SIEMENS
Ingenuity for life

Wiring and Voting Architectures for failsafe Digital Input (F-DI) and Output Modules (F-DO) of the ET 200M

SIMATIC Safety Integrated for Process Automation

https://support.industry.siemens.com/cs/ww/en/view/37236961

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

© Siemens AG 2018 All rights reserved

Table of contents

© Siemens AG 2018 All rights reserved

© Siemens AG 2018 All rights reserved

© Siemens AG 2018 All rights reserved

1 Automation functions

1.1 Functionality of the application example

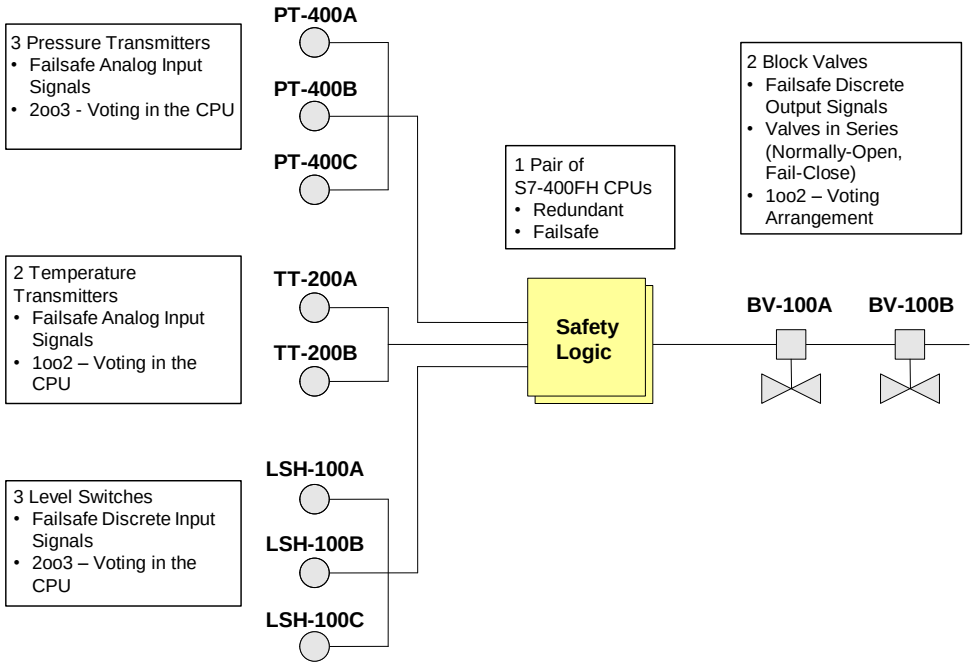
Task

Several failsafe digital signals shall be monitored and failsafe actuators shall be controlled in a plant. Depending on importance and failure risk, there are several options of wiring and voting the signals. The voting can, for example, be realized in the digital input modules and/or in the CPU.

Figure 1-1 shows an exemplary plant component in which the valves (BV100A and BV100B) require fail-safe closing in a container, depending on

- pressure
- level and
- temperature.

Figure 1-1 Example 1 Overview:



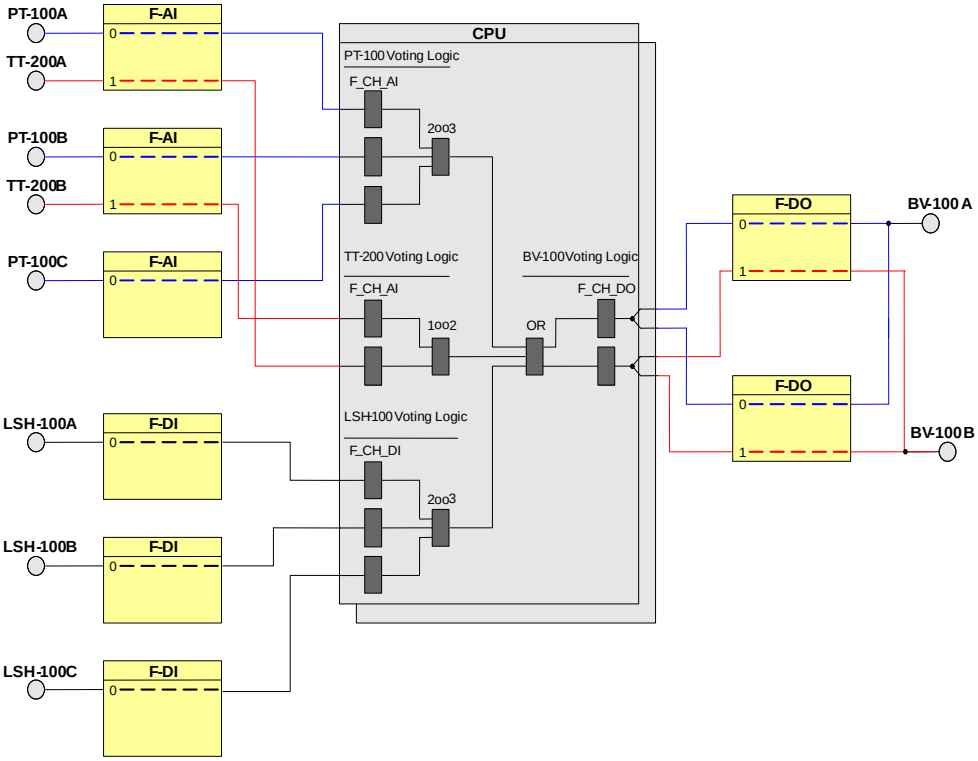
The various possibilities of wiring and voting failsafe signals are illustrated in this application example. Additional the wiring and voting of failsafe outputs are illustrated too.

© Siemens AG 2018 All rights reserved

Solution

Figure 1-2 illustrates a plausible plant unit layout, in which different wiring and voting architectures for analog and digital signals are used.

Figure 1-2 Example 1 system configuration



Note

In all function examples, the fail-safe digital input module SM 326 - DI 24 x DC 24V with Order Number 6ES7326-1BK02-0AB0 is used. This is hereafter referred to as F-DI.

© Siemens AG 2018 All rights reserved

1.2 Presented architectures

Recommended architectures

The following recommended architectures are presented in this application example:

- **One sensor (1oo1) and one F-DI (1oo1)**
  Typical application when a single sensor has the required Safety Integrity Level and there is no need for increased availability (explained in Chapter 2).
- **One sensor (1oo1) and redundant F-DI (2oo2)**
  Typical application when a single sensor has the required Safety Integrity Level and there is a need for increased availability. (explained in Chapter 3)
- **Two sensors (1oo2) and one F-DI with evaluation in the F-DI (1oo1)**
  Typical application when a single sensor does not have the required Safety Integrity Level and there is no need for increased availability (explained in Chapter 4).
- **Two sensors (1oo2) and redundant F-DI with evaluation in the F-DI (2oo2)**
  Typical application when a single sensor does not have the required Safety Integrity Level and there is a need for increased availability (explained in Chapter 5).
- **Two sensors (1oo2) with evaluation in the user program**
  Typical application when a single sensor does not have the required Safety Integrity Level and the data of both sensors must be visible in the automation system. (explained in Chapter 6).
- **Two sensors (1oo2) and redundant F-DI (2oo2) with evaluation in the user program**
  Typical application when a single sensor does not have the required Safety Integrity Level and the data of both sensors must be visible in the automation system. This architecture can be configured for increased availability with redundant F-DI (2oo2) (explained in Chapter 7).
- **Control of a single actuator (1oo1) on an F-DO (1oo1)**
  From the point of view of the safety system, all connected actuators are 1oo1 outputs. Each connected actuator should react in the manner specified in the safety logic (explained in Chapter 8).
- **Control of a single actuator (1oo1) with redundant F-DO (2oo2)**
  Typical application to increase the availability of the F-DO. The actuator is controlled by a pair of redundant F-DO (explained in Chapter 9).

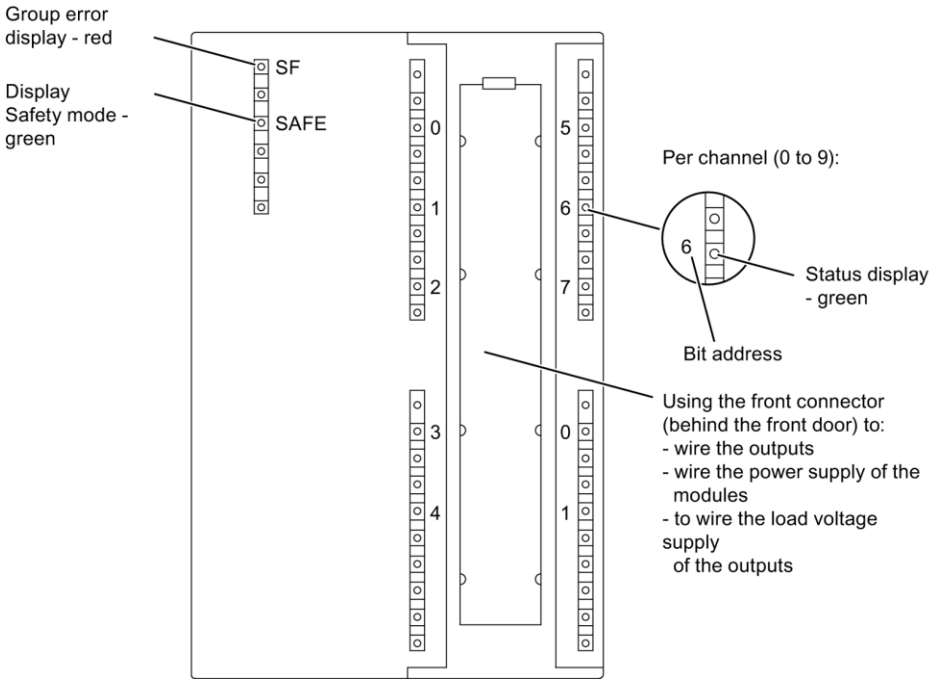
© Siemens AG 2018 All rights reserved

1.3 Properties for the fail-safe digital input module

This chapter describes how to connect discrete 24VDC input signals to the system. The S7-300 fail-safe input module described, is the SM 326 - DI 24 x DC 24V. This module has 24 channels, but can be configured for an internal 1oo2 evaluation between 2 permanently assigned channels in order to implement some of the described evaluation architectures. For simplification, this module will be referred to as F-DI in this document.

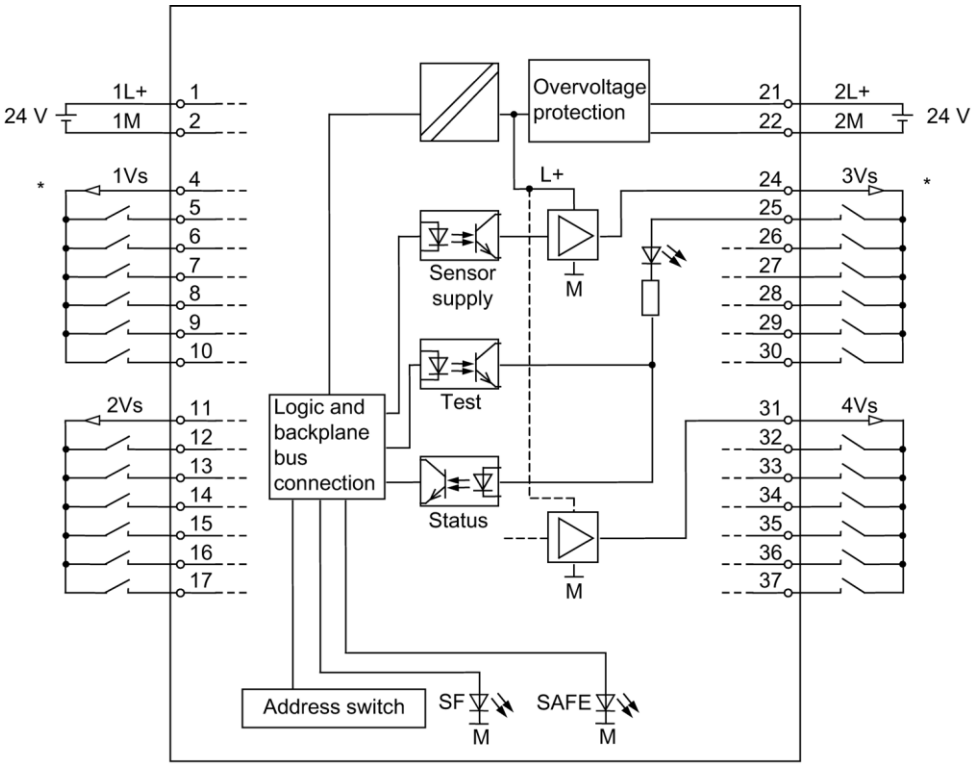
Figure 1-3 shows the front view of the F-DI, Figure 1-4 the connection and schematic diagram.

Figure 1-3 Front view



© Siemens AG 2018 All rights reserved

Figure 1-4 Connection and schematic diagram



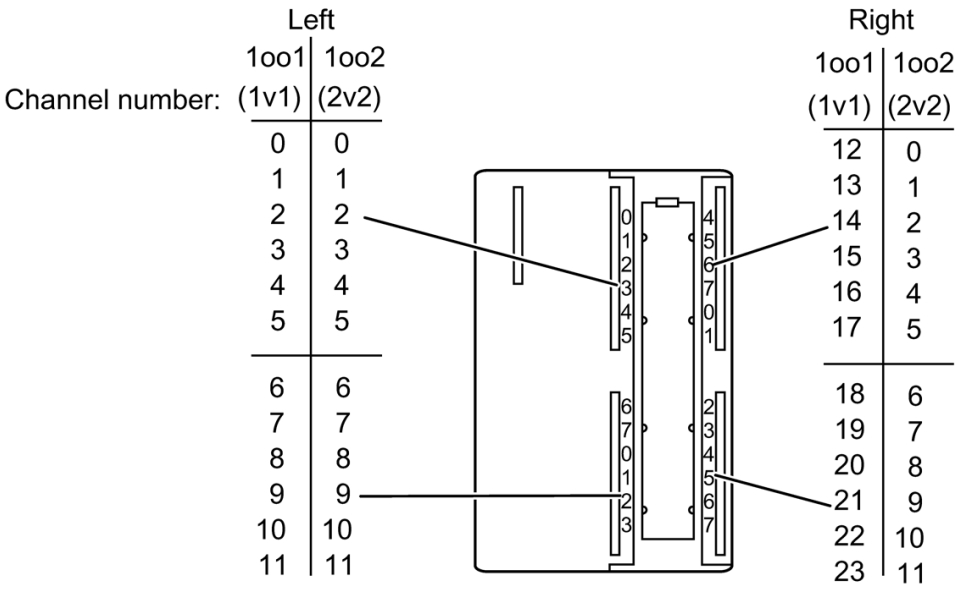
* The representation of NO contacts matches the module labeling. Usually, the sensors must be equipped with NC contacts in order to ensure the safe state of process variables.

The F-DI needs to be powered from two points. The 1L+/1M terminals (1 and 2) supply power to the channels on the left side of the module (Terminals 4 to 17). The 2L+/ 2M terminals (21 and 22) supply power to the channels on the right side of the module (Terminals 24 to 37). The field devices can be supplied via Terminals xV_s (4, 11, 24 and 31). They supply the power for their assigned group of six input channels.

The channels can be evaluated either individually (1oo1) or in pairs (i.e. Channel 0 and 12, Channel 1 and 13, or generally Channel x and Channel x+ 12) for 1oo2. The 1oo1 evaluation includes single-sensor architectures with optional 1oo2 evaluation in the CPU. In the 1oo2 evaluation, two sensors are generally required; their signal states are evaluated in the module. Figure 1-5 shows the assignment of the channel numbers for the 1oo1 and 1oo2 evaluation in the F-DI

© Siemens AG 2018 All rights reserved

Figure 1-5 Channel numbers for F-DI 24 x DC 24V



© Siemens AG 2018 All rights reserved

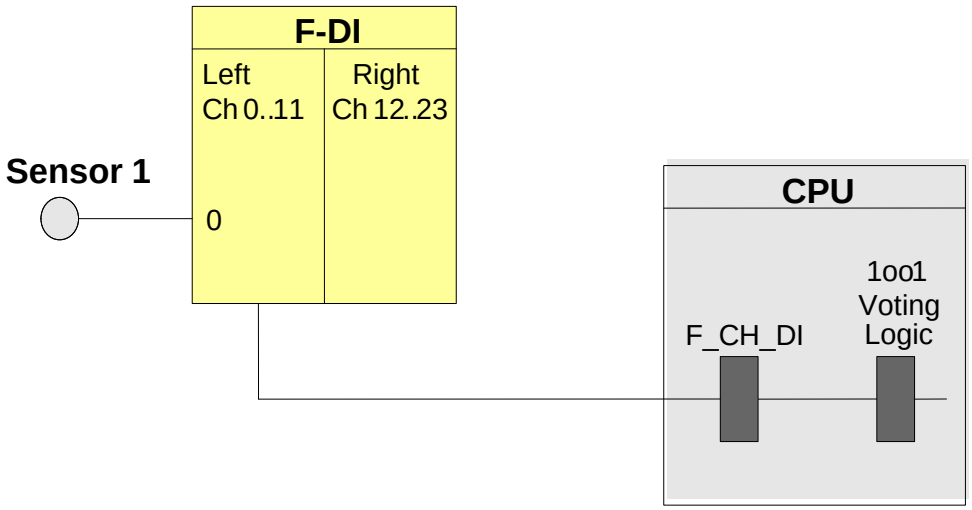
2 Hardware configuration and wiring of one sensor (1oo1) and one F-DI (1oo1)

The one-sensor evaluation scheme (or 1oo1) refers to applications that do not require increased availability. 1oo1 evaluation means that only one sensor is present. If the sensor signals a trigger condition, the safety logic is triggered.

Note The I/O assemblies in this architecture are certified for the Safety Integrity Level **SIL2**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

In the 1oo1 basic architecture, one sensor is wired to one F-DI input. Figure 2-1 shows a block diagram (with sensor wired to Channel 0).

Figure 2-1 1oo1 architecture



With a hardware configuration according to Figure 2-1, it is possible to achieve a maximum of **SIL2**.

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 2-1 Failure combinations

Failed component detected?		Triggering of the safety function possible?
Sensor 1	**F-DI**	
No	No	Yes (not required)
X	Yes	Yes
Yes	X	Yes

© Siemens AG 2018 All rights reserved

2.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + PFD_{F\text{-}DI+} PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} value for one 1oo1 sensor is calculated using this formula[1].

$$PFD_{Sensor} \approx \lambda_{DU} \cdot \frac{T_1}{2}$$

© Siemens AG 2018 All rights reserved

[1] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

2.2 Wiring

2.2.1 Conventional wiring

In the 1oo1 evaluation scheme, the F-DI can power the sensor or, alternatively, an external power source can be used.

Figure 2-2 shows an example in which the F-DI powers the connected sensor. The sensor is wired to Channel 0 (Terminal 5). Power is supplied to the F-DI at 1L+/1M (Terminals 1 and 2). The sensor is powered via $1V_s$ (Terminal 4).

Figure 2-2 1oo1 wiring internal sensor supply

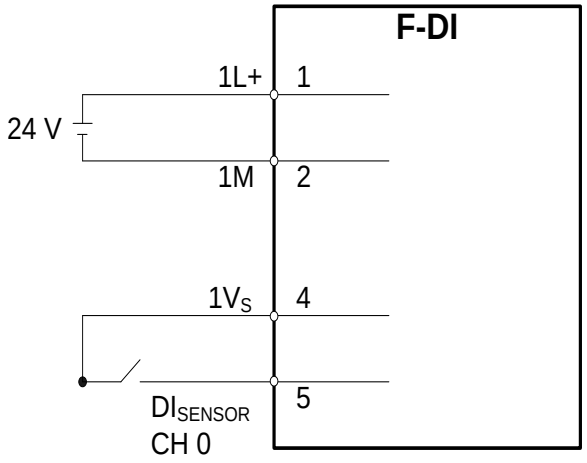
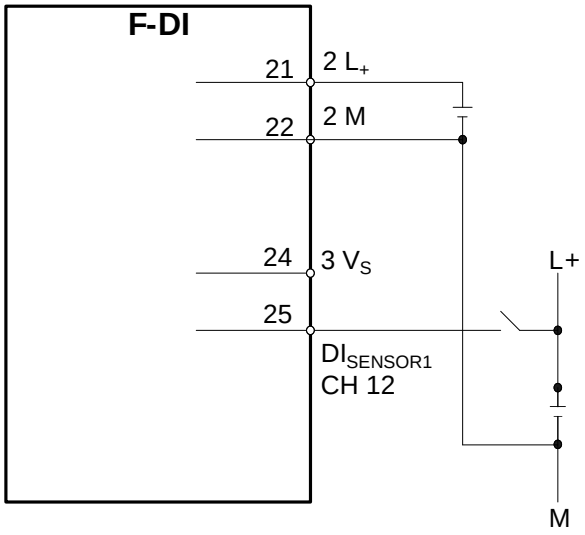


Figure 2-3 shows an example in which an external power source is used. The sensor is wired to Channel 12 (Terminal 25). The F-DI is powered by 2L+/2M (Terminals 21 and 22). The external source L+ powers the sensor.

Figure 2-3 1oo1 wiring external sensor supply



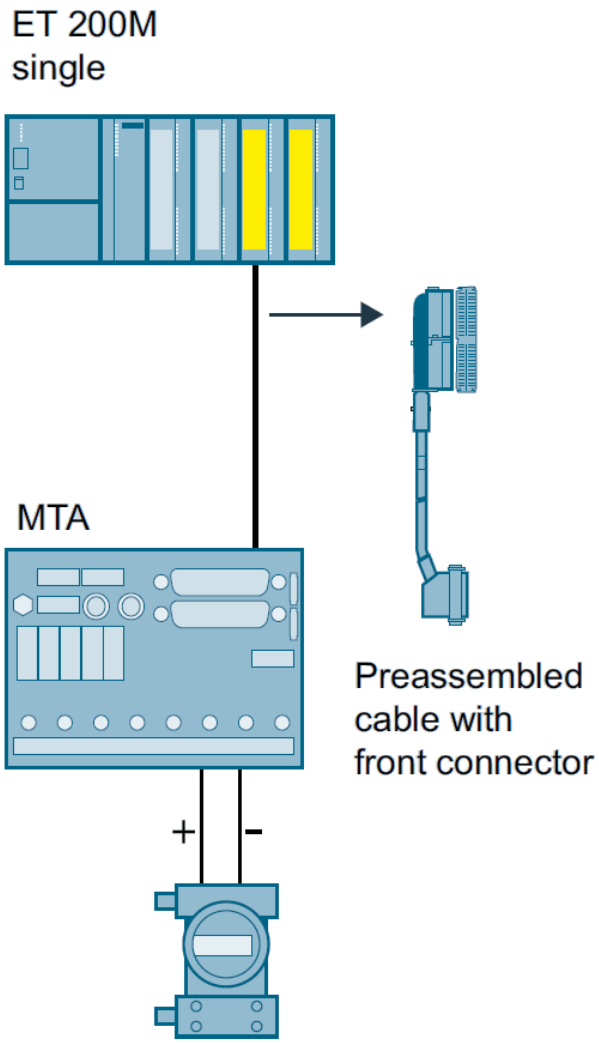
© Siemens AG 2018 All rights reserved

2.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

Figure 2-4 MTA Wiring



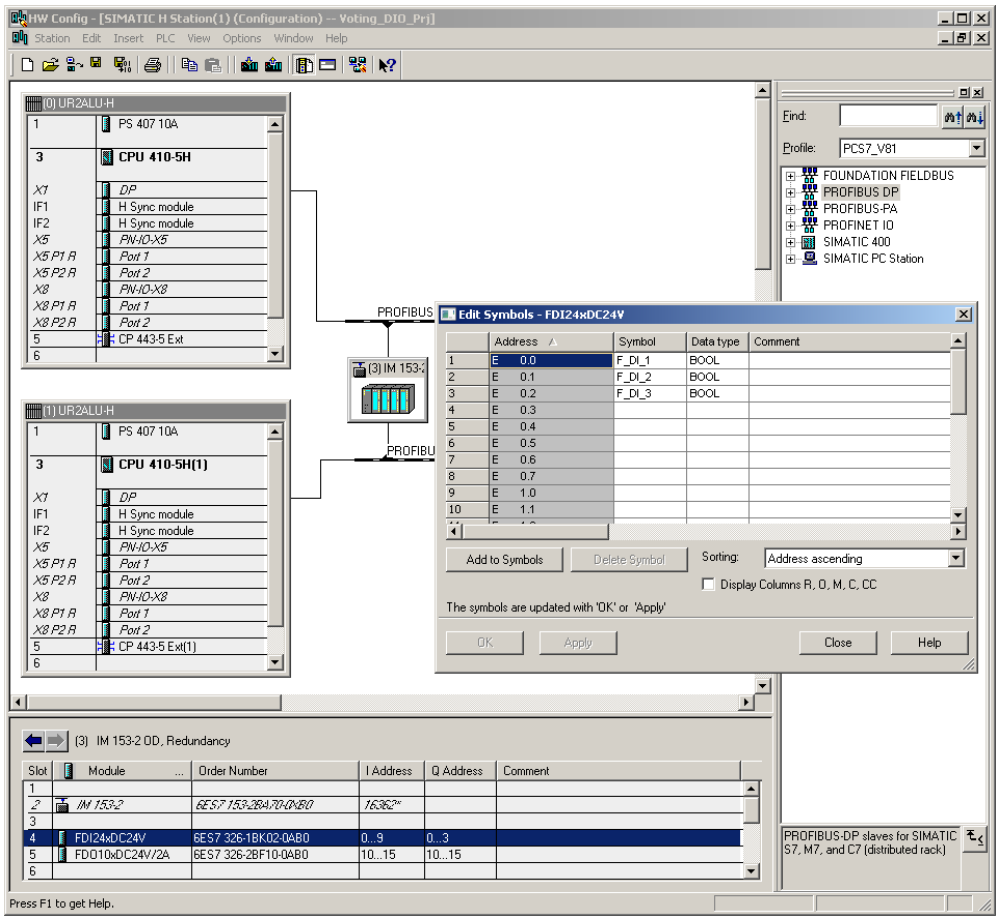
© Siemens AG 2018 All rights reserved

2.3 Hardware configuration

For configuration, select the F-DI in the hardware catalog and insert it into an existing ET 200M station. Then assign clear symbol names for the used channels of the module.

You can find an example for a hardware configuration using an F-DI in Figure 2-5. The sensor signal in this example is wired to Channel 0 of the F-DI. For further information on HW Config, see \4\.

Figure 2-5 1oo1 system processing



The required parameters for operating the F-DI are set in the object properties of the F-DI in HW Config (see Figure 2-6).

The parameters are summarized in Table 2-2.

© Siemens AG 2018 All rights reserved

Figure 2-6 1oo1 hardware parameters

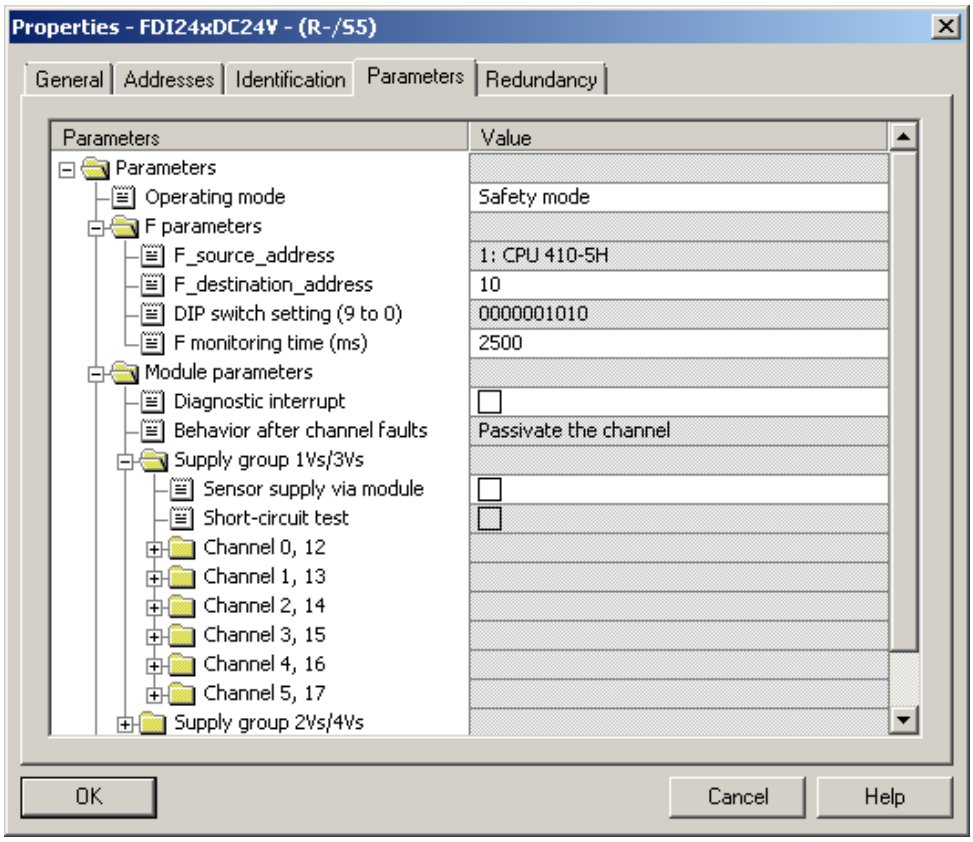


Table 2-2 1oo1 hardware configuration parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Operating mode	Display of the F-DI operating mode **Note:** In order to use the integrated safety functions available in the F-DI, this parameter must be set to **safety mode**.	Safety mode
F-parameters		
F_destination_address	The F_destination_address uniquely identifies the PROFIsafe target. It must be unique across the station. When enabling the safety mode, the address is assigned automatically and can be changed if necessary.	1 to 1022
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-DI. **Note:** Siemens Industry Online Support provides a spreadsheet that helps users to calculate F-monitoring times (see \10\).	10 to 10000

© Siemens AG 2018 All rights reserved

Module parameters		
Diagnostic interrupt	Diagnostic alarm capability for the F-DI. A diagnostic alarm is triggered by various error events that can be detected by the F-DI. These events are then signaled to the CPU. **Note:** In addition to diagnostic interrupts being enabled at the module level, individual diagnostic events must be enabled at the channel level.	Release
Module parameters for a power supply group		
Sensor supply via module	Selection whether the sensor is powered by the F-DI or not. **Note:** This option must be enabled to enable short circuit diagnostics (see below).	Release / lock
Short-circuit test	Selection whether the short circuit detection for the supply group is enabled or not. **Note:** This option can only be enabled if the sensor is supplied by the module. The short-circuit test deactivates the power supply for the sensor for short time intervals.	Release / lock
Channel/channel pair parameters		
Enabled	Selection whether the channel pair is enabled for signal processing in the safety program or not.	Release / lock
Evaluation of the sensors	Setting the evaluation scheme for the channel pair.	1oo1evaluation / 1oo2evaluation
Type of sensor interconnection	Display of the sensor indication (1 channel, 2 channels, etc.). **Note:** With "1oo1 evaluation", the sensor type is set to **1-channel**. With 2-channel sensor interconnection, the following two settings are also available.	1-channel / 2-channel equivalent / 2-channel non-equivalent
Behavior at discrepancy	With 2-channel sensor connection, the set value is forwarded to the safety program in the event of a discrepancy during the discrepancy time	Supply last valid value / Supply 0.value
Discrepancy time (ms)	The discrepancy time can be set in 10ms increments. If a discrepancy lasts longer than the set time, a discrepancy error is signaled. **Note:** "2-channel sensor interconnection" and "Provide last valid value" increase the reaction time of the system and the set discrepancy time.	10 to 30000

Note **The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.**

In this case, you will find further information in the documentation or the Help section of the module.

© Siemens AG 2018 All rights reserved

2.4 Creating the logic

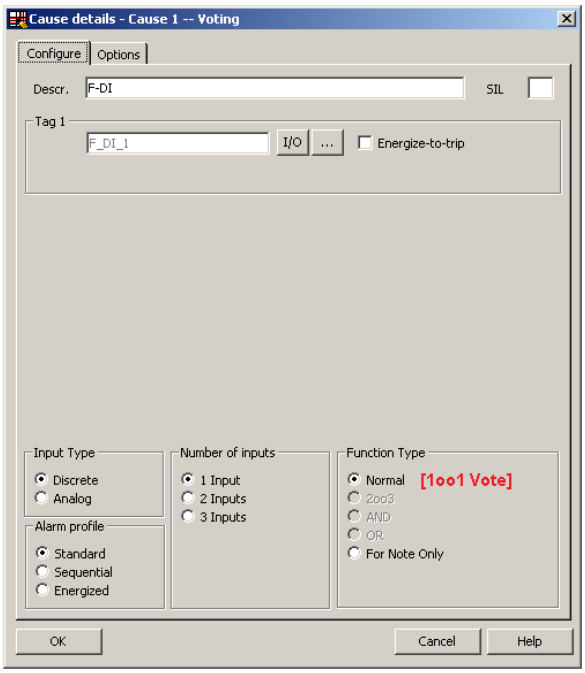
2.4.1 Configuration with Safety Matrix

After the hardware has been configured, the evaluation logic for the signal can be implemented in the CPU. One method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

Figure 2-7 illustrates how a cause for monitoring an input TAG is configured in the Safety Matrix. The following settings must be used:

- Discrete input type
- 1 input
- Function type Normal (1oo1 Evaluation)
- Select the tag by pressing the "I/O" button to select the symbolic name from the symbol table (e.g. F_DI_1).

Figure 2-7 1oo1 Safety Matrix configuration



Depending on the requirements, additional options may be used (e.g. Energize-to-trip, Time Delay, Bypass, or Inhibit).

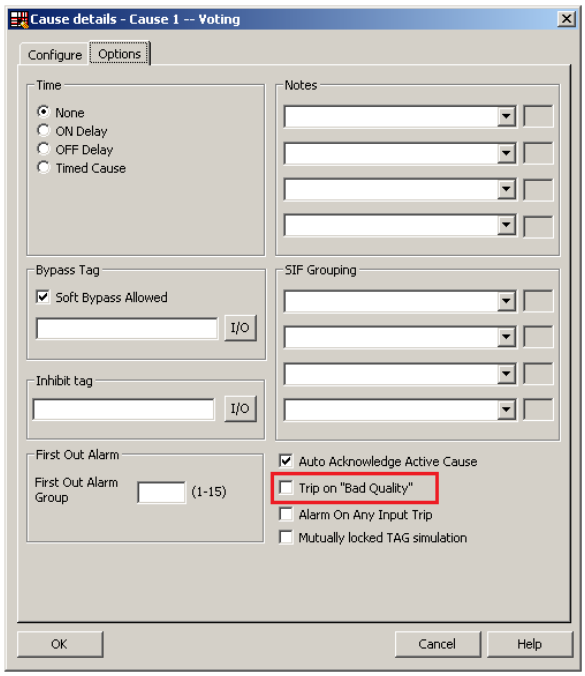
One option highlighted in Figure 2-8 is shutdown in case of a channel fault (Trip On Bad Quality). If this option is selected, a channel fault (QBAD) is considered as a bad process state.

In the case of De-energize-to-trip causes with discrete input signals, channel faults result in the enabling of the cause even if the "Trip On Bad Quality" option is deactivated.

If there is no channel fault and the sensor detects a bad process state, the cause becomes active and triggers the linked effects.

© Siemens AG 2018 All rights reserved

Figure 2-8 1oo1 Safety Matrix - Options



2.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for monitoring the input signal by means of the CFC Editor.

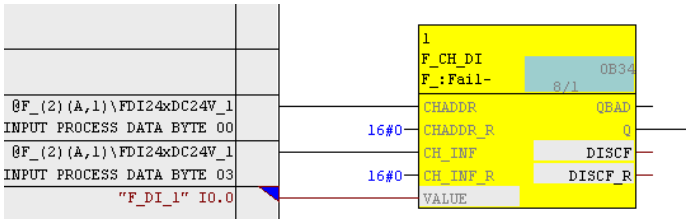
There are two ways to implement the CFC logic:

- without channel fault evaluation (direct triggering in the event of a channel fault)
- with channel fault evaluation (delayed triggering in the event of a channel fault)

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 2-9 illustrates a sample logic for reading a single input signal in CFC Editor. Note that in this example, a "0" signal at the input will result in shutdown.
(1 = good condition, 0 = shutdown).

Figure 2-9 1oo1 CFC logic - without channel fault evaluation



The logic in Figure 2-9 works as follows:

- When the input signal returns a normal value (i.e. 1), the output of the evaluation logic is 1 (i.e. no shutdown command).
- When the input signal returns a critical process condition (i.e. "0"), the shutdown logic is triggered.
- The "Q" output of the F-channel driver is connected to the shutdown logic.
- In the event of a channel fault, the F-channel driver outputs the substitute value "0" at the Q output, which corresponds to a shutdown command.

© Siemens AG 2018 All rights reserved

Logic with channel fault evaluation (delayed triggering in the event of a channel fault)

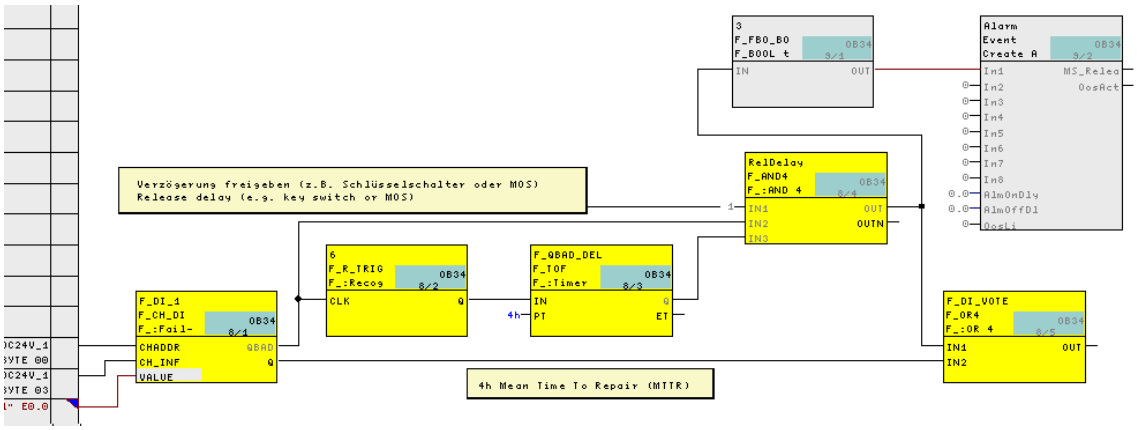
A channel fault in the F-DI always leads to the output of the substitute value "0" at the Q output of the F-channel driver. If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period.

Figure 2-10 illustrates a sample logic for reading a single input signal in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown). If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

The delay can be enabled, disabled or aborted via input IN1 of the RelDelay block.

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

Figure 2-10 1oo1 CFC logic – with channel fault evaluation (delayed triggering in the event of a channel fault)



The logic in Figure 2-10 works as follows:

- If the F-channel driver does not display a channel fault (QBAD "0"), the output of the evaluation logic (OUT output of the F_DI_VOTE block) follows the process signal (Q output of the F_DI_1 block).
- If the F-channel driver signals a channel fault, a pulse with the length of the delay time is generated from the rising edge of QBAD. If the delay is enabled, the shutdown command is delayed as long as QBAD is present and the delay time is running. After expiry of the delay time or if the channel fault or the release goes, the bridging is terminated and the output of the evaluation logic follows the process signal (Q output of the F_DI_1 block).
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.
- A bridging of the safety function when a channel fault occurs is signaled with the event block "Alarm".

© Siemens AG 2018 All rights reserved

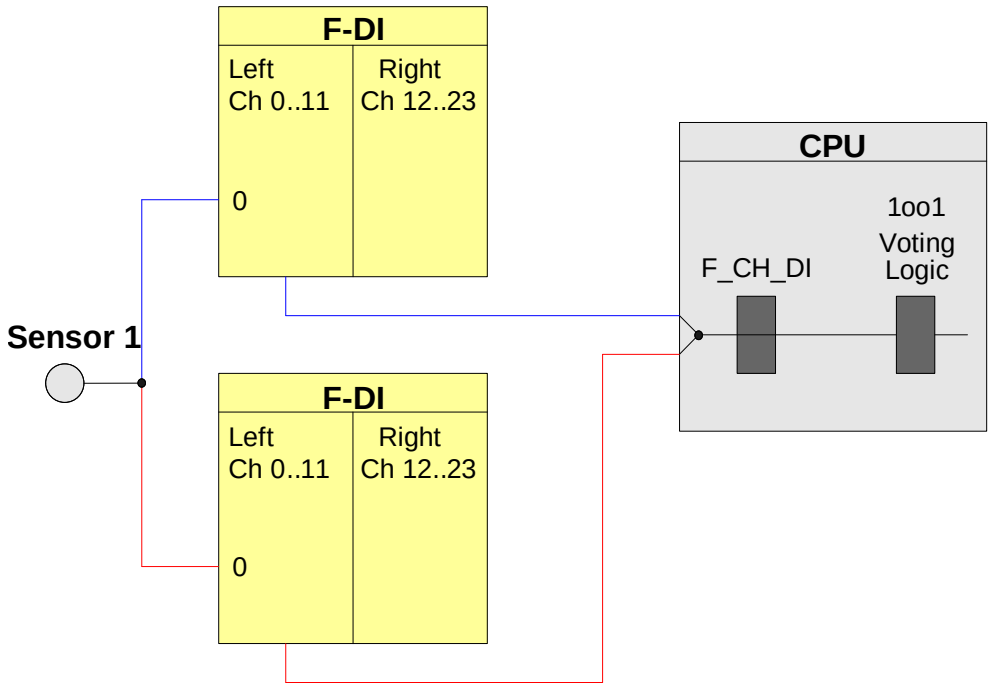
3 Hardware configuration and wiring of one sensor (1oo1) with redundant F-DI (2oo2)

This architecture increases the availability of the system by means of redundant F-DIs. In the CPU, the F_CH_DI block performs a 2oo2 evaluation of the signals from the redundant F-DIs.

Note The I/O modules are certified in this architecture for achieving Safety Integrity Level **SIL2**. However, to be SIL-compliant, the entire safety function – including the sensors – must be assessed according to IEC 61508/IEC 61511.

In this architecture, a single sensor is wired to a redundant F-DI; Figure 3-1 shows a corresponding block diagram. The sensor in this example is wired to Channel 0 of both F-DI. The modules are configured as redundant modules in HW Config. The safety program requires only one F-channel driver (F_CH_DI). The F-channel driver is connected by the compiler to the two F module drivers and selects a valid input signal.

Figure 3-1 1oo1 architecture with redundant F-DIs (2oo2)



With a hardware configuration according to Figure 3-1, it is possible to achieve a maximum of **SIL2**.

© Siemens AG 2018 All rights reserved

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 3-1 Failure combinations

Failed component detected?			Triggering of the safety function possible?
Sensor 1	**F-DI 1**	**F-DI 2**	
No	No	No	Yes (not required)
No	No	Yes	Yes (not required)
No	Yes	No	Yes (not required)
X	Yes	Yes	Yes
Yes	X	X	Yes

Note The redundancy of the F-DI does not increase the Safety Integrity Level.

3.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the fail-safe function.

© Siemens AG 2018 All rights reserved

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + 2\ PFD_{F\text{-}DI+}\ PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} value for one 1oo1 sensor is calculated using the following formula[2]:

$$PFD_{Sensor} \approx \lambda_{DU} \cdot \frac{T_1}{2}$$

[2] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

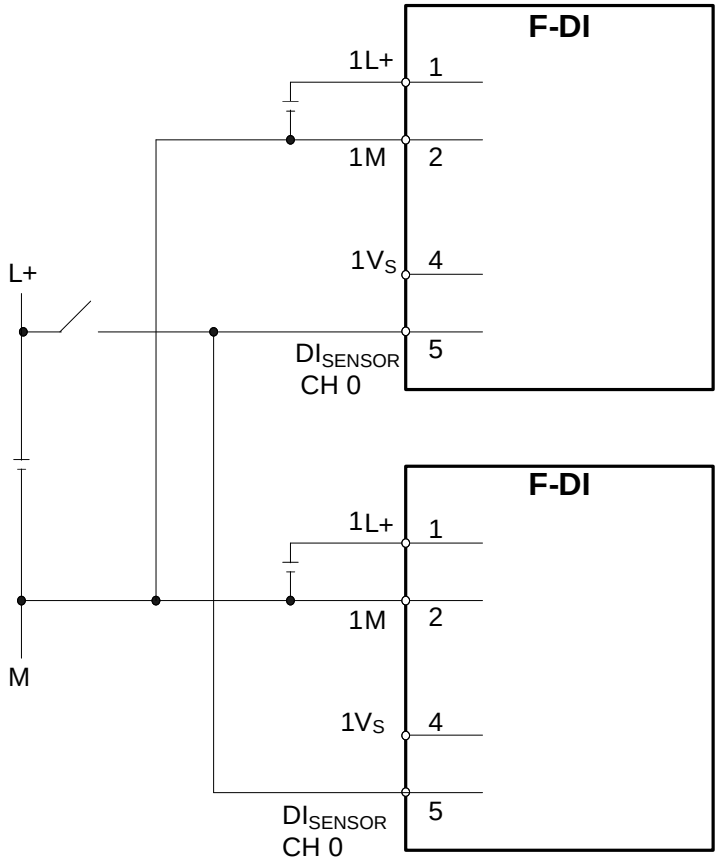
3.2 Wiring

3.2.1 Conventional wiring

In the 1oo1 evaluation scheme with redundant F-DIs, an external power source must be used.

Figure 3-2 shows a relevant example. The sensor is wired to Channel 0 (Terminal 5) of both F-DI. Both F-DI are powered at 1L+/1M (Terminals 1 and 2). The L+ voltage powers the sensor.

Figure 3-2 A sensor with an external sensor supply and redundant F-DI



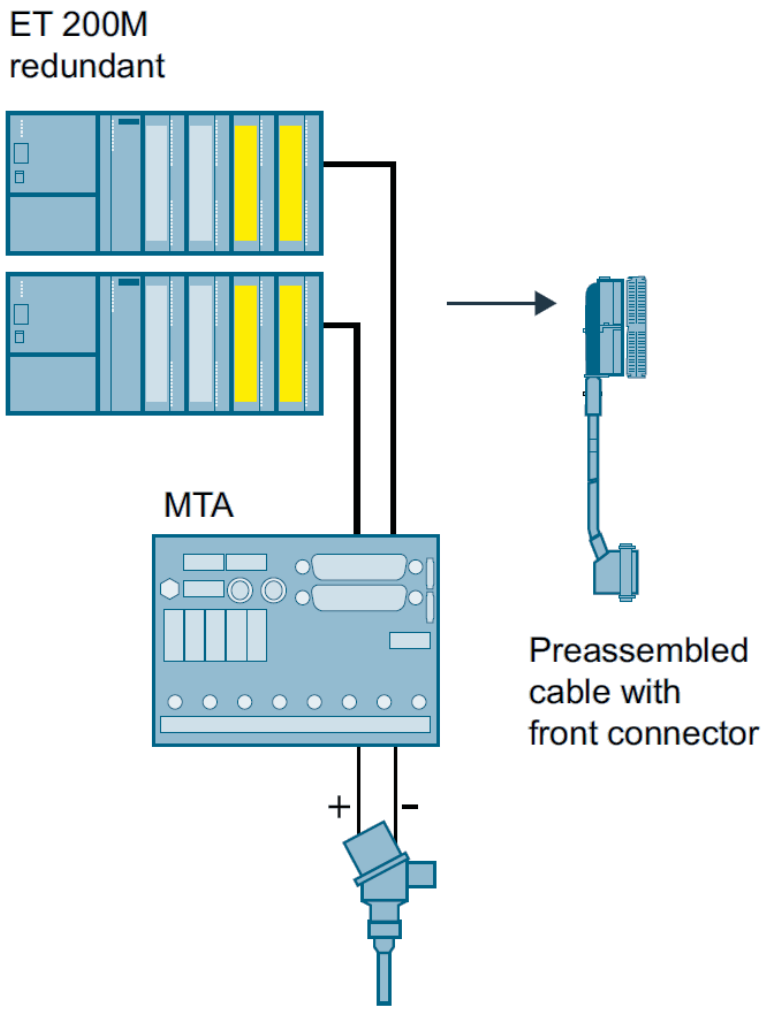
© Siemens AG 2018 All rights reserved

3.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

Figure 3-3 MTA Wiring

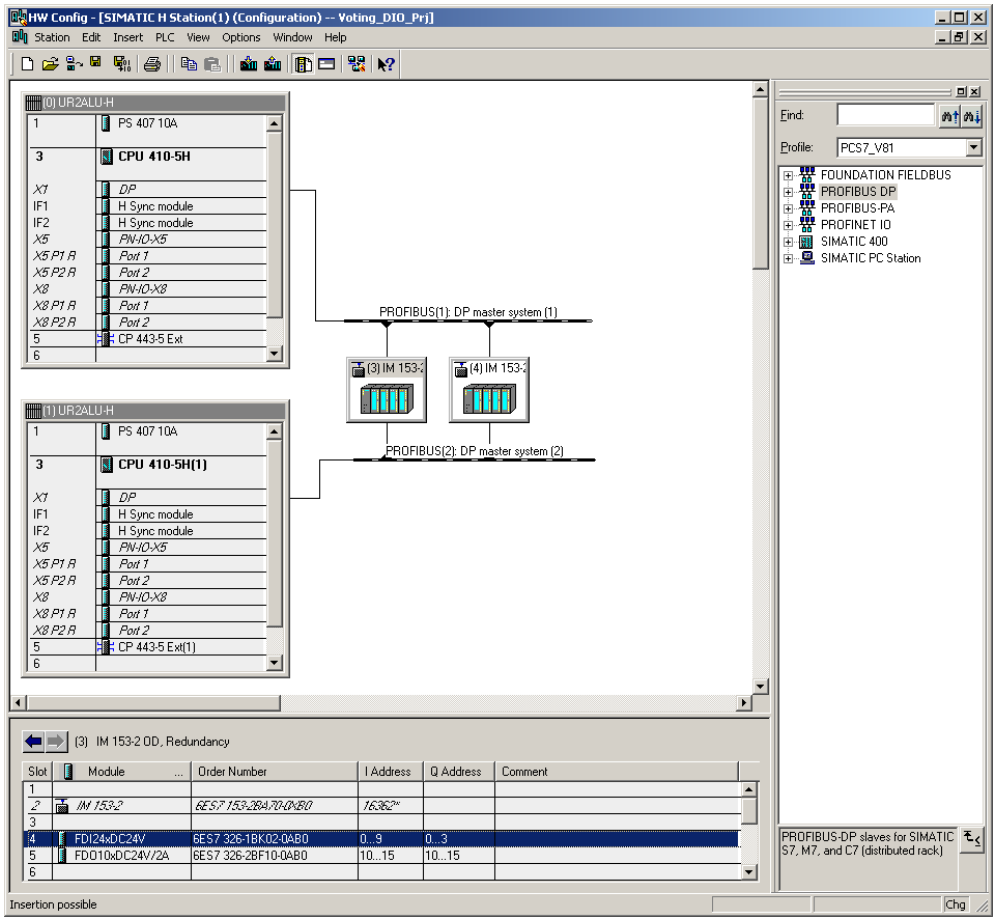


© Siemens AG 2018 All rights reserved

3.3 Hardware configuration

The 1oo1 evaluation scheme with redundant F-DI is configured in HW Config. Figure 3-4 illustrates a possible hardware configuration. In this example, there are two ET 200M racks with PROFIBUS addresses 3 and 4. Each ET 200M contains one F-DI in Slot 4. For additional information about HW Config, refer to \4\.

Figure 3-4 A sensor withe and redundant F-DI



The two F-DI must be configured as a redundant pair in HW Config. The F-DI redundancy settings can be accessed through the object properties of the F-DI. For the hardware configuration example in Figure 3-4, the redundancy settings are configured with PROFIBUS address 3 using the F-DI in the ET 200M. The redundancy settings are shown in Figure 3-5 and summarized in Figure 3-2.

© Siemens AG 2018 All rights reserved

Figure 3-5 Redundant F-DI redundancy parameters

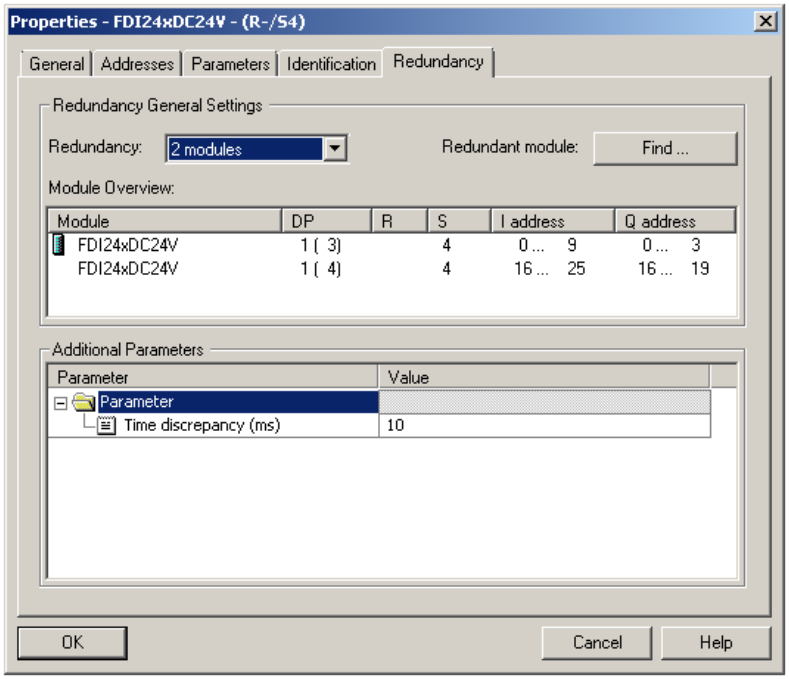


Figure 3-2 Redundant F-DI redundancy parameters

Parameters	**Description / Recommendations**	**Desired setting or permissible value range**
Redundancy	Shows whether the F-DI is acting as part of a redundant pair or not. **Note:** The parameter is set to **2 modules** for this architecture.	2 modules
Redundant module	Used to select the redundant partner module (only modules of the same type are displayed).	Select module
Discrepancy time (ms)	The maximum permitted time for which the redundant input signals may differ from one another.	10 - 30000

Note

The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

After the redundancy settings have been configured, the hardware parameters for the redundant F-DI pair can be set as described in Section 2.3. The parameters only have to be set on one of the two F-DI. They are copied onto the second F-DI by the system.

© Siemens AG 2018 All rights reserved

3.4 Creating the logic

Although this evaluation scheme requires a pair of redundant F-DI, only one F_CH_DI F-channel driver is needed in the logic. The F-channel driver can be added and configured automatically from the SIMATIC Safety Matrix or manually using the CFC Editor. In both cases, the F-channel driver must be interconnected to the symbolic name assigned to the lower input address.

The logic is compiled when the F-channel driver is configured and the logic is fully available. If the option to generate module drivers is selected during compilation, the corresponding F_PS_12 module drivers are automatically added to the logic and interconnected during the compilation. The F-channel driver selects the valid input signal and, in the event of a fault, switches to the input signal of the redundant module.

3.4.1 Configuration with Safety Matrix

After the sensor has been added to the hardware configuration, the evaluation logic for the signal can be implemented in the CPU. One method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

The actual configuration of the Safety Matrix is the same as that of a single sensor signal with an F-DI.
You can find the description in Chapter 2.4.1.

© Siemens AG 2018 All rights reserved

3.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for monitoring the input signal by means of the CFC Editor.

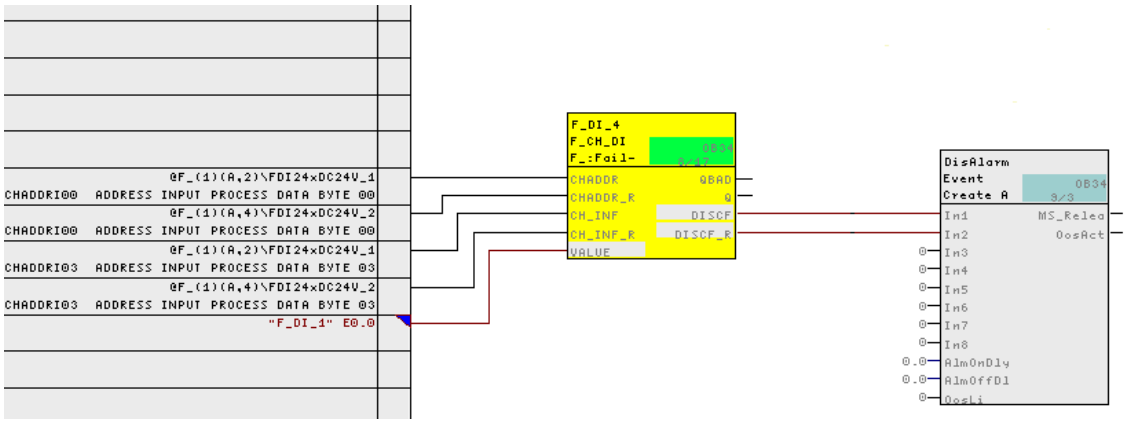
To read in an input signal from redundant F-DI, only one F-channel driver F_CH_DI, which is interconnected to the lower input address, is required. As long as one of the F-DI supplies a "1" signal and does not signal a fault, this signal is output at the F-channel driver output. A channel fault in both F-DI always leads to the output of the substitute value "0" at Q output of the F-channel driver.

If the F-channel driver of both F-DI receives different input values or if a channel fault is detected by a module, the value of the module which provides a "1" signal (good condition) is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output. Interconnect these signals to an event block to signal the error and to check the signals.

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 3-6 illustrates sample logic for reading a redundant single input signal in CFC Editor. The discrepancy error is signaled with the event block "Alarm". Note that in this example, a "0" signal at the input will result in shutdown.
(1 = good condition, 0 = shutdown).

Figure 3-6 1oo1 CFC logic - without channel fault evaluation, with a message of the discrepancy error



The example logic in Figure 3-6 works as follows:

- If both F-DI signal a normal value and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the Q output of the F_CH_DI block.
- If one F-DI signals a normal value and there is no channel fault (i.e. 0), the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If one F-DI signals a normal value, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output.
- If both F-DI signal a critical process status or a channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- The output of the logic (Q output of the F_DI_4 block) is connected to the corresponding shutdown logic.

Logic with channel fault evaluation (delayed triggering in the event of a channel fault)

When using redundant F-DI, the failure of an F_DI does not result in a channel fault. A channel fault only occurs if the sensor fails or if there is a fault in the wiring between the sensor and the redundant F_DI. A channel fault always leads to the output of the substitute value "0" at the Q output of the F-channel driver.

If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period. **Fehler! Verweisquelle konnte nicht gefunden werden.** illustrates a sample logic for reading a single input signal in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

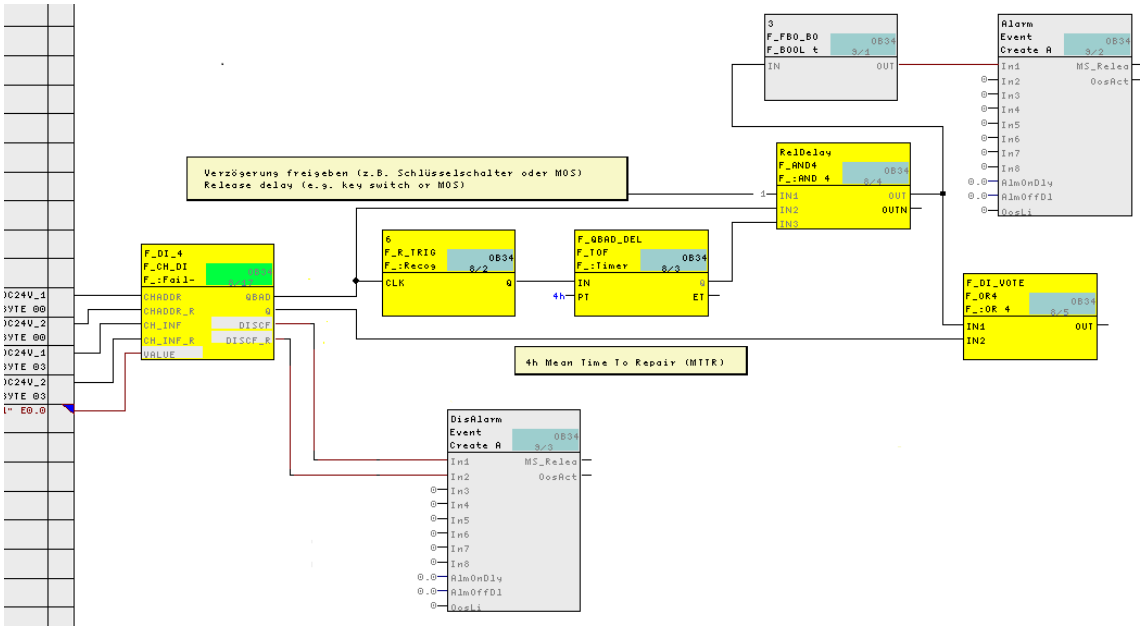
In order to be able to transfer the process to the safe state in hazardous situations, the delay can be enabled or aborted via input IN1 of the RelDelay block.

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of

© Siemens AG 2018 All rights reserved

a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

Figure 3-7 1oo1 CFC logic - with channel fault evaluation (delayed triggering in the event of a channel fault), with a message of the discrepancy error



The example logic in Figure 3-7 works as follows:

- If the input signals of both F-DI signal a normal value (i.e. 1) and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the OUT output of the F_DI_VOTE block.
- If the input signal of a module signals a critical process state (i.e. 0) and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output.
- If the input signal of a module signals a channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If the input signals of both modules signal a critical process status and no channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- If the input signals of both modules signal a channel fault, a pulse with the length of the delay time is generated from the rising edge of QBAD. If the delay is enabled, the shutdown command is delayed as long as QBAD is present and the delay time is running. After expiry of the delay time or if the channel fault or the release goes, the bridging is terminated and the output of the evaluation logic follows the input signal.
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.
- A bridging of the safety function when a channel fault occurs on both modules is signaled with the event block "Alarm".

© Siemens AG 2018 All rights reserved

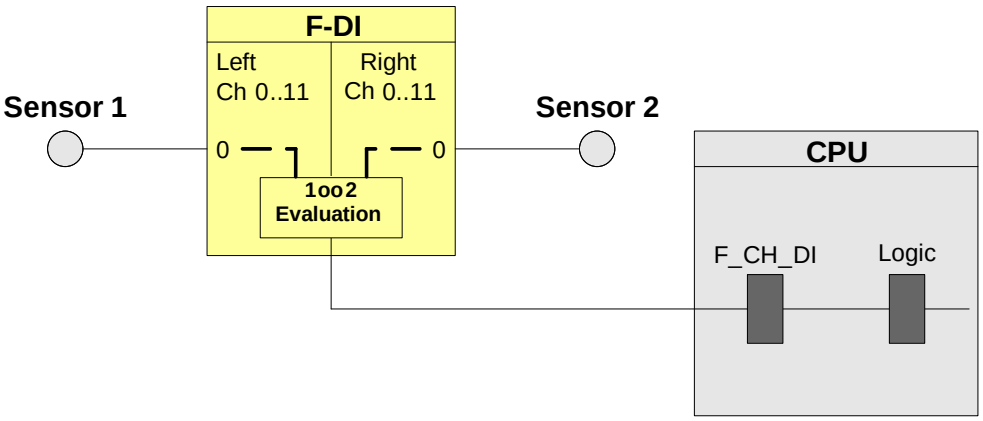
4 Hardware configuration and wiring for two sensors (1oo2) with evaluation in the F-DI

The evaluation scheme for two sensors (1oo2) refers to applications that require two sensors to achieve the required security level. In the 1oo2 evaluation, a response by one of the two sensors causes the safety logic to be triggered. In this example, the 1oo2 evaluation is performed in the F-DI.

Note The I/O assemblies in this architecture are certified for the Safety Integrity Level **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

The 1oo2 architecture with evaluation in the F-DI is shown in Figure 4-1. In the block diagram, the first sensor is wired to Channel 0 on the left side of the F-DI and the second sensor is wired to Channel 0 (12) on the right side. The F-DI is then configured for the 1oo2 evaluation.

Figure 4-1 1oo2 evaluation in the F-DI symbol processing



With a hardware configuration according to Figure 4-1, it is possible to achieve a maximum of **SIL3**.

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 4-1 Failure combinations

Failed component detected?			Triggering of the safety function possible?
Sensor 1	**Sensor 2**	**F-DI**	
No	No	No	Yes (not required)
X	X	Yes	Yes
X	Yes	X	Yes
Yes	X	X	Yes

© Siemens AG 2018 All rights reserved

4.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + PFD_{F\text{-}DI+} PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} value for one 1oo2 sensor is calculated using the following formula[3]:

$$PFD_{Sensor} \approx \frac{{\lambda_{DU}}^2 \cdot {T_1}^2}{3} + \beta \cdot \lambda_{DU} \cdot \frac{T_1}{2}$$

© Siemens AG 2018 All rights reserved

[3] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

4.2 Wiring

4.2.1 Conventional wiring

In a 1oo2 evaluation in the F-DI, the power for supplying the sensors can be provided by the F-DI or an external source.

Figure 4-2 shows an example in which the F-DI powers the two connected sensors. The first sensor is wired to Channel 0 on the left side (Terminal 5) and the second sensor is wired to Channel 0 (12) on the right side (Terminal 25). Power is supplied to the F-DI at 1L+/1M (Terminals 1 and 2) and 2L+/2M (Terminals 21 and 22). The sensors are powered via $1V_S$ (Terminal 4) and $3V_S$ (Terminal 24).

Figure 4-2 1oo2 evaluation in the F-DI - wiring - internal sensor supply

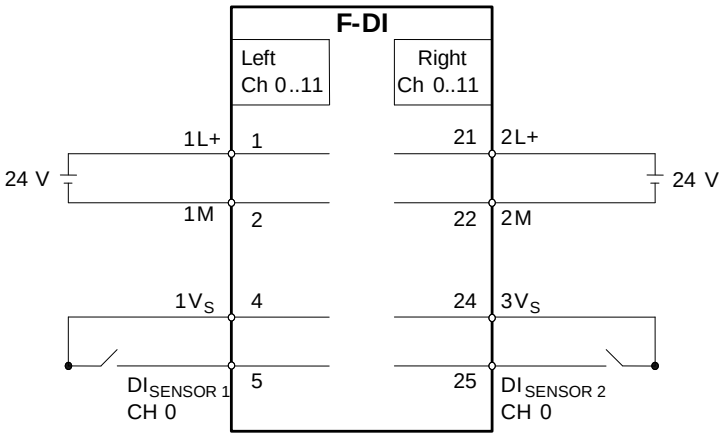
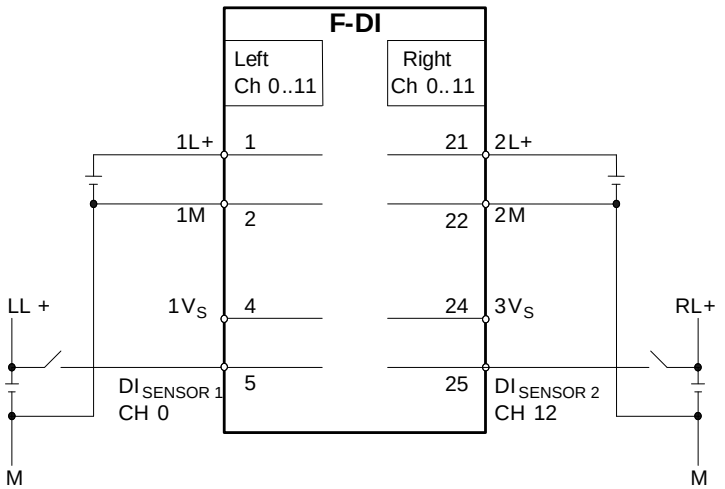


Figure 4-3 shows an example in which an external power source is used. As in Figure 4-2, the first sensor is wired to Channel 0 on the left side (Terminal 5) and the second sensor is wired to Channel 0 (12) on the right side (Terminal 25). Power is supplied to the F-DI at 1L+/1M (Terminals 1 and 2) and 2L+/2M (Terminals 21 and 22). The sensors are powered by the two power sources LL+ and RL+.

Figure 4-3 1oo2 evaluation in the F-DI - wiring - external sensor supply



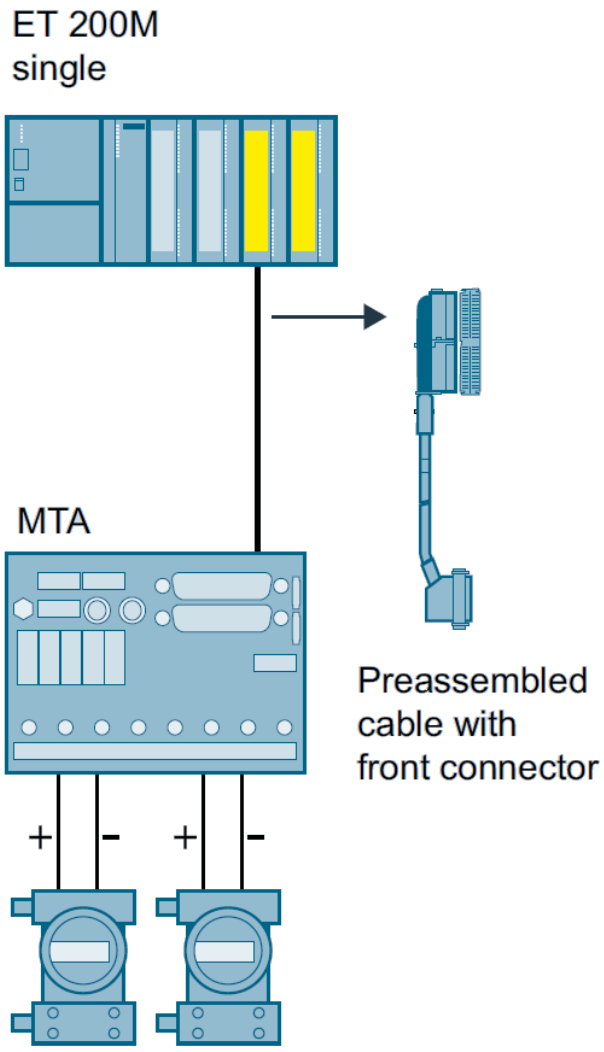
© Siemens AG 2018 All rights reserved

4.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

Figure 4-4 MTA Wiring



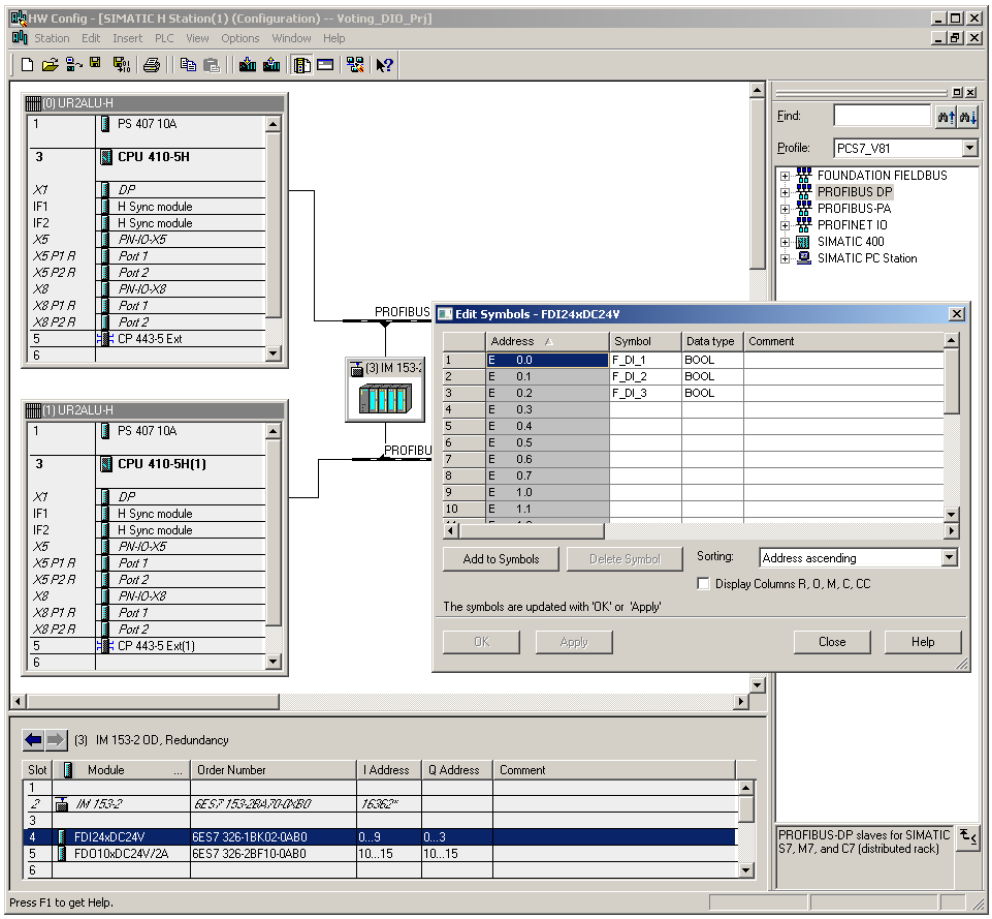
© Siemens AG 2018 All rights reserved

4.3 Hardware configuration

To configure, select the F-DI in the hardware catalog and add it into an existing ET 200M station. Then assign clear symbol names for the used channels of the module. Note that the F-DI itself carries out the 1oo2 signal selection, only one input signal is provided to the CPU logic.

Figure 4-5 illustrates a hardware configuration with one F-DI. In this example, both sensors are wired to Channel 0 on the left and right side of the F-DI. The signal is accessed via the symbol for the lower address (I0.0) of the module.

Figure 4-5 1oo2 evaluation in the F-DI - symbol processing



The parameters for operating the F-DI are set in the object properties of the F-DI in HW Config (see Figure 4-6).

The parameters are summarized in Table 4-2.

© Siemens AG 2018 All rights reserved

Figure 4-6 1oo2 evaluation in the F-DI - hardware parameters

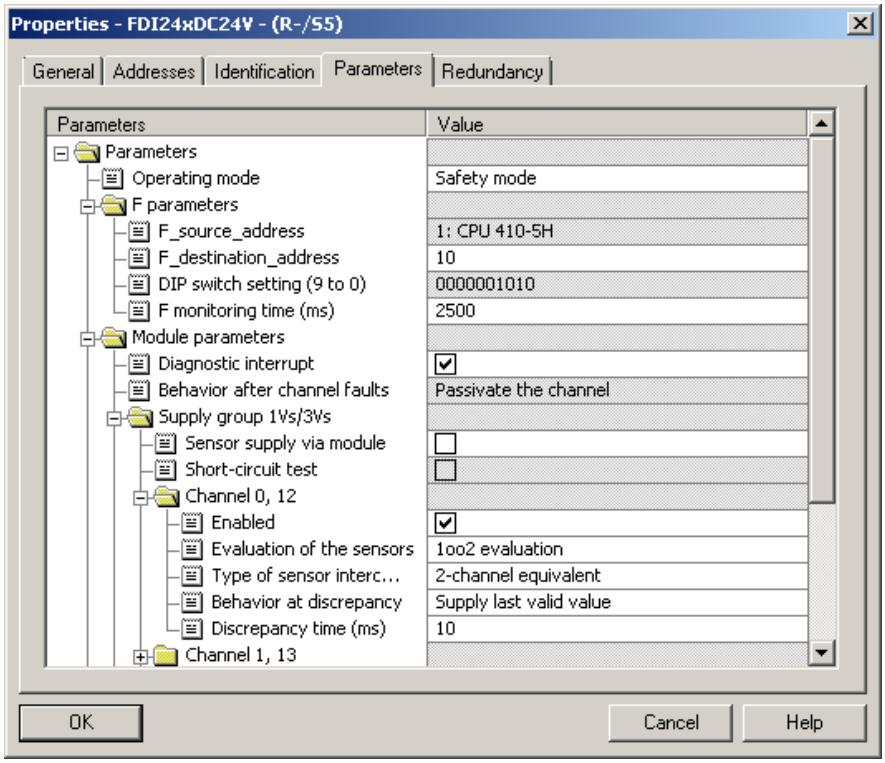


Table 4-2 1oo2 evaluation in the F-DI - hardware configuration parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Operating mode	Display of the F-DI operating mode **Note:** In order to use the integrated safety functions available in the F-DI, this parameter must always be set to **safety mode**.	Safety mode
F-parameters		
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-DI. **Note:** Siemens Industry Online Support provides a spreadsheet that helps users to calculate F-monitoring times (see \10\).	10 to 10000
Module parameters		
Diagnostic interrupt	Diagnostic alarm capability for the F-DI. A diagnostic alarm is triggered by various error events that can be detected by the F-DI. These events are then signaled to the CPU. **Note:** In addition to diagnostic interrupts being enabled at the module level, individual diagnostic events must be enabled at the channel level.	Release

© Siemens AG 2018 All rights reserved

Parameters	Description / Recommendations	Desired setting or permissible value range
Module parameters for a power supply group		
Sensor supply via module	Selection whether the sensor is powered by the F-DI or not. **Note:** This option must be enabled to enable short circuit diagnostics (see below).	Release / lock
Short-circuit test	Select whether the short circuit detection for the F-DI is enabled or not. **Note:** This option can only be enabled if the sensor is supplied by the module. The short-circuit test deactivates the power supply for the sensor for short time intervals.	Release / lock
Parameters for single channels or channel pairs		
Enabled	Selection whether the channel/channel pair is enabled for signal processing in the safety program or not.	Release / lock
Evaluation of the sensors	Setting the evaluation process. **Note:** For an F-DI with 1oo2 evaluation on the module itself (not in the CPU), this parameter is set to **1oo2**. • The 1oo2 evaluation is performed in the F-DI. • In the CPU logic, the sensor signal selected by the F-DI is read in with an F_CH_DI and used in the safety logic.	1oo2
Type of sensor interconnection	Selection of sensor interconnection (1 channel, 2 channels, etc.).	2-channel equivalent
Behavior at discrepancy	Selection of the value provided to the CPU Safety program after a discrepancy has been detected. **Note:** • If **Provide last valid value** was selected, the last value before the discrepancy started is provided to the safety program until either the discrepancy ends or the discrepancy time expires (and then an error is signaled). • If **Provide 0 value** is selected, the value 0 is provided to the safety program and the discrepancy time is ignored.	Supply last valid value/ Supply 0-value
Discrepancy time (ms)	Selection of the discrepancy time for each pair of F-DI channels. When two equivalent sensors monitor the same process variable, the sensors often react with a slight delay. If a discrepancy between two sensor values is detected, no error is signaled until the discrepancy time has expired.	10 to 30000

© Siemens AG 2018 All rights reserved

Note **The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.**

In this case, you will find further information in the documentation or the Help section of the module.

© Siemens AG 2018 All rights reserved

4.4 Creating the logic

4.4.1 Configuration with Safety Matrix

After the 1oo2 evaluation is performed in the F-DI, only the result is available to the CPU logic. The CPU logic therefore corresponds to the 1oo1 evaluation. One logic implementation method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

In this case, the actual configuration of the Safety Matrix is the same as that of a single sensor signal with an F-DI.
You can find the description in Chapter 2.4.1.

4.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for evaluating the input signal by means of the CFC Editor. After the 1oo2 evaluation has already been executed on the F-DI, the logic in the CPU corresponds to a 1oo1 evaluation.

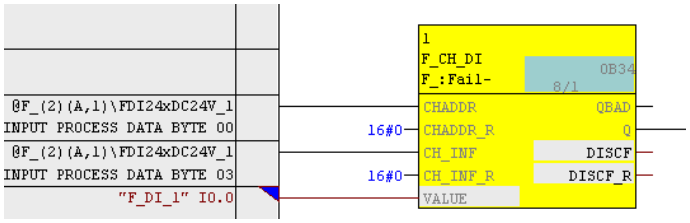
There are two ways to implement the CFC logic:

- without channel fault evaluation (direct triggering in the event of a channel fault)
- with channel fault evaluation (delayed triggering in the event of a channel fault)

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 4-7 illustrates a sample logic for reading a single input signal in CFC Editor which does not take a channel fault into account. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

Figure 4-7 1oo2 evaluation in the F-DI - CFC logic - without channel fault evaluation



The example logic in Figure 4-7 works as follows:

- When the input signal returns a normal value (i.e. 1), the output of the evaluation logic is 1 (i.e. no shutdown command).
- When the input signal returns a critical process condition (i.e. "0"), the shutdown logic is triggered.
- The "Q" output of the F-channel driver is connected to the shutdown logic.
- In the event of a channel fault, the F-channel driver outputs the substitute value "0" at the Q output, which corresponds to a shutdown command.

© Siemens AG 2018 All rights reserved

Logic with channel fault evaluation (delayed triggering in the event of a channel fault)

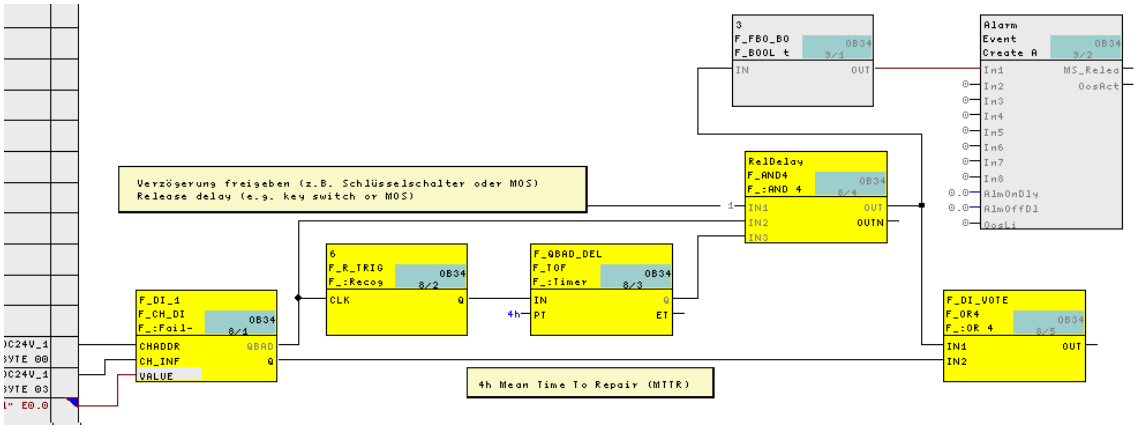
A channel fault in the F-DI always leads to the output of the substitute value "0" at the Q output of the F-channel driver. If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period.

Figure 4-8 illustrates a sample logic for reading a single input signal in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown). If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

The delay can be enabled, disabled or aborted via input IN1 of the RelDelay block.

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

Figure 4-8 1oo2 evaluation in the F-DI - CFC logic - with channel fault evaluation (delayed triggering in the event of a channel fault)



The example logic in Figure 4-8 works as follows:

- If the F-channel driver does not display a channel fault (QBAD "0"), the output of the evaluation logic (OUT output of the F_DI_VOTE block) follows the process signal (Q output of the F_DI_1 block).
- If the F-channel driver signals a channel fault, a pulse with the length of the delay time is generated from the rising edge of QBAD. If the delay is enabled, the shutdown command is delayed as long as QBAD is present and the delay time is running. After expiry of the delay time or if the channel fault or the release goes, the bridging is terminated and the output of the evaluation logic follows the process signal (Q output of the F_DI_1 block).
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.
- A bridging of the safety function when a channel fault occurs is signaled with the event block "Alarm".

© Siemens AG 2018 All rights reserved

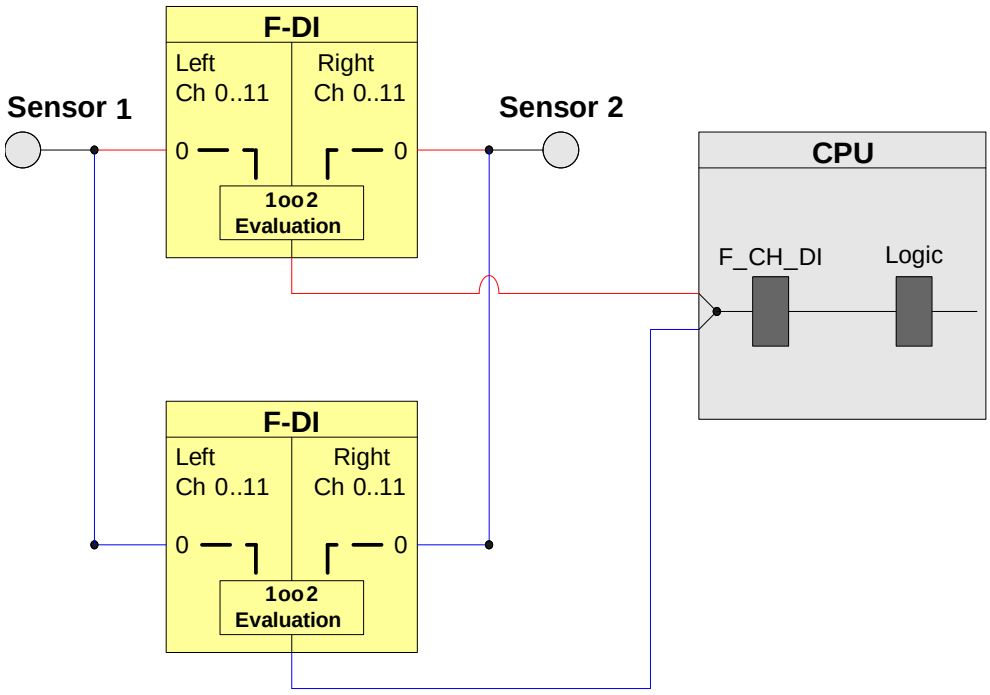
5 Hardware configuration and wiring of two sensors (1oo2) with redundant F-DI (2oo2) and evaluation in the F-DI

This architecture increases the availability of the system by means of redundant F-DI. In the CPU, the F_CH_DI block performs the 2oo2 evaluation of the signals from the redundant F-DI.

Note The I/O modules are certified in this architecture for achieving Safety Integrity Level **SIL3**. However, to be SIL-compliant, the entire safety function – including the sensors – must be assessed according to IEC 61508/IEC 61511.

In this architecture, 2 sensors are wired to a pair of redundant F-DI. Figure 5-1 shows a corresponding block diagram. In this example, the first sensor is wired to Channel 0 on the left side of both F-DI and the second sensor is wired to Channel 0 (12) on the right side.
The F-DI are configured as a redundant pair in HW Config. Each F-DI performs a 1oo2 evaluation of the two sensor signals. The safety program requires only one F-channel driver (F_CH_DI). The F-channel driver connects to the two fail-safe module drivers and selects a valid input signal.

Figure 5-1 1oo2 architecture with redundant F-DI (2oo2)



The hardware configuration according to Figure 5-1 is suitable for achieving **SIL3**.

© Siemens AG 2018 All rights reserved

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 5-1 Failure combinations

Failed component detected?				Triggering of the safety function possible?
Sensor 1	**Sensor 2**	**F-DI 1**	**F-DI 2**	
No	No	No	X	Yes (not required)
No	No	X	No	Yes (not required)
X	Yes	X	X	Yes
Yes	X	X	X	Yes
X	X	Yes	Yes	Yes

Note The redundancy of the F-DI does not increase the Safety Integrity Level.

5.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + 2\ PFD_{F\text{-}DI+}\ PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} value for one 1oo2 sensor is calculated using the following formula[4]:

$$PFD_{Sensor} \approx \frac{{\lambda_{DU}}^2 \cdot {T_1}^2}{3} + \beta \cdot \lambda_{DU} \cdot \frac{T_1}{2}$$

[4] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

© Siemens AG 2018 All rights reserved

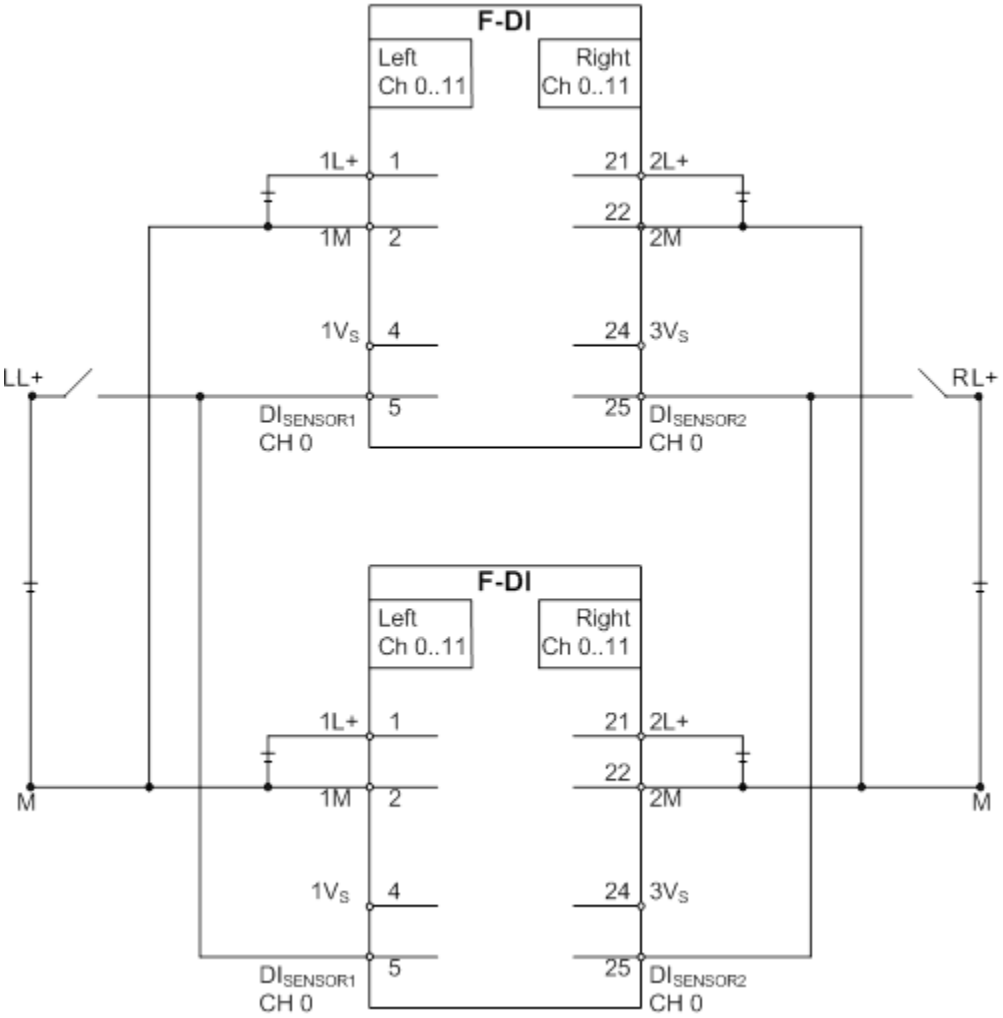
5.2 Wiring

5.2.1 Conventional wiring

In the 1oo2 evaluation scheme with redundant F-DI and evaluation of the sensors in the F-DI, an external power source must be used.

Figure 5-2 shows a relevant example. In both F-DI, the first sensor is wired to Channel 0 on the left side (Terminal 5) and the second sensor is wired to Channel 0 (12) on the right side (Terminal 25). Both F-DI are powered at 1L+/1M (Terminals 1 and 2) and 2L+/2M (Terminals 21 and 22). The power sources LL+ and RL+ supply the sensors.

Figure 5-2 1oo2 evaluation in the F-DI with redundant F-DI (2oo2) external power supply



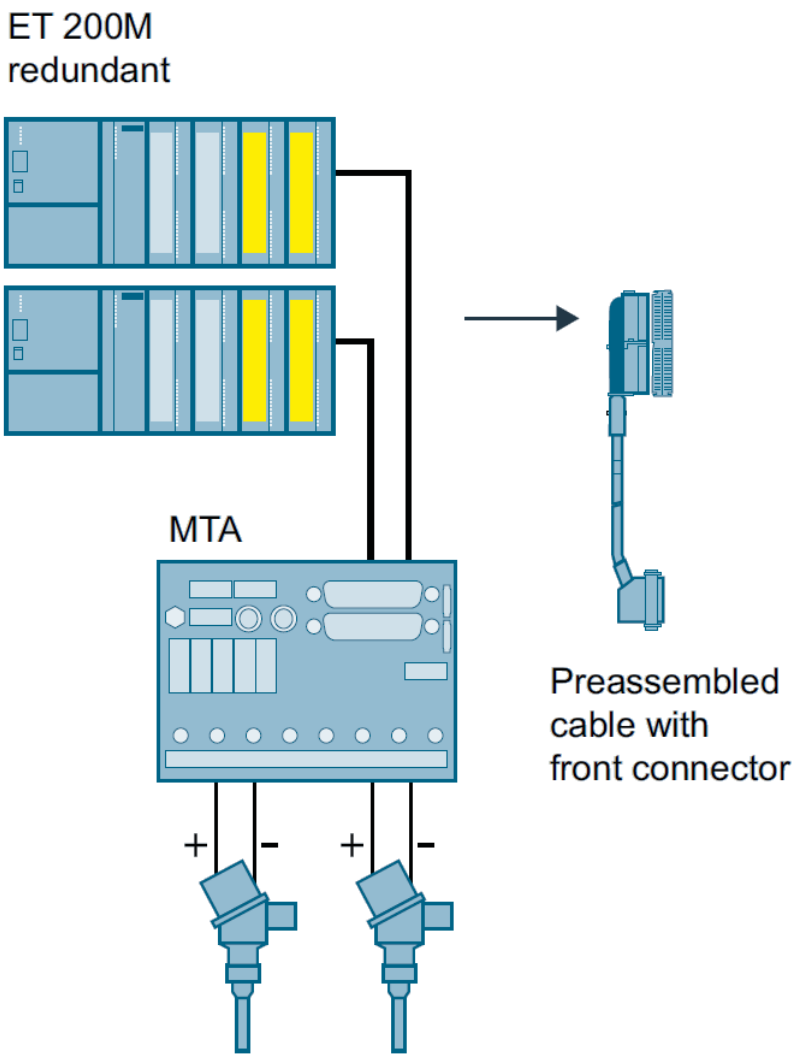
© Siemens AG 2018 All rights reserved

5.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

Figure 5-3 MTA Wiring



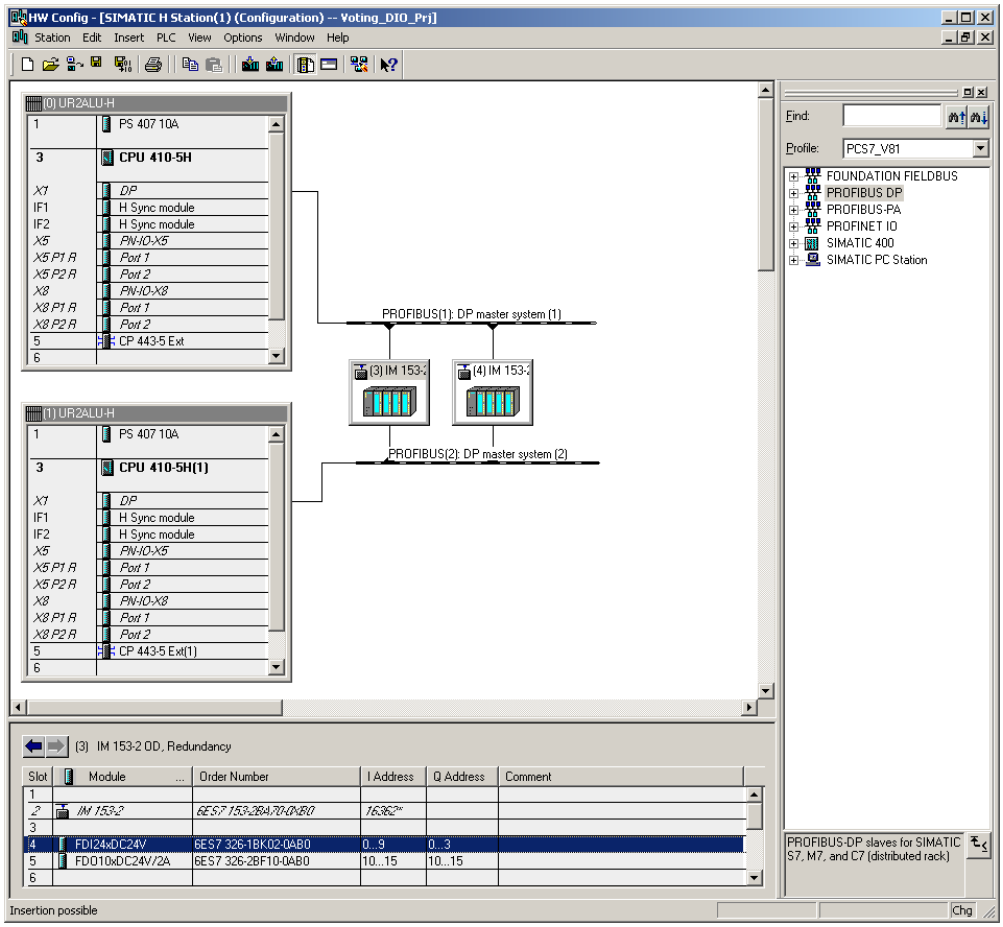
© Siemens AG 2018 All rights reserved

5.3 Hardware configuration

The 1oo2 evaluation scheme with evaluation in the F-DI and in the redundant F-DI is configured in HW Config.

Figure 5-4 shows a hardware configuration. In this example, there are two ET 200M racks with PROFIBUS addresses 3 and 4. Each ET 200M contains one F-DI in Slot 4.
For further information on HW Config, see \4\.

Figure 5-4 1oo2 evaluation in the F-DI with redundant F-DI - configuration



The two F-DI must be configured as a redundant pair in HW Config. The F-DI redundancy settings can be accessed through the object properties of the F-DI. For the hardware configuration example in Figure 5-5, the redundancy settings are configured with PROFIBUS address 3 using the F-DI in the ET 200M. The redundancy settings are shown in Figure 5-5 and summarized in Table 5-2.

© Siemens AG 2018 All rights reserved

Figure 5-5 1oo2 evaluation in the F-DI with redundant F-DI - redundancy parameters

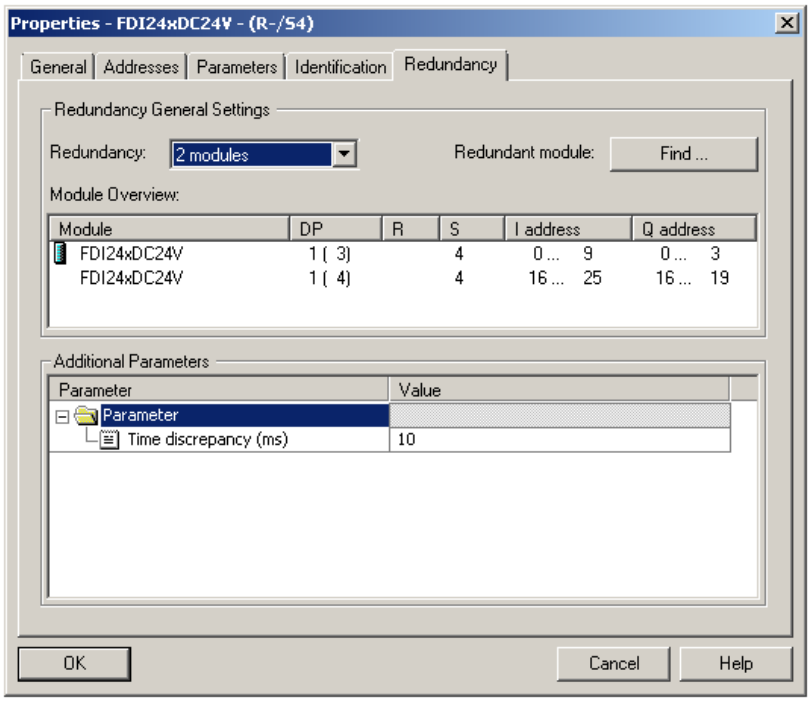


Table 5-2 1oo2 evaluation in the F-DI with redundant F-DI - redundancy parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-DI is acting as part of a redundant pair or not. **Note:** The parameter is set to **2 modules** for this architecture.	2 modules
Redundant module	Used to select the redundant partner module (only modules of the same type are displayed).	Select module
Discrepancy time (ms)	The maximum permitted time for which the redundant input signals may differ from one another.	10 - 30000

Note

The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

After the redundancy settings have been configured, the remaining hardware parameters for the redundant F-DI pair can be set as described in Section 4.3. The parameters only have to be set on one of the two modules. They are copied onto the second module by the system.

© Siemens AG 2018 All rights reserved

5.4 Creating the logic

Although this evaluation scheme requires a pair of redundant F-DI, only one F_CH_DI F-channel driver is needed in the logic. The F-channel driver can be added and configured automatically from the SIMATIC Safety Matrix or manually using the CFC Editor. The F-channel driver must be interconnected to the symbolic name assigned to the lower input address.

The logic is compiled when the F-channel driver is configured and the logic is fully available. If the option to generate module drivers is selected during compilation, the corresponding F_PS_12 module drivers are automatically added to the logic and interconnected during the compilation. The F-channel driver selects the valid input signal and, in the event of a fault, switches to the input signal of the redundant F-DI.

5.4.1 Configuration with Safety Matrix

After the 1oo2 evaluation is performed in the F-DI, only the result is available to the CPU logic. The CPU logic therefore corresponds to the 1oo1 evaluation. One method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

The actual evaluation logic for the 1oo2 evaluation of the sensor signals with redundant F-DI is the same as described in Section 2.4.1.

© Siemens AG 2018 All rights reserved

5.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for monitoring the input signal by means of the CFC Editor. After the 1oo2 evaluation has already been executed on the F-DI and the F_CH_DI F-channel driver selects between the redundant F-DI, the logic in the CPU corresponds to a 1oo1 evaluation as described in Chapter 3.4.2.

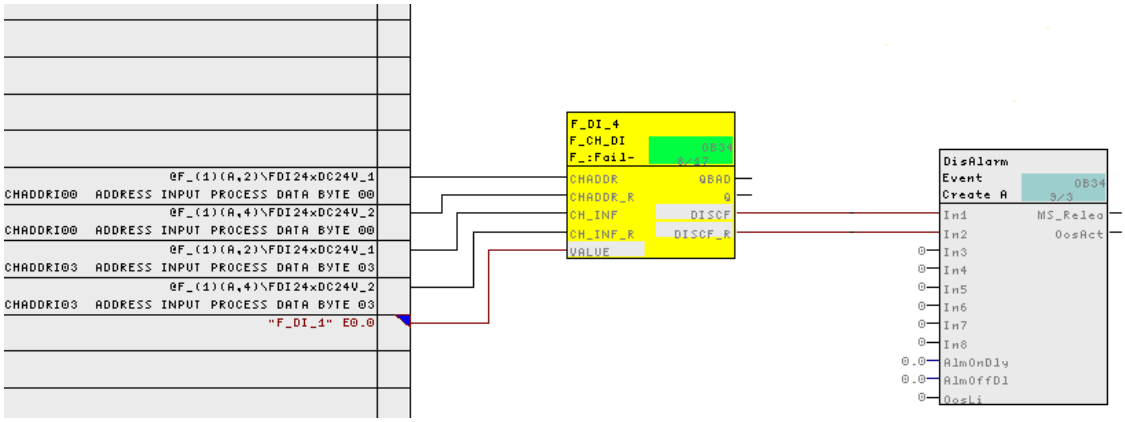
There are two ways to implement the CFC logic:

- without channel fault evaluation (direct triggering in the event of a channel fault)
- with channel fault evaluation (delayed triggering in the event of a channel fault)

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 5-6 illustrates a sample logic for reading a single input signal in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

Figure 5-6 1oo2 selection in the F-DIs with redundant F-DI – CFC logic – without channel fault evaluation



The example logic in Figure 5-6 works as follows:

- If both F-DI signal a normal value and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the Q output of the F_CH_DI block.
- If one F-DI signals a normal value and there is no channel fault (i.e. 0), the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If one F-DI signals a normal value, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output.
- If both F-DI signal a critical process status or a channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- The output of the logic (Q output of the F_DI_4 block) is connected to the corresponding shutdown logic.

Logic with channel fault and discrepancy fault evaluation (delayed triggering in the event of a channel fault)

When using redundant F-DI, the failure of an F-DI does not result in a channel fault. A channel fault only occurs if the sensor fails or if there is a fault in the wiring between the sensor and the redundant F-DI. A channel fault always leads to the output of the substitute value "0" at the Q output of the F-channel driver.

If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period. Figure 5-7 illustrates a sample logic for reading a single input signal in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

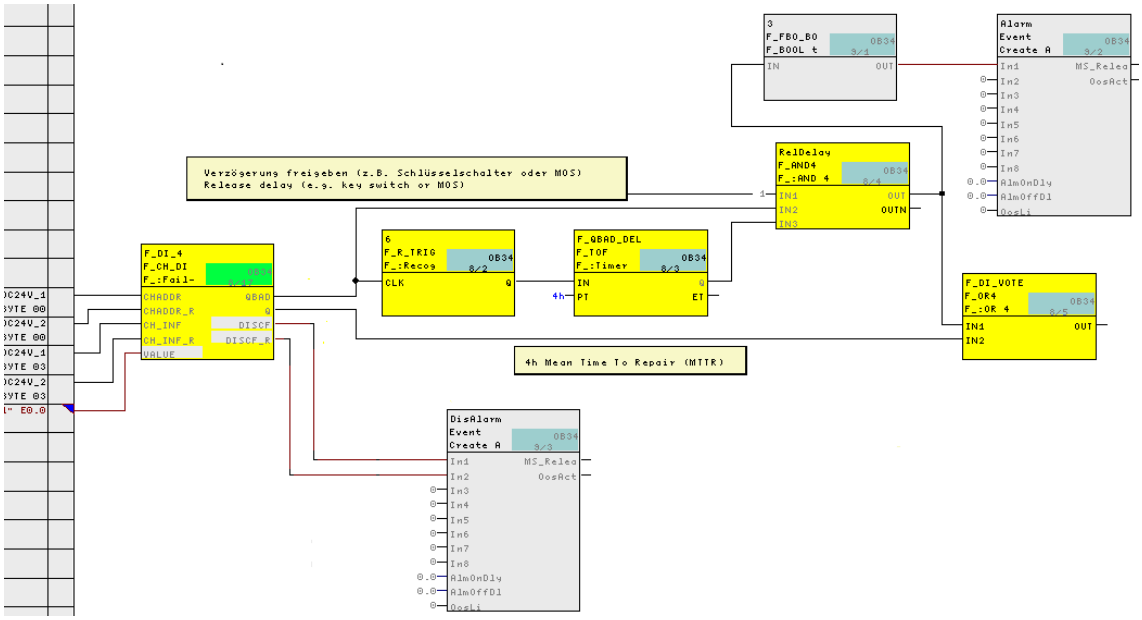
If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

In order to be able to transfer the process to the safe state in hazardous situations, the delay can be enabled or aborted via input IN1 of the RelDelay block.

© Siemens AG 2018 All rights reserved

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

Figure 5-7 1oo2 with redundant F-DI - CFC logic - with channel fault evaluation (delayed triggering in the event of a channel fault)



The example logic in Figure 5-7 works as follows:

- If the input signals of both F-DI signal a normal value (i.e. 1) and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the OUT output of the F_DI_VOTE block.
- If the input signal of a module signals a critical process state (i.e. 0) and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output.
- If the input signal of a module signals a channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command) since the value of the module which delivers a "1" signal is output. At the same time, a discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If the input signals of both modules signal a critical process status and no channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- If the input signals of both modules signal a channel fault, a pulse with the length of the delay time is generated from the rising edge of QBAD. If the delay is enabled, the shutdown command is delayed as long as QBAD is present and the delay time is running. After expiry of the delay time or if the channel fault or the release goes, the bridging is terminated and the output of the evaluation logic follows the input signal.
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.
- A bridging of the safety function when a channel fault occurs on both modules is signaled with the event block "Alarm".

© Siemens AG 2018 All rights reserved

6 Hardware configuration and wiring of two sensors (1oo2) with evaluation in the user program

The 1oo2 evaluation scheme refers to applications that require two sensors to achieve the required security level. In the 1oo2 evaluation, a response by one of the two sensors causes the safety logic to be triggered. In this example, the 1oo2 evaluation is performed in the CPU. Both input signals are visible in the CPU, which facilitates diagnostics in the event of a fault and enables further evaluations of the signals (e.g. 1oo2D, 2oo2 or temporary operation with one sensor).

Note This architecture can achieve the Safety Integrity Level **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

There are two basic configuration variants for this architecture:

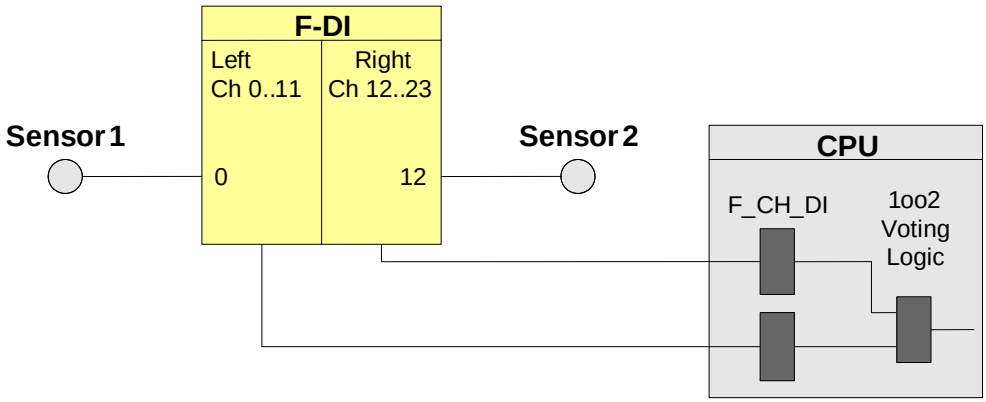
- **Configuration with an F-DI:** The two sensors are wired to opposite channels of the same F-DI, in this case to Channel 0 on the left side and Channel 0 (12) on the right side of the F-DI, as shown in Figure 6-1.
- **Configuration with two F-DI** The two sensors are wired to two F-DI, in this case, to Channel 0 of both F-DI, as shown in Figure 6-2.

© Siemens AG 2018 All rights reserved

6.1 Configuration with a F-DI:

The two sensors are wired to opposite channels of the same F-DI, in this case to Channel 0 on the left side and Channel 0 (12) on the right side of the F-DI, as shown in Figure 6-1.

Figure 6-1 1oo2 evaluation in the CPU architecture



The hardware configuration according to Figure 6-1 is suitable for achieving **SIL3**.

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 6-1 Failure combinations

Failed component detected?			Triggering of the safety function possible?
Sensor 1	Sensor 2	F-DI	
No	No	No	Yes (not required)
X	Yes	X	Yes
Yes	X	X	Yes
X	X	Yes	Yes

6.1.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + PFD_{F\text{-}DI+} PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} for one 1oo2 sensor is calculated using the following[5] formula:

$$PFD_{Sensor} \approx \frac{{\lambda_{DU}}^2 \cdot {T_1}^2}{3} + \beta \cdot \lambda_{DU} \cdot \frac{T_1}{2}$$

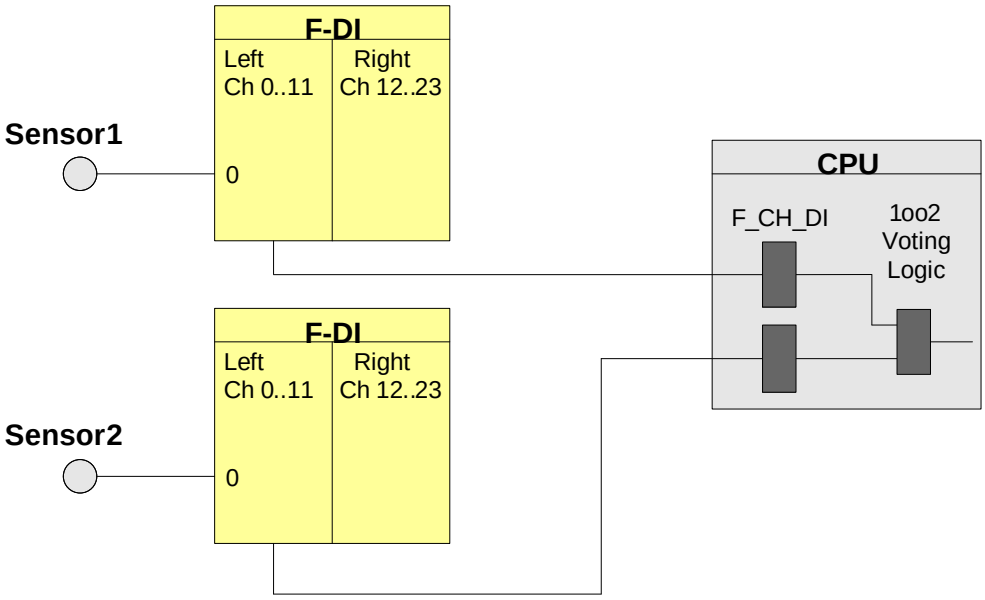
[5] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

© Siemens AG 2018 All rights reserved

6.2 Configuration with two F-DI

The two sensors are wired to two F-DI, in this case, to Channel 0 of both F-DI, as shown in Figure 6-2.

Figure 6-2 1oo2 evaluation in the CPU architecture



The hardware configuration according to Figure 6-2 is suitable for achieving **SIL3**.

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 6-2: Failure combinations

Failed component detected?				Triggering of the safety function possible?
Sensor 1	**Sensor 2**	**F-DI 1**	**F-DI 2**	
No	No	No	No	Yes (not required)
X	X	X	Yes	Yes
X	X	Yes	X	Yes
X	Yes	X	X	Yes
Yes	X	X	X	Yes

© Siemens AG 2018 All rights reserved

6.2.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = (PFD_{Sensor} + PFD_{F\text{-}DI})_{1oo2} + PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The *PFD* for this 1oo2 architecture is calculated using the following[6] formula:

$$PFD_{Sensor,F-DI} = PFD_{Sensor} + PFD_{F-DI}$$

$$(PFD_{Sensor} + PFD_{F-DI})_{1oo2} \approx \left(\frac{4}{3} \cdot PFD_{Sensor,F-DI}{}^{2}\right) + (\beta \cdot PFD_{Sensor,F-DI})$$

$$PFD_{Sensor} \approx \lambda_{DU} \cdot \frac{T_1}{2}$$

© Siemens AG 2018 All rights reserved

6.3 Wiring

6.3.1 Conventional wiring

In this 1oo2 evaluation scheme, the sensors can be powered by the F-DI or an external power source.

Figure 6-3 shows an example in which the F-DI powers the two connected sensors. The first sensor in the diagram is wired to Channel 0 (Terminal 5) and the second sensor is wired to Channel 12 (Terminal 25). Power is supplied to the F-DI at 1L+/1M (Terminals 1 and 2) and 2L+/2M (Terminals 21 and 22). The sensors are powered via $1V_s$ (Terminal 4) and $3V_s$ (Terminal 24).

Figure 6-3 1oo2 evaluation in the CPU - wiring - internal sensor supply

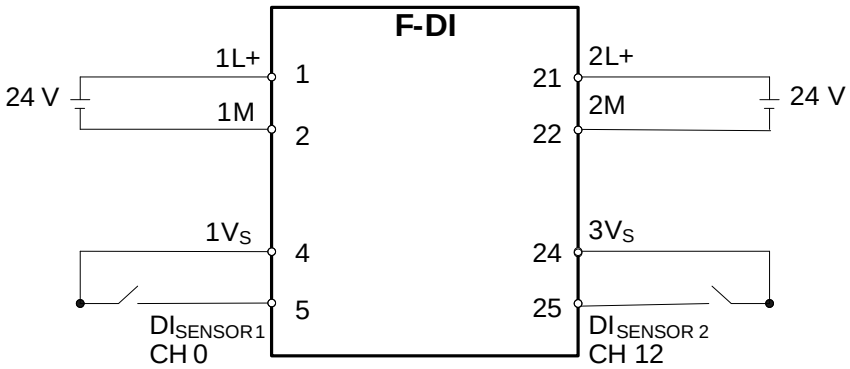
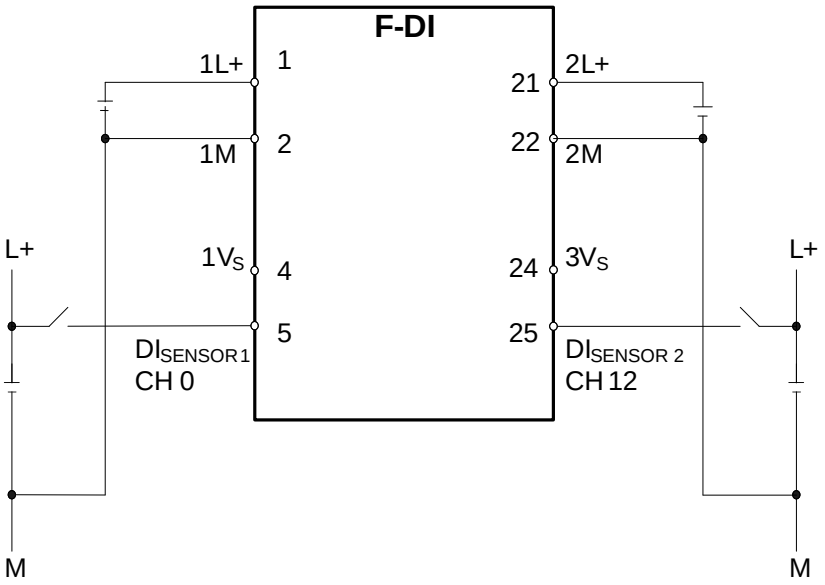


Figure 6-4 shows an example in which an external power source (L+) is used to power the sensors.

[6] The formula was taken from sheet 4 of IEC 61508, IEC 61511 and VDI 2180.

Figure 6-4 1oo2 evaluation in the CPU - wiring - external sensor supply



6.3.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

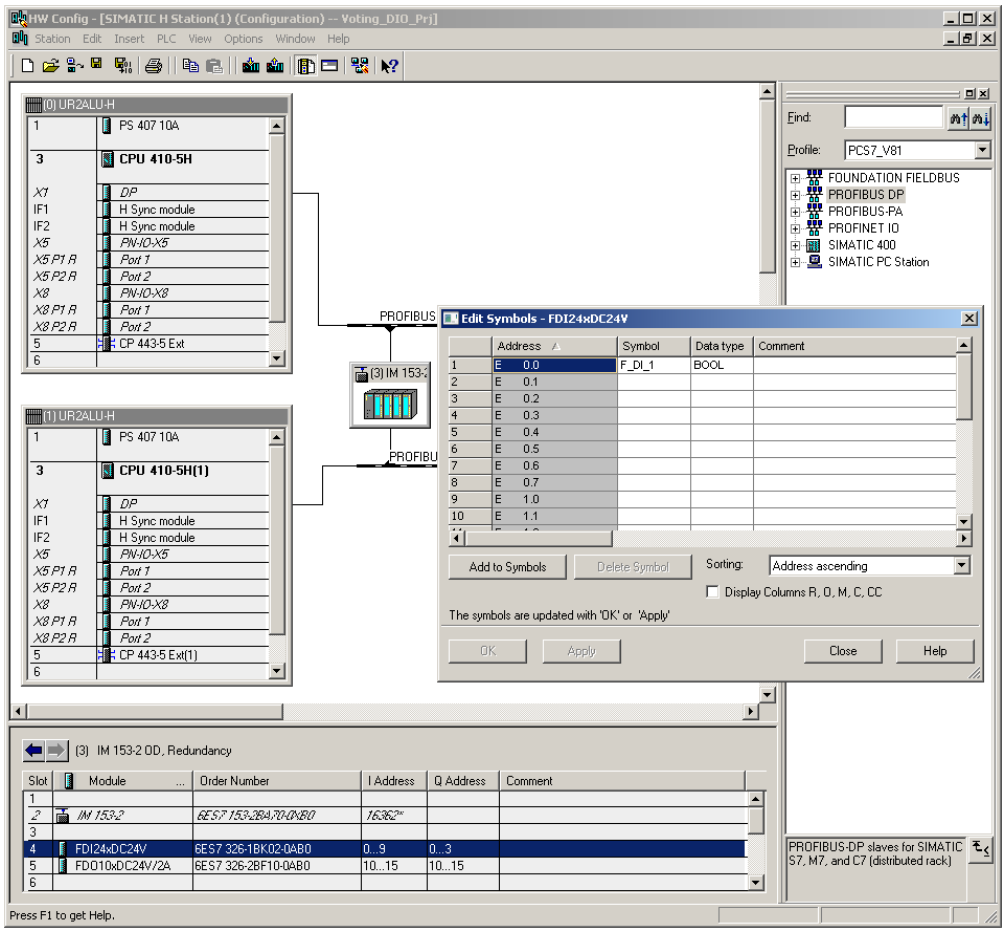
© Siemens AG 2018 All rights reserved

6.4 Hardware configuration

To configure, select the F-DI in the hardware catalog and add it into an existing ET 200M station. Then assign clear symbol names for the used channels of the module.

Figure 6-5 illustrates a hardware configuration with one F-DI. In this example, the two input signals are wired to Channels 0 and 12 of the F-DI. For additional information about HW Config, refer to \6\.

Figure 6-5 1oo2 evaluation in the CPU - symbol processing



The parameters for operating the F-DI are set in the object properties of the module in HW Config (see Figure 6-6).

The parameters are summarized in Table 6-3.

© Siemens AG 2018 All rights reserved

Figure 6-6 1oo2 evaluation in the CPU - hardware parameters

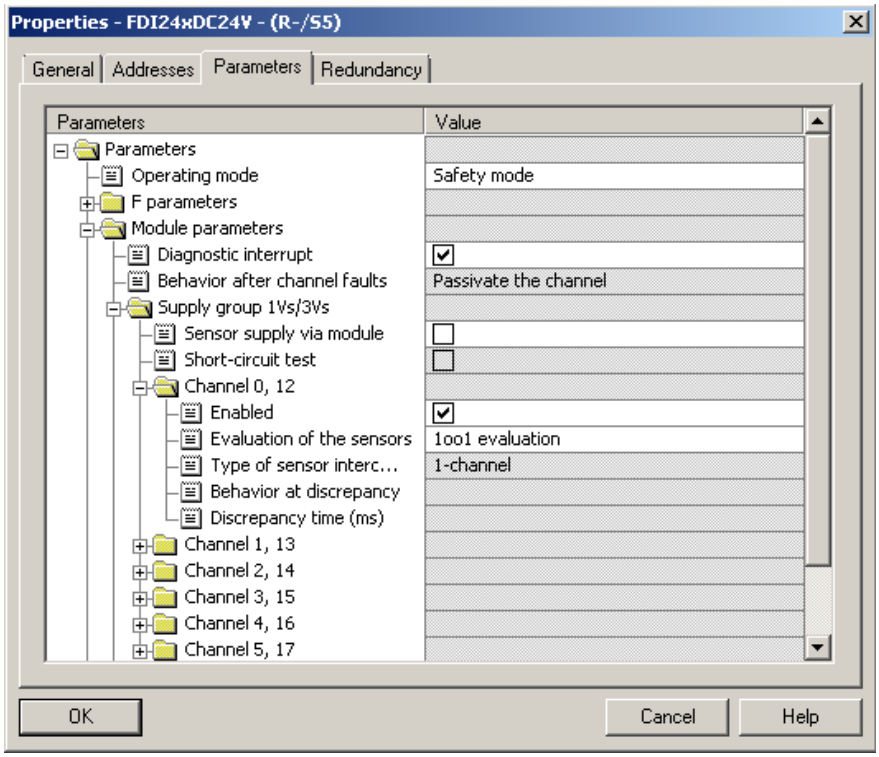


Table 6-3 1oo2 evaluation in the CPU - hardware configuration parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Operating mode	Display of the F-DI operating mode **Note:** In order to use the integrated safety functions available in the F-DI, this parameter must be set to **safety mode**.	Safety mode
F-parameters		
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-DI. **Note:** Siemens Industry Online Support provides a spreadsheet that helps users to calculate F-monitoring times (see \10\).	10 to 10000
Module parameters		
Diagnostic interrupt	Diagnostic alarm capability for the F-DI. A diagnostic alarm is triggered by various error events that can be detected by the F-DI. These events are then signaled to the CPU. **Note:** In addition to diagnostic interrupts being enabled at the module level, individual diagnostic events must be enabled at the channel level.	Release
Module parameters for a power supply group		
Sensor supply via module	Selection whether the sensor is powered by the F-DI or not. **Note:** This option must be enabled to enable the short circuit diagnostics (see below).	Release / lock

© Siemens AG 2018 All rights reserved

Parameters	Description / Recommendations	Desired setting or permissible value range
Short-circuit test	Select whether the short circuit test for the channel is enabled or not. **Note:** This option is only useful if simple switches without their own power supply are used. The short-circuit test deactivates the power supply for the sensor for short time intervals.	Release / lock
Channel/channel pair parameters		
Enabled	Selection whether the channel/channel pair is enabled for signal processing in the safety program or not.	Release / lock
Evaluation of the sensors	Setting the evaluation process. **Note:** For a 1oo2 evaluation in the CPU, this parameter must be set to **1oo1**. • Within the FD itself, each of the two sensors is rated as a 1oo1 signal. • The actual 1oo2 evaluation happens occurs within the CPU logic.	1oo1
Type of sensor interconnection	Display of the sensor indication (1 channel, 2 channels, etc.). **Note:** With "1oo1 evaluation", the sensor type is set to **1-channel**.	1-channel

Note

The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

© Siemens AG 2018 All rights reserved

6.5 Creating the logic

6.5.1 Configuration with Safety Matrix

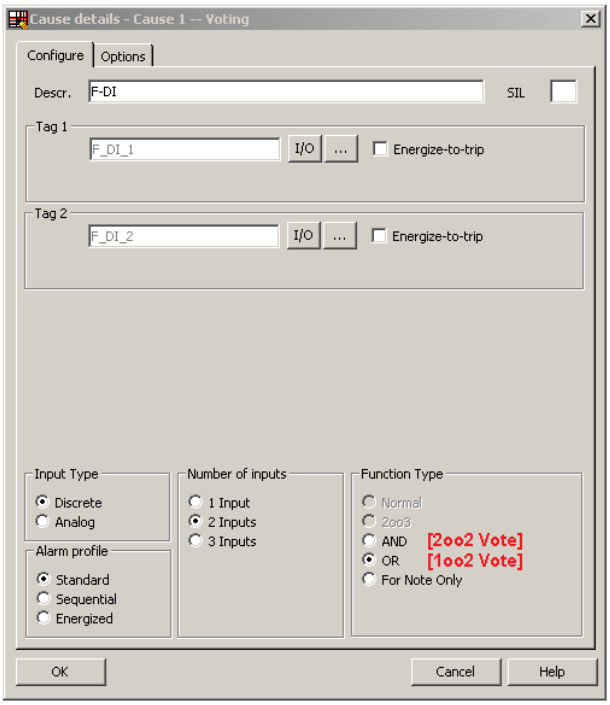
After the two sensors have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented in the CPU. One method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

Figure 6-7 shows a cause for the 1oo2 evaluation in the Safety Matrix. The cause has the following attributes:

- Discrete input type
- 2 inputs
- OR Function type (1oo2 Vote)
- Select the tag by pressing the "I/O" button to select the symbolic name from the symbol table (e.g. F_DI_1).

The cause is configured with the OR (1oo2 Vote) function type. If at least one sensor is released for triggering, the cause activates and triggers the linked effect(s).

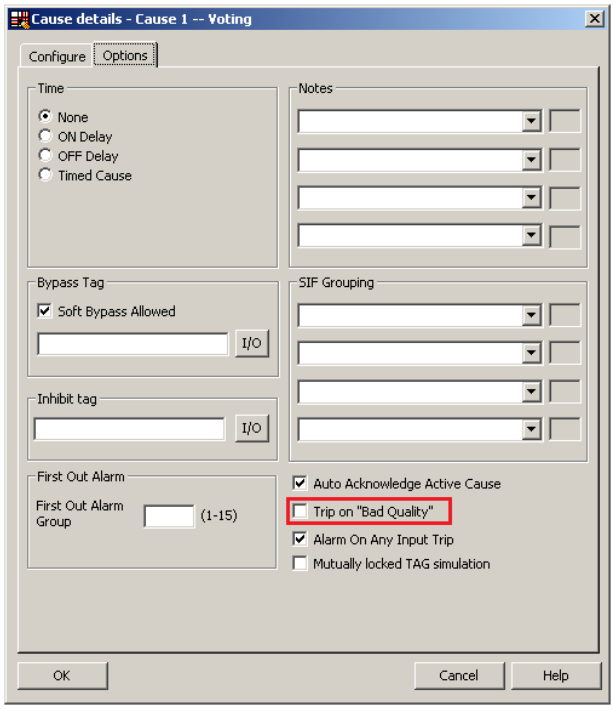
Figure 6-7 1oo2 evaluation in the CPU Safety Matrix - configuration



Depending on the requirements, additional options may be used (e.g. Energize-to-trip, Time Delay, Bypass, Inhibit). One option highlighted in Figure 6-8 is shutdown in case of a channel fault (Trip On Bad Quality). If this option is selected, a channel fault (QBAD) is considered as a bad process state.
In the case of De-energize-to-trip causes with discrete input signals, channel faults result in the enabling of the cause even if the "Trip On Bad Quality" option is deactivated.
With an OR operation (1oo2) in the cause, the cause becomes active if one of the sensors signals a critical process status or if a channel fault occurs when "Trip On Bad Quality" is enabled.

© Siemens AG 2018 All rights reserved

Figure 6-8 1oo2 evaluation in the CPU Safety Matrix - options



6.5.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the 1oo2 evaluation logic for the CPU with the CFC Editor. After the two sensors have been added to the hardware configuration, the 1oo2 evaluation logic (or another evaluation procedure) can be implemented in the CPU.

There are two ways to implement the CFC logic:

- Without channel fault evaluation (direct triggering in the event of a channel fault)
- With channel fault evaluation (delayed triggering in the event of a channel fault)

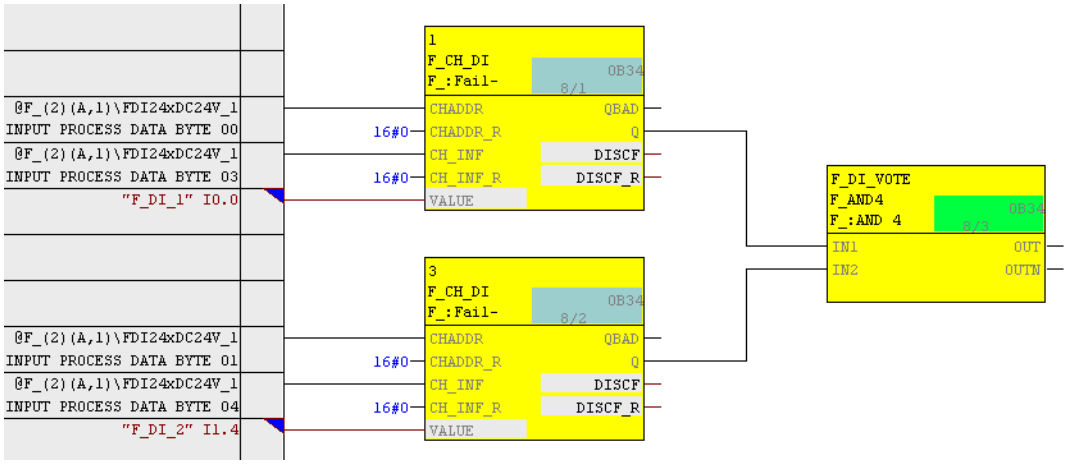
Note that an OR function can also be used to perform a 2oo2 evaluation.

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 6-9 illustrates a sample logic for a 1oo2 evaluation in the CFC Editor. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

© Siemens AG 2018 All rights reserved

Figure 6-9 1oo2 evaluation in the CPU - CFC logic - without channel fault evaluation



The example logic in Figure 6-9 works as follows:

- If both input signals return a normal process state (i.e. "1"), the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the OUT output of the block F_DI_VOTE.
- If one or both input signals return a critical process state (i.e. 0), the output of the evaluation logic is 0 (i.e. a triggering command).
- If a channel fault is detected at one or both inputs, the replacement value "0" is output by the input driver at the Q output. The output of the evaluation logic (OUT output of the F_DI_VOTE block) is 0 (i.e. triggering command).

Logic with channel fault evaluation (delayed triggering in the event of a channel fault)

If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period.

Figure 6-10 illustrates a sample logic for reading input signals in CFC Editor, which takes into account a channel fault with delay. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

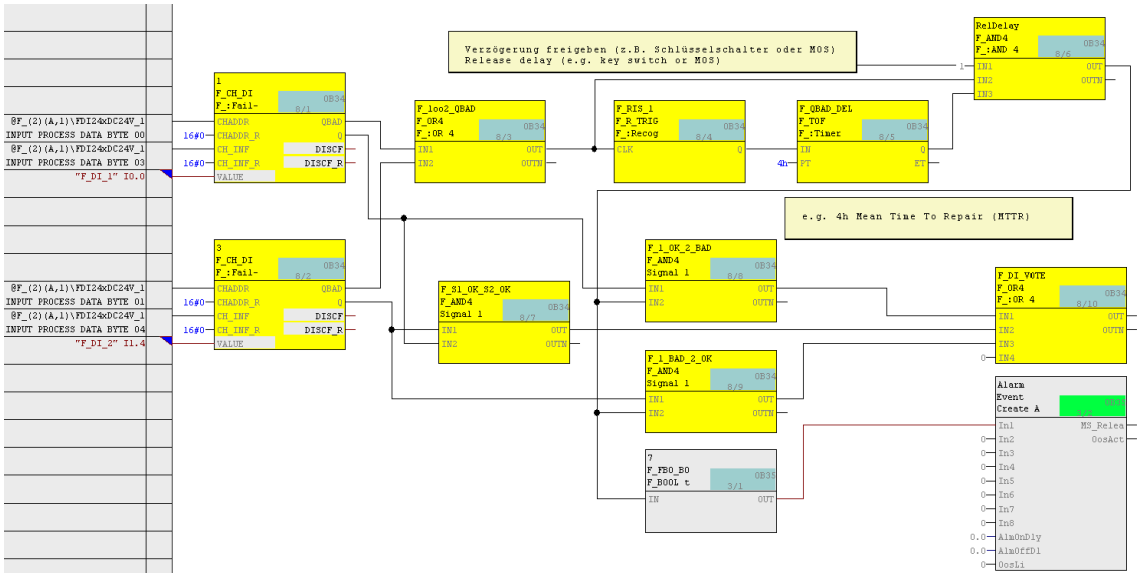
If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

In order to be able to transfer the process to the safe state in hazardous situations, the delay can be enabled or aborted via input IN1 of the RelDelay block.

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

© Siemens AG 2018 All rights reserved

Figure 6-10 1oo2 evaluation in the CPU CFC logic - with channel fault evaluation (delayed triggering in the event of a channel fault)



The logic in Figure 6-10 works as follows:

- If both input signals return a normal value and no channel fault ("1") the output of the evaluation logic is "1" (i.e. no triggering command). The output of the evaluation logic here is the OUT output of the F_DI_VOTE block.
- If one input signal returns a critical process state and there is no channel fault (i.e. 0), the output of the evaluation logic is 0 (i.e. no shutdown command).
- If one input signal returns a good status and the other returns a channel fault, a pulse with the length of the delay time is generated from the rising edge of QBAD. If the delay is enabled, the shutdown command is delayed as long as QBAD is present and the delay time is running. After expiry of the delay time or if the channel fault or the release goes, the bridging is terminated and the output of the evaluation logic follows the input signals.
- If both input signals return a critical process status or a channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.
- A bridging of the safety function when a channel fault occurs is signaled with the event block "Alarm".

© Siemens AG 2018 All rights reserved

7 Hardware configuration and wiring of two sensors (1oo2) with redundant F-DI (2oo2) and evaluation in the user program

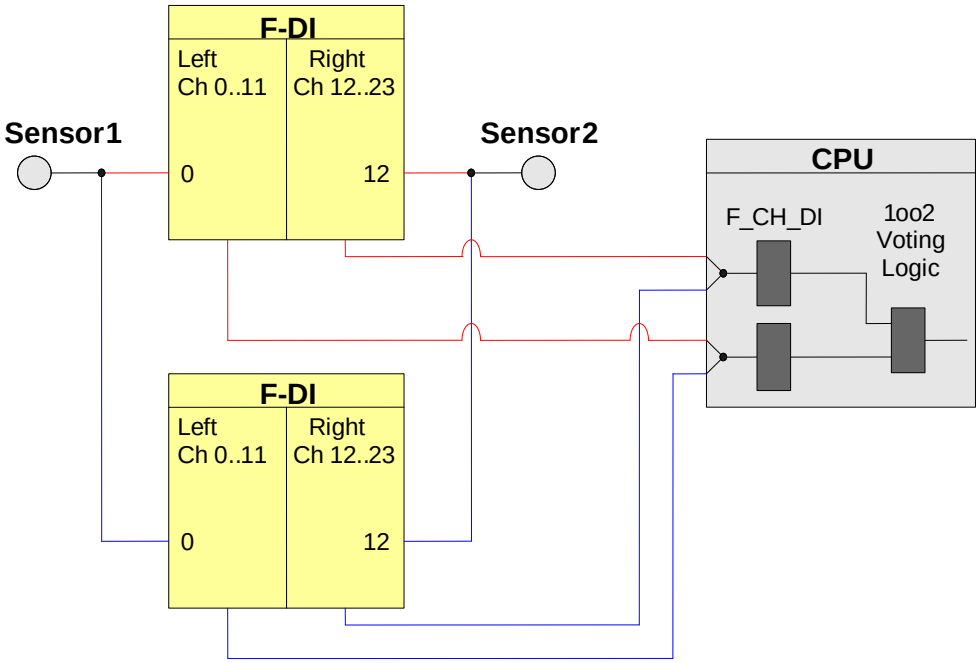
To increase availability, the 1oo2 evaluation scheme can be implemented with a pair of redundant F-DI.

Note

The I/O modules are certified in this architecture for achieving Safety Integrity Level **SIL3**. However, to be SIL-compliant, the entire safety function – including the sensors – must be assessed according to IEC 61508/IEC 61511.

In the redundant 1oo2 architecture, both sensors are wired to a pair of redundant F-DI; an example is shown in Figure 7-1. In this example, the sensors are each wired to Channels 0 and 12 of the F-DI. If both sensors are connected to a module as shown in the example, this must be on the opposite side of the module to avoid common cause faults. The modules are configured as redundant modules in HW Config. The safety program requires only one F-channel driver (F_CH_DI) for each sensor signal. The F-channel driver is connected by the compiler to the two fail-safe module drivers and selects a valid input signal.

Figure 7-1 1oo2 evaluation in the CPU with redundant modules (2oo2) - architecture



The hardware configuration according to Figure 7-1 is suitable for achieving **SIL3**.

© Siemens AG 2018 All rights reserved

The following table shows you when the safety function can be triggered by a corresponding logic.

Table 7-1 Failure combinations

Failed component detected?				Triggering of the safety function possible?
Sensor 1	**Sensor 2**	**F-DI 1**	**F-DI 2**	
No	No	No	X	Yes (not required)
No	No	X	No	Yes (not required)
Yes	X	X	X	Yes
X	Yes	X	X	Yes
X	X	Yes	Yes	Yes

Note The redundancy of the F-DI does not increase the Safety Integration Level.

7.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the safety function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using this formula:

$PFD_{Ein} = PFD_{Sensor} + 2\ PFD_{F\text{-}DI+}\ PFD_{CPU}$

The $PFD_{F\text{-}DI}$ and PFD_{CPU} values can be found in Chapter 10.

The PFD_{Sensor} value for an 1oo2 sensor is calculated using the following[7] formula:

$$PFD_{Sensor} \approx \frac{{\lambda_{DU}}^2 \cdot {T_1}^2}{3} + \beta \cdot \lambda_{DU} \cdot \frac{T_1}{2}$$

[7] The formula was taken from sheet 4 of IEC 61508, IEC 61511 and VDI 2180.

© Siemens AG 2018 All rights reserved

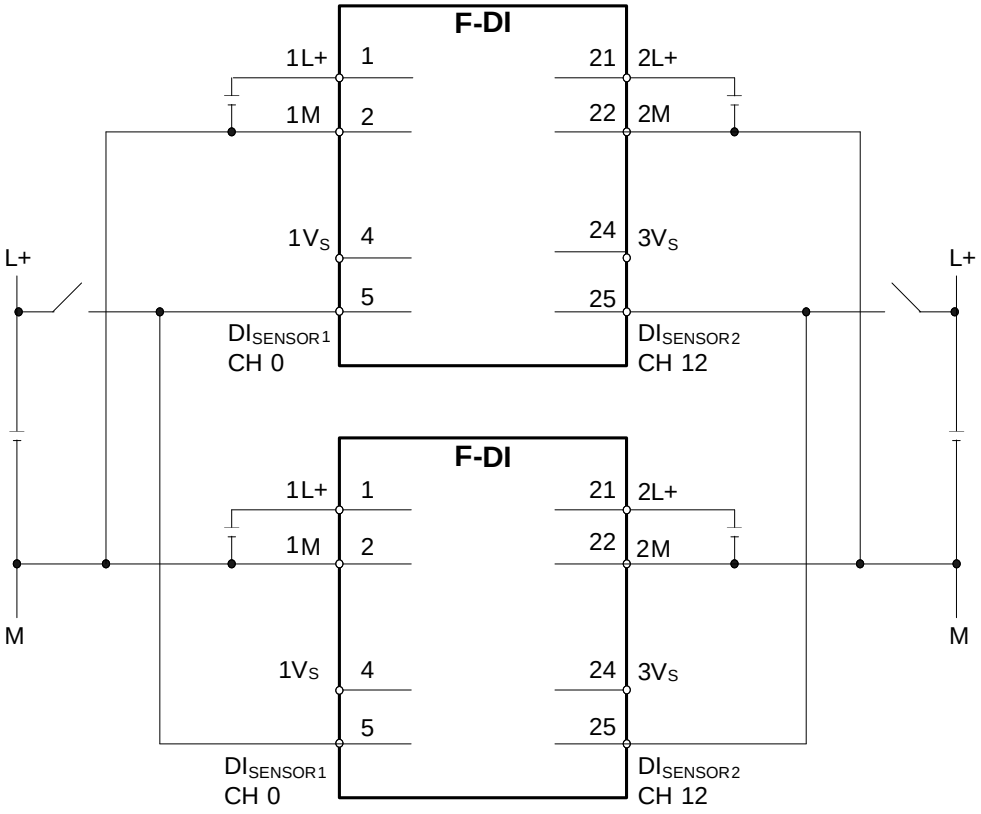
7.2 Wiring

7.2.1 Conventional wiring

In the 1oo2 evaluation scheme with evaluation in the CPU and redundant F-DI, the sensors must be powered from an external source.

Figure 7-2 shows an example. For both F-DI, the first sensor in the diagram is wired to Channel 0 (Terminal 5) and the second sensor is wired to Channel 12 (Terminal 25). Both F-DI are powered at 1L+/1M (Terminals 1 and 2) and 2L+/2M (Terminals 21 and 22). The L+ voltage powers both sensors.

Figure 7-2 1oo2 evaluation in the CPU with redundant F-DI wiring - external sensor supply



7.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the sensors and the ET 200M signal modules is greatly simplified through the use of an F-DI MTA for this evaluation scheme.

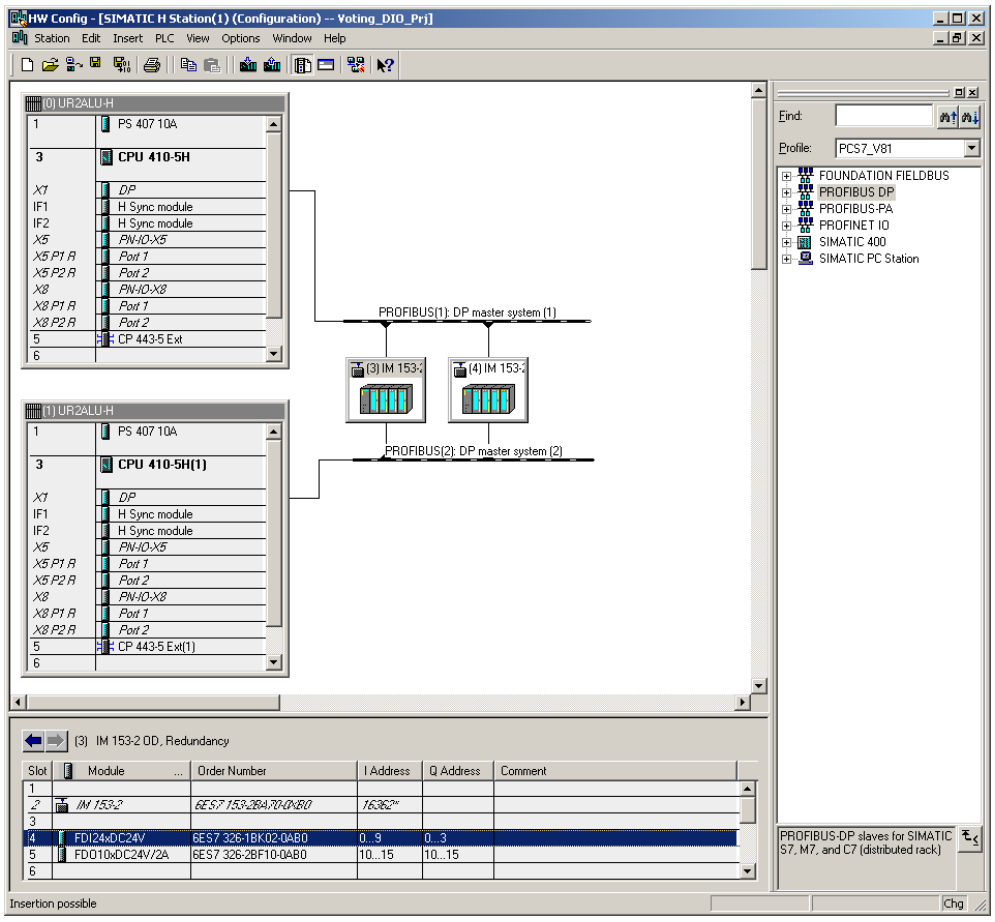
Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

© Siemens AG 2018 All rights reserved

7.3 Hardware configuration

For the 1oo2 evaluation scheme with evaluation in the CPU and redundant F-DI, the F-DI are configured in HW Config. Figure 7-3 shows an example configuration. In this example, there are two ET 200M racks with PROFIBUS addresses 3 and 4. Each ET 200M contains one F-DI in Slot 4. For additional information about HW Config, refer to \4\.

Figure 7-3 1oo2 evaluation in the CPU with redundant F-DI (2oo2) - configuration



The two F-DI must be configured as a redundant pair in HW Config. The F-DI redundancy settings can be accessed through the object properties of the F-DI. For the example in Figure 7-3, the redundancy settings are configured with PROFIBUS address 3 using the F-DI in the ET 200M. The redundancy setting is shown in Figure 7-4 and summarized in Figure 7-2.

© Siemens AG 2018 All rights reserved

Figure 7-4 1oo2 evaluation in the CPU with redundant F-DI (2oo2) redundancy parameters

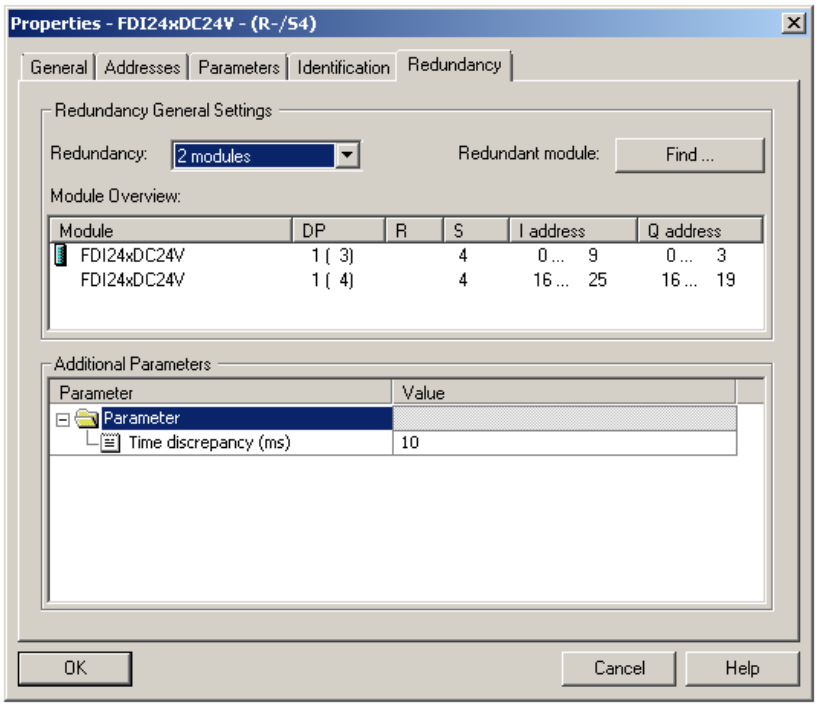


Figure 7-2 1oo2 evaluation in the CPU with redundant F-DI (2oo2) redundancy parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-DI act as part of a redundant pair or not. **Note:** The parameter should always be set to 2 modules for this architecture.	2 modules
Redundant module	Used to select the redundant partner module (only modules of the same type are displayed).	Select module
Discrepancy time (ms)	The maximum permitted time in which the redundant input signals may differ.	10 - 30000

Note

The hardware parameter names and configuration interface may differ from those in this section due to the F-DI version and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

After the redundancy settings have been configured, the remaining hardware parameters for the redundant F-DI pair can be set as described in Section 6.4. The parameters only have to be set on one of the two modules. They are copied onto the second module by the system.

© Siemens AG 2018 All rights reserved

7.4 Creating the logic

Although this evaluation scheme uses redundant F-DI, only three F_CH_AI F-channel drivers are needed in the logic (an F-channel driver for each of the two input signals). The F-channel drivers can be added and configured automatically from the SIMATIC Safety Matrix or manually using the CFC Editor. The F-channel driver must be interconnected to the symbolic names assigned to the lower input addresses.

The logic is compiled when the F-channel drivers are configured and the logic is fully available. If the option to generate module drivers is selected during compilation, the corresponding F_PS_12 module drivers are automatically added to the logic and interconnected during the compilation. The F-channel driver select the valid input signal and, in the event of a fault, switch to the input signal of the redundant F-DI.

7.4.1 Configuration with Safety Matrix

After the two sensors have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented in the CPU. One method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\).

The evaluation logic for the 1oo2 evaluation with redundant F-DI in the CPU is the same as described in Section 6.5.1.

7.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the 1oo2 evaluation logic with redundant F-DI in the CPU with the CFC Editor. After the two sensors have been added to the hardware configuration, the 1oo2 evaluation logic (or another evaluation procedure) can be implemented in the CPU.

There are two ways to implement the CFC logic:

- Without channel fault evaluation (direct triggering in the event of a channel fault)
- With channel fault evaluation (delayed triggering in the event of a channel fault)

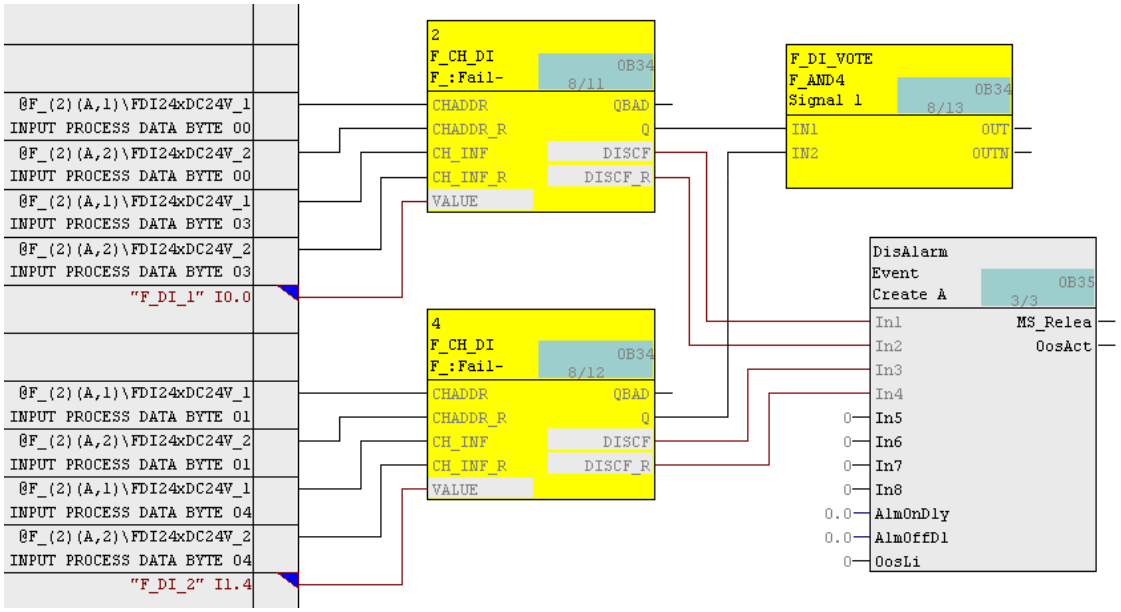
Note that an OR function can also be used to perform a 2oo2 evaluation.

Logic without channel fault evaluation (direct triggering in the event of a channel fault)

Figure 7-5 illustrates a sample logic for a 1oo2 evaluation in the CFC Editor. Note that in this example, a "0" signal at the input will result in shutdown. (1 = good condition, 0 = shutdown).

© Siemens AG 2018 All rights reserved

Figure 7-5 1oo2 evaluation in the CPU with redundant F-DI - CFC logic - without channel fault evaluation



The example logic in Figure 7-5 works as follows:

- If both F_CH_DI signal a normal process state (i.e. "1"), the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the OUT output of the block F_DI_VOTE.
- If one or both F_CH_DI signal a critical process state (i.e. 0), the output of the evaluation logic is 0 (i.e. a triggering command).
- If one F-DI signals a channel fault for one or both values, the output of the evaluation logic is 1 (i.e. no shutdown command) since the F_CH_DI outputs the value of the F-DI which delivers no channel fault.
- If one or both F_CH_DI receives different signals and no channel fault from the redundant F-DI, the output of the evaluation logic is 1 (i.e. no shutdown command) since the F_CH_DI outputs the value of the F-DI which delivers a "1" signal. At the same time, a discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If an F_CH_DI of both redundant F-DI receives a channel fault, the substitute value "0" is output as the Q output. The output of the evaluation logic (OUT output of the F_DI_VOTE block) is 0 (i.e. triggering command).

Logic with channel fault evaluation (delayed triggering in the event of a channel fault)

If the specification of the safety function allows it, an evaluation of the channel fault can be used to, for example, continue the process for a limited period to perform maintenance or repair during this period.

If a channel fault occurs, if the function is enabled, shutdown is delayed for the time set at the PT input of the F_QBAD_DEL block (4 hours in the example).

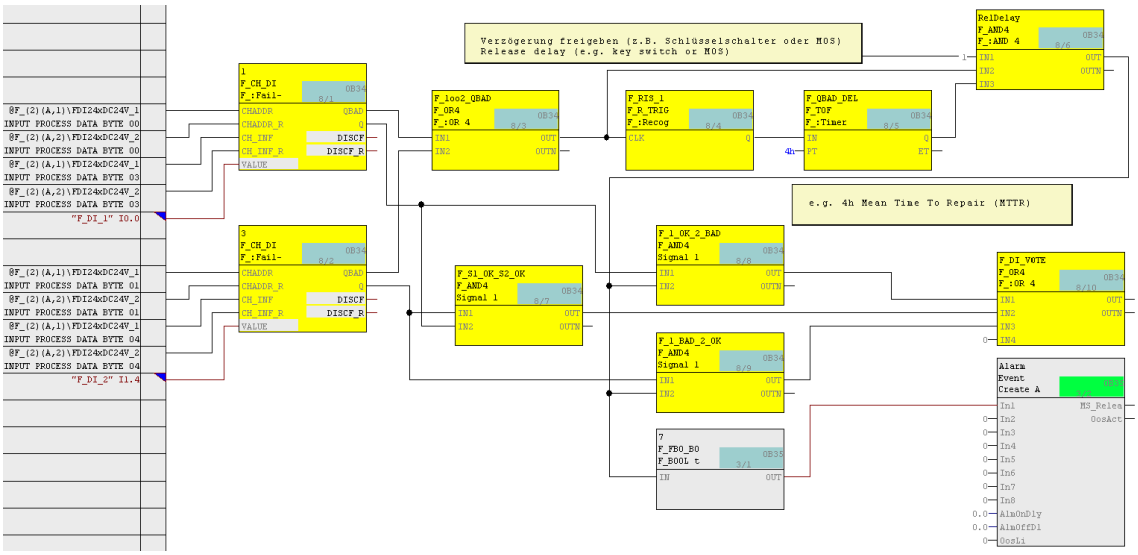
In order to be able to transfer the process to the safe state in hazardous situations, the delay can be enabled or aborted via input IN1 of the RelDelay block.

In the SRS (Safety Requirement Specification), suitable alternative measures must be defined for this period to ensure compliance with the required SIL. Note also that no distinction is made here between channel and module errors. In the case of a module error, several safety functions may be delayed; this requires an additional risk assessment and possibly further measures.

© Siemens AG 2018 All rights reserved

Figure 7-6 illustrates sample logic for a 1oo2 evaluation in the CFC Editor, with redundant F-DI which takes into account channel faults with delay. Note that in this example, a "0" signal on an input signals a critical process condition and triggers shutdown. (1 = good condition, 0 = shutdown).

Figure 7-6 1oo2 evaluation in the CPU with redundant F-DI - CFC logic - with channel fault evaluation (delayed triggering in the event of a channel fault)



The example logic in Figure 7-6 works as follows:

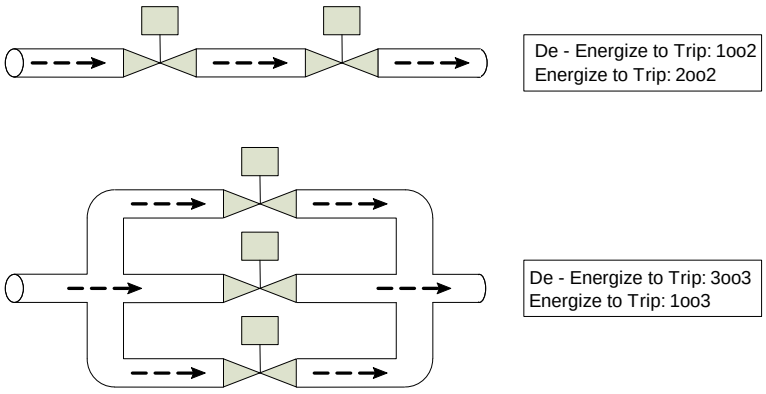
- If both F_CH_DI signal a normal value and there is no channel fault, the output of the evaluation logic is 1 (i.e. no shutdown command). The output of the evaluation logic here is the OUT output of the F_DI_VOTE block.
- If one of the F_CH_DI signal a critical process status and no channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- If one F-DI signals a critical process state of a fault for one or both sensors, the output of the evaluation logic is 1 (i.e. no shutdown command) since the F_CH_DI outputs the value of the F-DI which delivers a "1" signal (2oo2). A discrepancy error is output at the DISCF or DISCF_R output and the event block.
- If both redundant F-DI of a sensor signal a critical process status or a channel fault, the output of the evaluation logic is "0" (i.e. shutdown command).
- The output of the evaluation logic (OUT output of the F_DI_VOTE block) is connected to the corresponding shutdown logic.

© Siemens AG 2018 All rights reserved

8 Hardware configuration and wiring for actuators

From the point of view of the safety system, all evaluation schemes for outputs are combinations of 1oo1 outputs. Each connected actuator should react in the manner specified in the safety logic. Due to the physical arrangement of the actuators, it is possible to realize different evaluation schemes (e.g. 1oo2, 2oo2, 1oo3) as shown in Figure 8-1.

Figure 8-1 Examples of different evaluation schemes through physical arrangements of the connected components

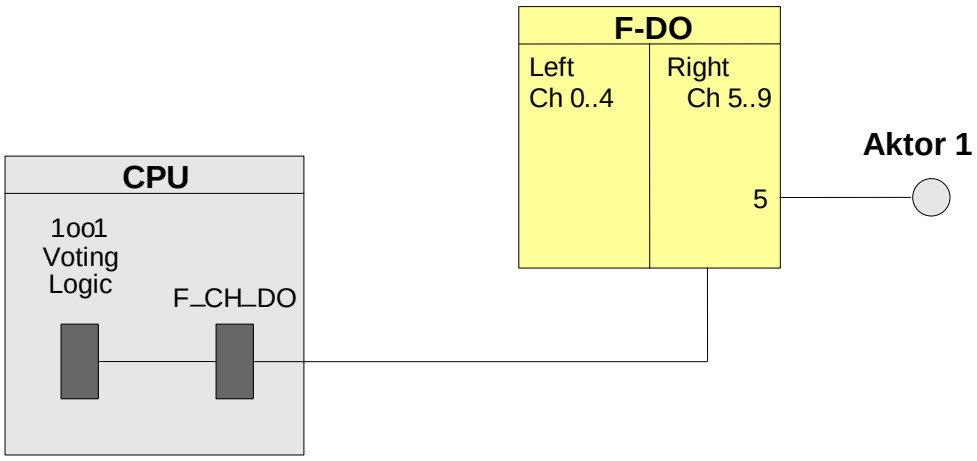


WARNING

Every F-DO channel is able to achieve a Safety Integrity Level of **SIL3** in safety functions with a de-energized safe state. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

The 1oo1 basic architecture, as shown in the block diagram in Figure 8-2, shows an actuator connected to Channel 5 of an F-DO.

Figure 8-2 F-DO - 1oo1 architecture



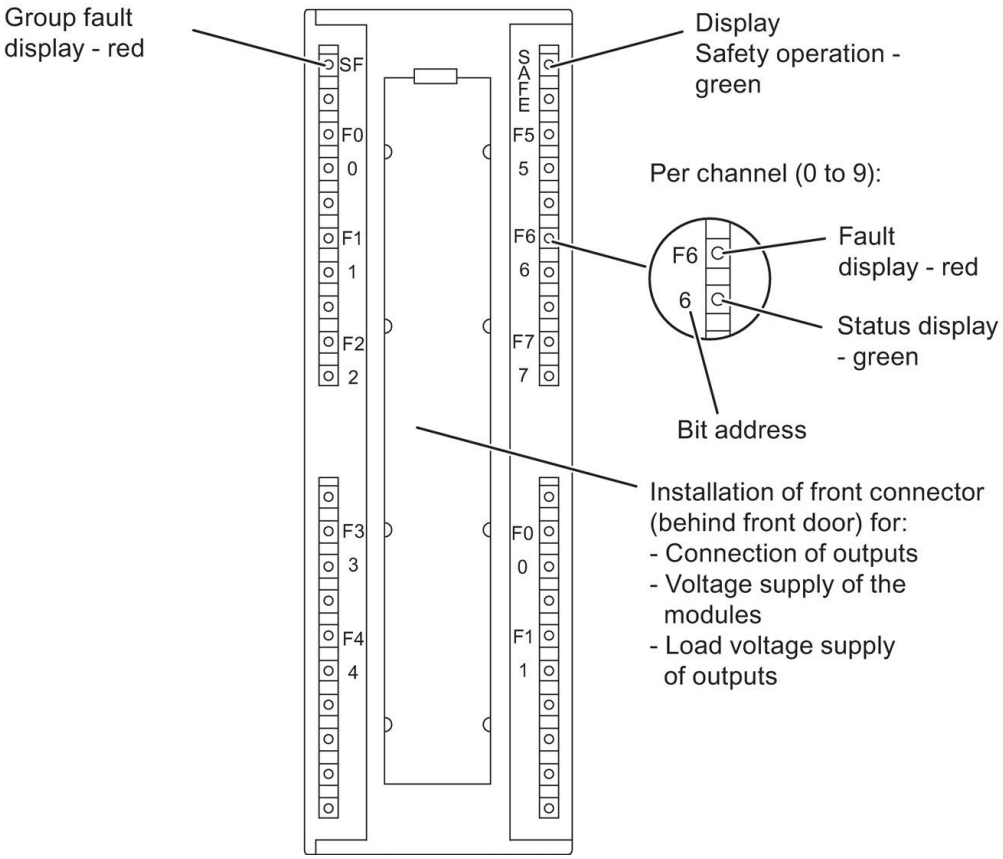
© Siemens AG 2018 All rights reserved

8.1 Properties for the fail-safe digital output module

This chapter describes the connection of discrete 24VDC actuators to the F-DO and their control. The S7-300 fail-safe module described is the SM 326 - F-DO 10 x DC 24V/2A PP. For simplification, the assembly will be referred to as F-DO in this document. The Order Number for the current version of the F-DO is: 6ES7326-2BF10-0AB0

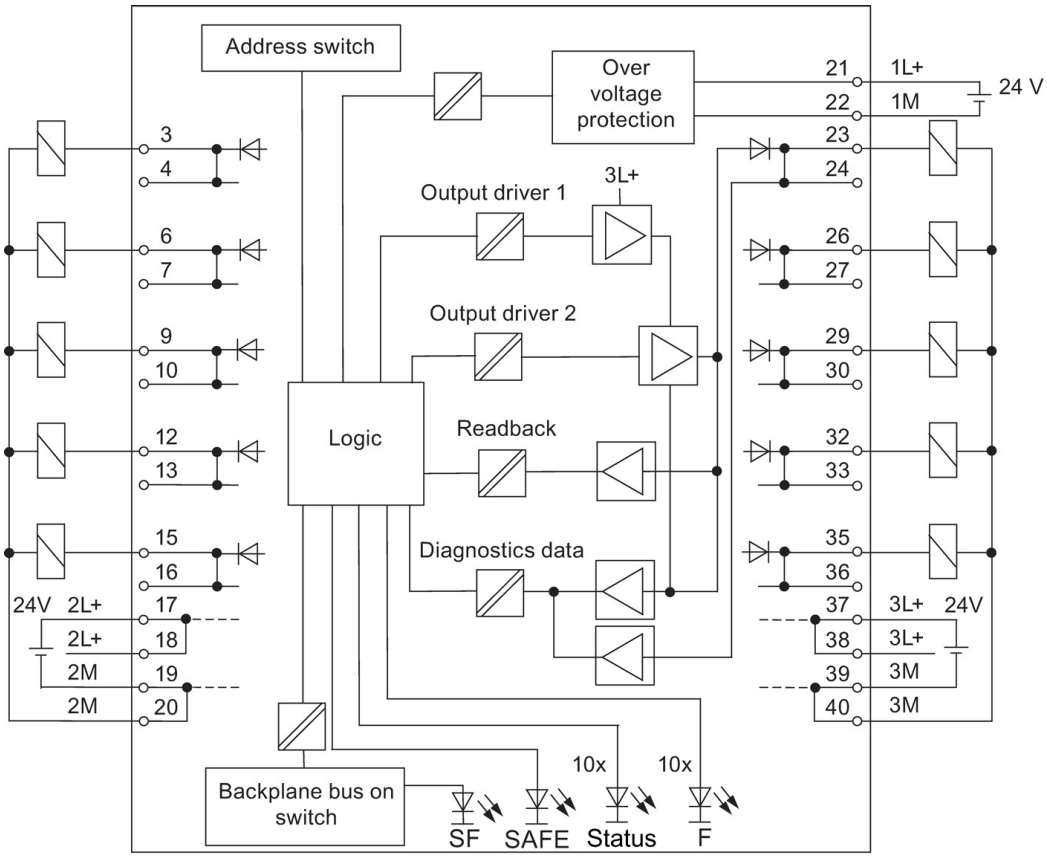
The front view of the F-DO is shown in Figure 8-3 and the connection and schematic diagram is shown in Figure 8-4.

Figure 8-3 F-DO front view



© Siemens AG 2018 All rights reserved

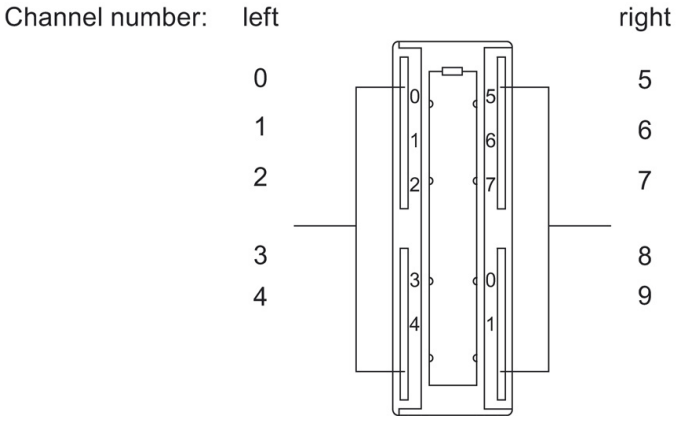
Figure 8-4 F-DO connection and schematic diagram



The F-DO is powered at three points. The module electronics are supplied at Terminals 1L+/1M. The supply of the voltage load for the channels on the left side takes place at Terminals 2L+/2M and for the right side at Terminals 3L+/3M. The F-DO has ten output channels isolated in two groups of five.

Figure 8-5 illustrates the channel number allocation.

Figure 8-5 Channel numbers for F-DO 10 x DC 24V/2A PP



© Siemens AG 2018 All rights reserved

8.2 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the fail-safe function.

PFD calculation formula

The PFD for this architecture is calculated using the following formula:

$PFD_{Out} = PFD_{F\text{-}DO} + PFD_{Final\ element}$

Note

The PFD value for the CPU (PFDCPU) has already been taken into account in the calculation of the input circuits and is therefore no longer included here.

The PFD value for PROFIsafe must also be added to the PFDCPU.

The $PFD_{F\text{-}DO}$ value can be found in Chapter 10.

For a connected component (1oo1), the $PFD_{Final\ element}$ is calculated using the following[8]formula:

$$PFD_{Final\ element} \approx \lambda_{DU} \cdot \frac{T_1}{2}$$

© Siemens AG 2018 All rights reserved

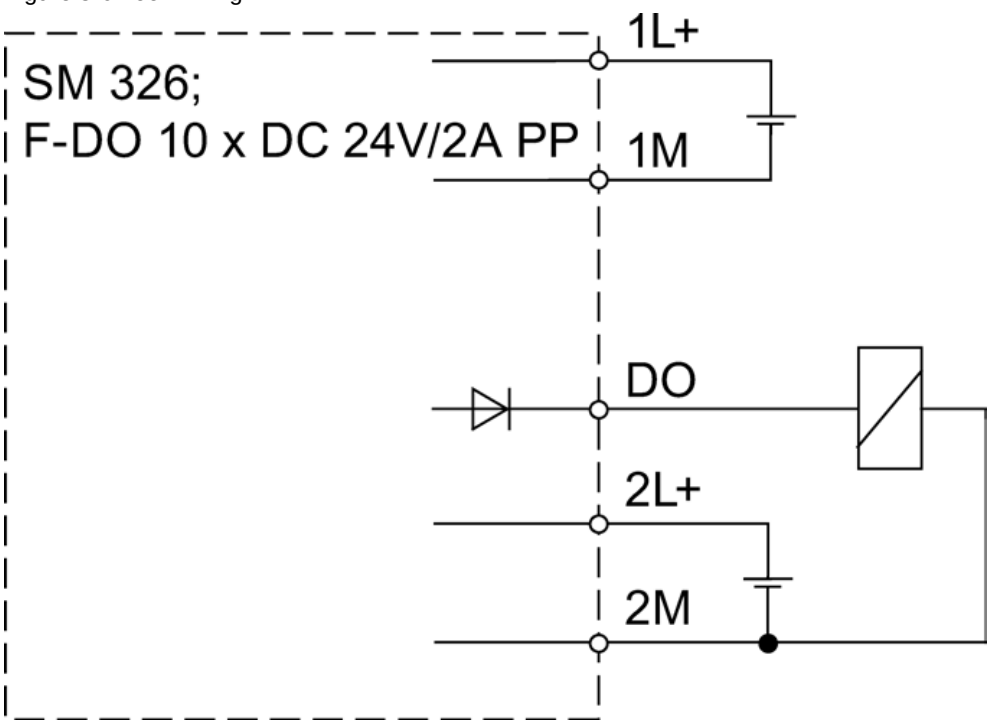
[8] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

8.3 Wiring

8.3.1 Conventional wiring

The F-DO wiring diagram for the 1oo1 evaluation scheme is shown in Figure 8-6. The actuator is wired to Channel 0 (Terminal 3). The F-DO is powered at 1L+/1M (Terminals 21 and 22). The supply of the voltage load for the channels on the left side of the front connector (Channel 0 - 4) takes place at 2L+/2M (Terminals 17/18 and 19/20).

Figure 8-6 1oo1 wiring



8.3.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the actuators and the ET 200M signal modules is greatly simplified through the use of an F-DO MTA for this evaluation scheme.

Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

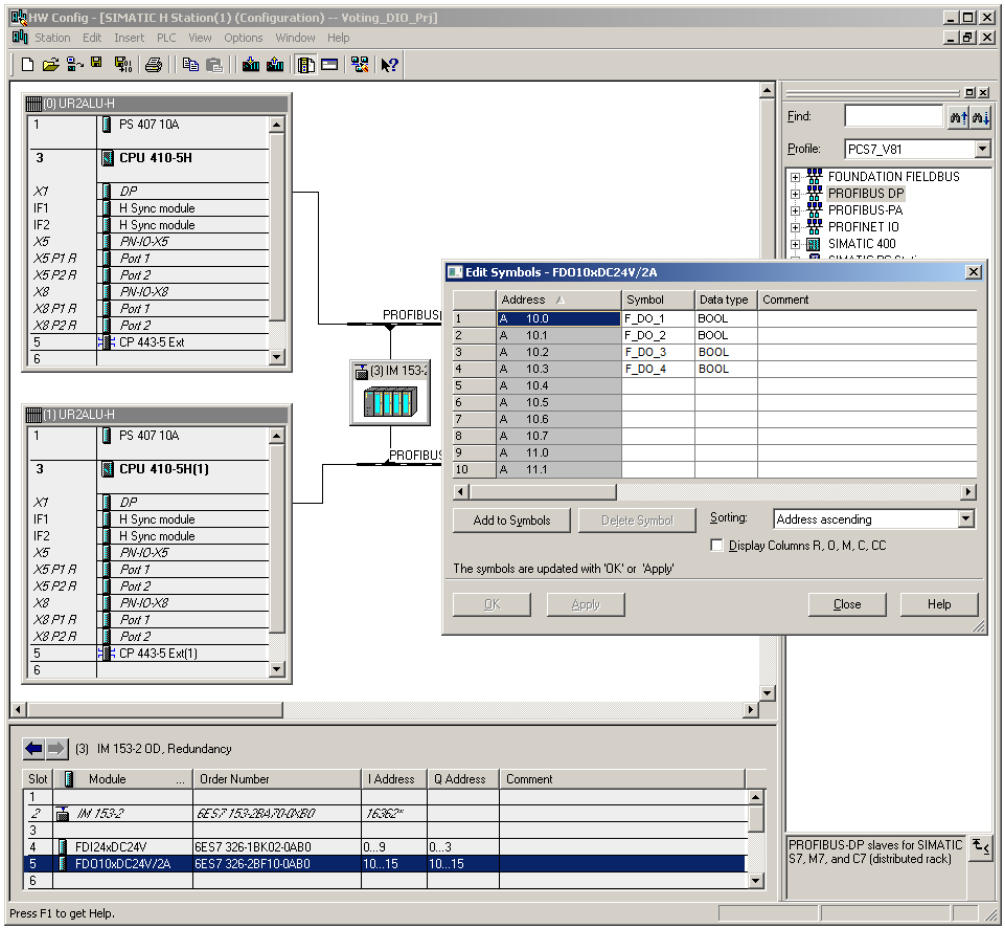
© Siemens AG 2018 All rights reserved

8.4 Hardware configuration

To configure, select the F-DO in the hardware catalog and add it into an existing ET 200M station. Then assign clear symbol names for the used channels of the F-DO.

Figure 8-7 shows an example of HW Config with an F-DO. The actuator in this example is wired to Channel 0 of the F-DO. For additional information about HW Config, refer to \4\.

Figure 8-7 F-DO 1oo1 system processing



The parameters for operating the F-DO are set in the object properties of the module in HW Config (see Figure 8-8).

The parameters are summarized in Table 8-1.

© Siemens AG 2018 All rights reserved

Figure 8-8 1oo1 hardware parameters

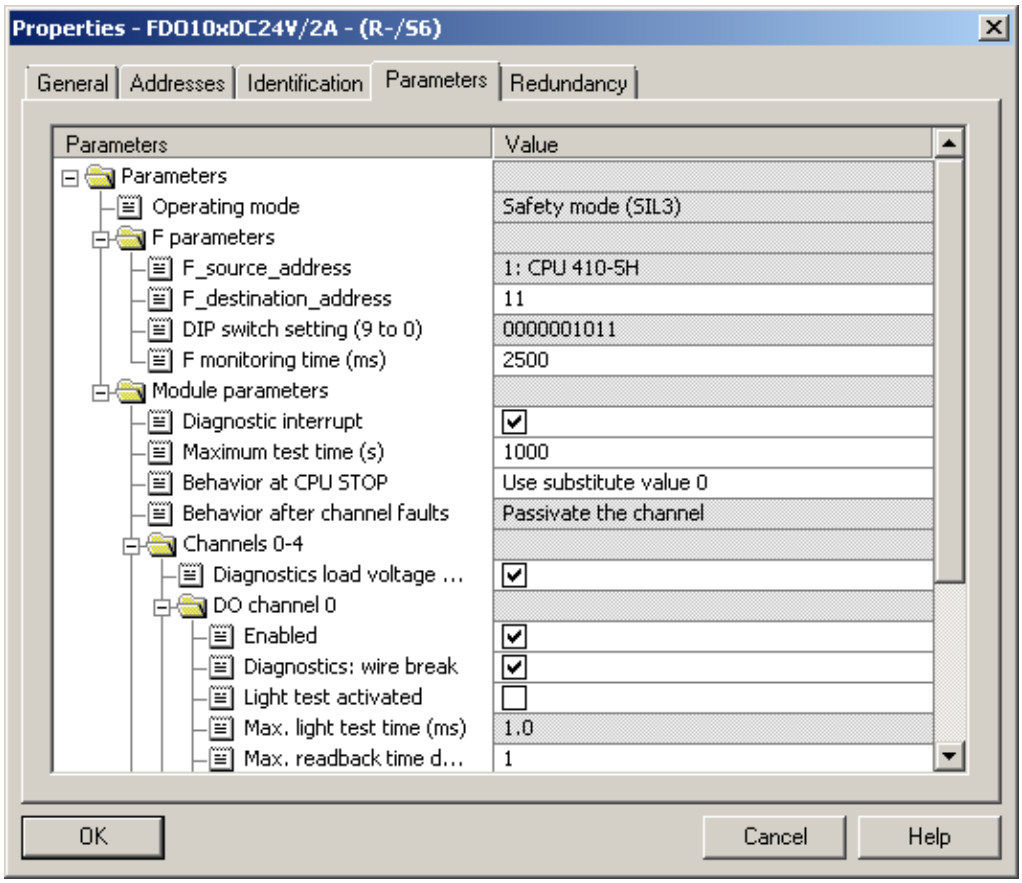


Table 8-1 1oo1 hardware configuration parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Module parameters		
Diagnostic interrupt	The diagnostic interrupt must be enabled for all modules in safety mode.	Release
Operating mode	Setting the F-DO operating mode. **Note:** In order to use the integrated safety functions available in the F-DO, this parameter must be set to one of the **safety modes**. The 6ES7326-2BF10-0AB0 can only be use in Safety mode (SIL3).	Safety mode according to SIL 3
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-DO. **Note:** Siemens Industry Online Support provides a spreadsheet that helps users to calculate F-monitoring times (see \10\).	10 to 10000
Maximum test time (s)	With this parameter, you set the repeat cycle of the test cycles (complete bit pattern test).	1000 / 100 (1000)
Behavior at CPU STOP	Select the behavior in the event of an F-CPU STOP or interruption of the PROFIsafe communication.	Use substitute value 0 / Keep last valid value

© Siemens AG 2018 All rights reserved

Channel parameters		
Diagnostics load voltage failure	Enables the voltage load monitoring diagnostics for Channels 0 - 4 (2L+) or Channels 5 - 9 (3L+)	Release / lock
Enabled	Enables the channel	Release / lock
Diagnostics: wire break	Enables diagnostic function for wire break detection	Release / lock
Light test activated	Activation of the light test When the light test is enabled, while an F-DO output is not active (output = 0), the output is enabled for a short time (output = 1) to test whether the output circuit is closed. With "dark" and "bright" periods, the actuator will not respond to the test in correspondingly short test times.	Release / lock
Max. time for light test (ms)	Since the error reaction time is extended by the max. light test time, set as short a time as possible. Actuators with a large capacity require a longer light test time.	0.6 ... 5.0 (1.0)
Max. read-back time for dark test (ms)	Since the error reaction time is extended by the max. dark test time, set as short a time as possible. Actuators with a large capacity require a longer dark test time.	Various values between 0.6 and 400 (1)
Can be configured as redundant	Activate the function if two outputs switch the same actuator.	Release / lock

Note

The hardware parameter names and configuration interface may differ from those in this section due to the version of the F-DO and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

© Siemens AG 2018 All rights reserved

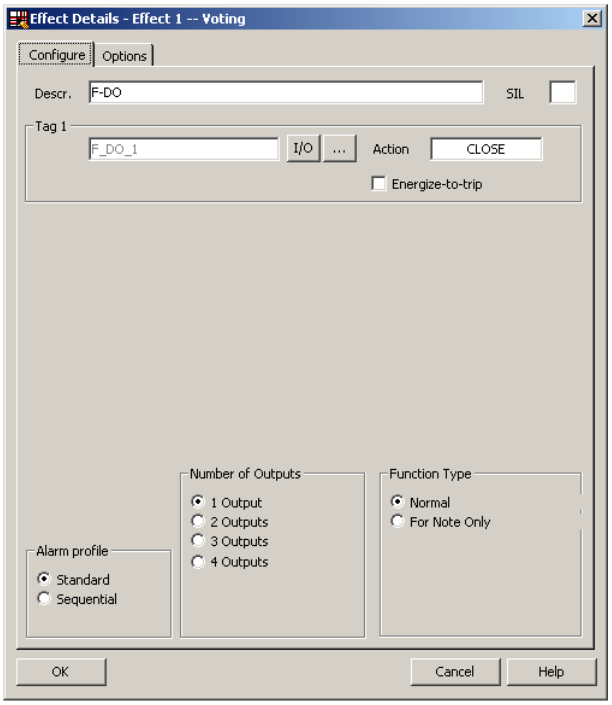
8.5 Creating the logic

8.5.1 Configuration with Safety Matrix

After the connected component has been added to the hardware configuration, the logic can be interconnected to the output in the CPU. The SIMATIC Safety Matrix Engineering Tool is a method for implementing the logic and for the interconnection to the output (for further relevant information, see \5\).

An effect for controlling an output from the Safety Matrix is displayed in Figure 8-9. In each effect, at least the field Tag 1 must be assigned with a tag. The symbolic name of the desired output (F_DO_1) from the symbol table is selected as the tag. The effect is triggered depending on the configured links. Depending on the process application, further options can be enabled in the effects (e.g. Energize-to-trip (switch-off with "1" signal), Time Delay, Bypass, Override).

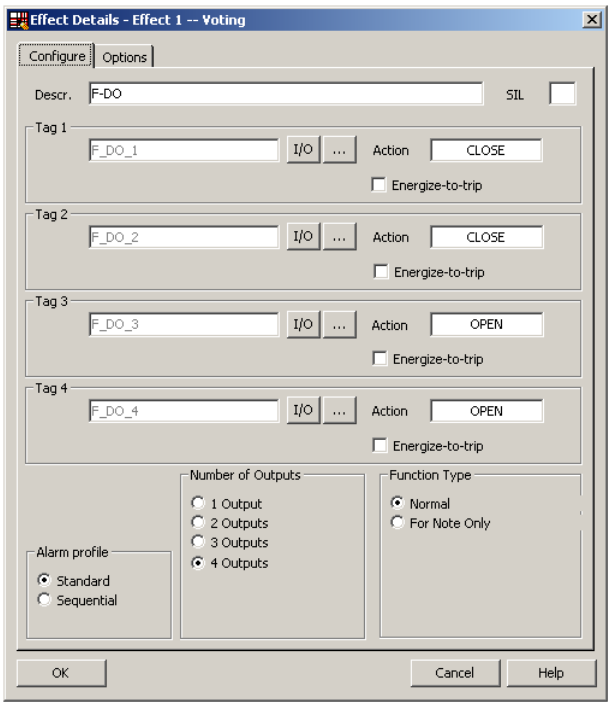
Figure 8-9 1oo1 Safety Matrix



Each effect can, as shown in Figure 8-10, control up to four tags. Depending on the arrangement of the actuators, different output architectures can be implemented with an effect (e.g. 1oo2, 2oo2, etc.). When the effect becomes active, each of the four output signals is switched to its specified active state ("0": if Energize-to-trip is not enabled or "1" if Energize-to-trip is enabled).

© Siemens AG 2018 All rights reserved

Figure 8-10 Safety Matrix effect with 4 tags



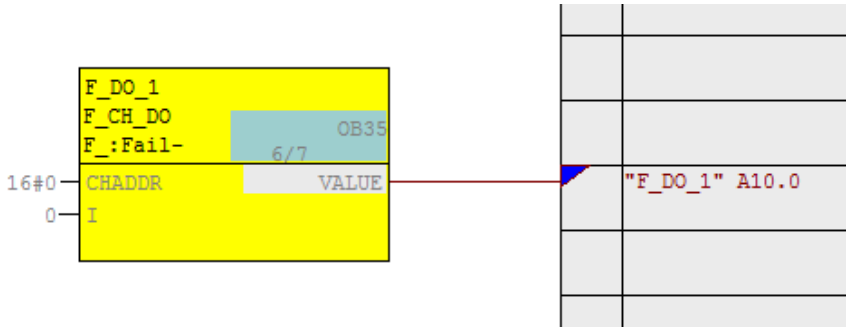
8.5.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, you can implement the logic for controlling an output of the F-DO in the CPU by means of the CFC Editor. After adding the F-DO to the hardware configuration and assigning symbolic names for the individual output channels, the evaluation logic can be linked in the CFC Editor.

Figure 8-11 shows the activation of an F-DO output in the CFC Editor. Note that in safety systems, in the good state of the process, a "1" signal is generally output and switched off with "0".

To achieve other F-DO evaluations in the system, the same triggering signal can be interconnected to several F-DO channels.

Figure 8-11 1oo1 CFC logic



The example logic in Figure 8-11 works as follows:

- The shutdown logic is connected to input "I" of the F-channel driver.
- If the shutdown logic signals a normal value (e.g. "1"), the output to the connected component is "1" (i.e. no shutdown).
- If the shutdown logic signals a triggering command (e.g. "0"), the output of the connected component is "0" (i.e. shutdown).

© Siemens AG 2018 All rights reserved

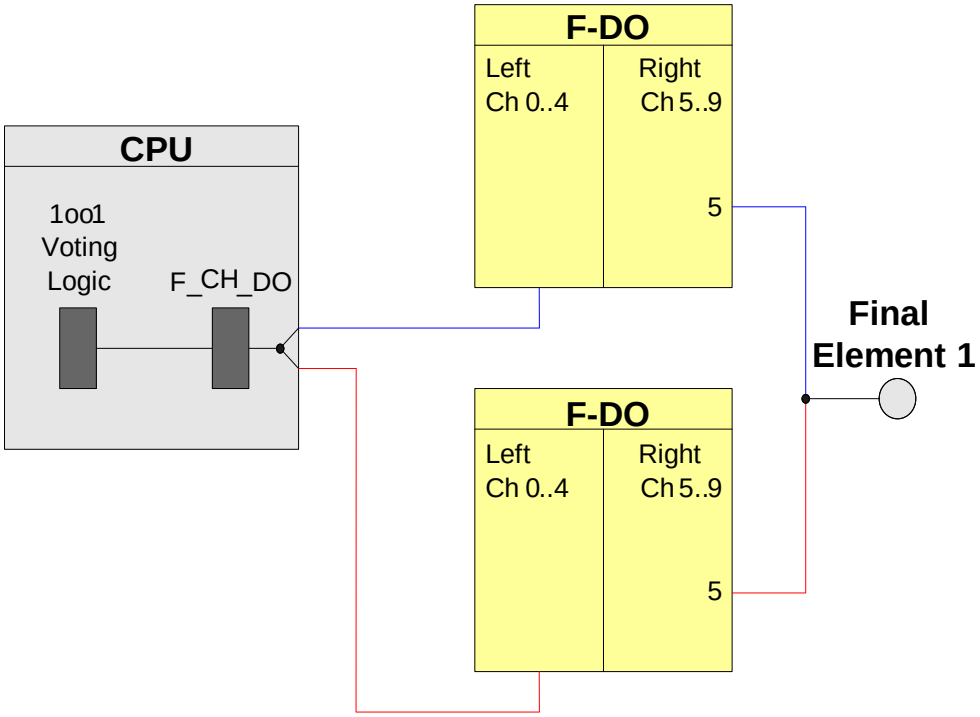
9 Hardware configuration and wiring for actuators with redundant F-DO

To increase the availability of the F-DO, the actuator can be controlled by a pair of redundant F-DO.

Note Every F-DO channel is able to achieve a Safety Integrity Level of **SIL3** in safety functions with a de-energized safe state regardless of module redundancy. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

The redundant control of an actuator from a pair of redundant F-DO is shown in the block diagram in Figure 9-1. The actuator in this example is wired to Channel 5 of the redundant F-DO. The modules are configured as a redundant pair in HW Config. An F-channel driver which distributes the signal to the two F-module drivers is sufficient to control the two outputs.

Figure 9-1 1oo1 with redundant F-DO (2oo2) - architecture



© Siemens AG 2018 All rights reserved

9.1 PFD calculation

The PFD (**P**robability of **F**ailure on **D**emand) value describes the probability of failure of the fail-safe function.

PFD calculation formula

The PFD value for this wiring & voting architecture is calculated using the following formula:

$PFD_{Out} = 2\ PFD_{F\text{-}DO} + PFD_{Final\ element}$

Note

The PFD value for the CPU (PFD_{CPU}) has already been taken into account in the calculation of the input circuits and is therefore no longer included here.

The PFD value for PROFIsafe must also be added to the PFD_{CPU}.

The $PFD_{F\text{-}DO}$ value can be found in Chapter 10.

For a connected component (1oo1), the $PFD_{Final\ element}$ is calculated using this formula[9]:

$$PFD_{Final\ element} \approx \lambda_{DU} \cdot \frac{T_1}{2}$$

© Siemens AG 2018 All rights reserved

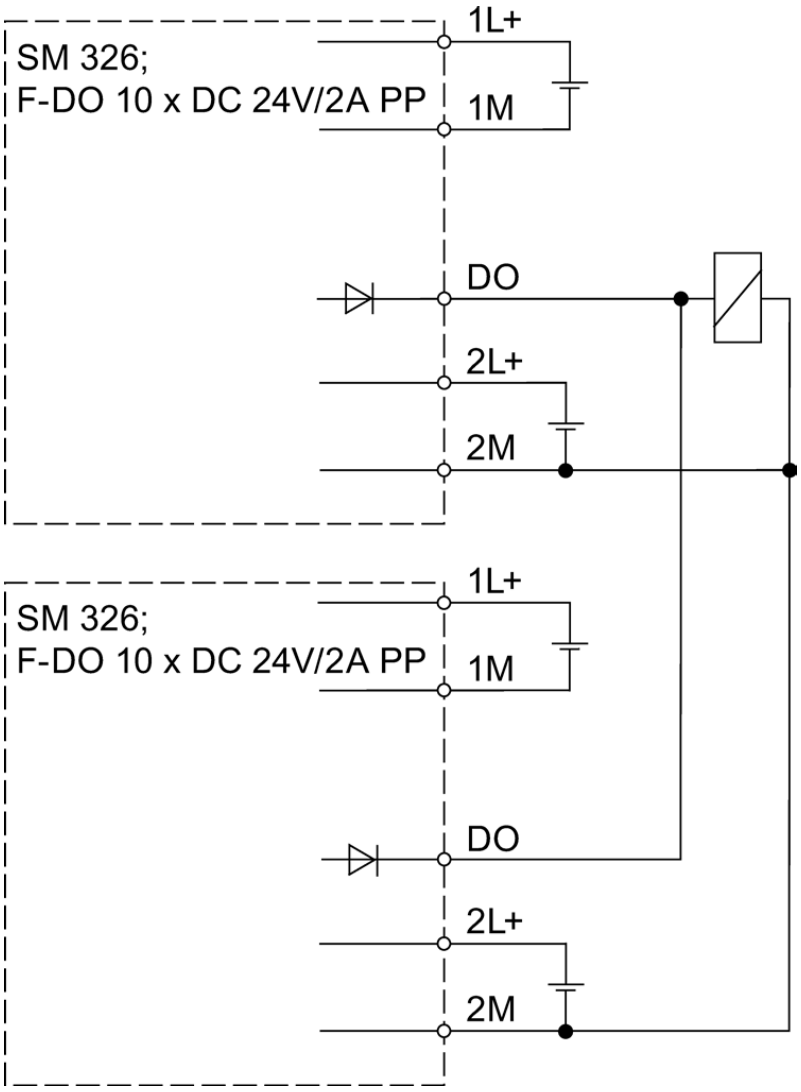
[9] The formula was taken from sheet 4 of IEC61508, IEC 61511 and VDI 2180

9.2 Wiring

9.2.1 Conventional wiring

An example for control with redundant F-DO is shown in Figure 9-2. The connected actuator is wired to Channel 5 (Terminal 24) of the redundant F-DO.

Figure 9-2 Redundant module - 1oo1 wiring



9.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). The wiring between the actuators and the ET 200M signal modules is greatly simplified through the use of an F-DO MTA for this evaluation scheme.

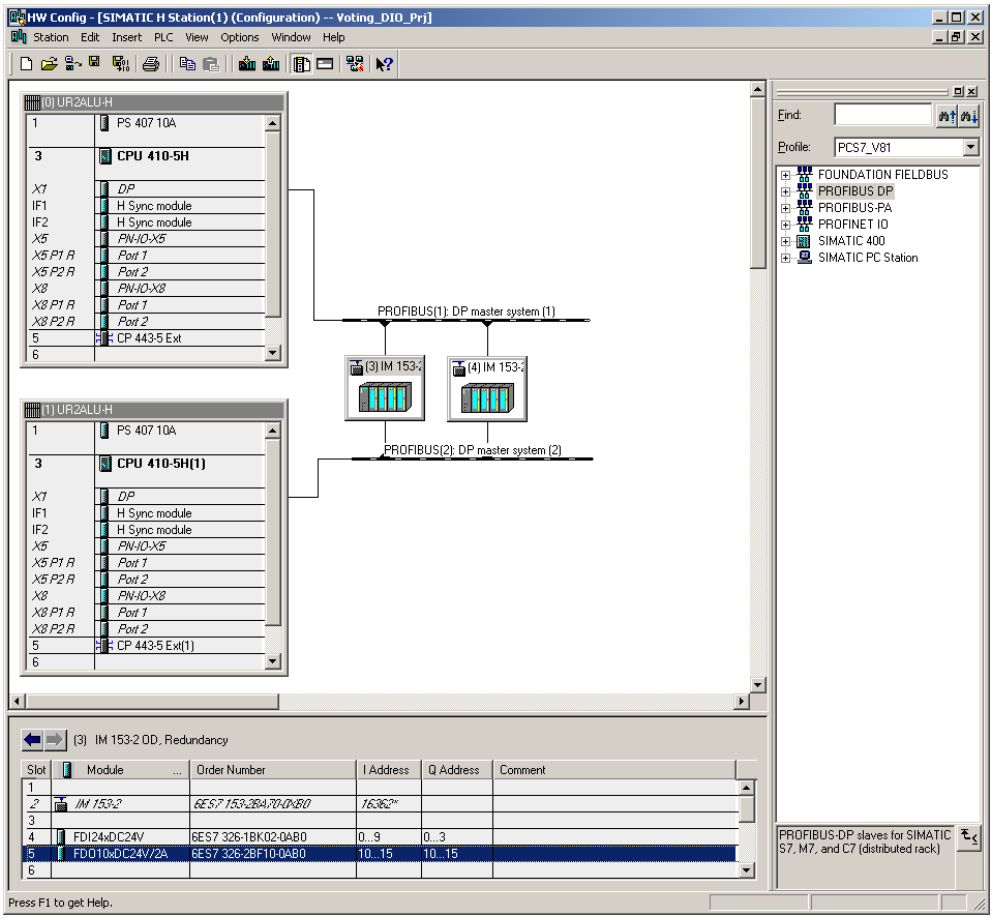
Further information can be found in the chapter "Marshalled Termination Assemblies (MTA)" (Chapter 12).

© Siemens AG 2018 All rights reserved

9.3 Hardware configuration

In the example in Figure 9-3, there are two ET 200M racks with PROFIBUS addresses 3 and 4. Each ET 200M contains one F-DO in Slot 4. For additional information about HW Config, refer to \4\.

Figure 9-3 1oo1 with redundant F-DO (2oo2) configuration



The two F-DO must be configured as a redundant pair in HW Config. The F-DO redundancy settings can be accessed through the object properties of the F-DO. In the Redundancy tab, select "2 modules" and select the partner module. The interface of the redundancy settings is shown in Figure 9-4 and the settings are summarized in Table 9-1.

© Siemens AG 2018 All rights reserved

Figure 9-4 1oo1 hardware with redundant F-DO (2oo2) redundancy parameters

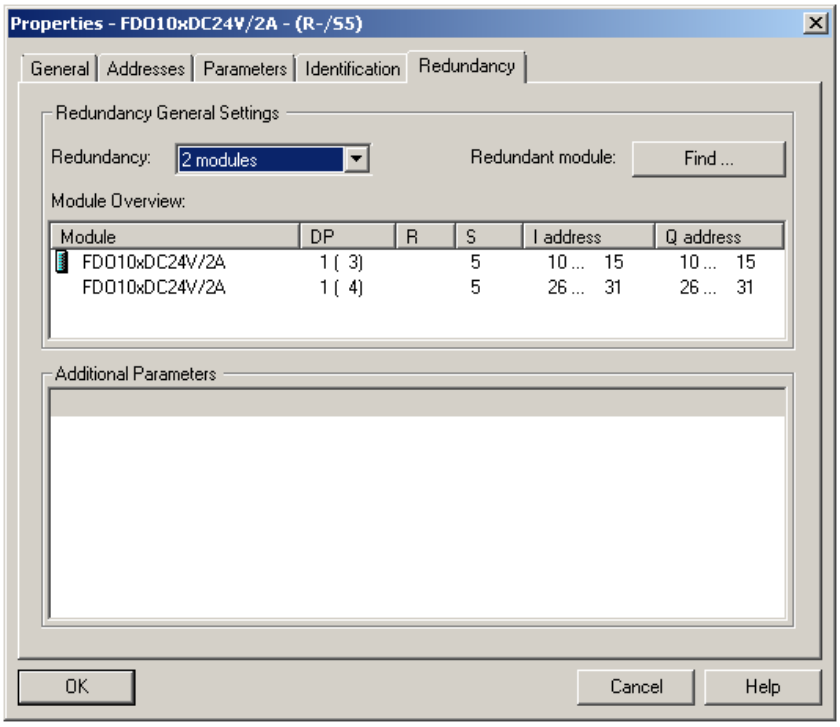


Table 9-1 1oo1 hardware with redundant F-DO (2oo2) redundancy parameters

Parameters	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-DO is acting as part of a redundant pair or not. **Note:** The parameter is set to **2 modules** for this architecture.	2 modules
Redundant module	Used to select the redundant partner module.	

Note

The hardware parameter names and configuration interface may differ from those in this section due to the version of the F-DO and hardware configuration pack.

In this case, you will find further information in the documentation or the Help section of the module.

After the redundancy settings have been configured, the remaining hardware parameters for the redundant F-DO pair can be configured as described in Section 8.4. The parameters only have to be set on one of the two F-DO. They are copied onto the second F-DO by the system.

© Siemens AG 2018 All rights reserved

9.4 Creating the logic

Although this evaluation scheme uses a pair of redundant F-DO, only one F_CH_DO F-channel driver is needed in the logic. The F_CH_DO can be added to the logic and configured automatically from the SIMATIC Safety Matrix or manually using the STEP 7 CFC Editor. In both cases, the F_CH_DO must be interconnected to the symbolic name of the output signal of the F-DO with the lower address.

The configuration is compiled when the F-channel driver is configured and the evaluation logic is fully available. If the option to generate module drivers is selected during compilation, the corresponding F_PS_12 module drivers are automatically added to the logic and interconnected during the compilation. The F-channel driver sends the signal to both module drivers, which transmit the signal to the modules.

9.4.1 Configuration with Safety Matrix

After the connected component has been added to the hardware configuration, the logic can be interconnected to the output in the CPU. The SIMATIC Safety Matrix Engineering Tool is a method for implementing the logic and for the interconnection to the output (for further relevant information, see \5\).

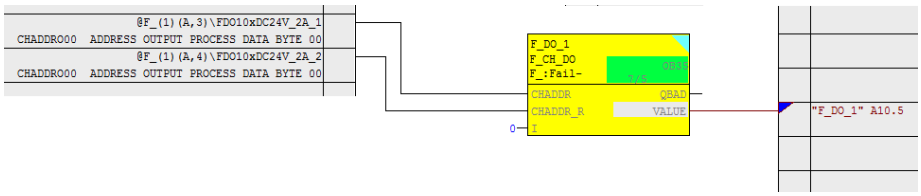
The actual configuration of the control of an output with redundant F-DO is the same as described in Section 8.5.1.

9.4.2 Configuration using CFC

As an alternative to using the Safety Matrix Tool, the logic for controlling the F-DO in the CPU can be implemented with the CFC Editor. After adding the F-DO to the hardware configuration and assigning symbolic names for the individual output channels, the evaluation logic can be implemented in the CFC Editor.

Figure 8-11 shows the activation of a redundant F-DO output in the CFC Editor. Note that in safety systems in the good state of the process a "1" signal is generally output and switched off with "0".

Figure 9-5 1oo1 with redundant F-DO CFC logic



The example logic in Figure 8-11 works as follows:

- The shutdown logic is connected to input "I" of the F-channel driver.
- If the shutdown logic signals a normal value (e.g. "1"), the output to the connected component is "1" (i.e. no shutdown).
- If the shutdown logic signals a triggering command (e.g. "0"), the output of the connected component is "0" (i.e. shutdown).

© Siemens AG 2018 All rights reserved

10 Calculating the PFD value

The PFD value for F-DI and F-DO can be found in the manual "Automation System S7-300 Fail-Safe Signal Modules" in the technical data of the SM 326 or as a download online.
References to the manual and the download can be found under \6\ and \9\.

Table 10-1 PFD value for F-DI

Fail-safe performance features		
after a service life of 20 years	1-channel	2-channel
Low demand mode (average **p**robability of **f**ailure on **d**emand) SIL 3	< 1.00E-04	< 1.00E-05

Table 10-2 PFD value for F-DO

Fail-safe performance features	
after a service life of 20 years	
Low demand mode (average **p**robability of **f**ailure on **d**emand) SIL 3	< 1.00E-05

You can find the PFD value for the F-CPU in the manual "Safety Engineering in SIMATIC S7“, or as a download online. References to the manual and the download can be found under \8\ and \9\.

Table 10-3 PFD value for F-CPU

CPU	**Order No.**	Low demand mode (average **p**robability of **f**ailure on **d**emand)	
after a service life of		10 years	20 years
CPU 410-5H	6ES7410-5HX08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 410E	6ES7410-5HM08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 410SIS	6ES7410-5FM08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 412-5H PN/DP	6ES7412-3HJ14-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 414-5H PN/DP	6ES7414-5HM06-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 416-5H PN/DP	6ES7416-5HS06-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 417-5H PN/DP	6ES7417-5HT06-0AB0	< 1.9 E-04	< 3.8 E-04

* When used in the extended temperature range up to max. 70 °C.

Table 10-44 PFD value for PROFIsafe communication

Fail-safe performance features	
after a service life of 20 years	
Low demand mode (average **p**robability of **f**ailure on **d**emand) SIL 3	< 1.00E-05*

*Note for S7-300/400 F-CPUs:
The PFDavg value is valid under the assumption that a maximum of 25 fail-safe I/Os are involved in a safety function. If more than 25 fail-safe I/Os are used, you must 3.5E-7 for each fail-safe I/O to this safety function.

© Siemens AG 2018 All rights reserved

11 Recommendations for power supply and grounding measures

This section provides guidelines on basic power supply and grounding measures for SIMATIC S7-400 F/FH systems. You can find more detailed information on this under \6\ and \7\.

11.1 Power supply

11.1.1 Infeed

The power feed should be routed to a power feed unit installed as part of the cabinet system. Note that each power feed should have an independent power feed unit. The power feed unit should have a number of terminals with overcurrent protection. To increase system availability, a circuit breaker should be used for overcurrent protection. A second power feed (which requires a second power feed unit in the cabinet) can be used for improved system availability.

The power feed unit should have a connection for each conductor of the infeed:

- Cable
- Neutral / return conductor and
- GND

The ground connection for the infeed should be marked or color coded so that it can be recognized as a ground connection. This ground connection must be connected to the housing with low resistance. The ground connection terminal should be held in place mechanically to ensure ground protection.

The infeed should have individual distribution terminals for connecting the loads in the cabinet. The distribution terminals should be grouped, each with a ground terminal for ground connections. Additional ground connections are required to ground the rack used for mounting the system components.

© Siemens AG 2018 All rights reserved

11.1.2 System power supply

The system power supply outputs cabinet-specific 24 V DC for the cabinet consumers. The system power supply should have multiple outputs with terminals for each line. The system supply should be isolated from all other ground references – as well as any load powered with system power.

System power can be supplied via a discrete power supply connected to the infeed (described in Section 11.1.1). The power supply is usually integrated per rack.

The power supply powers the controllers and I/O modules with 24 V DC. The power supply for the communication modules, as well as the communication itself, passes via the backplane bus modules. When using isolated modules, the backplane current and communication from the field I/O are galvanically isolated. This isolation has two benefits:

- Isolation of control level and field level
- Protection of the control level from noise and overvoltage

Larger systems can use the system power supply for the field level and a dedicated rack power supply for the control level. This is advantageous if the field devices require more power than what is provided by the SIMATIC standard power supplies. In such cases, the design should support redundant power supplies. Redundant power supply architectures increase system reliability in online repairs

as long as common components (such as a common line protection circuit breaker) are avoided.

System availability can also be increased by means of other technologies, such as uninterruptible power supplies or DC backup systems. The use of such technologies requires knowledge of the system (e.g. power supply buffering times, reaction of control and I/O devices to power interruption, etc.).

11.2 Grounding

11.2.1 Objective

There are three basic goals for grounding a system:

- Operator protection
- Protection against lightning or other sources of voltage peaks
- Elimination of electrical interference

The prevention of unwanted effects due to electrical interference is based on the linear ground path method. The flow of non-static electrical energy requires a loop in which the sum of the currents to a participant equals zero. To prevent the flow of currents (i.e. electro-magnetic noise), the system design should not include loops. The concept of a linear grounding (or common reference point) involves a direct connection that prevents the formation of any loops. From any point in a system with ground connection, there should be only one path leading from that point to the grounding point.

The linear grounding method is limited when using distributed process control systems. A distributed system is a system in which components are distributed locally in a plant. In this type of architecture, the linear grounding method can be efficiently applied to system components called units (functions) (or isolation islands). A unit can be defined as follows:

- Galvanic isolation of other units
- Physical separation of other units (functions), so that electrical disturbances are diverted locally

In systems with units, each part uses a local, linear ground bar to reduce lightning and electronic noise.

© Siemens AG 2018 All rights reserved

11.2.2 Implementation

The grounding recommendations given in this section are specific to cabinets with power supplies that supply system components with 24 VDC. The grounding rules are simplified by placing the system supply in the individual cabinets. If the energy is shared between the cabinets, the equipment should be in the immediate vicinity to keep a single grounding reference point and maintain connections. A system with a centralized power supply should be located within a lightning protection zone (usually within a building or construction). For all systems outside a common lightning protection zone, isolation techniques should be used to reduce the susceptibility to interference. Typical isolation barriers include local power supplies, optical communication for data highways, and potential-isolated signal transmission techniques (e.g. relay contacts, etc.).

Grounding

The cabinet design should keep the energy supply separate from other access openings. The electric current should be connected to a single distribution unit within the cabinet. As part of the power feed unit, there should be a connection point for the cabinet grounding. This connection should include the necessary conductors for the proper operation of the protection device and for operator protection. The GND connection of the cabinet should be marked or color-coded. If multiple current sources are used (e.g. for redundancy), independent power feed units should be used and each current source should have its own cabinet ground connection.

© Siemens AG 2018 All rights reserved

Shield terminations

Field wiring shield terminations should be standard for I/O modules. The physical terminations for shielding should be provided at the termination location of the field signal wires, referred to as a shielding bus. The shielding bus should be isolated from mounting plates or rail assemblies within cabinets. Shielding buses must accommodate a ground connection. The ground connection connects a shielding bus to the local equal potential ground bar (LEPG).

To complete the shield installation, the LEPG bar must be connected to a ground reference. The ground is preferably connected to a grounding system, which is also used for grounding the neutral conductors of the power supply system. Most industrial plants support a centralized grounding point for connecting "locally" diverted grounding systems. The connection to ground reference should be as follows:

- Low impedance (0.5 ohms or less)
- As short a physical path as possible
- Separate and independent from the safety ground connections required for operator protection

Note that the grounding of shields at one location provides protection from low frequency noise encountered in industrial environments. Care should be taken to ensure no other connections to ground occur for shields.

DC grounding

Power supplies are typically installed in the cabinets to supply the operating voltage of 24 V DC. The power supplies have no connection to ground or power feeds. Depending on the user requirements, the system works in either an ungrounded mode (floating) or connected to a user-specified reference point.

System configuration

S7-400 F/FH systems (including controllers and I/O modules) can work in grounded or ungrounded mode. To accommodate both operating modes, the system configuration includes a jumper that creates a reference potential to ground connection. When the jumper is removed, the reference potential is disconnected from the housing ground.
Depending on the product, the bridge is either part of the assembly (see Figure 11-1) or the system backplane (see Figure 11-2).

Figure 11-1 Jumper installation location on IM-153 (ET 200M connection)

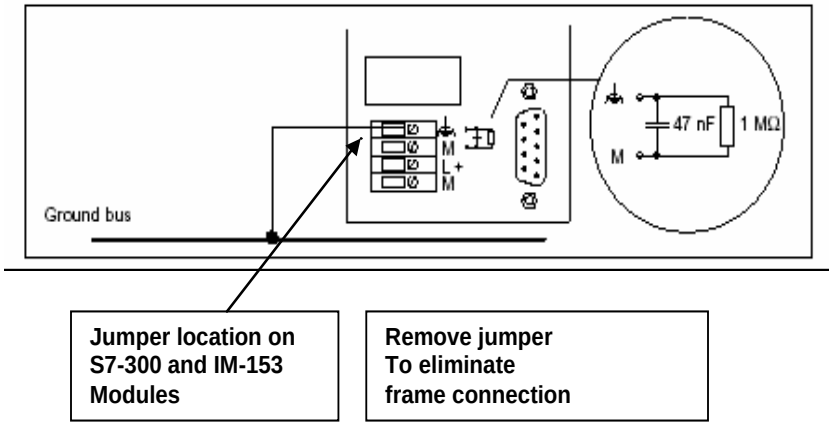
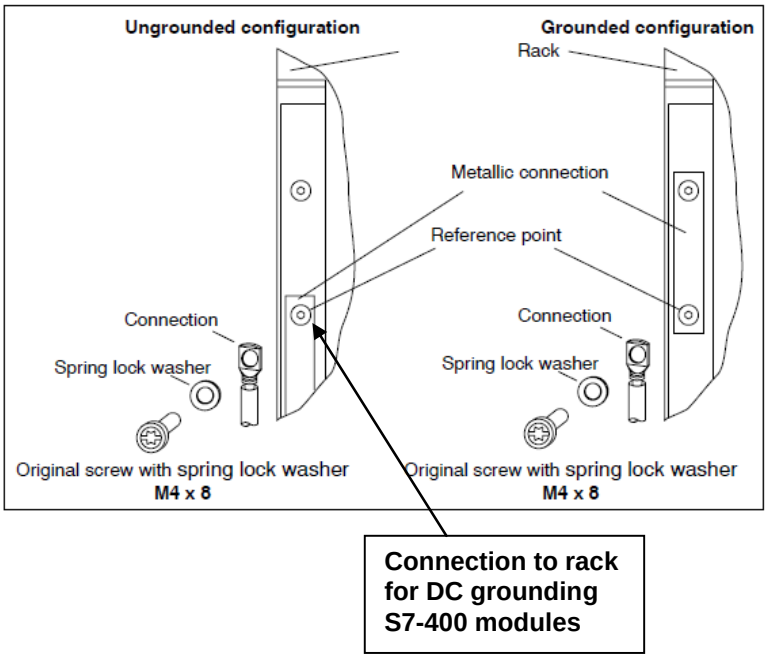


Figure 11-2 Grounding location for S7-400 module racks



© Siemens AG 2018 All rights reserved

12 Marshalled Termination Assemblies (MTA)

12.1 F-DI Marshalled Termination Assemblies (MTA)

Siemens offers MTAs (Marshalled Termination Assemblies) and preconfigured cables for easy connection of field devices to ET 200M signal modules. The MTA for the F-DI simplifies wiring between sensors and the F-DI.

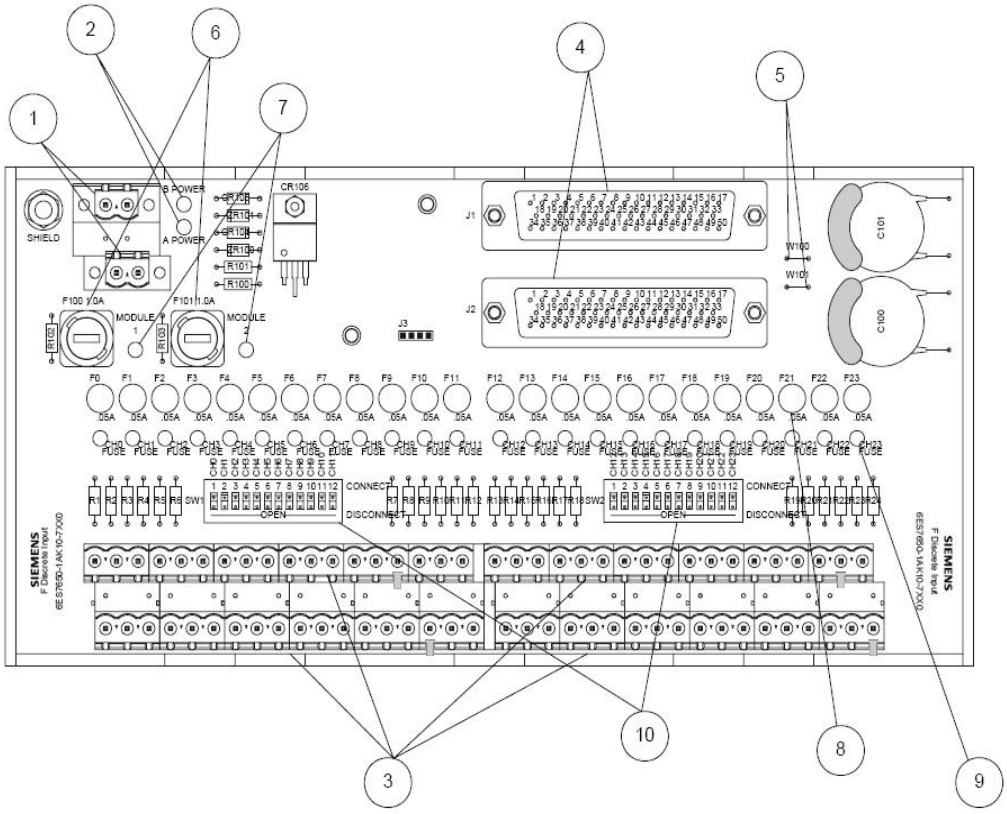
The Order Number for the current version of the F-DI MTA is:
6ES7 650-1AK11-7XX0.

The F-DI MTA in Figure 12-1 contains the following features:

- Redundant power connections
- LED display of the redundant power supply
- Power-Monitor plug-in (optional)
- Dual plug for redundant signal module operation
- Current fuse per module
- LED display of the power supply to the field device based on individual channels
- Fuse of field voltage per channel
- Interruptions per channel
- Shield connections available for the channel cabling
- Grounding stud for shield connection with earth
- Plug connections for connecting the power supply and field devices for easy maintenance

© Siemens AG 2018 All rights reserved

Figure 12-1 F-DI MTA - layout

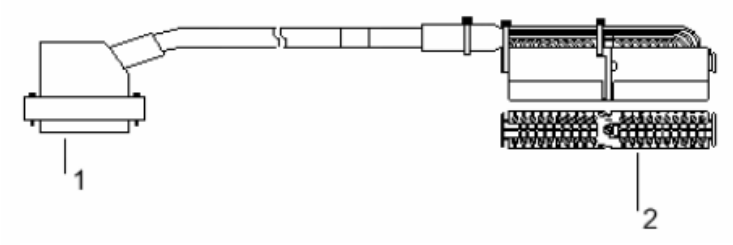


Item	Description
1	Input power connections
2	Input power indicators
3	Field wiring connections
4	I/O module connections
5	Shield disconnect jumpers (W100 & W101)
6	Module power fuses
7	Module power indicators
8	Channel power fuse (1 of 24)
9	Channel power indicator (1 of 24)
10	Channel power disconnect switches (SW1 & SW2)

The F-DI MTA and the F-DI are connected to each other by means of a prefabricated connection cable. The custom length cable is shown below in Figure 12-2. The connection cable from the F-DI MTA to the F-DI is shown in Figure 8-3.

© Siemens AG 2018 All rights reserved

Figure 12-2 F-DI MTA - connecting cable



Item	Part Name
1	50-pin Female Sub-D connector
2	40-pin Siemens connector (6ES7 392-1AM00-0AA0)

Figure 12-3 F-DI MTA - connection to F-DI

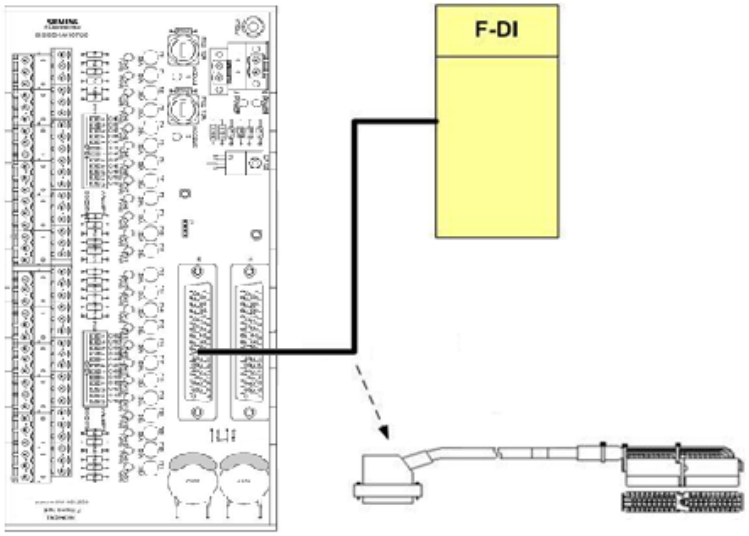
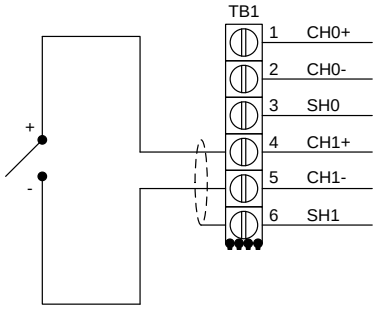


Figure 12-4 illustrates an example of how to wire a 2-wire sensor to the F-DI MTA. For evaluation architectures that use redundant modules, a second connection cable is connected to the corresponding connector on the MTA.

Figure 12-4 F-DI MTA - connection for a 2-wire sensor



For more information about F-DI MTA (including power connections, power monitoring, fuses, and software configuration settings in PCS 7), see \3\.

© Siemens AG 2018 All rights reserved

12.2 F-DO Marshalled Termination Assemblies (MTA)

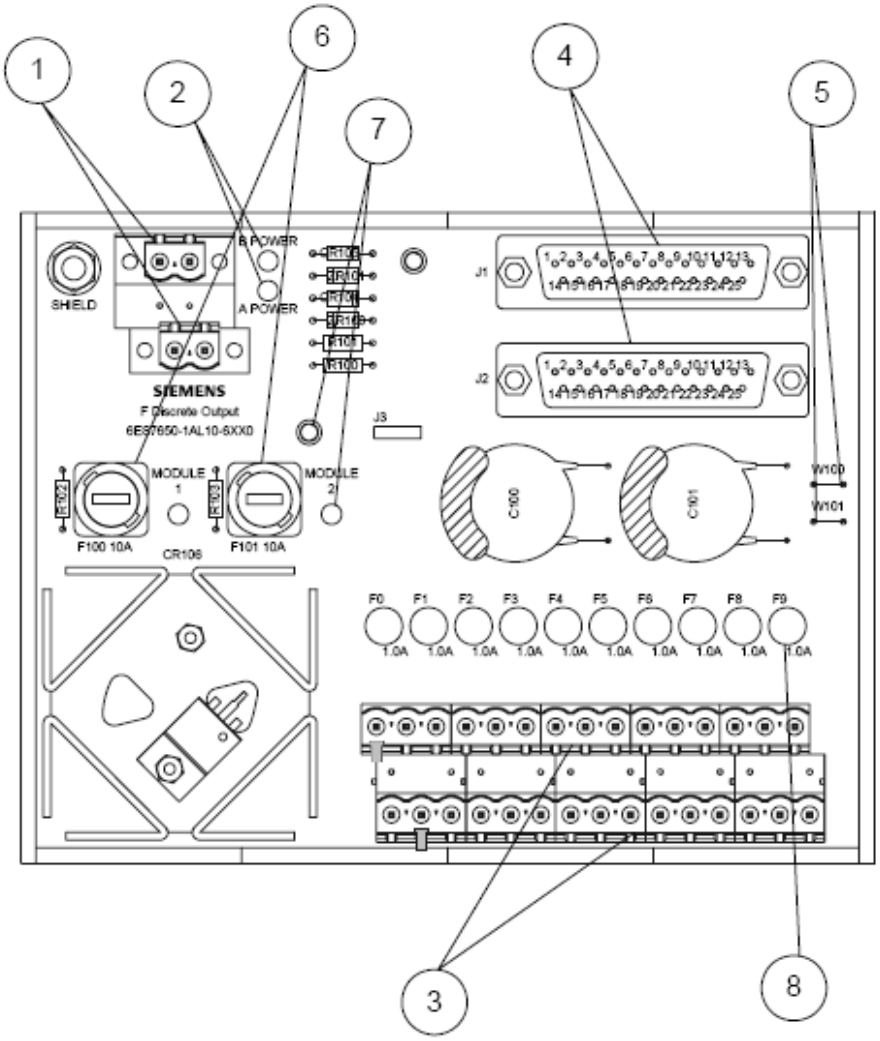
The MTA for the F-DO simplifies the wiring between the F-DO and the actuators. The Order Number for the current version of the F-DO MTA is: 6ES7 650-1AL11-6XX0.

The F-DO MTA in Figure 12-5 contains the following features:

- Redundant power connections
- LED display of the redundant power supply
- Power-Monitor plug-in (optional)
- Dual plug for redundant signal module operation
- Current fuse per module
- Fuse of field voltage per channel
- Shield connections available for the channel cabling
- Grounding stud for shield connection with earth
- Plug connections for connecting the power supply and field devices for easy maintenance

© Siemens AG 2018 All rights reserved

Figure 12-5 F-DO MTA - layout

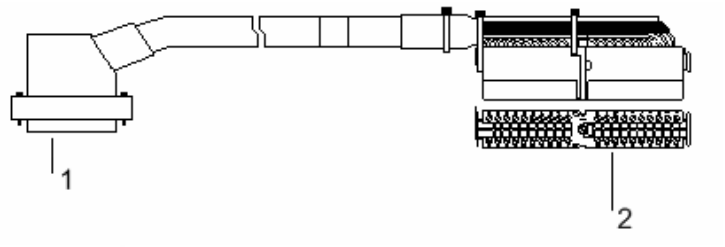


Item	Description
1	Input power connections
2	Input power indicators
3	Field wiring connections
4	I/O module connectors
5	Shield disconnect jumpers (W100 & W101)
6	Module power fuses
7	Module power indicators
8	Channel power fuse (1 of 10)

The F-DO MTA and the F-DO are connected to each other by means of a pre-assembled connecting cable. The custom length cable is shown below in Figure 12-6. The connection from the F-DO MTA to the F-DO is shown in Figure 12-7.

© Siemens AG 2018 All rights reserved

Figure 12-6 F-DO MTA - connecting cable



Item	Part Name
1	25-pin Female Sub-D connector
2	40-pin Siemens connector (6ES7 392-1AM00-0AA0)

Figure 12-7 F-DO MTA - connection to F-DO

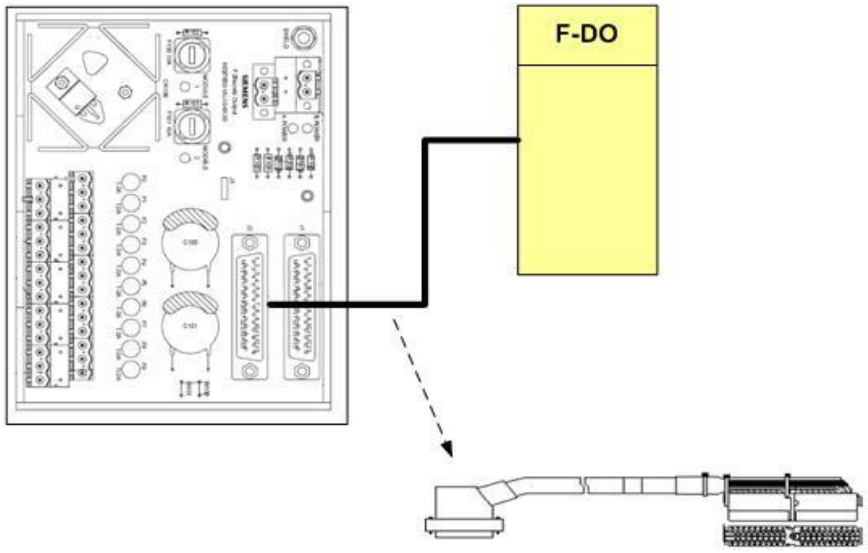
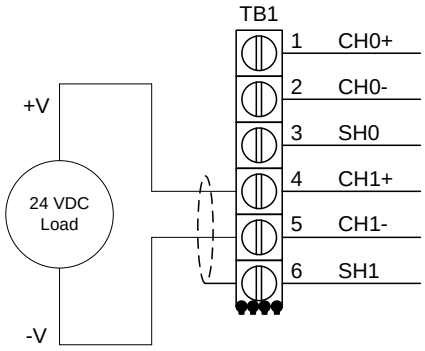


Figure 12-8 shows F-DO MTA wiring for load connection to the field connection. For evaluation architectures that use redundant modules, a second connection cable is connected to the corresponding connector on the MTA.

Figure 12-8 F-DO MTA - load connection to field connection



For more information about F-DO MTA (including power connections, power monitoring, fuses, and software configuration settings in PCS7), see \3\.

© Siemens AG 2018 All rights reserved

13 Appendix

13.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, and application examples – all the information you need is accessible with just a few mouse clicks at:
https://support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

You send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

Service offer

Our range of services includes, inter alia, the following:

- Product trainings
- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

© Siemens AG 2018 All rights reserved

13.2 Links and literature

Table 13-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/37236961
\3\	ET 200M Marshalled Termination Assemblies Remote I/O Modules https://support.industry.siemens.com/cs/ww/en/view/22091986
\4\	SIMATIC Configuring Hardware and Communication Connections STEP 7 https://support.industry.siemens.com/cs/ww/en/view/109751824
\5\	SIMATIC Industrial Software Safety Matrix https://support.industry.siemens.com/cs/ww/en/view/100675874
\6\	SIMATIC Automation System S7-300 ET 200M Distributed I/O Device Fail-safe signal modules https://support.industry.siemens.com/cs/ww/en/view/19026151
\7\	Automation System S7-400 Hardware and Installation https://support.industry.siemens.com/cs/ww/en/view/1117849
\8\	SIMATIC Industrial Software Safety Engineering in SIMATIC S7 https://support.industry.siemens.com/cs/ww/en/view/12490443
\9\	Which values can you use with F CPUs and products of the ET 200 family for PFD and PFHD? https://support.industry.siemens.com/cs/ww/en/view/27832836
\10\	SIMATIC S7 F Systems: Execution times of fail-safe blocks, runtime of the F shutdown group, monitoring and response times https://support.industry.siemens.com/cs/ww/en/view/22557362
\11\	SIMATIC Industrial software S7 F/FH Systems - Configuring and Programming https://support.industry.siemens.com/cs/ww/en/view/109742100

© Siemens AG 2018 All rights reserved

13.3 Change documentation

Table 13-2

Version	Date	Modifications
V1.0	01/2010	First version
V2.0	07/2018	Complete revision