SIEMENS

Safety Manual • 09/2014

# Energize to Trip Requirement for SIL 3 according to IEC 61511

## SIMATIC S7-400F/FH

http://support.automation.siemens.com/WW/view/en/109106504

# Warranty and Liability

We do not accept any liability for the 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 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 a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Industry Sector.

**Security information**

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

© Siemens AG 2015 All rights reserved

# Table of Contents



© Siemens AG 2015 All rights reserved

# 1 Task Definition

Safety Integrated is the holistic safety concept for automation and drive technology from Siemens. It is based on the closed-circuit principle. The closed-circuit principle does not require power to perform the safety function (de-energize to trip).

However, there are also applications that are based on the open-circuit principle and require power to perform the safety function (energize to trip). Examples of such applications:

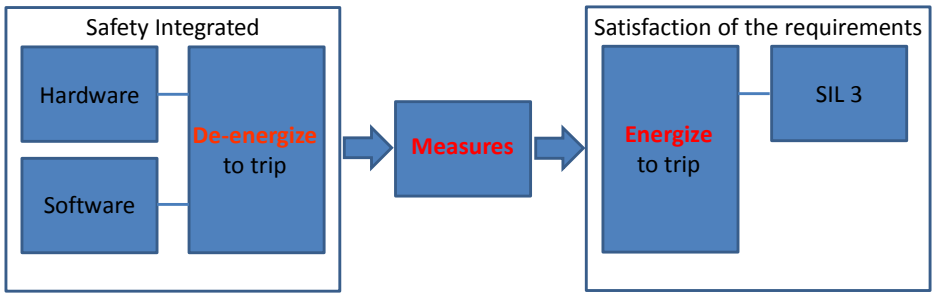
- Ventilation systems
- Smoke dampers

The automation task described here has the following safety-related requirements for a solution:

- Achievement of SIL 3 according to IEC 61511
- Use of the "energize to trip" principle

When using Safety Integrated hardware and software based on the "de-energize to trip" principle, additional measures are necessary to meet the above requirements as these requirements are based on the contrasting "energize to trip" principle (see figure below):

Figure 1-1 From "de-energize to trip" to "energize to trip"




The description of these measures and verification that SIL 3 according to IEC 61511 is achieved are core elements of this documentation.

**Note** The method can also be applied to IEC 62061.

© Siemens AG 2015 All rights reserved

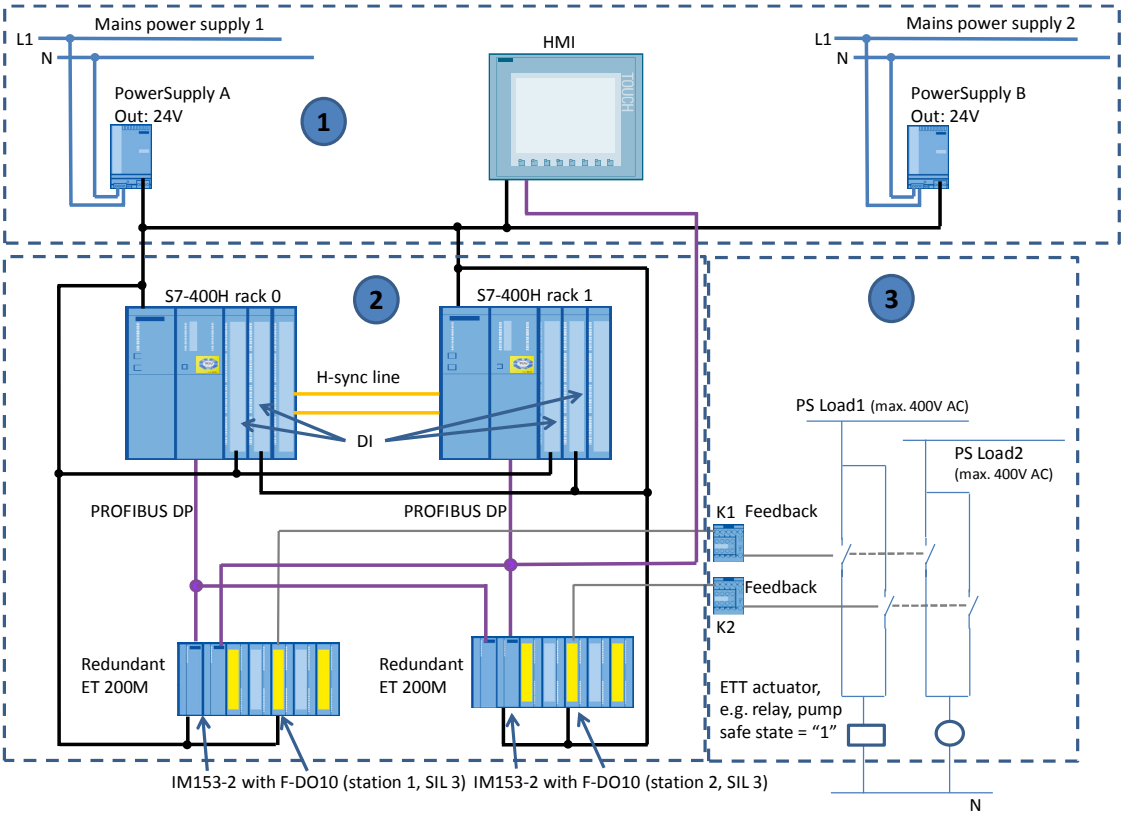
# 2 Solution

## 2.1 Overview

### Diagrammatic representation

The diagrammatic representation below shows the most important components of the solution:

Figure 2-1 Overview of the most important hardware components




**Note** The numbers 1, 2 and 3 refer to statements in chapter 2.2.

Within a redundant S7-400H system with fail-safe functionality, a redundant ET 200M I/O device with fail-safe output modules (F-DO) provides the triggering of the safety function.

An HMI informs of occurring faults.

**Note** The designation of the CPUs follows the following convention:

Each CPU is an H-CPU within an S7-400H H-system. An additional license provides them with additional safety functionality. As this document deals primarily with the safety aspect of the application, each CPU is referred to as an F-CPU.

© Siemens AG 2015 All rights reserved

## 2.2 Classification of the sections in the overview

**Sections of the overview**

The overview of the most important hardware components (Figure 2-1) is divided into three sections (dashed border):

Table 2-1 Reference to Figure 2-1

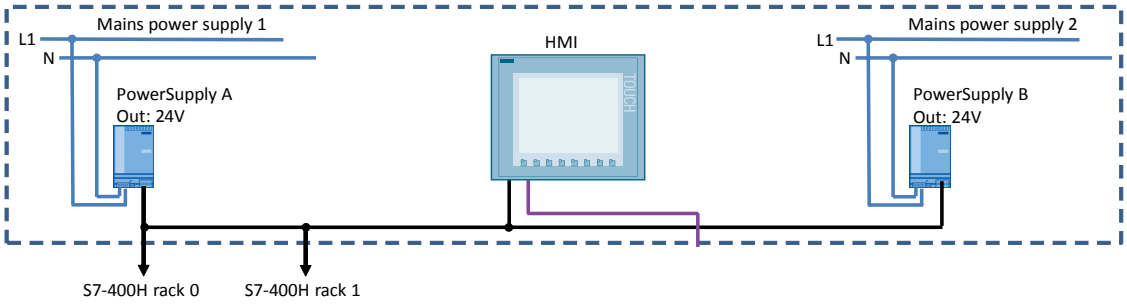
| No. | Explanation |
|---|---|
| 1 | Mains power supply 1 and 2 and HMI |
| 2 | H-system with redundant I/O |
| 3 | Connected actuators |

The aim of this classification is to facilitate the following description, i.e., which areas are the focuses of this safety manual and which ones are not described in greater detail. The following sections explain these three sections accordingly.

© Siemens AG 2015 All rights reserved

### 2.2.1 Mains power supply 1 and 2 and HMI

Figure 2-2 Mains power supply 1 and 2 and HMI




**Mains power supply 1 and 2**

Ensuring the power supply to maintain the safe state is a systematic requirement according to IEC 61508. Calculated proof for the probability of failure of the power supply is not required.

This description assumes that there are two mains power supplies. The absence of interaction is important; i.e., the state (or a state change) of one mains power supply has no effect whatsoever on the other mains power supply.

| | |
|---|---|
| **WARNING** | **Death or severe personal injury may result if the systematic requirements are not ensured.**<br>The user must ensure that the systematic requirements are met. |

A description of the compliance with the systematic requirements is not part of this safety manual. The aspects described here start with the interface following PowerSupplies A and B, starting with S7-400H racks 0 and 1.

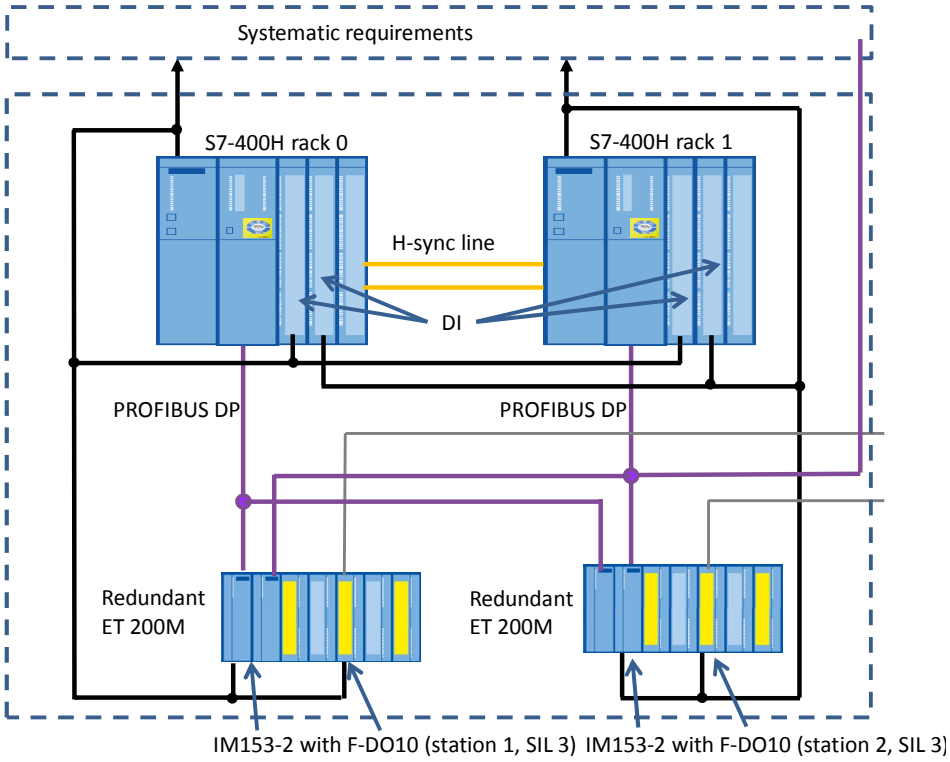
**HMI**

A failure of the power supply has to be output to a permanently manned receiving station. The power supply failure can be signaled acoustically and/or, as shown here, visually via operator control and monitoring equipment (HMI).

Ensuring that a message is transmitted is part of the systematic requirement and has to be ensured by the user.

### 2.2.2 H-system with redundant I/O

Figure 2-3 H-system with redundant I/O

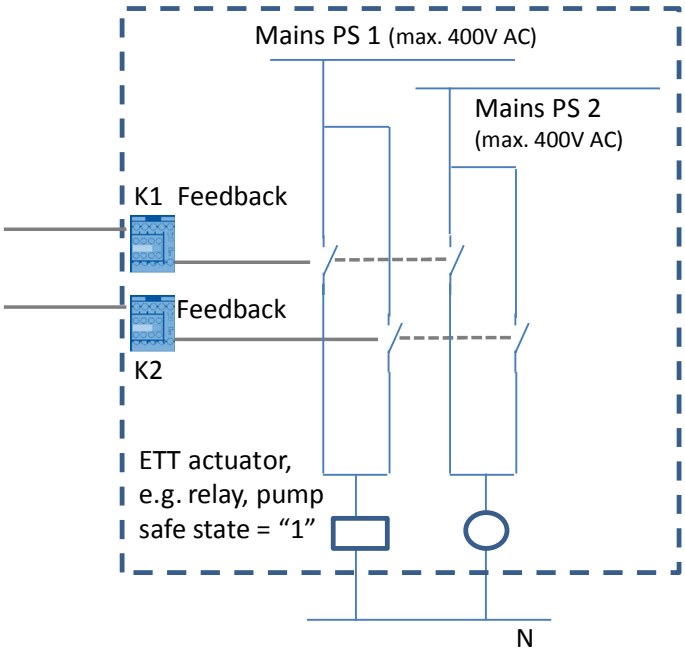



Starting with the power supply of the H-system, an FMEA (failure mode and effects analysis) is performed in this section. The objective of the FMEA is to analyze potential failures and assess the behavior of the F-DO as maintaining the safety function is particularly determined by the states of the binary outputs of the F-DO.

© Siemens AG 2015 All rights reserved

### 2.2.3 Connected actuators

Figure 2-4 Connected actuators

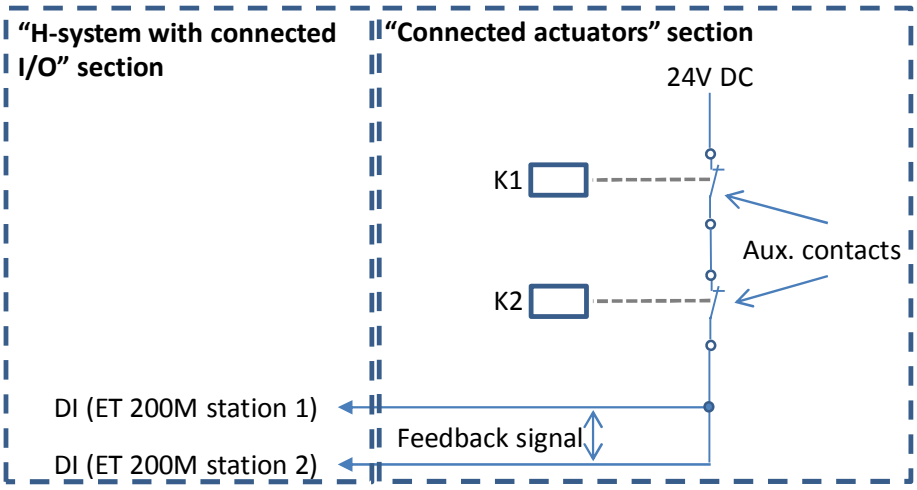



.

Appropriate actuators are controlled using the contactors K1 and K2. The assessment of the actuators is not part of this safety manual. When selecting the actuators, the user has to consider the occurring load currents (see also the "Technical data - F-DO10xDC24V" chapter in \3\).

The FMEA addressed in chapter 2.2.2 considers the readback signals of the contactors K1 and K2 retrieved via the auxiliary contacts (indicated in Figure 2-4 by the term "feedback" and illustrated in greater detail in Figure 2-5).

Figure 2-5 Reading back the auxiliary contacts of contactors K1 and K2




© Siemens AG 2015 All rights reserved

## 2.3 Description of the core functionality

**Note**

Regarding the F-DO, the following sections contain simplified wording such as:

- The F-DO is set
- The F-DO keeps its value, or similar phrases

This always refers to the individual outputs of the F-DO that are necessary for triggering the safety function.

### Concept

Triggering the safety function is achieved by at least one F-DO controlling a contactor (TRUE signal to contactor coil).

In contrast to the "de-energize to trip" principle where a failure of the power supply would provide a FALSE signal of the F-DO and therefore the safe state, the "energize to trip" principle requires that the power supply of the system be ensured as a TRUE signal for the safe state is required on at least one F-DO.

The power supply is ensured by the use of two mains power supplies non-reacting to each other. The power supply failure can be signaled acoustically and/or, as shown here, visually via operator control and monitoring equipment (HMI).

When using the "energize to trip" principle, it is mandatory to use F-DOs with diagnostics capability.

### The special role of the F-DOs

The F-DOs with diagnostics capability are the certified SIMATIC component F-DO 10xDC24V/2A, article no. 6ES7326-2BF10-0AB0.

For this F-DO, "Keep last valid value" in the event of a fault can be configured as the safety-related setting. Such faults are:

- Abort of PROFIsafe communication
- F-CPU stop

By integrating the F-DO into a user function (for the application), up to SIL 3 according to IEC 61511 can be achieved. Such an application is practically implemented in a redundant configuration as shown, for example, in \2\.

© Siemens AG 2015 All rights reserved

## 2.4 Hardware and software components

**Requirements**

The components used must meet the following requirements:

- Redundant F-DO10xDC24V/2A PP
- Redundant control system (S7-400H)
- Redundant IM 153-2 interface module of the distributed I/O
- Fail-safe power supply, for example uninterruptible power supply (UPS)
- Trigger unit (closed-circuit current) must comply with at least SIL 2 or the required safety level
- Short-circuit-proof wiring
- Readback contacts (standard connection) for ETT actuators

### 2.4.1 Hardware components

The safety concept described here can be implemented with the following hardware components:

© Siemens AG 2015 All rights reserved

Table 2-2

| Component | Type | No. | Article no. |
|---|---|---|---|
| **Central configuration** | | | |
| Power supply | PS 407, 20A, 120/230V UC, 5V DC/20A | 2 | 6ES7407-0RA01-0AA0 |
| CPU416-5H PN/DP, 16MB F. | S7-400H/F/FH | 2 | 6ES7416-5HS06-0AB0 |
| **Distributed configuration** | | | |
| Power supply | PS 307, input: 120/230V AC, output: 24V DC/10A | 2 | 6ES7307-1KA02-0AA0 |
| ET200 M | IM 153-2 interface module | 2 | 6ES7153-2BA02-0XB0 |
| F-digital output | SM326 F-DO10xDC24V/2A PP | 2 | 6ES7326-2BF10-0AB0 |

**Note**

Follow the instructions for installing the S7-400. They can be found in the installation manual: \4\. Standards, certificates and approvals can be found in the system description: \8\

Instructions for installing the ET 200M can be found here: \3\

| NOTICE | **Except the F digital output module (6ES7326-2BF10-0AB0), you can also use hardware components similar to the ones listed in the above table.**<br><br>**Similar hardware components are the ones listed in the TÜV certificate (certificate number: Z10 09 07 67803 004 Rev 3.19). The certificate can be found here: \7**<br><br>**However, please note that different hardware components may have different safety-related characteristic values ((SIL CL, PFD). Therefore, for the overall PFD value over the entire safety chain, values can occur that may no longer achieve the desired SIL.**<br><br>**Accordingly, the statements also apply to standard components involved in the safety function. Different standard components have different MTBF values and therefore different probabilities of failure.** |
|---|---|

| WARNING | **Due to the "energize to trip" principle used, the power supply of the F-components must be ensured. The load power supplies must meet the requirements of the SIMATIC Safety Modules.** |
|---|---|

© Siemens AG 2015 All rights reserved

### 2.4.2 Software components

This application is valid for:

- STEP 7 V5.4 SP4 or higher
- F Systems V6.0 or higher
  - S7 F Systems Lib *V1_3*
  - CFC V6.0 SP2 HF3 or higher
- When used with PCS7: PCS7 V6.0 SP3 or higher with the STEP 7 and CFC version included.

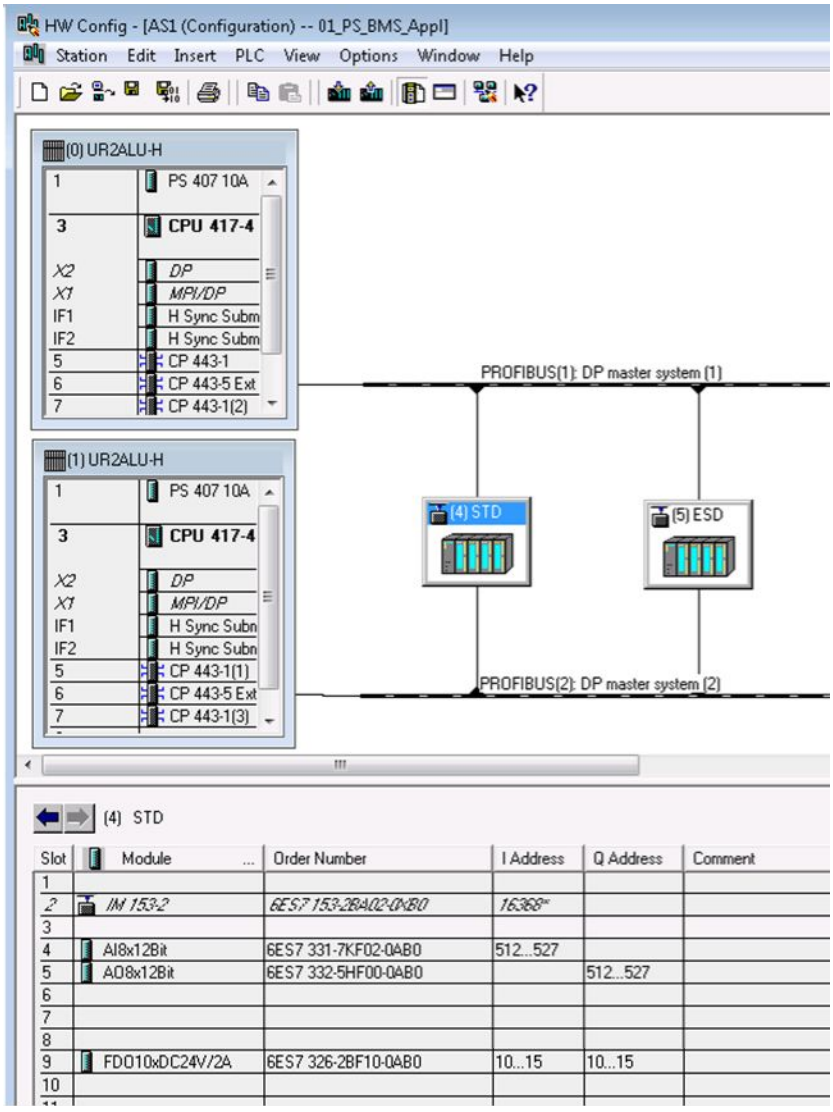
# 2.5 Configuration and parameterization

## 2.5.1 Configuring the F-CPU

The controller is configured in a redundant and fail-safe manner.

The figure below shows the STEP 7 hardware configuration. Safety mode has to be activated in the configuration.

Figure 2-6 Configuration example for ETT application




**Note** Instead of the external CP 443-5, you can also use the internal DP interface of the H-CPU.

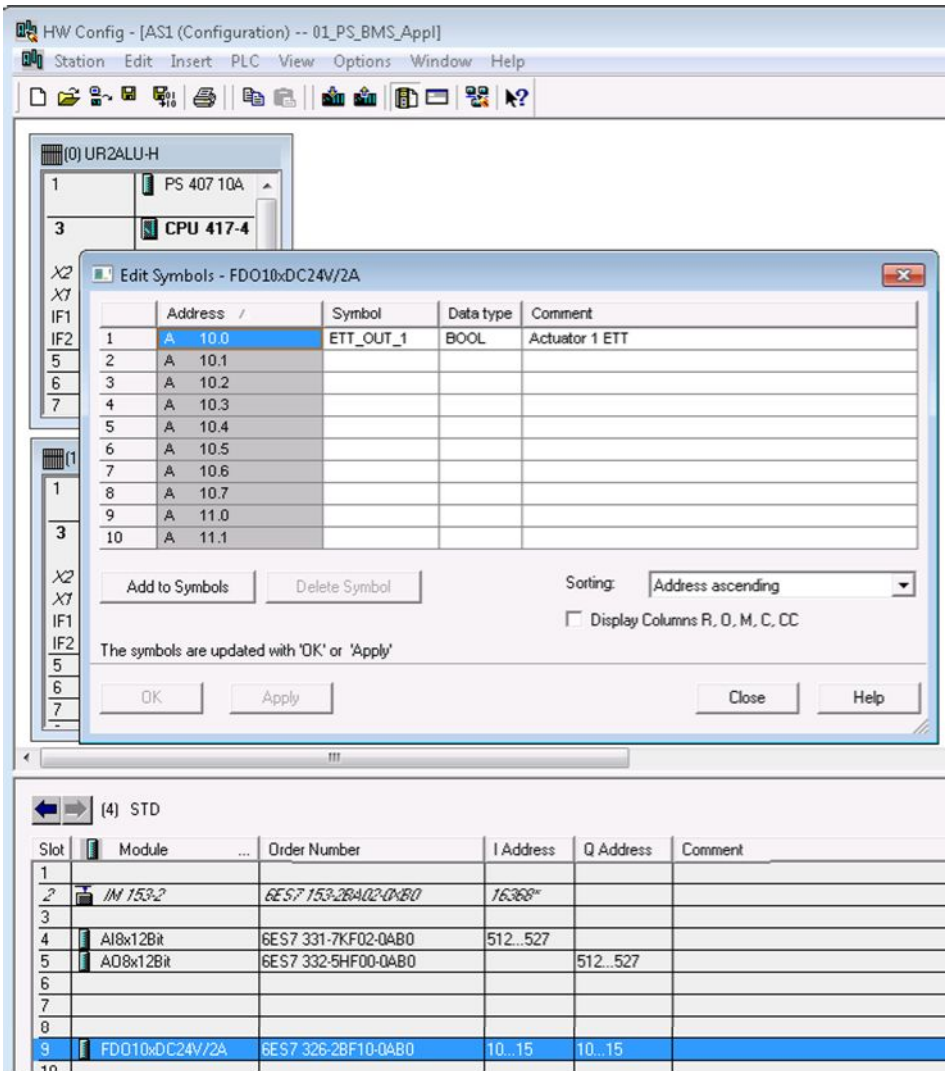
© Siemens AG 2015 All rights reserved

## 2.5.2 Parameterizing the outputs of the F-DO

The actuator is controlled from two fail-safe output modules that are inserted in different ET 200M stations. Due to the installation in different ET 200M stations connected to the redundant control system via a redundant PROFIBUS, the hardware fault tolerance (HFT) is 1.

When inserting the modules into the STEP 7 hardware configuration (next figure), the automation system assigns the addresses for the inputs and outputs available on the module. To be able to access the addresses from the logic, symbolic names are assigned to the addresses.

Figure 2-7 Example of parameterizing the outputs of the F-DO




© Siemens AG 2015 All rights reserved

### 2.5.3 Safe control of actuators

#### Options

Basically, there are two ways to safely control an actuator:

- Module redundancy
- Channel redundancy

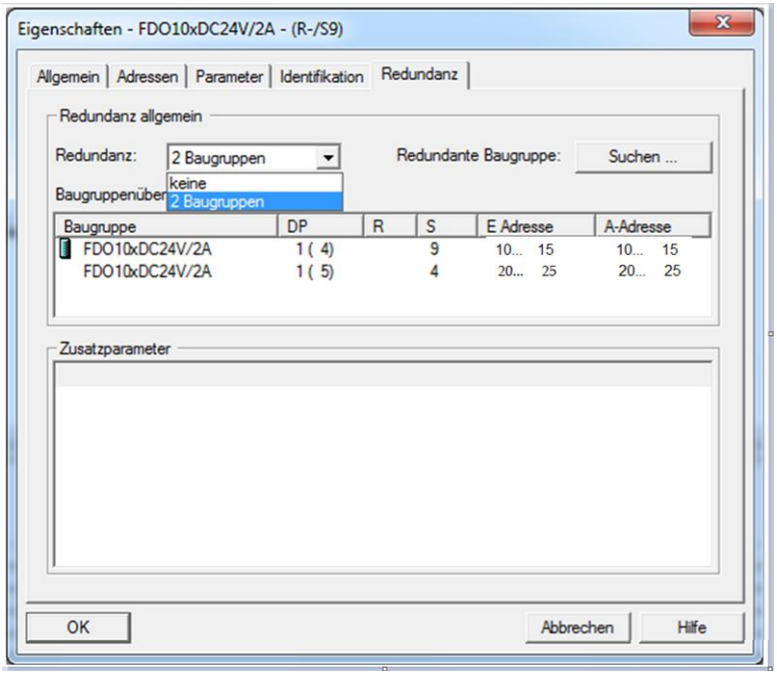
The following section describes module redundancy.

#### Module redundancy

For module redundancy, a redundancy partner for a module is defined in the STEP 7 hardware configuration. All settings on the module are automatically transferred to the redundancy partner.

In the case described here, module and redundancy partner are the F-DO 10xDC24V/2A that have already been mentioned and are inserted in different stations of the ET 200M.

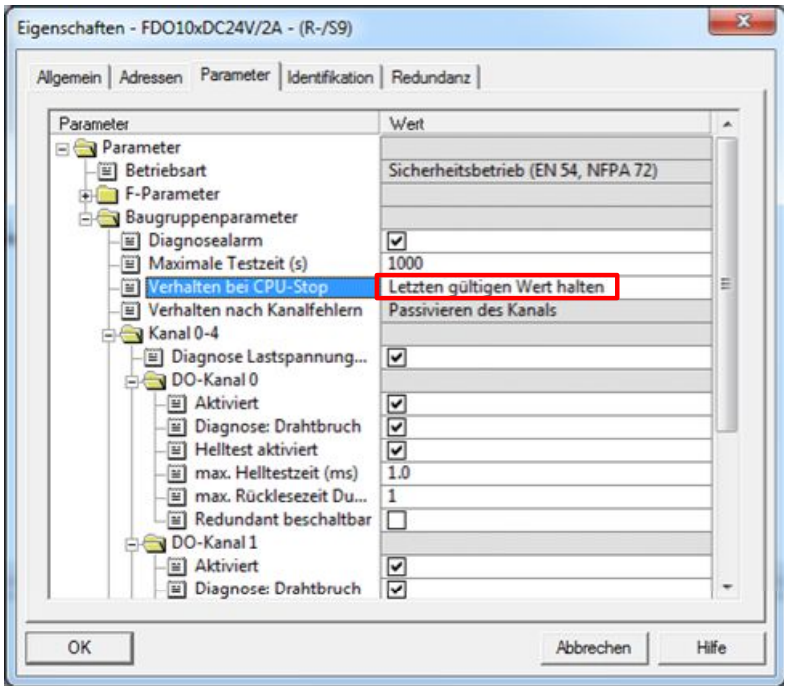
Figure 2-8 Module redundancy of the F-DO10xDC24V




For the F-DO, "Keep last valid value" must be set:

© Siemens AG 2015 All rights reserved

Figure 2-9 "Keep last valid value" setting




For outputs that have to be enabled to establish the safe state, it must be ensured that the actuator can be controlled at any time. This requires that the electric circuit be monitored even when the output is not enabled. The F-DO10xDC24V/2A PP (6ES7326-2BF10-0AB0) can test the electric circuit by running a light test. To do this, activate the "Enable light test" function by checking the check box (see Figure 2-9).

**Note** Unused channels have to be deactivated (unchecked).

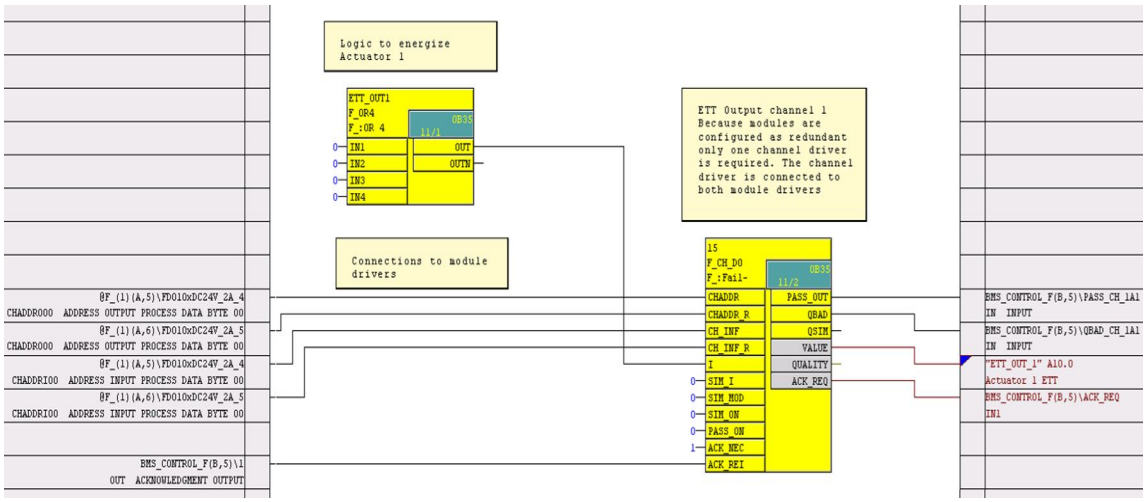
### Safety program

The logic of the safety function is implemented in the safety program. To set and reset an output on a redundant module, only one channel driver (F_CH_DO) is placed in the safety program and interconnected with the symbolic name of the output with the lower address.

When compiling the CFC, the system detects that a redundant partner exists for the module with the output and interconnects the channel driver with both F output modules (CHADDR and CH_INF with a module and CHADDR_R and CH_INF_R with the redundant partner).

© Siemens AG 2015 All rights reserved

Figure 2-10 ETT application F-program




## Maximum load

The maximum permitted load that can be switched by the F-DO10xDC24V/2A is 5W. (See the "Technical data - F-DO10xDC24V" chapter in \3\.)

© Siemens AG 2015 All rights reserved

# 3 Safety Function

A distinction has to be made between events that cause the triggering of the safety function and fault scenarios of which staff is informed and which have to be cleared but which do not trigger the safety function.

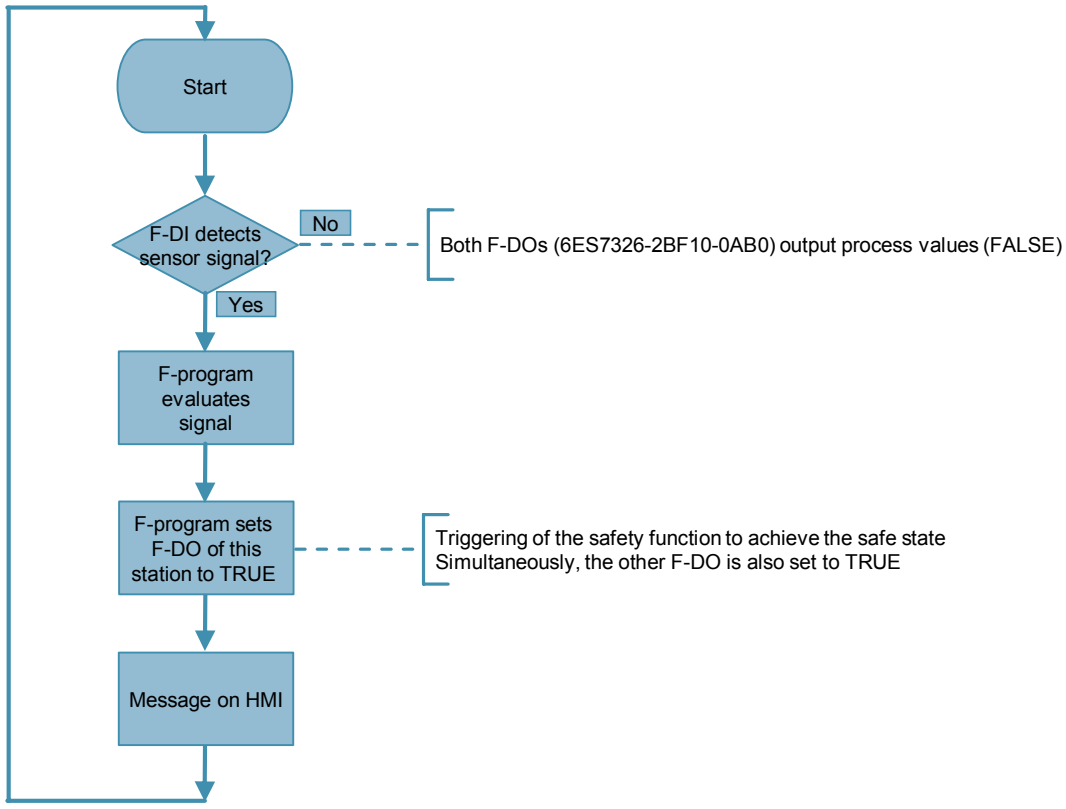
## 3.1 Triggering of the safety function

Events that cause the triggering of the safety function must be programmed in the F-program. At the same, detection of these events is the trigger for triggering the safety function.

For example, a sensor (e.g., a smoke detector) can transfer a binary signal to the F-program via the F-DI. In the F-program, the safety function is triggered that results in the setting of the F-DO.

This scenario describes the method of operation of the "energize to trip" principle.

Figure 3-1 Triggering of the safety function




© Siemens AG 2015 All rights reserved

## 3.2 Faults that do not result in the triggering of the safety function

The following faults do not trigger the safety function and are therefore not part of the "energize to trip" principle:

- Passivation of an F-DO
- Failure of an F-CPU
- Failures of the IM 153-2 interface module

However, these cases are analyzed within the scope of the FMEA to explain the response of the safety system to these faults.

For fault scenarios where an F-DO is passivated, please note the following:

| | |
|---|---|
| **NOTICE** | **Hazards can occur due to actuators that start unexpectedly if you implement reintegration of the F-I/O through automatic reintegration.**<br>Actuators that start unexpectedly can cause dangerous situations.<br>Preferably use an acknowledgement signal for reintegration. |

© Siemens AG 2015 All rights reserved

# 4 Review of Systematic Requirements and Safety Requirements by Means of an FMEA

**Note** FMEA: **F**ailure **M**ode and **E**ffects **A**nalysis

An FMEA was performed for the items of the following tables.

Table 4-1 Failure of the power supply

| No. | Subject | Trigger safety function? | Information to receiving station? | Total failure of safety system? | Note |
|---|---|---|---|---|---|
| 1 | Partial power supply failure | no | yes | no | |
| 2 | Total power supply failure | No longer possible | Must be ensured by the user (systematic requirement according to IEC 61508) | yes | This case can be regarded as highly improbable. |

Table 4-2 Short circuit, overvoltage, wire break

| No. | Subject | Trigger safety function? | Information to receiving station? | Total failure of safety system? | Note |
|---|---|---|---|---|---|
| 1 | Short circuit to ground | no | yes | no | |
| 2 | Overvoltage (on one power supply) | no | yes | no | |
| 3 | Overvoltage (on both power supplies) | No longer possible | Must be ensured by the user (systematic requirement according to IEC 61508) | yes | This case can be regarded as highly improbable. |
| 4 | Wire break (to one actuator) | no | yes | no | |
| 5 | Wire break (to both actuators) | No longer possible | yes | yes | This case can be regarded as highly improbable. |

© Siemens AG 2015 All rights reserved

Table 4-3 Passivation of the F-DO

| No. | Subject | Trigger safety function? | Information to receiving station? | Total failure of safety system? | Note |
|---|---|---|---|---|---|
| 1 | Both F-DO set to FALSE and one F-DO passivated | no | yes | no | |
| 2 | Both F-DO set to FALSE and passivate both | No longer possible | Only if the cause is not the failure of both CPUs. | yes | This case can be regarded as highly improbable. |
| 3 | One F-DO set to FALSE and this F-DO is passivated | Has already been triggered and is maintained | yes | no | |
| 4 | One F-DO set to FALSE and the other F-DO passivated | Has already been triggered and is maintained | yes | no | The safety function is maintained due to the parameterization of the F-DO with "Keep last valid value". |
| 5 | One F-DO set to FALSE and passivate both | Has already been triggered and is maintained | Only if the cause is not the failure of both CPUs. | no | This case can be regarded as highly improbable. |
| 6 | Both F-DO set to TRUE and one F-DO passivated | Has already been triggered and is maintained | yes | no | |
| 7 | Both F-DO set to TRUE and passivate both | Has already been triggered and is maintained | Only if the cause is not the failure of both CPUs | no | The safety function is maintained due to the parameterization of the F-DO with "Keep last valid value". |

© Siemens AG 2015 All rights reserved

# 5 Verification of the achievable SIL 3

To determine the SIL or verify that SIL 3 according to IEC 61508 can be achieved, the PFD must be calculated. Based on IEC 61508-6, VDI/VDE 2180 Sheet 4 provides approximation formulas that can be used under certain conditions (listed in chapter 6.1 of VDI/VDE 2180 Sheet 4). These requirements are usually met in the process industry.

The starting point for calculating the overall PFD (see also Annex B of IEC 61511-2:2003) is the following model where the overall PFD is calculated from the sum of

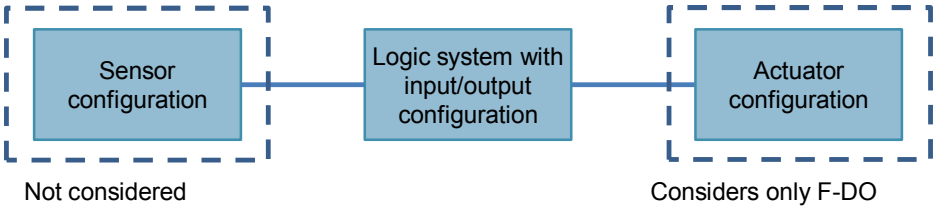
- the PFD of the sensor component
- the PFD of the logic system and
- the PFD of the actuator component.

This document does not assess the sensor and the F-DI. It is assumed that the information that causes the triggering of the safety function exists in the F-CPU as safe information. This safe information can either arrive at the F-CPU via an F-DI or it is generated by the user in the safety program.

When looking at the actuators, the interface is on the F-DO. The F-DO is the subject matter, possible actuators (e.g., contactors) are not specified any further and therefore not assessed at this point.

© Siemens AG 2015 All rights reserved

Figure 5-1 Considered items of the model




The protective equipment is shown as a subsystem structure. The individual subsystems include the associated components so that the following applies to the calculation of the overall PFD:

$PFD = PFD_{Sensor} + PFD_{F-DI} + PFD_{F-CPU} + PFD_{F-DO} + PFD_{Actuator} + P_{TE}$ where $PFD_{Sensor}, PFD_{F-DI}, und\ PFD_{Actuator}$ are not considered here.

The $PFD_{F-CPU}$, the $P_{TE}$ (TE: transmission error) and the $PFD_{F-DO}$ are considered here.

**PFD of the F-CPU**

The $PFD_{F-\mathrm{CPU}}$ of the F-CPU used can be found, for example, in \6\.

**Transmission error**

The probability of dangerous transmission errors for digital communication processes $P_{TE}$ is considered once in the calculation. The following applies to PROFIsafe communication:

$P_{TE} = 10^{-5}$

Actuator configuration

Various wiring architectures are available for the connection of actuators.

**PFD of the F-DO**

The $PFD_{F-DO}$ of the F-DO used can be found, for example, in \6\.

# 6 Summary

A fail-safe application contains systematic requirements that are the basis for implementing a safety system. These basic requirements must be ensured by the user.

In the case discussed here, the "energize to trip" principle is used within the safety concept. It requires power to perform the safety function, which places greater emphasis on the consideration of the power supply as a systematic requirement.

Furthermore, other faults are considered that are neither part of a systematic requirement nor part of the "energize to trip" principle, but which should nevertheless be analyzed.

All of these three points (once again listed below) are dealt with within the scope of an FMEA.

- Ensuring the power supply as a systematic requirement
- The safety system based on the "energize to trip" principle
- Other fault scenarios

All of these three points must be considered independently of each other. The systematic requirements and the "other fault scenarios" are not part of "energize to trip"; however, due to this, they are analyzed in an FMEA.

The use of the H-system is also not part of the "energize to trip" principle. There is no redundancy regarding the safety functionality; at any time, only one F-CPU is involved in the process. Only the availability is increased by the H-system. However, availability and safety must always be considered independently of each other.

© Siemens AG 2015 All rights reserved

# 7 References

Table 7-1

| | Subject | Title |
|---|---|---|
| \1\ | Siemens Industry Online Support | http://support.automation.siemens.com |
| \2\ | FAQ about the "Keep last valid value" function | http://support.automation.siemens.com/WW/view/en/65954737 |
| \3\ | SIMATIC Manual | SIMATIC Automation System S7-300 ET 200M Distributed I/O Device<br>Fail-safe signal modules<br>Installation and Operating Manual<br>http://support.automation.siemens.com/WW/view/en/19026151 |
| \4\ | SIMATIC Manual | SIMATIC<br>Automation System S7-400 Hardware and Installation Manual<br>http://support.automation.siemens.com/WW/view/en/1117849 |
| \5\ | MTBF values for SIMATIC products | http://support.automation.siemens.com/WW/view/en/16818490 |
| \6\ | PFD values for SIMATIC products | http://support.automation.siemens.com/WW/view/en/27832836 |
| \7\ | Certificate for SIMATIC S7 F/FH Systems | http://support.automation.siemens.com/WW/view/en/48191415 |
| \8\ | SIMATIC Manual | SIMATIC<br>Automation System S7-400 Configuration and Use System Description<br>http://support.automation.siemens.com/WW/view/en/22586851 |

© Siemens AG 2015 All rights reserved

# 8 History

Table 8-1

| Version | Date | Modifications |
|---|---|---|
| V1.0 | 02/2015 | First release |
| | | |