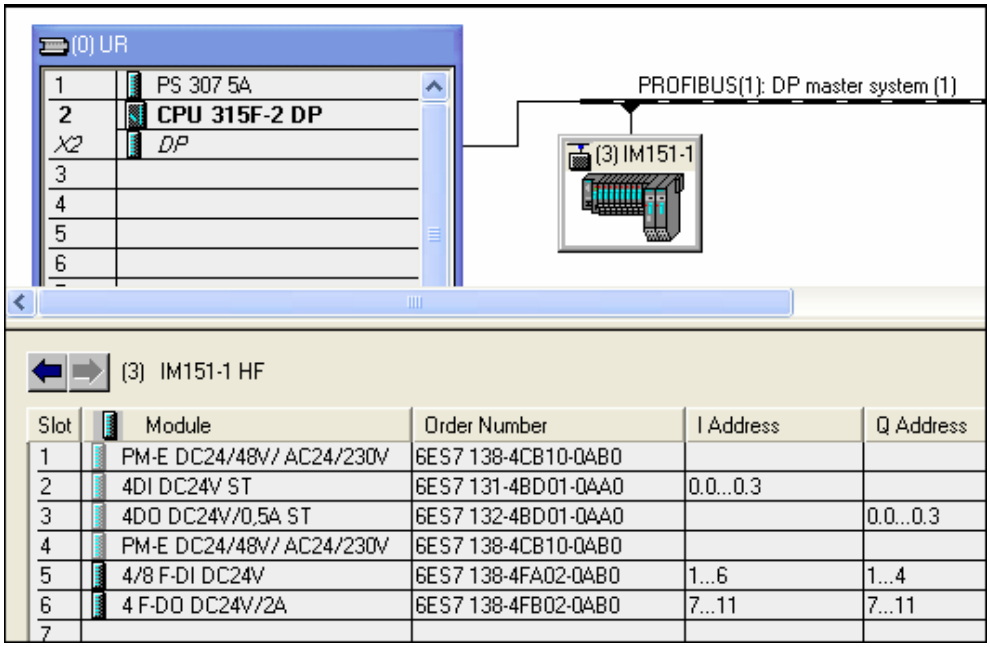
4.5 Important hardware component settings

Below, several important settings from the hardware configuration of STEP 7 are shown for your information. In the STEP 7 project (sample code, see chapter 6) of the functional example on hand, these settings have already been made.

Changes at the settings are possible (e.g. due to individual requirements). Should you implement the changes (e.g. add an additional module), the sample code has to be adapted accordingly.

4.5.1 Overview of the configuration

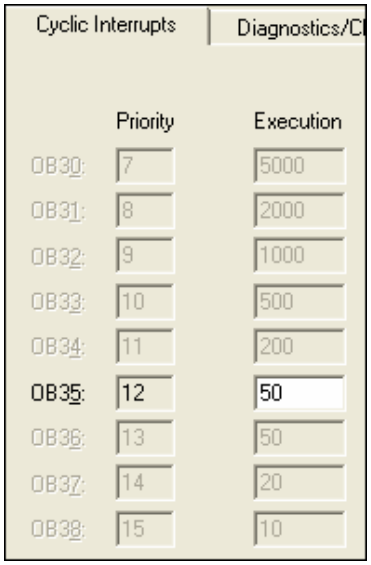
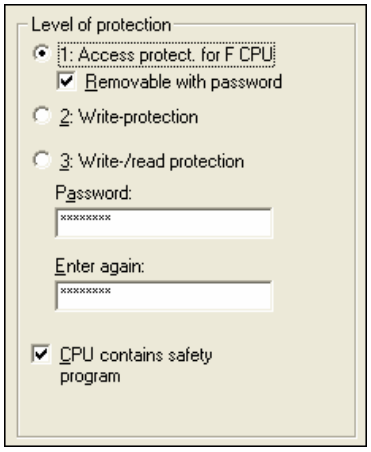
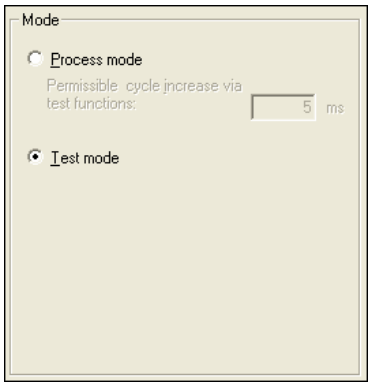
Figure 4-3



The PROFIBUS address is set at the IM 151 HF component via DIP switches. In this functional example the address 3.

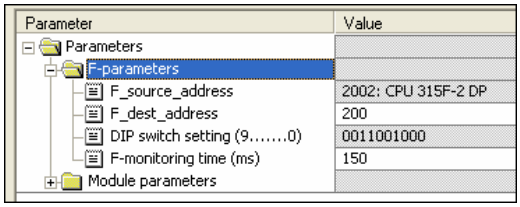
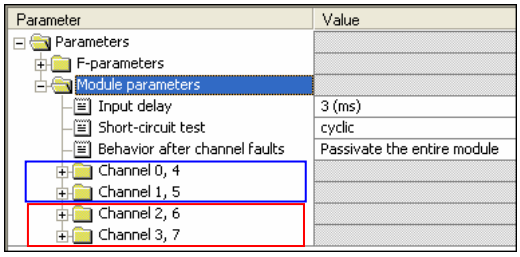
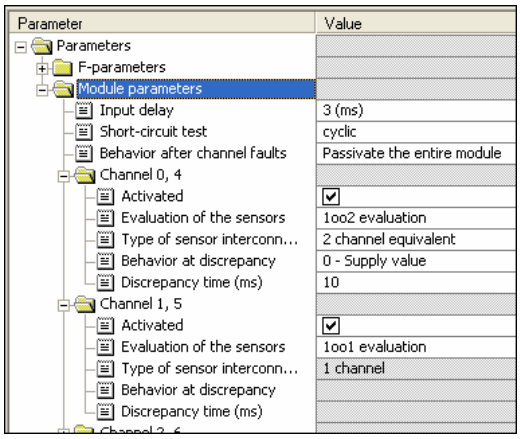
4.5.2 Setting the CPU 315F-2 DP

You reach the input dialog in the HW configuration of STEP 7 by double-clicking ”CPU 315F-2 DP“ (see Figure 4-3).

Input dialog	Notes
	**“Cyclic Interrupts“ tab:** The call time of OB35 is configured with “50ms“. Important: The monitoring time of the F-I/O-modules must be larger than the call time of OB35. Please use the Cotia table for selecting the monitoring time (“min. F monitoring time“ sheet). In chapter 5 you find the link to the Cotia table.
	**“Protection” tab:** A “Password” **must** be allocated in order to be able to set the parameter “CPU contains safety program”. It is only in this case that all required F blocks for safe operation of the F-I/O-modules are generated during the compilation of the STEP 7 hardware configuration. Password used this functional example: siemens
	**“Protection” tab:** Mode used here is “Test Mode“: The Mode field is not relevant for safety operation.

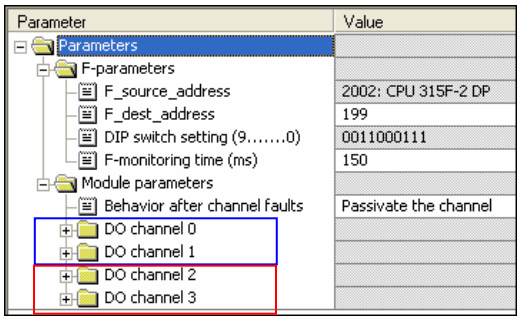
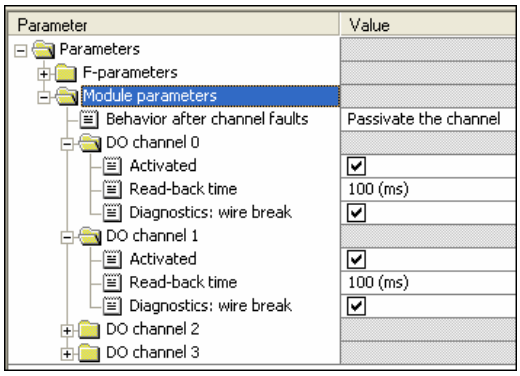
4.5.3 Settings of the F-DI

You reach the input dialog in the HW configuration of STEP 7 by double-clicking ”4/8 F-DI DC24V“ (see Figure 4-3).
All input screens are available in the “Parameter“ tab.

Input dialog	Note
	“DIP switch setting (9…0)“: The displayed value must be set at the F-DI. “F-monitoring time (ms)“: “150ms“ Important: The F-monitoring time must be larger than the call time of OB35. Please use the Cotia table for selecting the monitoring time (“min. F-monitoring time“ sheet). In chapter 5 you find the link to the Cotia table.
2 	“Short-circuit test”: “cyclic“ The two channel emergency stop button contains the power supply via the module. “Behavior after channel faults“: “Passivate the entire module“ “Channel 0.4“: “activate“ The two break contacts of the emergency stop push button are polled with a 1oo2 evaluation. “Channel 1.5“: “activate“ “1“ is read at channel 1. This directly controls the TEST indicator light. Unused channels: “deactivate“
	**“Channel 0.4“:** “Evaluation of the sensors“: “1oo2 evaluation“ “Type of sensor interconnection“: “2 channel equivalent“ “Behavior of discrepancy”: “0-Supply value” “Discrepancy time (ms)”: “10ms“ **“Channel 1.5“:** “Evaluation of the sensors“: “1oo1 evaluation“ “Type of sensor interconnection“: “1 channel“

4.5.4 Settings of the F-DO

You reach the input dialog in the HW configuration of STEP 7 by double-clicking ”4 F-DO DC24V/2A“ (see Figure 4-3).
All input screens are available in the “Parameter“ tab.

Input dialog	Note
	“DIP switch setting (9…0)“: The displayed value must be set at the F-DO. “F-monitoring time (ms)“: „150ms“ Important: The F-monitoring time must be larger than the call time of OB35. Please use the Cotia table for selecting the monitoring time (“min. F-monitoring time“ sheet). In chapter 5 you find the link to the Cotia table.
	“Behavior after channel faults“: “Passivate the channel“
	“Channel 0“ and “Channel 1“: “activate“ Unused channels: “deactivate“
	**“Channel 0“ and “Channel 1“:** “Read-back time”: “100ms” The read-back time defines the duration of the switch-off procedure for the channel. If the respective channel switches high capacity loads, the read back time should be set sufficiently large. We recommend specific tests for selecting the readback time settings so that the following criteria are met: As small as possible, however, large enough so that the output channel is not passivated. “Diagnostics: wire break: “activated”

5 Basic Performance Data

Load memory and main memory

	Total	Standard blocks	F blocks (fail-safe)
Load Memory	56.5 Kbytes	1.2 Kbytes	55.3 Kbytes
Main memory	39.1 Kbytes	0.5 Kbytes	38.6 Kbytes

Determining the memory parameters:

- Open STEP 7 project of the functional example in the SIMATIC Manager
- Determine load memory and main memory for all blocks in the block container

Runtimes

		Time	Note
Total cycle time (standard program and safety program)	minimum	1ms	Read from S7-CPU
	maximum	12ms	
Maximum runtime safety program		13ms	Calculated with Cotia table

Determining the total cycle time:

- Load STEP 7 project into S7-CPU, set S7-CPU to run, and operate the functional example.
- Read the measured cycle time in the “Module Information CPU / Scan Cycle Time“ tab

Determine max. runtime of the safety program:

- The value is calculated with the Cotia table for ”S7 Distributed Safety“ V5.4.
- This file is available on the internet under the following entry ID: **21627074**

  http://www4.ad.siemens.de/ww/view/en

6 Sample Code

In this chapter you learn how to download the sample code, which functions are realized, how the STEP 7 program is structured and how the functions are operated.

The functional example consists of the documentation on hand and a respective STEP 7 project, the ”sample code“. Using the sample code and the setup described in chapter 4, you can reproduce the functions described here. Fur further problems you can use the sample code as a basis.

6.1 Download sample code

The sample code is available on the HTML-page of this functional example as a ZIP-file. In order to use the sample code, please proceed as follows:

Load sample code on PC/PG

- Load ZIP-file into any directory on the PC/PG.
  Name of the ZIP-file: 22304119_as_fe_i_011_v10_code_pass.zip
- Open the SIMATIC Manager
- Dearchive the ZIP-file into a STEP 7 project

Load STEP7 project to F-CPU

- Activate the “Blocks“ folder in the SIMATIC Manager
- Load the hardware configuration into F-CPU
- Select “Edit safety program” in the “Options“ menu
- Press ”Download“ in the “Safety Program“ window
- Press ”Yes“ in the “Cycle program download“ window
- Enter password “siemens“ in the “Set Permission for the Safety Program“ window and press “OK“
- Press ”Close“ in the “Safety Program“ window

Note In all cases, the password used for the safety-relevant part of the sample code is: siemens

6.2 Functions realized in the sample code

In the sample code, a “hazardous load“ is simulated via an indicator light. The indicator light can be switched on via a button and be switched off via an emergency stop button.
For demonstrating the passivation and reintegration of F-I/O-modules, four scenarios have been realized in the sample code. The following table gives an initial overview. An overview of all states and mode transitions is available in Figure 6-6.

Table 6-1

Scenario	Chapter	Description
Normal operation	6.2.1	In “normal operation“ no F-module has been passivated. An output is switched at an F-DO via a push button. This output can be switched off via an emergency stop button connected at an F-DI.
Manual reintegration	6.2.2	During wire-break at the F-DO only the affected channel of the F-DO is passivated. After repairing the wire break and acknowledgement by the user via a button, the channel is reintegrated.
Automatic reintegration	6.2.3	During wire-break at the F-DI, the entire F-DI is passivated. After repairing the wire-break, the F-DI is automatically reintegrated.
F-communication errors	6.2.4	The connection between F-CPU and the decentralized station is interrupted. Thereafter, the entire F-I/O is passivated. After restoring the connection and acknowledgement by the user via a button, the entire F-I/O is reintegrated.

In the following chapters, the above scenarios are described in greater detail. For clarification, in the “Overview hardware configuration“ view the respectively affected buttons and indicator lights are marked by a thick frame.

6.2.1 Scenario: Normal operation

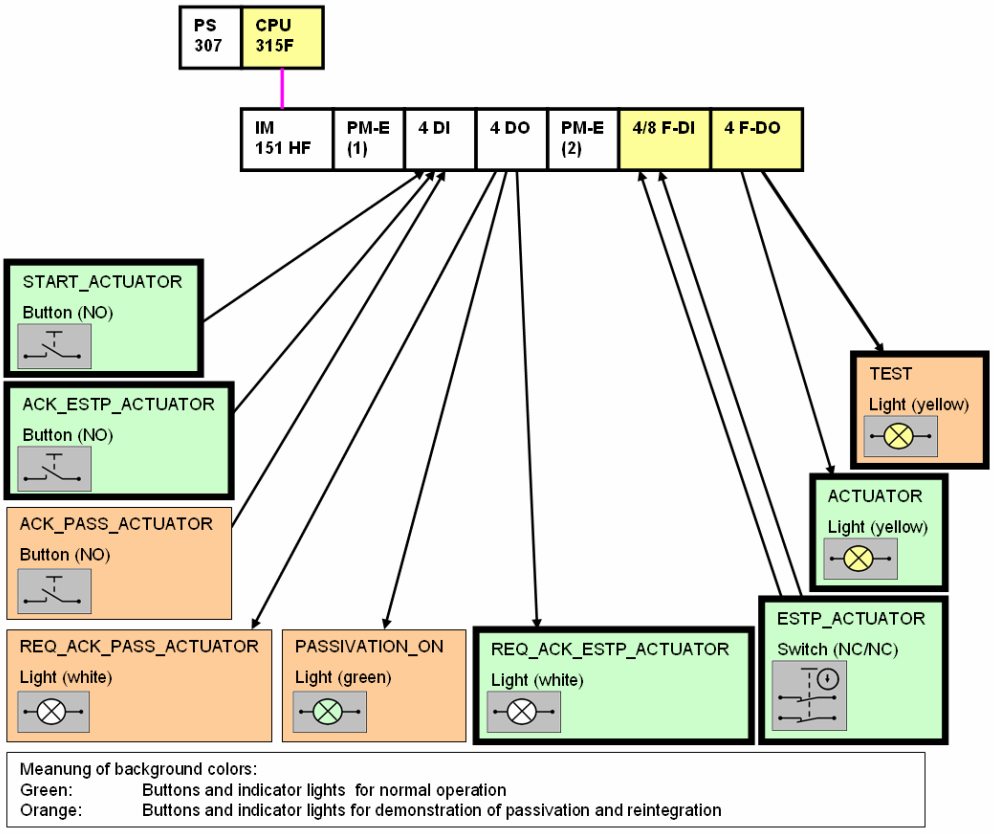
The ACTUATOR indicator light is switched on if the START_ACTUATOR button is pressed and the ESTP_ACTUATOR emergency stop button is not activated.

The TEST indicator light is always switched on. It is controlled with ”1“ via the input of the F-DI constant.

Pressing the ESTP_ACTUATOR emergency stop button switches the ACTUATOR indicator light off.

After unlocking the ESTP_ACTUATOR emergency stop button and acknowledgement via the ACK_ESTP_ACTUATOR button, the ACTUATOR indicator light can be switched on again via the START_ACTUATOR button.

Figure 6-1: Overview for hardware setup



6.2.2 Scenario: Manual reintegration

Disconnecting the F-DO and the switched on ACTUATOR indicator light (simulated wire-break) a channel error, hence passivation, is triggered. The PASSIVATION_ON indicator light is switched on.

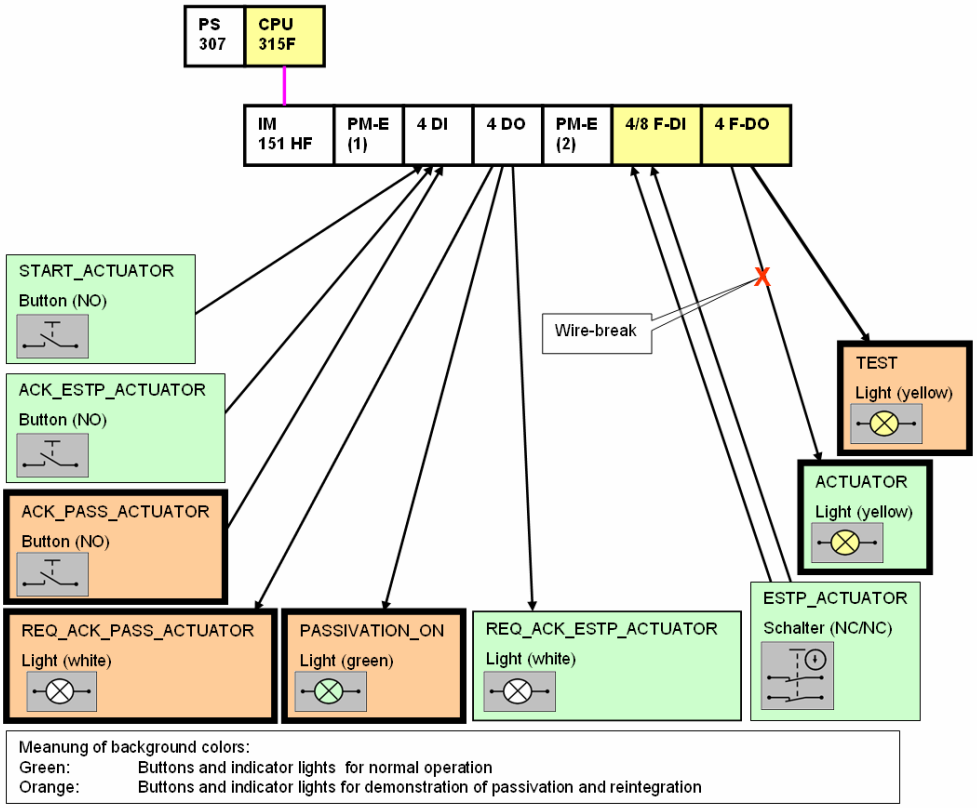
The F-DO is configured with “Passivate channels“, therefore not the entire F-DO is passivated, but only the affected channel. This is made clear by the fact that the TEST indicator light remains switched on.

After restoring the connection, the channel remains passivated, the ACTUATOR indicator light remains switched off.
An acknowledgement is requested from the user by switching on the REQ_ACK_PASS_ACTUATOR indicator light.

After the user has acknowledged via the ACK_PASS_ACTUATOR button, the passivation of the channel is cancelled. The channel however remains switched off.

The ACTUATOR indicator light is only switched on again after the user has additionally acknowledged START_ACTUATOR button.

Figure 6-2: Overview for hardware setup



6.2.3 Scenario: Automatic reintegration

Disconnecting an F-DI and the ESTP_ACTUATOR emergency stop button, a channel error, hence passivation, is triggered.

The PASSIVATION_ON indicator light is switched on, the ACTUATOR indicator light is switched off. The F-DI is configured with “Passivate the entire module“, which is why the entire F-DI is passivated. This is made clear by the fact that the TEST[1] indicator light is switched off.

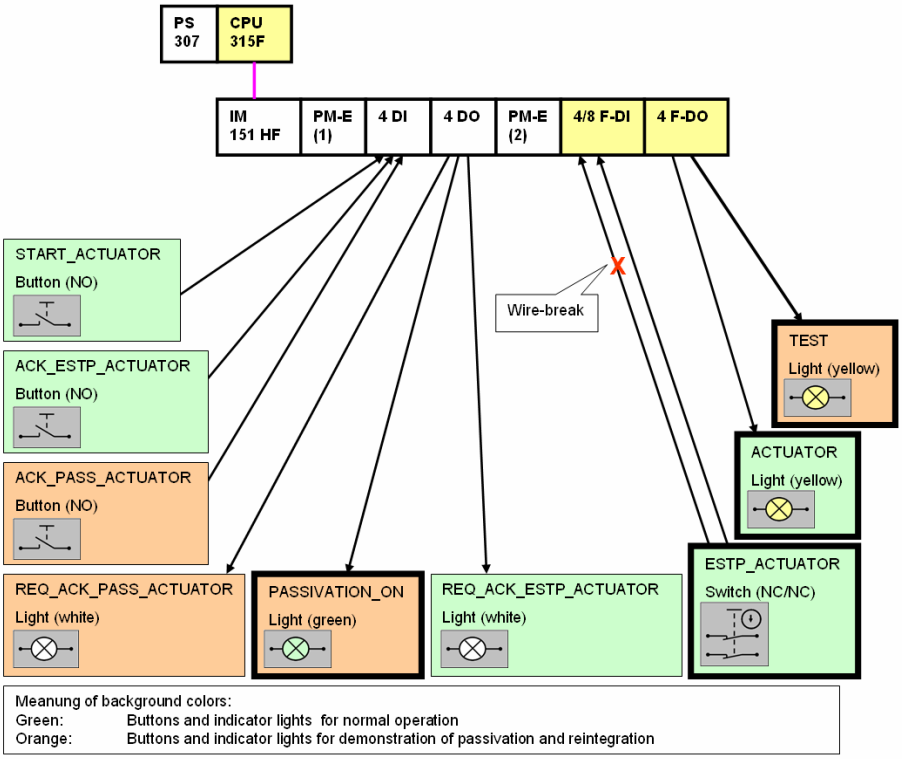
After restoring the connection, the module is automatically reintegrated, the TEST indicator light is switched on.

After acknowledging the user via the ACK_ESTP_ACTUATOR button, the ACTUATOR indicator light can be switched on via the START_ACTUATOR button.

Warning

Automatic reintegration is only permitted if an automatic startup of the plant is not possible after the error has been removed.

Figure 6-3: Overview for hardware setup



[1] TEST indicator light is controlled with ”1“ via the input of the F-DI. Due to passivation of the entire module, the safety program now reads “0“ at the input instead of “1“.

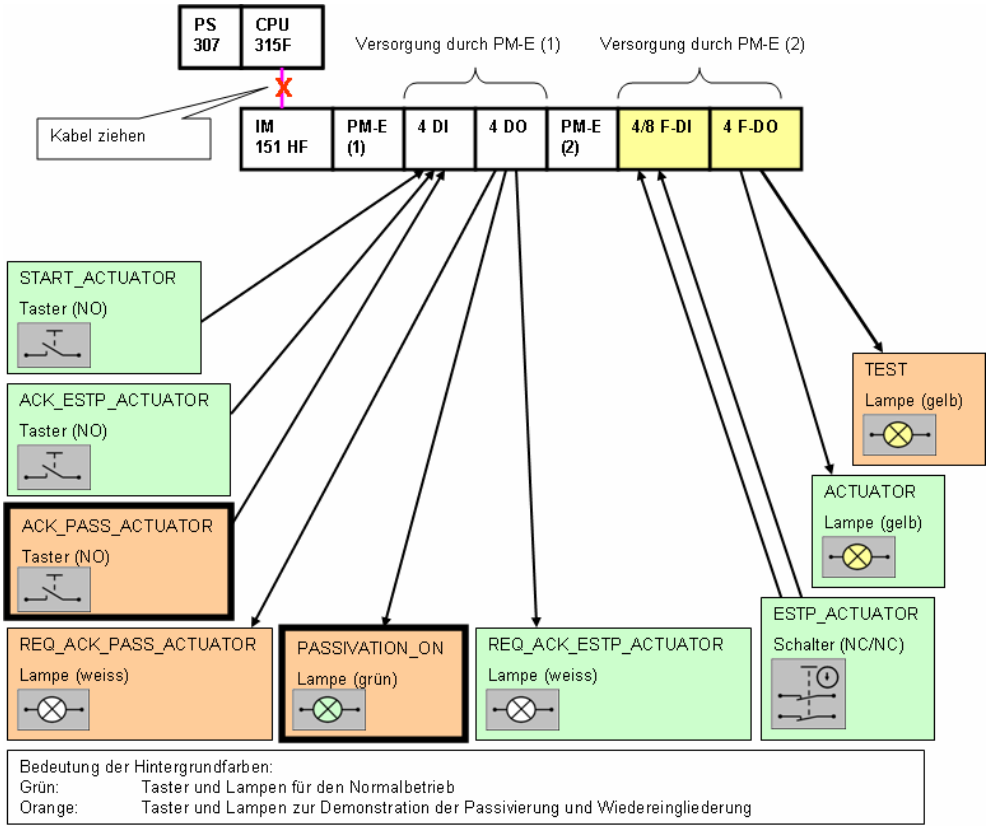
6.2.4 Scenario: F-communication error

Disconnecting the F-CPU and the decentralized station (unplugging the PROFIBUS DP cable) causes passivation of the entire F-I/O-modules in the distributed station.

After restoring the connection (plugging the PROFIBUS DP cable back in) the F-I/O-modules remain passivated. The switched on PASSIVATION_ON indicator light indicates this.

If the user acknowledges via ACK_PASS_ACTUATOR, the F-I/O is reintegrated.

Figure 6-4: Overview for hardware setup



6.2.5 Overview of the scenarios:

Figure 6-6 (on the next page) indicates the states and mode transitions of the sample code following scenarios:

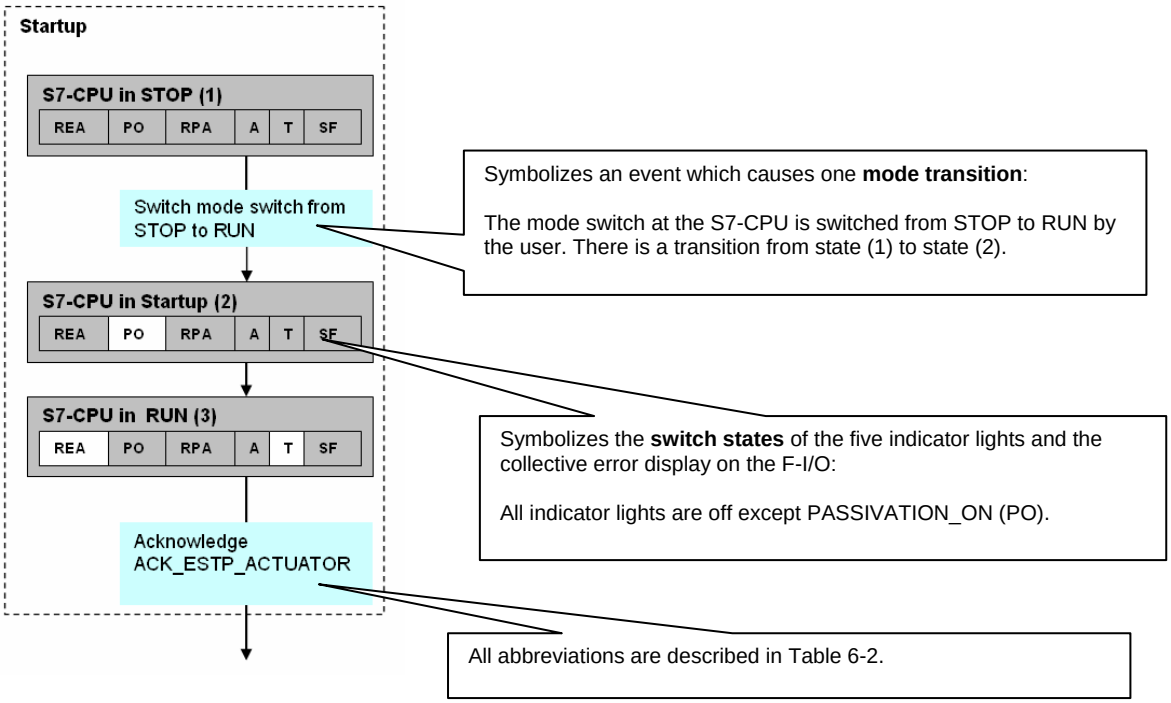
- Startup
- Normal operation
- Manual reintegration
- Automatic reintegration

The following figure shows you:

- What effect pressing the button has?
- When do which indicator lights come on?

The following Figure 6-5 explains the used representation method, using the example of the ”Startup“ scenario.

Figure 6-5



Overview of buttons and indicator lights

Table 6-2

Symbol	Abbreviations	HW component	Function
START_ACTUATOR	---	Button	Switch on ACTUATOR indicator light
ACK_ESTP_ACTUATOR	---	Button	Acknowledge ACTUATOR emergency stop actuator
ACK_PASS_ACTUATOR	---	Button	Acknowledge ACTUATOR passivation
ESTP_ACTUATOR	---	Emergency stop push button at F-DI	ACTUATOR emergency stop
REQ_ACK_ESTP_ACTUATOR	**REA**	Indicator light	Acknowledge ACTUATOR emergency stop requirement
REQ_ACK_PASS_ACTUATOR	**RPA**	Indicator light	Acknowledge ACTUATOR passivation requirement
PASSIVATION_ON	**PO**	Indicator light	Passivation exists
ACTUATOR	**A**	Indicator light at F-DO	Simulation of “hazardous load“
TEST	**T**	Indicator light at F-DO	Only switched off if F-DI passivated.
---	**SF**	LED on F-module	Collective error display

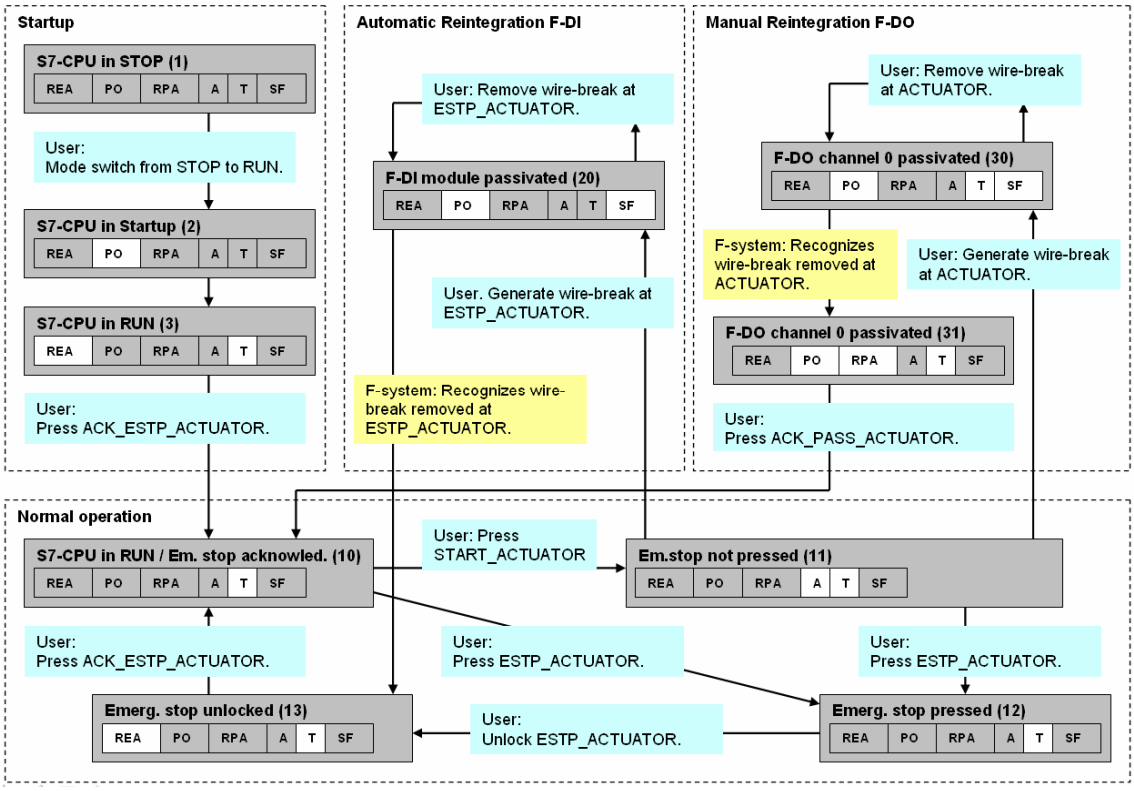
Meaning of background colors

Table 6-3

Section	Color	Meaning
Mode transitions / actions	light blue	Action by user
	light yellow	Action by F-system
Overview of indicator light:	white	Indicator light is switched on
	gray	Indicator light is switched off

Overview of states and mode transitions of the sample code

Figure 6-6



6.3 Explanations for the STEP 7 program

6.3.1 Interaction of STEP 7 blocks

The following figure displays the interaction between the STEP 7 blocks and the connection to the process I/O. The description of the process signals is available in chapter 4.3.

Figure 6-7

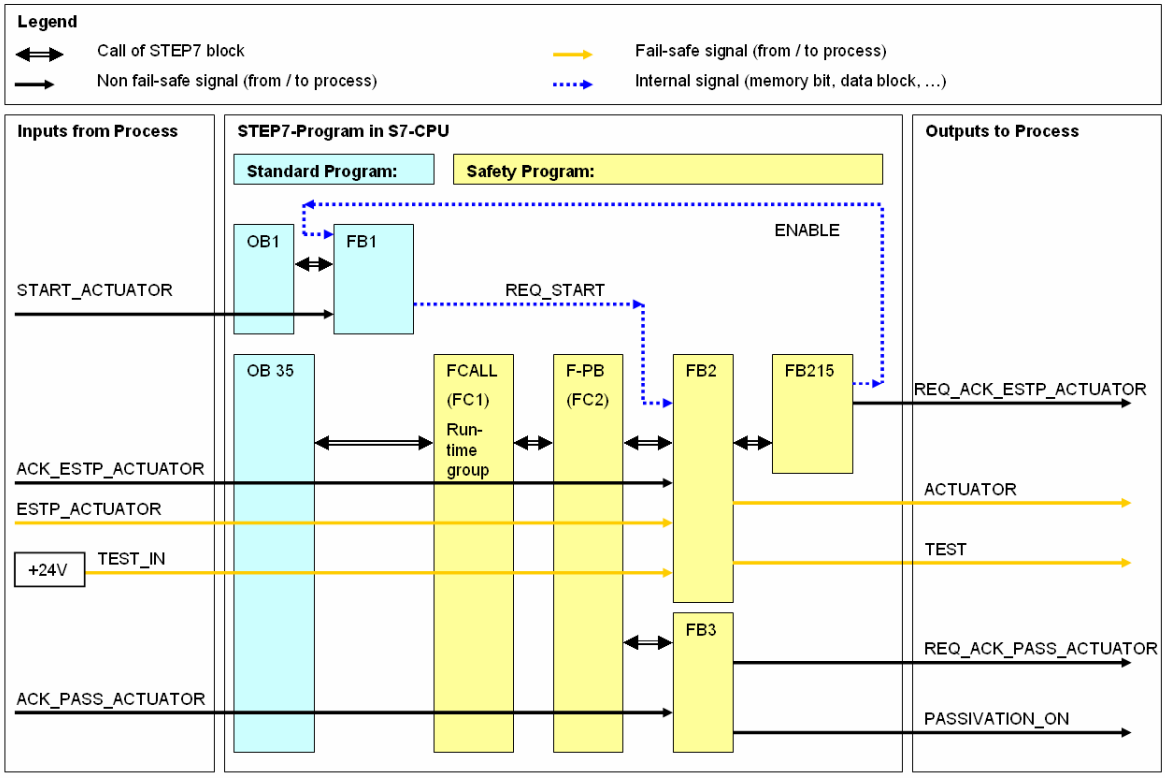


Table 6-4

Program	Block	Name	Tasks
Standard program	OB1	---	Cyclic program: Call of FB1 (START)
	OB35	---	Periodic call of F-runtime group (FCALL)
	FB1	START	Operational switching: Generating the start requirement (REQ_START)
Safety program	FCALL	FCALL	F run-time group (FCALL)
	F-PB	COORDINATION	F-program block: Calls FB2 and FB3
	FB2	MODE	Call FB215 (F_ESTOP1): Controlling ACTUATOR and TEST
	FB3	REINTEGRATION	Display passivation, automatic F-DI reintegration, manual F-DI and F-DO reintegration,
	FB215	F_ESTOP1	F-block from Distributed Safety library: “Emergency stop up to stop category 1“ Creating ENABLE for emergency stop circuit

6.3.2 Description: F-I/O-module data blocks

Function and design of the F-blocks:

- See chapter 7.2

The following F-I/O-module data blocks are used in the sample code:

- DB819: F-I/O-module data block of F-DI
- DB820: F-I/O-module data block of F-DO

6.3.3 Description: OB1

Function of the standard block:

- Cyclic call of FB1 (START)

Parameter of the standard block:

- None

6.3.4 Description: OB35

Function of the standard block:

- Periodic call of F-runtime group (FCALL): The safety program is called every 50 msec.

Parameter of the standard block:

- None

6.3.5 Description: FB1, DB2 (START)

Function of the standard block:

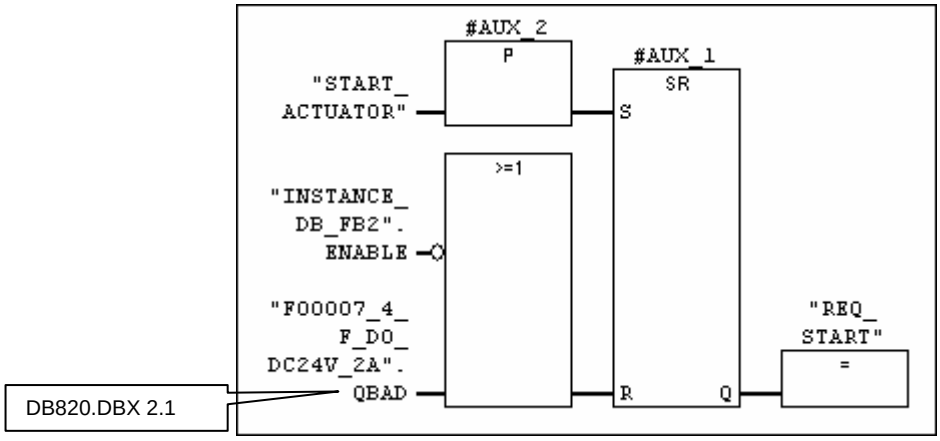
- Operational switching: Generating the standard requirement REQ_START for the ACTUATOR indicator light.

Parameter of the standard block:

- None

FB1 / Network 1

Figure 6-8



Overview of the signals of the network:

Table 6-5

Signal	Source / Target	Meaning
START_ACTUATOR	From process (button)	Start button for ACTUATOR
INSTANCE_DB_FB2.**ENABLE**	From F-block FB215	Enable from emergency-stop circuit
F00007_4_F_DO_DC24V_2A.**QBAD**	From F-I/O-module data block of F-DO	Display, whether F-DO has been passivated
REQ_START	To F-block FB2	Start request for ACTUATOR

Description of the network function:

The standard requirement REQ_START for the ACTUATOR indicator light is generated if the following conditions are true at the same time (AND):

- The START_ACTUATOR start button was pressed
- The ENABLE from the emergency-stop circuit (FB215) exists
- The F-DO is not passivated

The start requirement REQ_START is evaluated in the F-block FB2.

FB215 is a block from the Distributed Safety library.

6.3.6 Description: FCALL

Function of the F-block:

- F run-time group: Call of safety program

Parameter of the F-block:

- None

6.3.7 Description: F-PB (COORDINATION)

Function of the F-block:

- Call of F-block FB2
- Call of F-block FB3

Parameter of the F-block:

- None

6.3.8 Description: FB2, DB3 (MODE)

Function of the F-block:

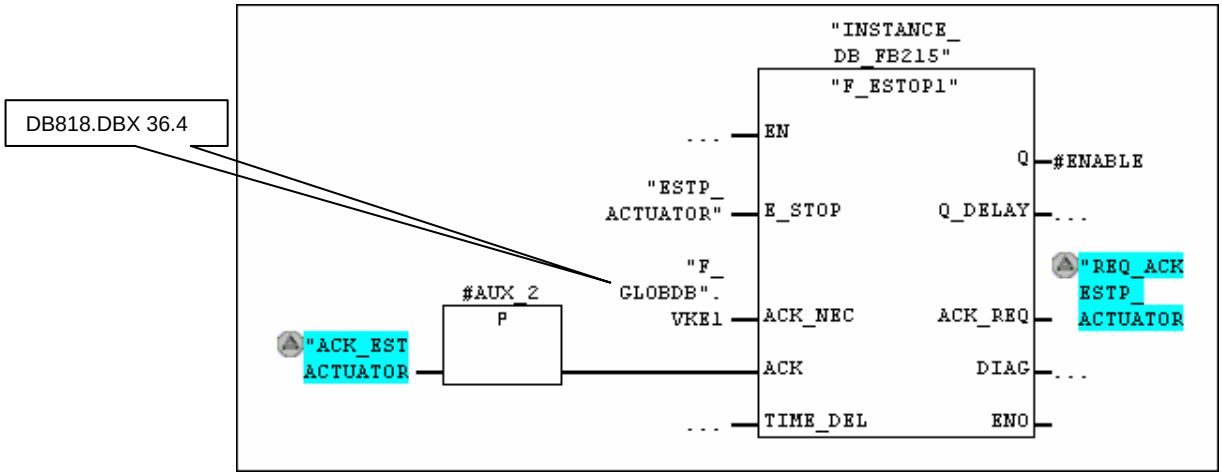
- Realizing the emergency stop functionality for the ACTUATOR indicator light
- Controlling both indicator lights, ACTUATOR and TEST

Parameter of the F-block:

- None

FB2 / Network 1

Figure 6-9



Overview of the signals of the network:

Table 6-6

Signal	Source / Target	Meaning
ACK_ESTP_ACTUATOR	From process (button)	Acknowledgement for emergency-stop circuit
ESTP_ACTUATOR	From process (button)	Emergency-stop button
F_GLOBDB.**VKE1**	From F-Global-DB[2]	Result of logic operation "1"
ENABLE	To FB1 (standard block)	Enable for emergency-stop circuit
REQ_ACK_ESTP_ACTUATOR	To process (indicator light)	Acknowledgement for emergency-stop circuit requirement

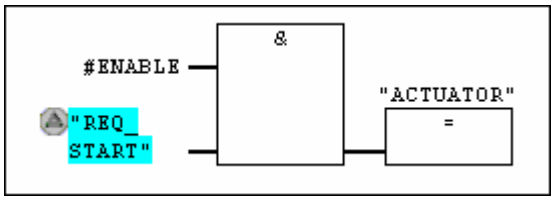
Description of the network function:

Here the emergency stop functionality for the ACTUATOR indicator light is realized The FB215 is called for this. FB215 is an F-block from the Distributed Safety library.

[2] The F-Global-data block (F_GLOBDB) is a fail-safe data block, which contains all global data of the safety program as well as additional information for the F-system.
Amongst other things, VKE0 and VKE1 provided there.

FB2 / Network 2

Figure 6-10



Overview of the signals of the network:

Table 6-7

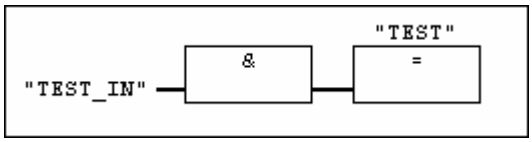
Signal	Source / Target	Meaning
ENABLE	From network 1	Enable from emergency-stop circuit
REQ_START	From FB1 (standard block)	Start requirement for ACTUATOR
ACTUATOR	To process (indicator light)	Representative for a “hazardous load”.

Description of the network function:

The ACTUATOR load is switched on if the ENABLE from the emergency-stop circuit is pending and the start requirement REQ_START is given.

FB2 / Network 3

Figure 6-11



Overview of the signals of the network:

Table 6-8

Signal	Source / Target	Meaning
TEST_IN	From process (“1”)	Signal from F-DI “1“ is constantly set at F-DI.
TEST	To process (indicator light)	Only for demonstration, no other function.

Description of the network function:

TEST is used to demonstrate passivation of the entire module. When there is no passivation, TEST is always switched on, as TEST_IN at the F-DI is constantly supplied with ”1“.

The TEST indicator light is only switched off if F-DI is passivated.

6.3.9 Description: FB3, DB4 (REINTEGRATION)

Function of the F-block:

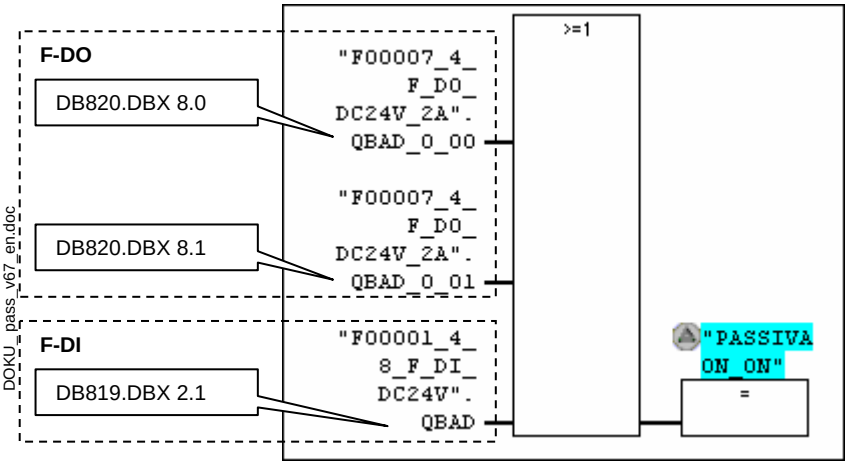
- Display of passivation at the PASSIVATION_ON indicator light
- Automatic reintegration of the F-DI
- Manual reintegration of F-DI/F-DO

Parameter of the F-block:

- None

FB3 / Network 1

Figure 6-12



Overview of the signals of the network:

Table 6-9

Signal	Source / Target	Meaning
F00007_4_F_DO_DC24V_2A.**QBAD_O_00**	From F-I/O-module data block of F-DO	If “1”: channel F-DO is passivated
F00007_4_F_DO_DC24V_2A.**QBAD_O_01**		If “1”: channel 1 of F-DO is passivated
F00001_4_8_F_DI_DC24V.**QBAD**	From F-I/O-module data block of F-DI	If “1”: **At least** one channel of the F-DI is passivated
PASSIVATION_ON	To process (indicator light)	If “1”: **At least** one channel of F-DI and/or F-DO is passivated

Description of the network function:

The PASSIVATION_ON indicator light indicates that at least one channel of F-DO and/or F-DI is passivated. Basically, there are two different methods to test whether at least one channel of a module is passivated:

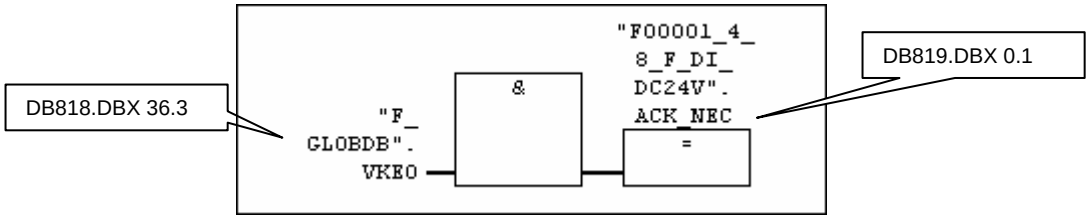
Table 6-10

	Method	Advantage
1	Polling all channels of the F-module: • for F-DI: via the “QBAD_I_xx“ variables • for F-DO: via the “QBAD_O_xx“ variables	The passivated channels can be identified individually.
2	Polling the entire F-module: • via the “QBAD“ variable.	Polling only possible once.

In the sample code both methods are used for demonstration purposes. “Method 2” can also be used here to detect whether the F-DO is passivated.

FB3 / Network 2

Figure 6-13



Overview of the signals of the network:

Table 6-11

Signal	Source / Target	Meaning
F_GLOBDB.VKE0[3]	From F-Global-DB	Result of logic operation “0“
F00001_4_8_F_DI_DC24V.**ACK_NEC**	To F-I/O-module data block of F-DI	F-DI is **automatically** reintegrated

Description of the network function:

Channel or module errors at the F-DI cause passivation of the F-DI at the entire module. After removing the error, the F-DI is automatically reintegrated.

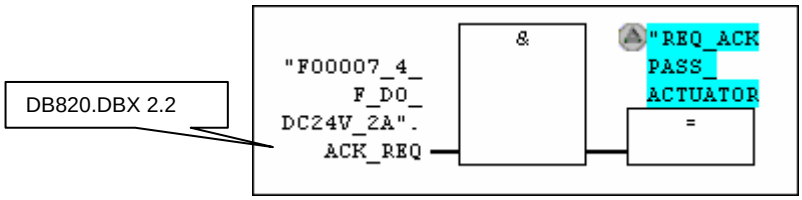
Warning

Automatic reintegration is only permitted if an automatic startup of the plant is not possible after the error has been removed.

[3] The F-Global data block (F_GLOBDB) is a fail-safe data block which contains all global data of the safety program as well as additional information for the F-system.
Amongst other things, VKE0 and VKE1 provided there.

FB3 / Network 3

Figure 6-14



Overview of the signals of the network:

Table 6-12

Signal	Source / Target	Meaning
F00007_4_F_DO_DC24V_2A.**ACK_REQ**	From F-I/O-module data block of F-DO	If “1”: The error that caused the passivation has been removed. Acknowledgement for reintegration by the user is now possible.
REQ_ACK_PASS_ACTUATOR	To process (indicator light)	Indicates to the user, that reintegration requires acknowledgement.

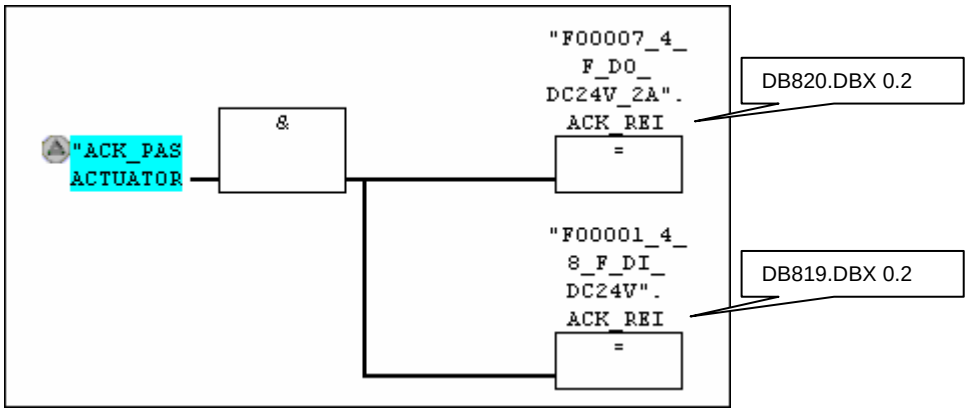
Description of the network function:

A channel error at the F-DO in the sample code causes passivation of the F-DO channels. After removing the error, the F-DO is manually reintegrated.

The REQ_ACK_PASS_ACTUATOR indicator light shows the user, that reintegration requires acknowledgement.

FB3 / Network 4

Figure 6-15



Overview of the signals of the network:

Table 6-13

Signal	Source / Target	Meaning
ACK_PASS_ACTUTOR	From process (button)	Acknowledgement by the user for manual reintegration
F00007_4_F_DO_DC24V_2A.**ACK_REI**	To F-I/O-module data block of F-DO	If “0->1“: F-DO is reintegrated.
F00001_4_8_F_DI_DC24V.**ACK_REI**	To F-I/O-module data block of F-DI	If “0->1“: F-DI is reintegrated.

Description of the network function:

F-DO and F-DI are reintegrated after acknowledgement by the user:

- Manual reintegration of the **F-DO** is necessary in the sample code after channel or F-communication error.
- Manual reintegration of the **F-DI** is necessary in the sample code only after F-communication error.

6.3.10 Description: FB 215, DB1 (F_ESTOP1)

The block is a TÜV certified application block from the Distributed Safety library.

Function and parameter of the F-blocks:

- See STEP 7 online-help

6.4 Operating instruction on the sample code

This chapter describes the operation of the functional example.

The operation is divided into different scenarios:

Table 6-14

Scenario	Chapter
Normal operation	6.4.1
Manual reintegration after wire-break at F-DO	6.4.2
Automatic reintegration after wire-break at F-DI	6.4.3
Reintegration after F-communication error	6.4.4

The following prerequisites must be fulfilled in order to operate the functional example:

- The hardware configuration, the standard program, and the safety program are located on the F-CPU
- Emergency stop unlocked

As a description, tables with uniform structure are used below. The columns of the table have the following meaning:

Table 6-15

Column name	Column content
“Step”	Number of the operational step
“Action”	Action of user
“State“	The number marks the state reached after executing the action. An overview of all status is available at Figure 6-6.
“Comment“	Comments on the step.
“Indicator light“	Here the switch status of the five indicator lights and the SF-LED is depicted which is set after executing the action. Switched indicator lights are marked with “1“. (*1)
“SF-LED“	The column indicates the status of the collective error display on the F-I/O-module (red LED). (*1)

(*1): To recognize more clearly which bits change during a mode transition, they are shaded in gray: If a bit is shaded gray, it has changed compared with its previous state.

6.4.1 Operation: Normal operation

Operation in the following table shows the procedure:

- Start und emergency stop of the load

A more detailed description of the scenario, with overview image on the hardware setup, is available in chapter 6.2.1.

Table 6-16

Step	Action	State (*1)	Comment	Indicator light / SF-LED A: REQ_ACK_ESTP_ACTUATOR B: PASSIVATION_ON C: REQ_ACK_PASS_ACTUATOR D: ACTUATOR E: TEST F: SF-LED of the F-modules					
				A	B	C	D	E	F
1	Mode switch at the F-CPU from STOP to RUN.	3		1	0	0	0	1	0
2	Press ACK_ESTP_ACTUATOR	10	Always after starting the F-CPU	0	0	0	0	1	0
3	Press START_ACTUATOR	11	Switch on load	0	0	0	1	1	0
4	Press ESTP_ACTUATOR	12	Press emergency stop	0	0	0	0	1	0
5	Unlock ESTP_ACTUATOR	13	Unlock emergency stop	1	0	0	0	1	0
6	Press ACK_ESTP_ACTUATOR	10	Acknowledge emergency stop	0	0	0	0	1	0
7	Press START_ACTUATOR	11	Switch load back on	0	0	0	1	1	0

Explanations on the table:

(*1):
In Figure 6-6 you find an overview of statuses and mode transitions of the sample code. The area in the figure marked as “Normal operation“ is relevant here.

6.4.2 Operation: Manual reintegration

Operation in the following table shows the procedure:

- Simulation of a wire-break at the load
- Passivating an F-DO channel
- Manual reintegration after removing the wire-break

Please observe the following:

- A wire-break at F-DO is only recognized when the channel is switched on.
- Reintegration of an F-DO may take several minutes.

A more detailed description of the scenario, with overview image on the hardware setup, is available in chapter 6.2.2.

Table 6-17

Step	Action	State (*1)	Comment	Indicator light / SF-LED A: REQ_ACK_ESTP_ACTUATOR B: PASSIVATION_ON C: REQ_ACK_PASS_ACTUATOR D: ACTUATOR E: TEST F: SF-LED of the F-DO module					
				A	B	C	D	E	F
---	---	11	This is the initial state for the following operations.	0	0	0	1	1	0
1	Disconnect F-DO ACTUATOR indicator light	30	Due to passivation of the channels the TEST indicator light remains switched on.	0	1	0	0	1	1
2	Restoring the connection	30	The state remains until the F-system recognizes that the wire-break has been removed.	0	1	0	0	1	1
		31	The F-system requests acknowledgement for reintegration.	0	1	1	0	1	0
3	Press ACK_PASS_ACTUATOR	10	After acknowledgement by the user, the F-DO channel is reintegrated.	0	0	0	0	1	0

Explanations on the table:

(*1):
In Figure 6-6 you find an overview of statuses and mode transitions of the sample code. The area in the figure marked as “Manual reintegration of F-DO“ is relevant here.

6.4.3 Operation: Automatic reintegration

Operation in the following table shows the procedure:

- Simulating a wire-break at the emergency stop button.
- Passivation of the entire F-DI
- Automatic reintegration after removing the wire-break

A more detailed description of the scenario, with overview image on the hardware setup, is available in chapter 6.2.3.

Table 6-18

Step	Action	State (*1)	Comment	Indicator light / SF-LED A: REQ_ACK_ESTP_ACTUATOR B: PASSIVATION_ON C: REQ_ACK_PASS_ACTUATOR D: ACTUATOR E: TEST F: SF-LED of the F-DI module					
				A	B	C	D	E	F
---	---	11	This is the initial state for the following operations.	0	0	0	1	1	0
1	Disconnecting F-DI and ESTP_ACTUATOR emergency stop	20	Due to passivation of entire module, the TEST and ACTUATOR indicator lights are switched off.	0	1	0	0	0	1
2	Restoring the connection	20	The state remains until the F-system recognizes that the wire-break has been removed.	0	1	0	0	0	1
		13	The F-DI module is reintegrated.	1	0	0	0	1	0

Explanations on the table:

(*1):
In Figure 6-6 you find an overview of statuses and mode transitions of the sample code. The area in the figure marked as “Automatic reintegration of F-DI“ is relevant here.

6.4.4 Operation: F-communication error

Operating in the following table shows the procedure:

- Pulling the PROFIBUS DP cable from the F-CPU
- Restoring the connection
- Reintegration

A more detailed description of the scenario, with overview image on the hardware setup, is available in chapter 6.2.4.

Table 6-19

Step	Action	State (*1)	Comment	Indicator light / SF-LED A: REQ_ACK_ESTP_ACTUATOR B: PASSIVATION_ON C: REQ_ACK_PASS_ACTUATOR D: ACTUATOR E: TEST F: SF-LED of F-DI and F-DO module					
				A	B	C	D	E	F
---	---	11	This is the initial state for the following operations.	0	0	0	1	1	0
1	Removing the PROFIBUS DP cable	-		0	0	0	0	0	0 (*2)
2	Restoring the connection	-		0	1	0	0	0	0 (*3)
3	Press ACK_PASS_ACTUATOR	10	After acknowledgement by the user, the F-I/O-module is reintegrated.	1	0	0	0	1	0

Explanations on the table:

(*1):
In Figure 6-6 you find an overview of statuses and mode transitions of the sample code.

(*2):
The BF-LED at “IM 151 HF“ lights up. The BF-LED at “IM 151 HF“ is blinking.

(*3):
The BF-LEDs are off.

7 Background Knowledge on the Functional Example

This chapter provides background knowledge on “Passivation and Reintegration“ in the ”S7 Distributed Safety“ system.

All of the information given is taken from the “S7 Distributed Safety“ manuals and the STEP7 online-help.

Note

If already familiar with passivation and reintegration, you won’t need to read this chapter.

This chapter is not necessary for setup and operation of this functional example.

Use the current “S7 Distributed Safety“ manuals for your current project.

The following topics are described:

Table 7-1

Topic	Chapter	Content
F-I/O-module	7.1	What are fail-safe I/O-modules? How does the user access inputs and outputs?
F-I/O-module data block	7.2	What is an F-I/O-module data block What is an F-I/O-module data block used for? What is the structure of an F-I/O-module data block?
Passivation (of entire module or channel)	7.3	What happens during passivation? What type of passivation exists? How is the “passivation of channels“ realized?
Reintegration (of entire module or channel)	7.4	What happens during reintegration? What type of reintegration exists?
Process: channel / module error (automatic reintegration)	7.5.1	Description of variants of passivation and reintegration: What is the principal procedure? Which variables are involved in the F-I/O-module data block?
Process: channel / module error (manual reintegration)	7.5.2	
Process: F-communication error	7.5.3	
Process: safety program	7.5.4	
Process: group passivation	7.5.5	

7.1 F-I/O-module

7.1.1 What are fail-safe I/O-modules?

Fail-safe I/O-modules differ from standard modules mainly by their internal two channel structure. Two integrated processors mutually monitor and test the input and output circuits automatically. The connected sensors and actuators are also monitored (wire-break, discrepancy, etc.). In case of an error, the processors turn the F-I/O-module fail-safe.

The F-CPU communicates with a distributed F-I/O-module via the fail-safe PROFIsafe profile. The PROFIsafe profile is integrated in the PROFIBUS and PROFINET telegrams.

7.1.2 How does the user access inputs and outputs?

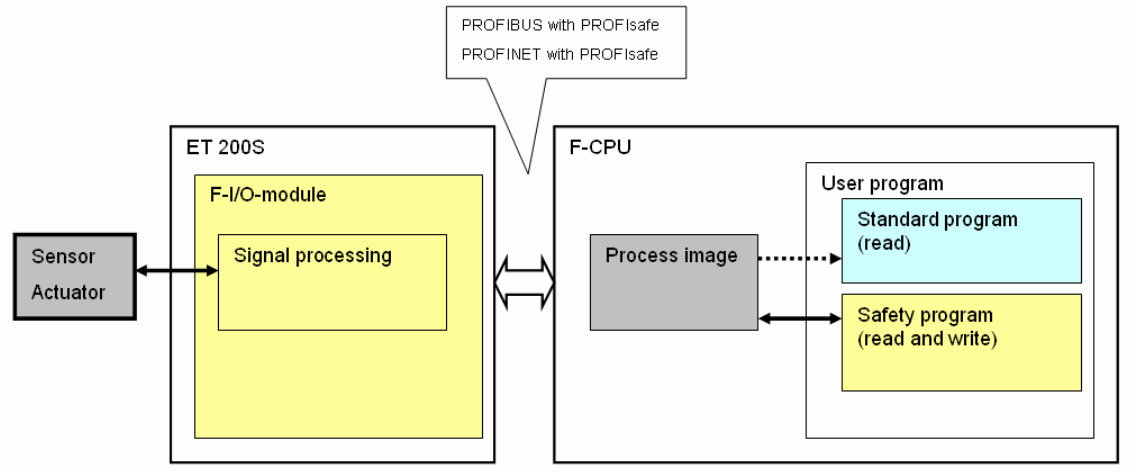
The inputs and outputs of an F-I/O-module are accessed via the process image of the F-CPU:

Table 7-2

Access to F-I/O-module	Process image	
	Inputs	Outputs
In standard program	read	read
In the safety program	read	write

The following figure illustrates the relationships.

Figure 7-1



7.2 F-I/O-module data block

7.2.1 What is an F-I/O-module data block

For every F-I/O-module one data block is **automatically** generated during compilation in the STEP 7 hardware configuration.

The F-I/O-module data block is the interface between the user program and the F-system. Control and status information of the F-I/O-module are exchanged via the interface.

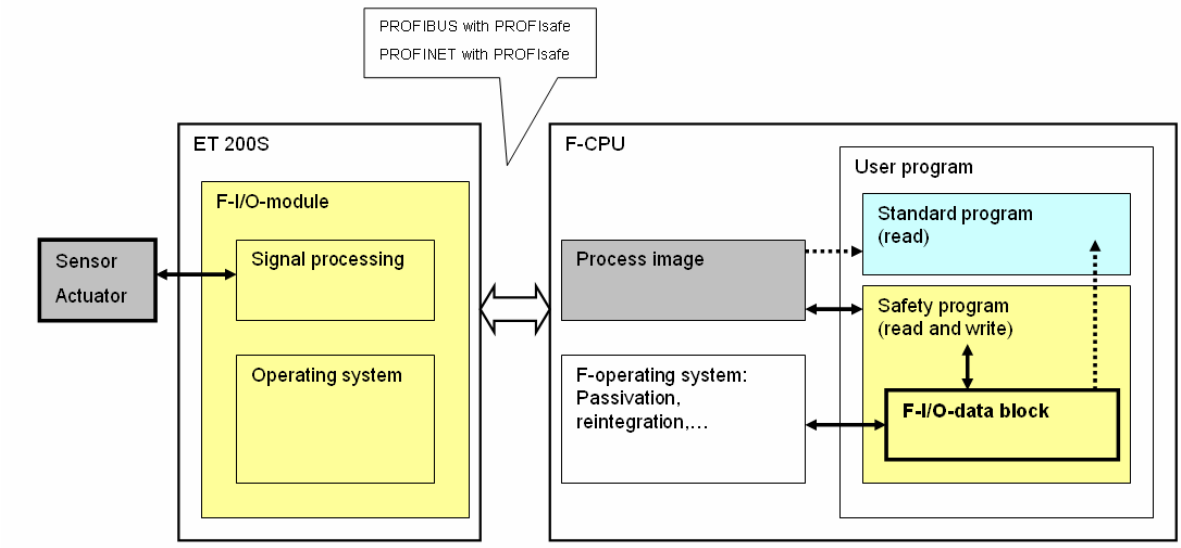
The F-I/O-module data block contains variables which can be accessed by the safety program as well as the standard program. The F-I/O-module data block does not contain any process values. The process values are located in the process image of the F-CPU.

Table 7-3

	Access to the F-I/O-module data block
In standard program	read
In the safety program	read and write

The following figure illustrates the relationships.

Figure 7-2



7.2.2 What is the F-I/O-module data block used for?

The following functions can be realized with the variables of the F-I/O-module data block:

- Checking whether current F-I/O-modules or individual F-I/O-module channels are passivated.
- Manual or automatic reintegration of F-I/O-modules after error recovery.
- Passivation and reintegration of F-I/O-modules via the safety program.
- Reconfiguration of fail-safe DP-standard slaves.

7.2.3 What is the structure of an F-I/O-module data block?

The two following tables explain the variables of the F-I/O-module data block. Both tables differ in the type of user access to the variables:

- Read and write access by the user: Table 7-5
- Read access by the user: Table 7-6

The variables of the F-I/O-module data block can, for example, be monitored with the variable table in STEP 7. The following table gives examples:

Table 7-4

Operand	Symbol	Comment
DB819.DBX 0.0	„F00001_4_8_F_DI_DC24V“.PASS_ON	Variable ”PASS_ON“ of F-DI
DB820.DBX 2.1	„F00007_4_F_DO_DC24V_2A“.QBAD	Variable ”QBAD“ of F-DO

The user has **read and write** access to the following variables in the F-I/O-module data block.

Table 7-5

Variable (Type)	**Declaration**	**Address**	**Default value**	**What reactions can be triggered by the user?**	**Reaction of the F-system**
PASS_ON (BOOL)	IN	0.0	0	Passivation and reintegration of F-I/O-module via the safety program.	**"PASS_ON = 1":** The F-I/O-module is reintegrated.
					"PASS_ON = 0": The F-I/O-module is reintegrated. The passivation was previously triggered with "PASS_ON = 1".
					Comment: PASS_OUT does not change its value when writing PASS_ON. The ACK_NEC and ACK_REI are not relevant here.
ACK_NEC (BOOL)	IN	0.1	1	Selecting the type of reintegration: • Manual: with user acknowledgement • Automatic: without user acknowledgement	**"ACK_NEC = 1":** Reintegration occurs manually. Reintegration requires user acknowledgement: Positive edge at ACK_REI
					"ACK_NEC = 0": Reintegration occurs automatically without acknowledgement by the user. For "F-communication error" automatic reintegration is not possible!
					Comment: Reintegration is only possible when the error causing the passivation has been removed. ACK_NEC is only relevant for "channel" and "module" errors.
ACK_REI (BOOL)	IN	0.2	0	Acknowledgement by the user at manual reintegration	**"ACK_REI = 0->1" (positive edge):** Reintegration occurs after positive edge.
					Comment: Acknowledgement by the user is only possible when the error causing the passivation has been removed. For "F-communication errors" acknowledgement by the user must always occur independent of ACK_NEC.
IPAR_EN (BOOL)	IN	0.3	0	---	Reconfiguration of fail-safe DP-standard slaves.

The user has **only read** access to the following variables in the F-I/O-module data block.

Table 7-6

Variable (Type)	**Declaration**	**Address**	**Default value**	**Which information does the user receive when reading the variables?**	
PASS_OUT (BOOL)	OUT	2.0	1	**"PASS_OUT= 1":** The F-I/O-module is passivated. Cause of the passivation: "F-communication error", "module error", "channel error" (see Table 7-9).	
				"PASS_OUT = 0 AND QBAD = 1": The F-I/O-module is passivated. Cause of the passivation: "PASS_ON = 1" was set in the safety program.	
				Comment: Depending on the settings in the hardware configuration of STEP 7 the entire module or only faulty channels are passivated.	
QBAD (BOOL)	OUT	2.1	1	**"QBAD = 1":** Currently the substitute value ("0") is used for **at least** one channel instead of the process value. Which channels are passivated is indicated via the QBAD_I_xx or QBAD_O_xx variables (see below).	
ACK_REQ (BOOL)	OUT	2.2	0	**"ACK_REQ = 1"**: The error that caused the passivation has been removed. Acknowledgement for manual reintegration (ACK_REI) by the user is now possible. Cause of the passivation: "F-communication error", "module error", "channel error" (see Table 7-9).	
				Comment: If the error causing the passivation has been removed, and this has been recognized by the F-system, the F-system sets "ACK_REQ = 1". After acknowledgement by the user, the F-operating system sets "ACK_REQ = 0".	
IPAR_OK (BOOL)	OUT	2.3	0	Reconfiguration of fail-safe DP-standard slaves.	
DIAG (BYTE)	OUT	3.0	0	Service information	
QBAD_I_xx (BOOL)	OUT	4.0 Bis 7.7	1	**"QBAD_I_xx = 1":** The input channel is passivated with number xx. The substitute value ("0") is used at input "xx".	Comment: With the variables it can be detected which channels are passivated. The channel number xx has the value range: 00 to 31
QBAD_O_xx (BOOL)	OUT	8.0 Bis 11.7	1	**"QBAD_O_xx = 1":** The output channel is passivated with number xx. The substitute value ("0") is used at output "xx".	Example: "QBAD_O_00 = 1" means: Substitute value ("0") is currently output at output channel.

7.3 Passivation (of entire module or channel)

7.3.1 What happens during passivation?

The entire F-I/O-module or individual channels of an F-I/O-module can be passivated by the F-system or the safety program. The extent of passivation varies depending on the trigger of the passivation:

Table 7-7

Cause of the passivation:	Extend of the passivation:
Safety program	The passivation affects the **entire F-module**. I.e. all channels of the F-I/O-module are passivated.
F-system	Passivation affects either the **entire F-module**, or only the **faulty channels**. The desired behavior can be adjusted via settings in the STEP 7 hardware configuration.

Passivation has the following effect:

Table 7-8

Passivation	Effect of passivation:
F-input module (F-DI)	The safety program is **not** provided with the process values pending at the input. The safety program is provided with the substitute values (”0“) in the process image of the inputs.
F-output module (F-DO)	The output values provided by the safety program in the process image of the outputs are **not** transmitted to the outputs. At the outputs the substitute values (“0“) are output.

Note During passivation of F-input modules (F-DI) the process image of the respective inputs is only reset when processing the safety program.

7.3.2 What type of passivation exists?

The following table gives an overview of the passivation.

Table 7-9

Cause of the passivation:			Effect of passivation:		Reaction in the F-I/O-module data block
Safety program	**Setting "PASS_ON = 1" in the F-I/O-module data block**		Passivation of the F-module		QBAD = 1 **All** channels: QBAD_I_xx = 1 QBAD_O_xx = 1
F-operating system	**Startup of the F-CPU** Establishing communication between the F-CPU and the F-I/O via the safety protocol according to PROFIsafe.		Passivation of the entire F-I/O		QBAD = 1 PASS_OUT = 1 **All** channels: QBAD_I_xx = 1 QBAD_O_xx = 1
	F-communication error Error at fail-safe communication between F-CPU and F-I/O.		Passivierung der F-Baugruppe		
	F-I/O error (*1)	**Module error** • Configuration error • Overtemperature	Passivation of the F-module		
		Channel error • Wire break • Short circuit • Discrepancy • Overload	Configuration: (*2)	"Passivation of entire module"	
				"Passivation channel"	QBAD = 1 PASS_OUT = 1 **Only** affected channel: QBAD_I_xx = 1 QBAD_O_xx = 1

Explanations on the table:

(*1): "F-I/O faults" causes the following reaction:

- The error is reported at the F-CPU (as standard reaction):
  - The error is reported to the F-CPU via the slave diagnostics.
  - OB82 for I/O errors is called in the F-CPU. If it does not exist, it goes to the F-CPU in STOP.
- Either the entire F-module or only the affected channels are passivated (F-specific reaction).

(*2): In the hardware configuration of STEP 7 the project settings can be selected: "Passivate the entire module" or "Passivate the channels".

7.3.3 How is the “passivation of channels“ realized?

Precondition

Passivation of channels requires:

- S7 Distributed Safety V5.4, and S7 F Configuration Pack V5.4 + SP1
- F-modules which support the passivation of channels

Currently, the following F-modules support passivation of channels:

Table 7-10

ET 200	F-module	Designation
ET 200 S	6ES7138-4FA02-0AB0	4/8 F-DI DC24V PROFIsafe
	6ES7138-4FB02-0AB0	4 F-DO DC24V/2A PROFIsafe
	6ES7138-4CF02-0AB0	PM-E F pm DC24V PROFIsafe
	6ES7138-4CF41-0AB0	PM-E F pp DC24V PROFIsafe
ET 200 M	6ES7326-2BF01-0AB0	SM 326F; DO 10xDC 24V/2A
	6ES7326-2BF40-0AB0	SM 326F; DO 8xDC 24V/2A P/M
	6ES7326-1RF00-0AB0	SM 326F; DI 8xNAMUR
	6ES7336-1HE00-0AB0	SM 336F; AI 6x13Bit
ET 200 PRO	6ES7148-4FA00-0XB0	8/16 F-DI DC24V PROFIsafe
	6ES7148-4FC00-0XB0	4/8 F-DI 4 F-DO DC24V/2A PROFIsafe
ET 200 ECO	6ES7148-3FA00-0XB0	4/8 F-DI DC24V PROFIsafe

Configuration

In the hardware configuration of STEP 7 the following project settings options exist:

- “Passivate the entire module“
- “Passivate channel“.

The configuration is made in the following tab of the F-I/O-module:

- “Module parameter“ -> “Behavior after channel error“

In chapter 4.5 you find two respective examples:

- F-DI with “Passivate the entire module“
- F-DI with “Passivate the channel“

The respective configurations are shaded.

7.4 Reintegration (of entire module or channel)

7.4.1 What happens during reintegration?

Reintegration has the following effect:

Table 7-11

Reintegration	Effect of reintegration:
F-input module (F-DI)	The safety program is provided with the process values pending at the input via the process image of the inputs.
F-output module (F-DO)	The output values provided by the safety program in the process image of the outputs are transmitted to the outputs.

7.4.2 Which types of reintegration exist?

The reintegration of an F-module can occur in two different ways (see Table 7-12):

- manually:
- automatically:

During manual reintegration, the user must acknowledge in the safety program for the reintegration of the F-system to be performed. ACK_REI (see Table 7-5) must be provided with a positive edge for this.

During automatic reintegration, the F-system integrates the F-module if the error causing the passivation has been removed. The user needs not acknowledge in the safety program.

Whether reintegration occurs manually or automatically is controlled via ACK_NEC (see Table 7-5):

- ACK_NEC = 1: Manual
  (Default value)
- ACK_NEC = 0: Automatic
  (must be set in the safety program by the user)

Warning

Automatic reintegration is only permitted if an automatic startup of the plant is not possible after the error has been removed.

The following table gives an overview of the reintegration.

Table 7-12

Cause of the passivation:			Reintegration	
			Manual or automatic	**Prerequisite for reintegration**
Safety program	**Setting "PASS_ON = 1" in the F-I/O-module data block**		automatic	„PASS_ON = 0"
F-operating system	**Startup of the F-CPU** **Startup of the F-CPU** Establishing communication between the F-CPU and the F-I/O via the safety protocol according to PROFIsafe.		automatic	Communication established
	F-communication error Error at fail-safe communication between F-CPU and F-I/O.		manual	F-system has recognized that the error causing the passivation has been removed. (*1)
	F-I/O error	**Module error** • Configuration error • Overtemperature	Depending on ACK_NEC: • If "0": automatic • If "1": manual (Default value)	
		Channel error • Wire break • Short circuit • Discrepancy • Overload		

Explanations on the table:

(*1):

After removing the error, the SF-LED of the affected F-module and the S7-message system does **not** indicate an error anymore.

The passivation of the F-module remains until reintegration (see chapter 7.5.1 and 7.5.2).

7.5 Processes during passivation and reintegration

The following chapter describes the processes during passivation and reintegration. Considered are the following variants:

Table 7-13

Variant	Chapter
Channel error and module error: automatic reintegration	7.5.1
Channel error and module error: manual reintegration	7.5.2
F-communication error: reintegration	7.5.3
Safety program	7.5.4
Group passivation	7.5.5

As a description, tables and figures with uniform structure are used below. The columns of the table have the following meaning:

Table 7-14

Column name	Column content
„State“	The numbers correspond to the number of the state.
“Description of status and *events“*	In the column the states and events are described. Events cause mode transitions. For better discrimination the events are given in *italics*.
“F-I/O-module data block” (*1)	The column lists the relevant variable of the F-I/O-module data block. The symbols in the columns have the following meaning: • ”0“, ”1“: Status of the bit • “0->1“: Positive edge • “x“: Status of the bit irrelevant
“SF-LED“ (*1)	The column indicates the status of the collective error display on the F-I/O-module (red LED).

(*1): To recognize more clearly which bits change during a mode transition, they are shaded in gray: If a bit is shaded gray, it has changed compared with its previous state.

The following background colors are used in the figures:

- Green background: the F-module is **not** passivated
- Red background: the F-module is passivated

7.5.1 Process: Channel / module error (automatic reintegration)

Precondition

The user has set “ACK_NEC = 0“ in the safety program.

Process sequences

If an error is pending at the F-module (channel or module error), the F-module is passivated by the F-system. If the error has been removed and “ACK_NEC = 0“, the F-module of the F-system is automatically reintegrated.

The following figure and table illustrates the process sequence.

Figure 7-3

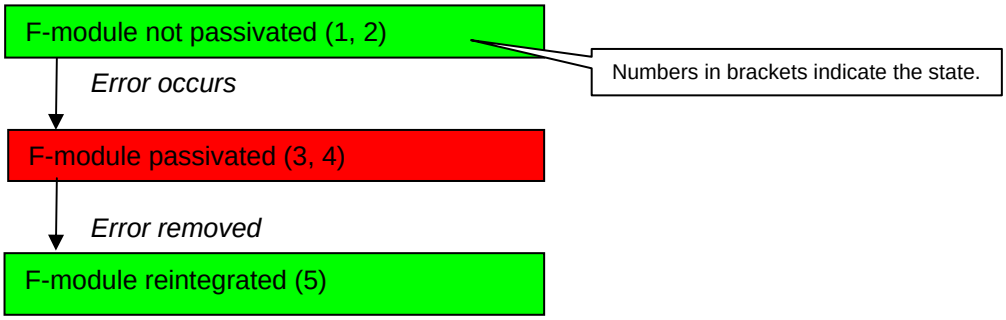


Table 7-15

State	Description of status and *events*	F-I/O-module data block / SF-LED A: ACK_NEC B: PASS_OUT C: QBAD D: SF-LED			
		A	B	C	D
1	F-module is not passivated	0	0	0	0
	Event: error occurs at the F-module				
2	F-module has recognized the error	0	0	0	1
	Event: F-system recognizes the error at the F-module				
3	F-system has passivated F-module	0	1	1	1
	Event: Removing the error at the F-module				
4	F-module has recognized that the error has been removed	0	1	1	0
	Event: F-system recognizes that the error at the F-module has been removed				
5	F-system has reintegrated the F-module	0	0	0	0

7.5.2 Process: channel / module error (manual reintegration)

Precondition

In the safety program the user acknowledges the reintegration by providing ACK_REI with a positive edge.

Process sequences

If an error is pending at the F-module (channel or module error), the F-module is passivated by the F-system. If the error has been removed and "ACK_NEC = 1"(default value), the F-module is only reintegrated after acknowledgement by the user.

The following figure and table illustrates the process sequence.

Figure 7-4

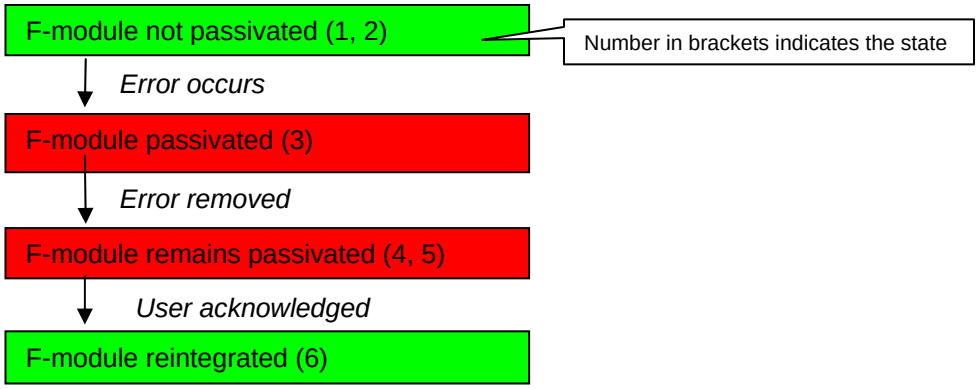


Table 7-16

State	Description of status and *events*	F-I/O-module data block / SF-LED A: ACK_NEC B: ACK_REI C: PASS_OUT D: QBAD E: ACK_REQ F: SF-LED					
		A	B	C	D	E	F
1	F-module is not passivated	1	0	0	0	0	0
	Event: error occurs at the F-module						
2	F-module has recognized the error	1	0	0	0	0	1
	Event: F-system recognizes the error at the F-module						
3	F-system has passivated the F-module	1	0	1	1	0	1
	Event: Removing the error at the F-module						
4	F-module has recognized that the error has been removed	1	0	1	1	0	0
	Event: F-system recognizes that the error at the F-module has been removed						
5	F-module remains passivated F-system requests user acknowledgement.	1	0	1	1	1	0
	Event: User acknowledges (positive edge)		*0->1*				
6	F-system has reintegrated the F-module	1	x	0	0	0	0

7.5.3 Process: F-communication error

Note For “F-communication error“ automatic reintegration is not possible!

Precondition

In the safety program the user acknowledges the reintegration by providing ACK_REI with a positive edge.

Process sequences

At F-communication error (e.g. due to disconnecting F-CPU and ET200) the entire affected F-I/O is passivated. If the error has been removed the F-I/O is only reintegrated after acknowledgement by the user. This applies irrespective of the ACK_NEC value. The following figure and table illustrates the process sequence.

Figure 7-5

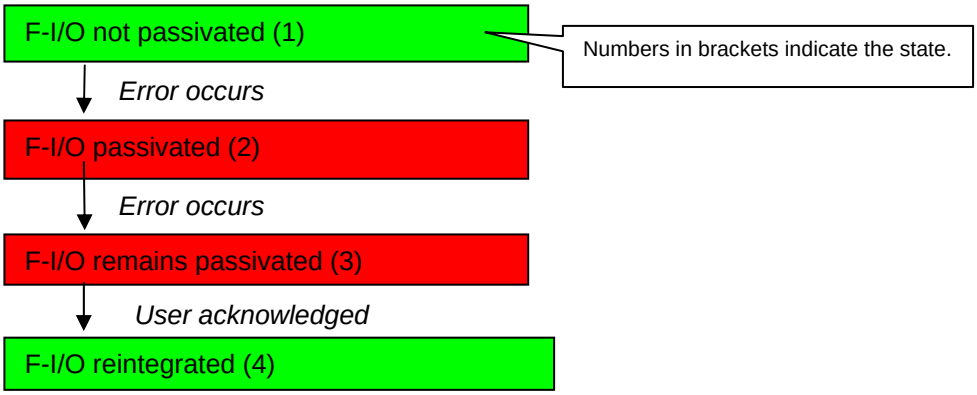


Table 7-17

State	Description of status and *events*	F-I/O data block F-DI and F-DO / SF-LED A: ACK_NEC B: ACK_REI C: PASS_OUT D: QBAD E: ACK_REQ F: SF-LED					
		A	B	C	D	E	F
1	F-I/O is not passivated	x	0	0	0	0	0
	Event: Error occurs						
2	F-module is passivated	x	0	1	1	0	0 (*1)
	Event: Error removed						
3	F-I/O has recognized that the error has been removed	x	0	1	1	1	0 (*2)
	Event: User acknowledges (positive edge)		*0->1*				
4	F-system has reintegrated the F-I/O	x	x	0	0	0	0

Explanations for the table: **(*1):** BF-LED at IM 151 HF is on. BF-LED at F-CPU is blinking.

(*2): The BF-LEDs are off.

7.5.4 Process: Safety program

Precondition

The user can passivate and automatically reintegrate F-modules via the safety program. The PASS_ON variable is used for this.

Process sequences

The F-module is passivated with “PASS_ON = 1“. The F-module is automatically reintegrated with “PASS_ON = 0“.

The following figure and table illustrates the process sequence.

Figure 7-6

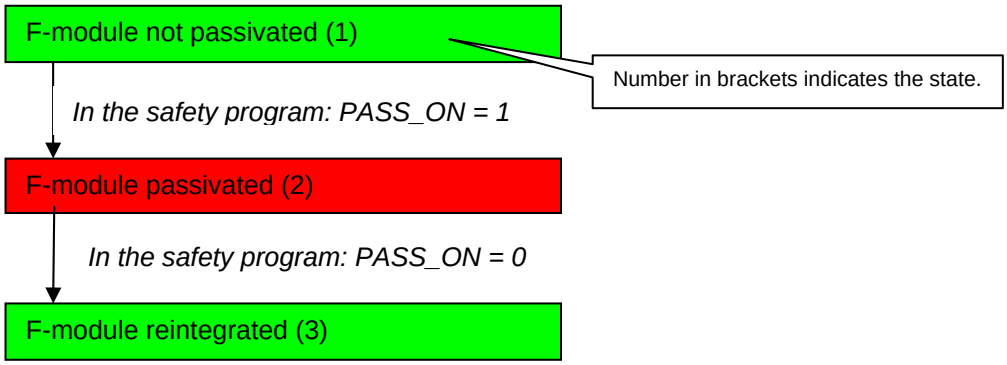


Table 7-18

State	Description of status and *events*	F-I/O-module data block / SF-LED A: PASS_ON B: PASS_OUT C: QBAD E: SF-LED			
		A	B	C	E
1	F-module is not passivated	0	0	0	0
	Event: User sets “PASS_ON = 1“ in the safety program	*1*			
2	F-system has passivated the F-module	1	0	1	0
	Event: User sets “PASS_ON = 0“ in the safety program	0			
3	F-system has reintegrated the F-module	0	0	0	0

7.5.5 Process: Group passivation

What is group passivation?

Group passivation refers to simultaneous passivation of several G-modules. The following example explains the application of group passivation:

An end-switch has been connected at an F-DI. The end-switch is used to monitor the position of an axis. The drive of this axis is controlled via an F-DO. During wire-break at the end-switch, the drive must be switched off for safety reasons. This can be realized via the safety program: During passivation of F-DI, the entire F-Do is passivated at the same time.

How is a group passivation realized?

In the safety program, individual F-modules can be grouped together. The characteristic of a group is:

- If 1 F-module “x“ from this group is passivated, then all other F-groups from this group are passivated.
- After manual or automatic reintegration of this F-module “x“, the remaining F-modules of the group are automatically reintegrated.

The PASS_OUT and PASS_ON bits of the respective F-I/O data blocks (chapter 7.2) are used for a group passivation:

- All PASS_OUT variables of the F-module of this group must have a OR logic operation
- The result of the OR logic operation must be assigned to all PASS_ON variables of the F-modules of this group

In the following example a group is realized. The group consists of an F-DI and an F-DO:

- If the F-DI is passivated, F-DO should also be passivated at the same time.
- If the F-DI is reintegrated, F-DO should also be reintegrated at the same time.

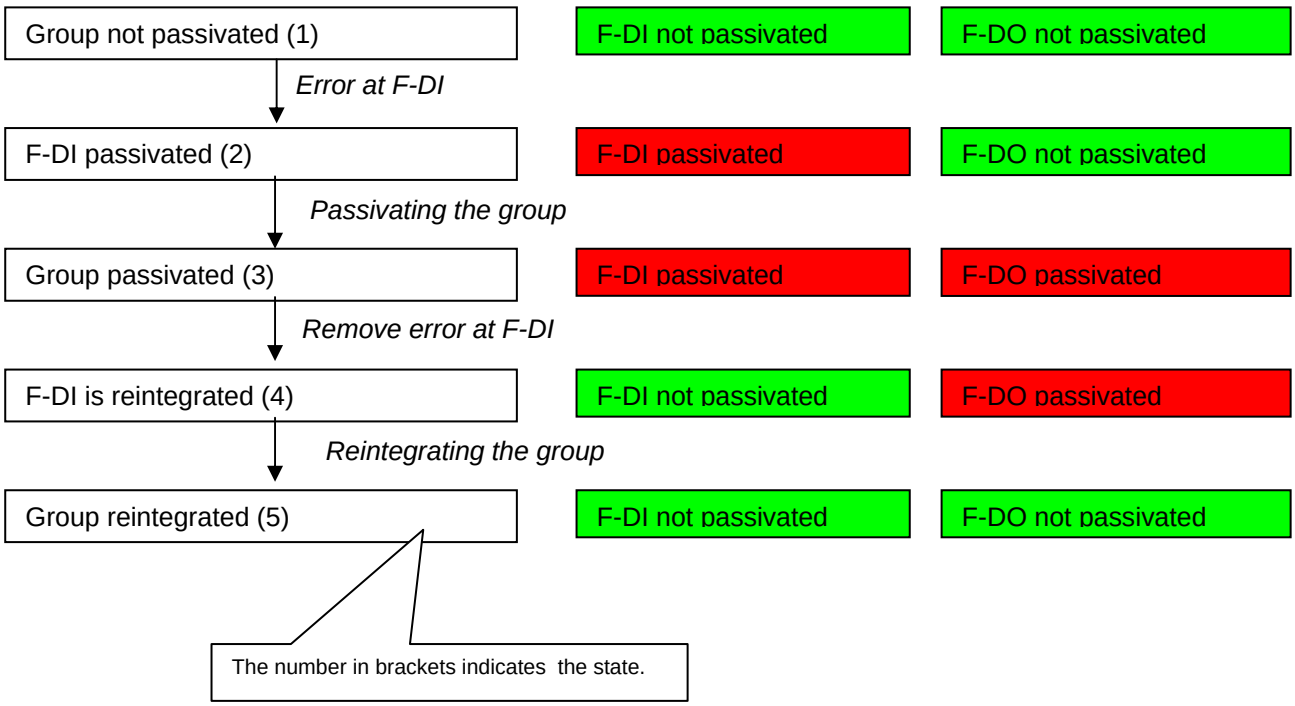
The example shows:

- What is the process of a group passivation?
- How do the relevant bits in the F-I/O data block of F-DI and F-DO behave?
- What is the design of the respective safety program?

The following figure and table illustrates the process sequence.

The following figure shows the process of a group passivation.

Figure 7-7



Warning

Automatic reintegration is only permitted if an automatic startup of the plant is not possible after the error has been removed.

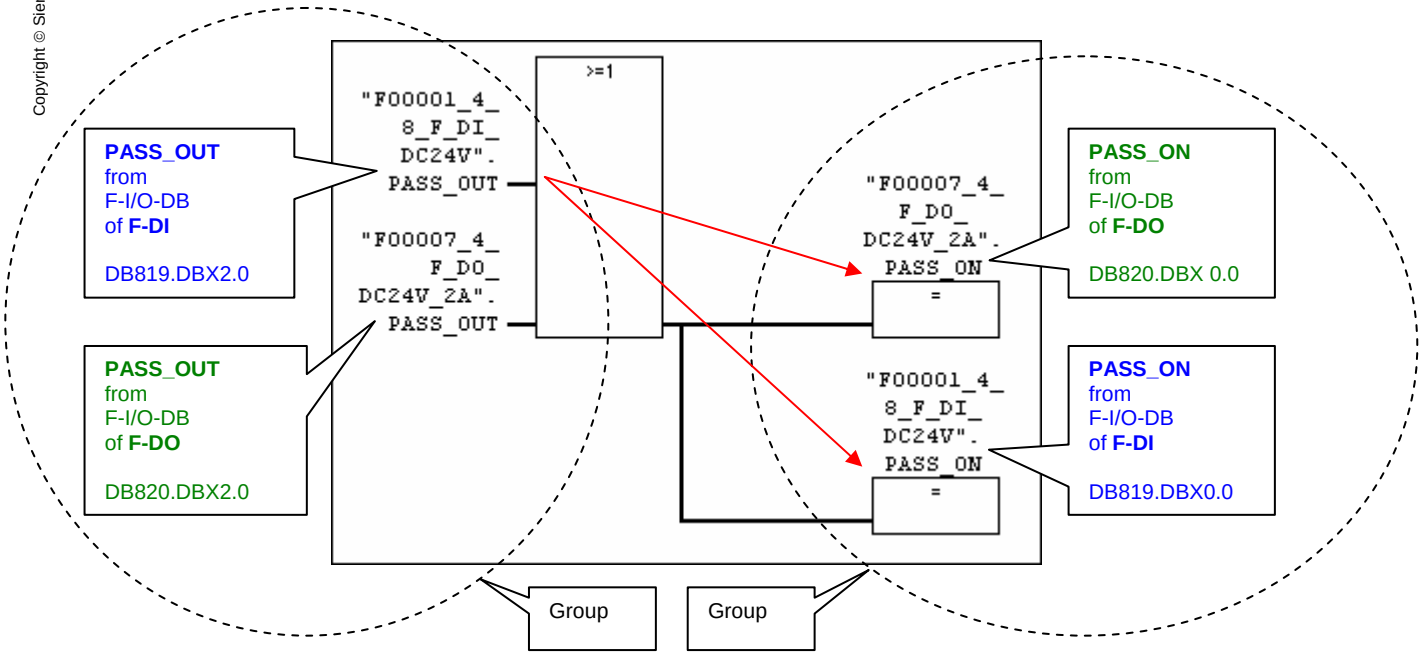
The following table explains the process of a group passivation.

Table 7-19

State	Description of status and *events*	F-I/O-module data block / SF-LED							
		F-DI				F-DO			
		A: PASS_OUT B: PASS_ON C: QBAD D: SF-LED				A: PASS_OUT B: PASS_ON C: QBAD D: SF-LED			
		A	B	C	D	A	B	C	D
1	Group is not passivated	0	0	0	0	0	0	0	0
	Event: F-operating system recognizes the error at the F-DI								
2	F-system has passivated the F-DI	1	0	1	1	0	0	0	0
	Event: Group is passivated via the safety program.								
3	F-system has also passivated the F-DO	1	1	1	1	0	1	1	0
	Event: F-system recognizes that the wire-break at the F-DI has been removed								
4	F-system has reintegrated the F-DI	0	1	0	0	0	1	1	0
	Event: Group is reintegrated via the safety program.								
5	Group is no longer passivated	0	0	0	0	0	0	0	0

The figure below shows the setup of the safety program:

Figure 7-8



The above network is not realized in the sample code. It only serves as an illustration.