SIEMENS
Ingenuity for life

Wiring and Voting Architectures for failsafe Analog Input Modules (F-AI) of the ET 200M

SIMATIC Safety Integrated for process automation

https://support.industry.siemens.com/cs/ww/en/view/24690377

Siemens Industry Online Support

Warranty and liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

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

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

Table of Contents

1 Automation functions

1.1 Functionality of the functional example

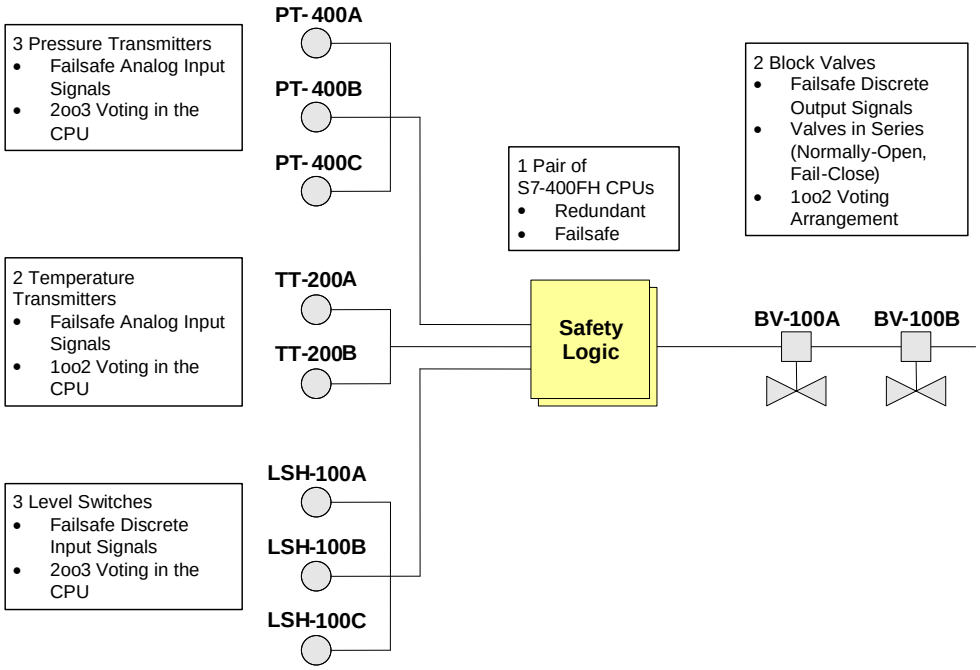
Task

Several analog signals in a system are to be monitored in a safety-oriented manner. Depending on the importance and risk of failure, there are several ways to wire and evaluate the signals. For instance, the evaluation can be performed in the analog input module and/or in the user program.

Fig. 1-1 illustrates an example of a plant unit, in which the valves (BV-100A and BV-100B) require fail-safe closing, depending

- on pressure,
- the filling level and
- the temperature.

Fig. 1-1: Example 1 - overview

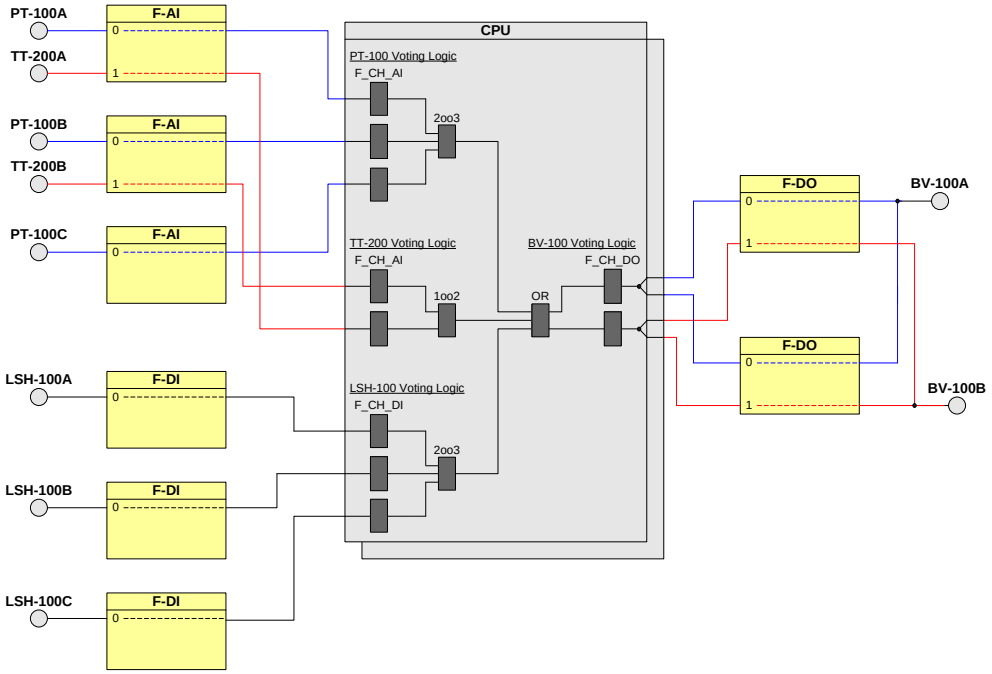


This functional example shows various possibilities of wiring and evaluating safety-related signals.

Solution

Fig. 1-2 illustrates a plausible plant unit layout, in which different connection and evaluation architectures of the analog signals are used.

Fig. 1-2: Example 1 – system configuration



Note

The fail-safe analog input module SM 336; F-AI 6 x 0/4 ... 20 mA HART with order number 6ES7 336-4GE00-0AB0 is used in all functional examples. This is hereafter referred to as F-AI.

1.2 Presented architectures

Recommended Architectures

The following architectures are presented in this Application Example:

- **One sensor (1oo1) and one F-AI (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-AI (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-AI with evaluation in the F-AI (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-AI with evaluation in the F-AI (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-AI (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 as redundant F-AI (2oo2) for increased availability (explained in Chapter 7).
- **Three sensors (2oo3) with evaluation in the user program**
  Typical application when several sensors are required in order to achieve the required safety integrity level and there is a desire for increased availability (explained in Chapter 8 and Chapter 9).

1.3 Properties for the fail-safe analog input module

Properties of the F-AI

- 6 analog inputs with galvanic isolation between channels and the backplane bus
- Input ranges:
  - 0 to 20 mA
  - 4 to 20 mA
- Short-circuit proof power supply of 2 or 4-wire transmitter via the module
- External sensor supply possible
- Group fault display (SF)
- Safety mode display (SAFE)
- Display for channel-specific fault (Fx)
- Display for HART status (Hx) (if you have activated HART communication for a channel and HART communication is running, the green HART status display lights up.)
- Programmable diagnostics
- Programmable diagnostic interrupt only in safety mode
- SIL3/Cat.4/PLe can be achieved without safety protector
- HART communication
- Firmware update using HW Config
- Identification data I&M
- Can be used with PROFIBUS DP and PROFINET IO

Use of inputs

You can use the inputs as follows:

- Each of the 6 channels for current measurement
  - 0 to 20 mA (without HART utilization)
  - 4 bis 20 mA (with/without HART utilization)
  - Functional range of HART communication: 1.17 to typ. 35 mA

Connection diagrams of the F-AI

The following pictures provide an overview of the address and terminal assignments of the F-AI (SM 336) considered in this document.

Fig. 1-3: SM 336 address assignment; F-AI 6 x 0/4...mA HART

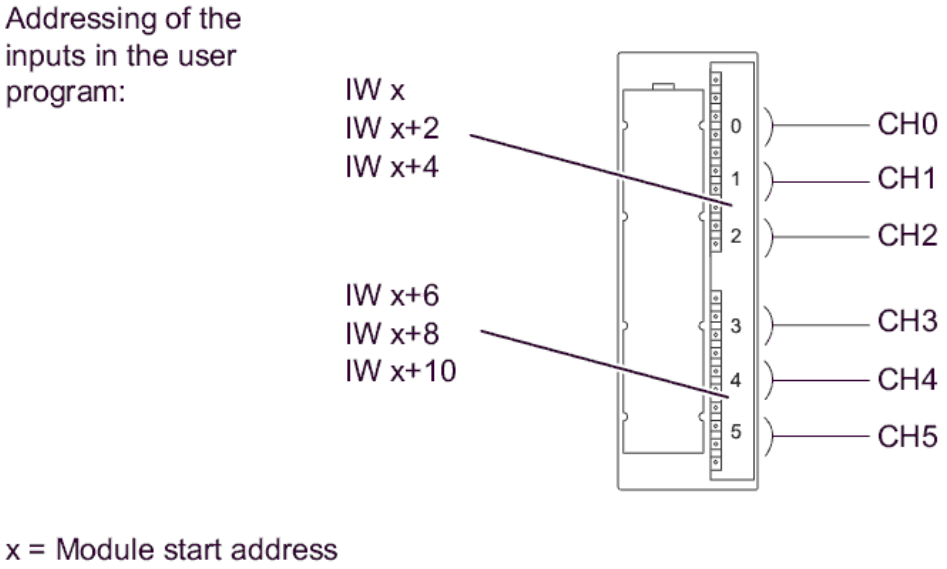


Fig. 1-4: SM 336 front view; F-AI 6 x 0/4...mA HART

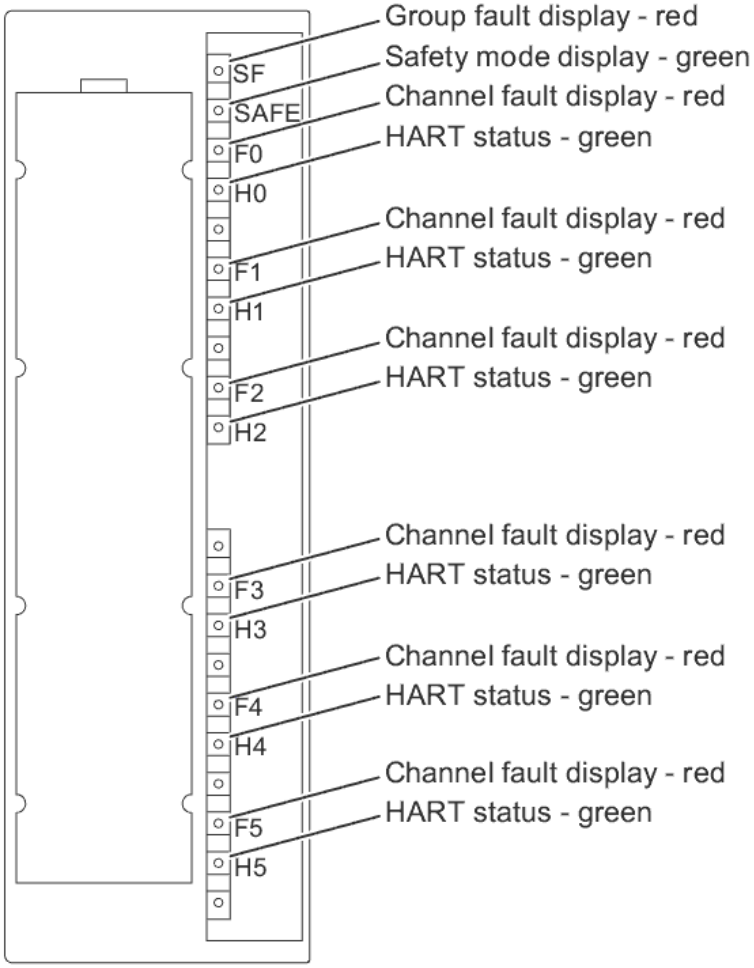


Fig. 1-5: SM 336 connection and basic circuit diagram; F-AI 6 x 0/4...mA HART

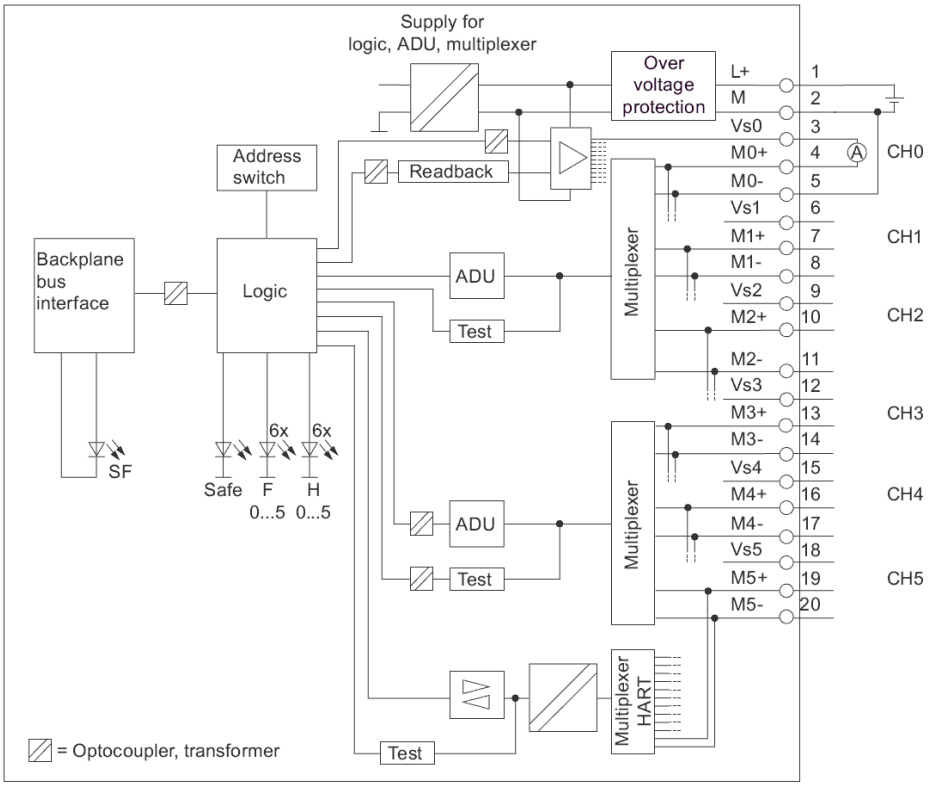
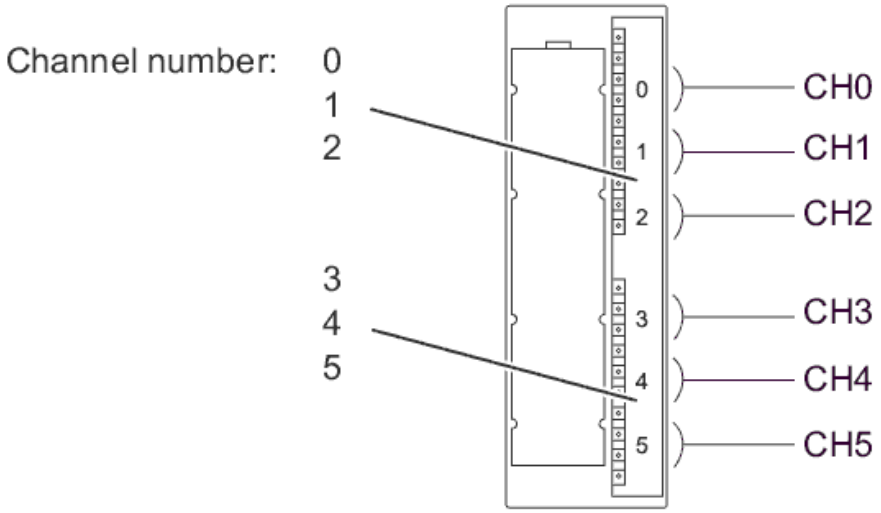


Fig. 1-6: SM336 channel numbers; F-AI 6 x 0/4...20mA HART



Recommendation

You are strongly advised to use the short-circuit proof **internal** sensor supply of the module. This internal sensor supply is monitored and its status is indicated by the Fx LED (see picture: Front view of SM 336 front view; F-AI 6 x 0/4 ... 20 mA HART).

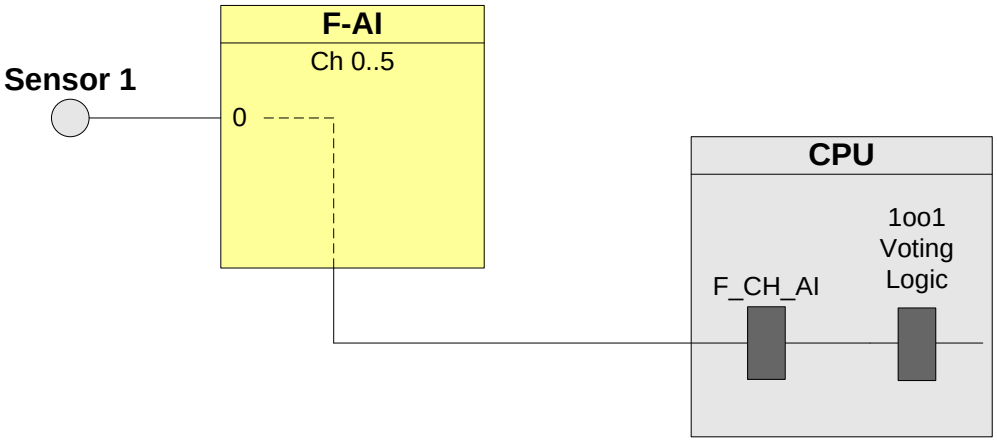
2 Hardware configuration and wiring of one sensor (1oo1) and one F-AI (1oo1)

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 indicates a trigger condition, the safety logic is triggered.

Note The I/O module in this architecture is 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.

In the 1oo1 basic architecture, one sensor is wired to one F-AI channel (in Fig. 2-1 on Channel 0).

Fig. 2-1: F-AI – 1oo1 architecture



With a hardware configuration according to Fig. 2-1, 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 2-1: Failure combinations

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

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 and evaluation architecture is calculated using this formula:

$$PFD_{In} = PFD_{Sensor} + PFD_{F\text{-}AI} + PFD_{CPU}$$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

2.2 Wiring

2.2.1 Conventional wiring

In the 1oo1 evaluation scheme, the sensor can be supplied with voltage as follows:

- **internally** through the F-AI or
- via an **external** voltage source

Internal power supply

Special features of the F-AI with internal power supply include:

- The short-circuit between sensor supply voltage Vsn and Mn+ is controlled.
- It is possible to detect undervoltage from the transmitter by reading back the sensor supply in the F-AI.

Wiring examples

illustrates a wiring example for a 2-wire transmitter.

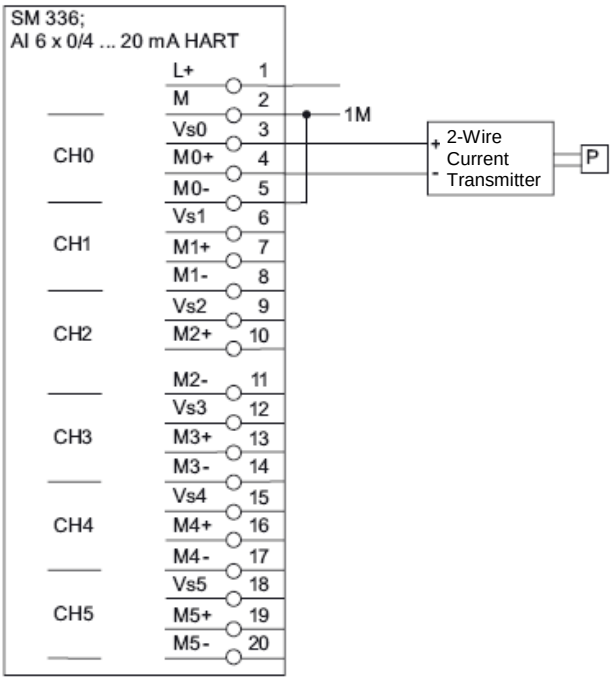
Fig. 2-3 illustrates a wiring example for a 4-wire transmitter.

In both figures, the transmitter is wired to channel 0 (terminals 3, 4, 5) and is powered by the F-AI.

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

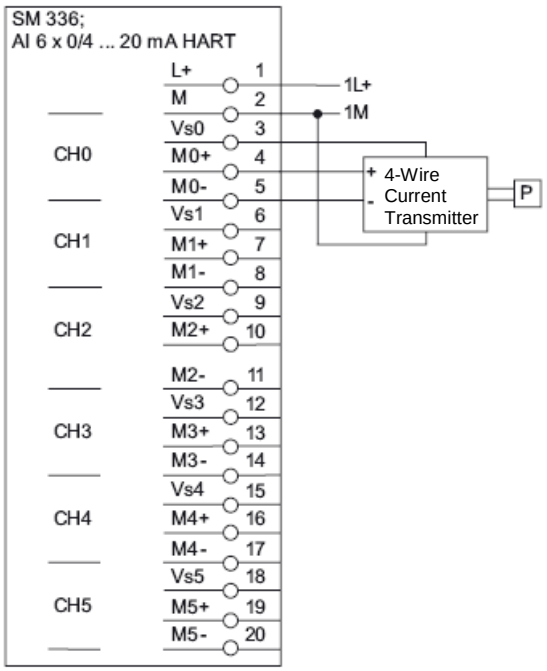
Wiring example for a 2-wire transmitter

Figure 2-2: Wiring for a 2-wire transmitter (internal sensor supply)



Wiring example for a 4-wire transmitter

Fig. 2-3: Wiring of a 4-wire transmitter (internal sensor supply)

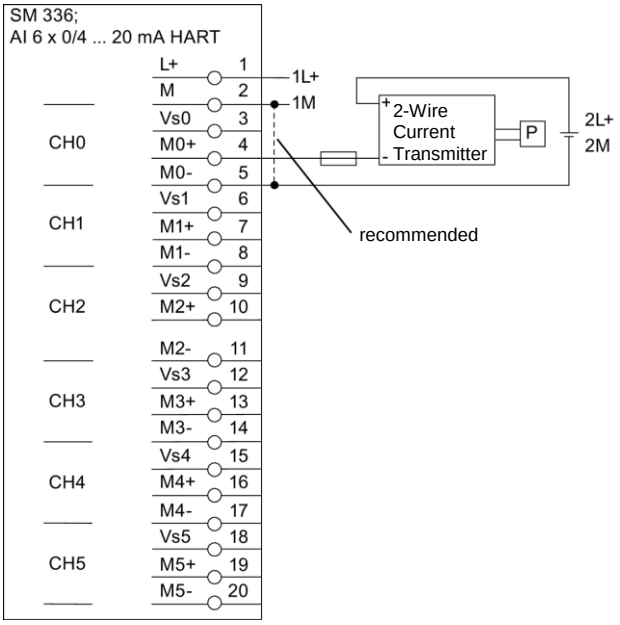


External power supply (2-wire transmitter)

Fig. 2-4 illustrates an external voltage source on a 2-wire transmitter. The sensor is wired to Channel 0 (terminals 4, 5). It is recommended to connect the M potentials together.

CAUTION	**The F-AI cannot detect an under-voltage in the transmitter. Therefore, you should use transmitters with under-voltage detection.**

Fig. 2-4: Wiring of a 2-wire transmitter (external sensor supply)

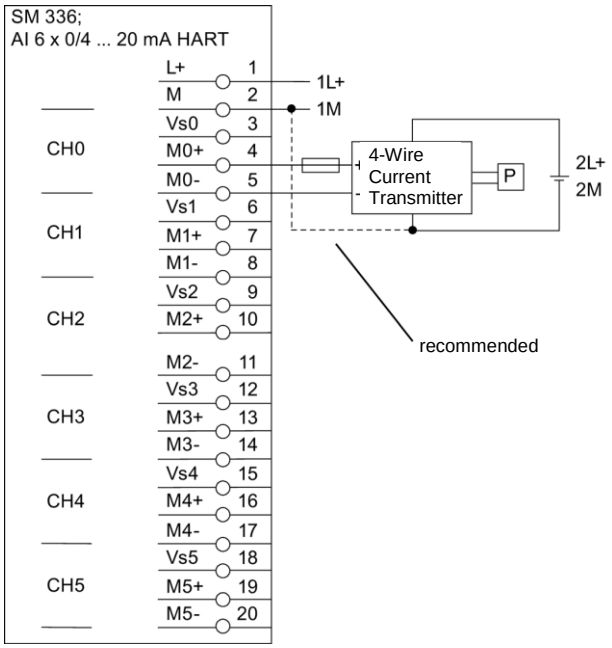


External power supply (4-wire transmitter)

Figure 2-5 illustrates an external voltage source with a 4-wire transmitter. The sensor is wired to Channel 0 (terminals 4, 5). It is recommended to connect the M potentials together.

CAUTION	**The F-AI cannot detect an under-voltage in the transmitter. Therefore, you should use transmitter with under-voltage detection.**

Fig. 2-5: Wiring of a 4-wire transmitter (external sensor supply)

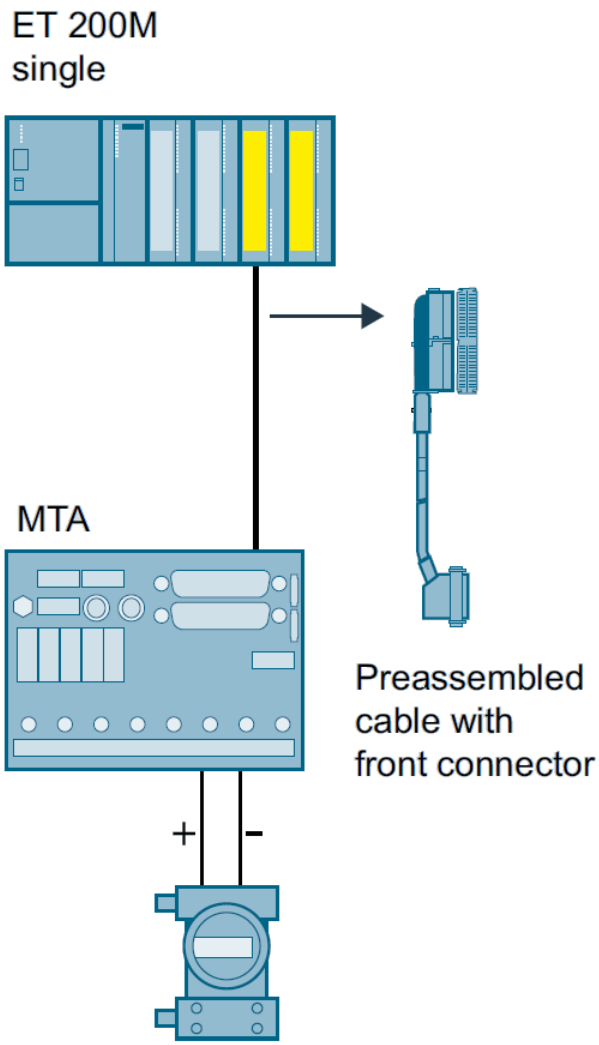


2.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

Fig. 2-6: MTA



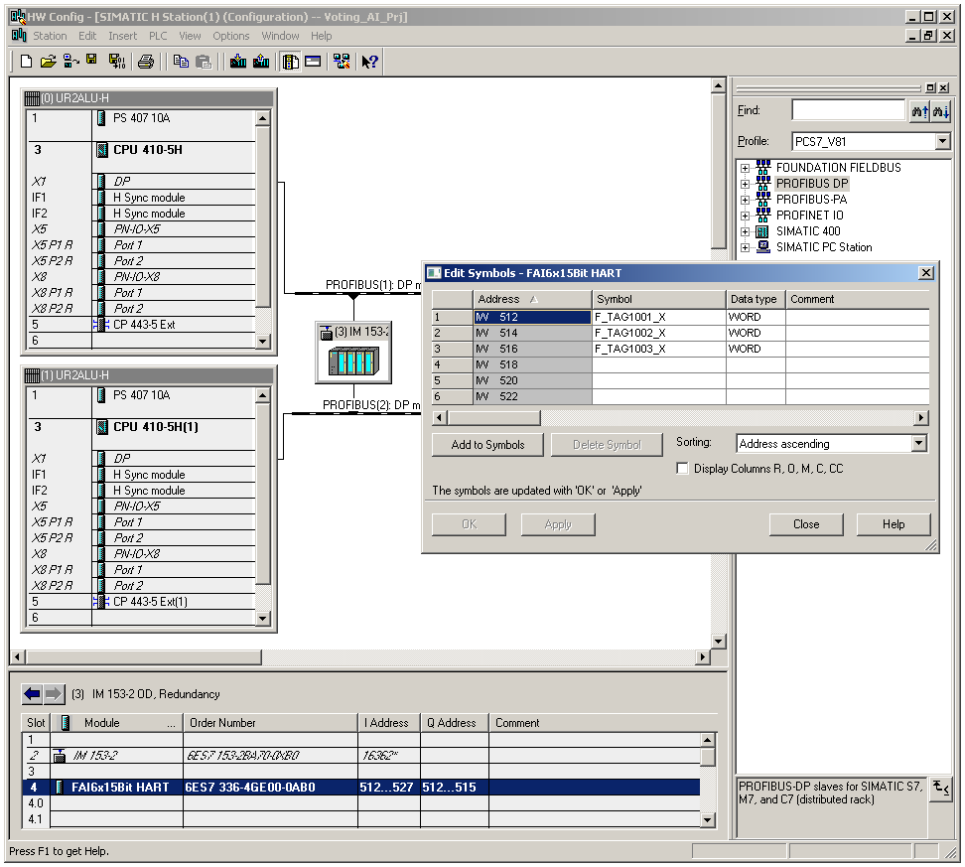
2.3 Parameters for hardware configuration

To configure, select the F-AI in the STEP 7 hardware catalog and add it into an existing ET 200M station. Select meaningful icon names for the analog channels in order to facilitate later configuration.

You can find an example for a hardware configuration using an F-AI in Fig. 2-7. The sensor signal in this example is wired to Channel 0 of the F-AI. Please note that the use of an F-AI MTA is not taken into account in the hardware configuration.

For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 2-7: Symbol processing



The required parameters for operating the F-AI are set in the object properties of the F-AI added (see Fig. 2-8).

The parameters are summarized in Table 2-2.

Fig. 2-8: Hardware parameters

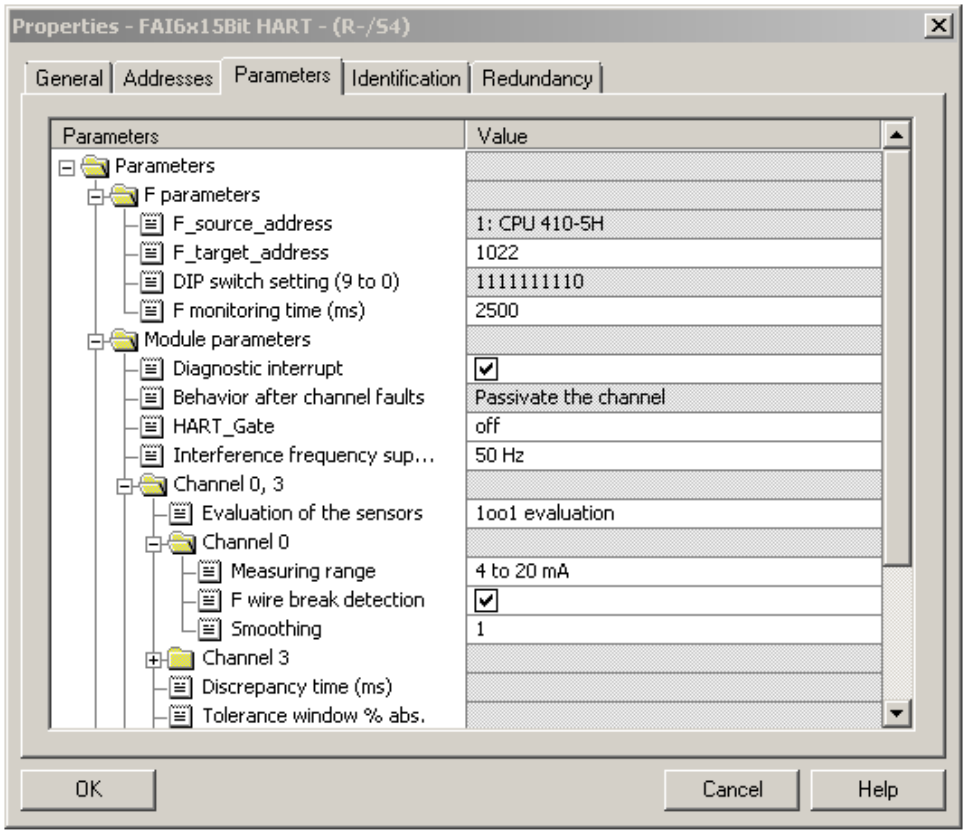


Table 2-2: Hardware configuration parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
F-parameters		
F_destination_address	PROFIsafe address of the F-signal module (setting via DIP switch).	1-1022 or 0000000001... 1111111110
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-AI. **Remark:** A worksheet is available on the Siemens Support website to help users calculate F-monitoring times (see \10\ in the "Links and Literature" chapter).	0...65535ms Default 2500ms

Parameter	Description / Recommendations	Desired setting or permissible value range
Module parameters		
Diagnostic interrupt	A diagnostic interrupt is triggered by various error events that can be detected by the module. These events are then reported to the CPU. **Remark:** If the diagnostic interrupt is released at the module level, individual diagnostic events must be also activated at the channel level.	Release / lock
Behavior after channel faults	Passivate the entire module/ passivate the channel. **Remark:** Irrelevant for F systems	Module/ Channel
HART_Gate	Acts as a fail-safe "main switch" across the modules. HART communication is blocked with "Off". HART communication is enabled with "On". The HART modem can be switched out of the safety program for maintenance purposes with "switchable".	Off/ On/ switchable
Noise suppression (Hz)	Selection for matching the integration time of the ADC to the network used. The integration time is: - 20 ms at 50 Hz - 16.66 ms at 60 Hz	50/60 Hz
Evaluation of the sensors	Channel activation by specifying the encoder evaluation. - Deactivated - 1oo1 (1v1) - 1oo2 (2v2) If 1oo1 is selected, the following parameters are not available: - Discrepancy time - Tolerance range - Unit value	1oo1 (1v1)
Measuring range	Measuring range selection for the channel.	0...20 mA 4...20 mA
F_wire-break detection	Select whether or not to enable wire break monitoring for the channel.	Release / lock
Smoothing	Number of measuring cycles through which smoothing is carried out.	1, 4, 16, 64

Note The hardware parameters and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

2.4 Configuring the logic

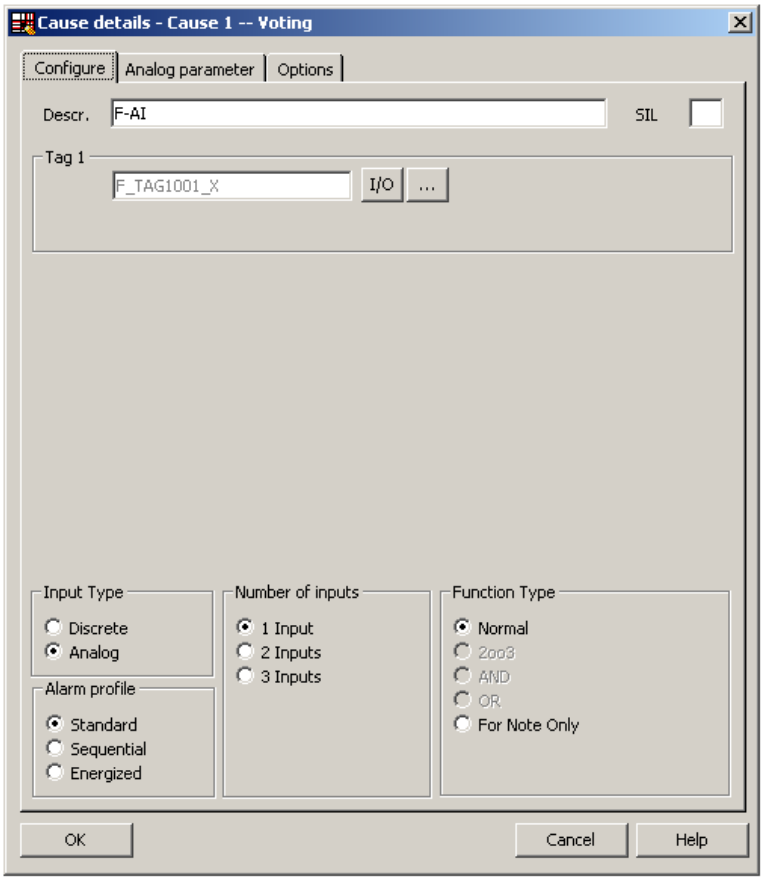
2.4.1 Configuring with Safety Matrix

Once the hardware has been configured, you can deploy the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

Fig. 2-9 illustrates how a cause for monitoring an input TAG is configured in the Safety Matrix. The following settings must be used:

- Input Type: Analog
- 1 input
- Function type: Normal (1oo1 evaluation)
- Enter the signal name in Tag 1 (e.g. F_TAG1001_X) or press the "I/O" button to select the symbol from the symbol table.

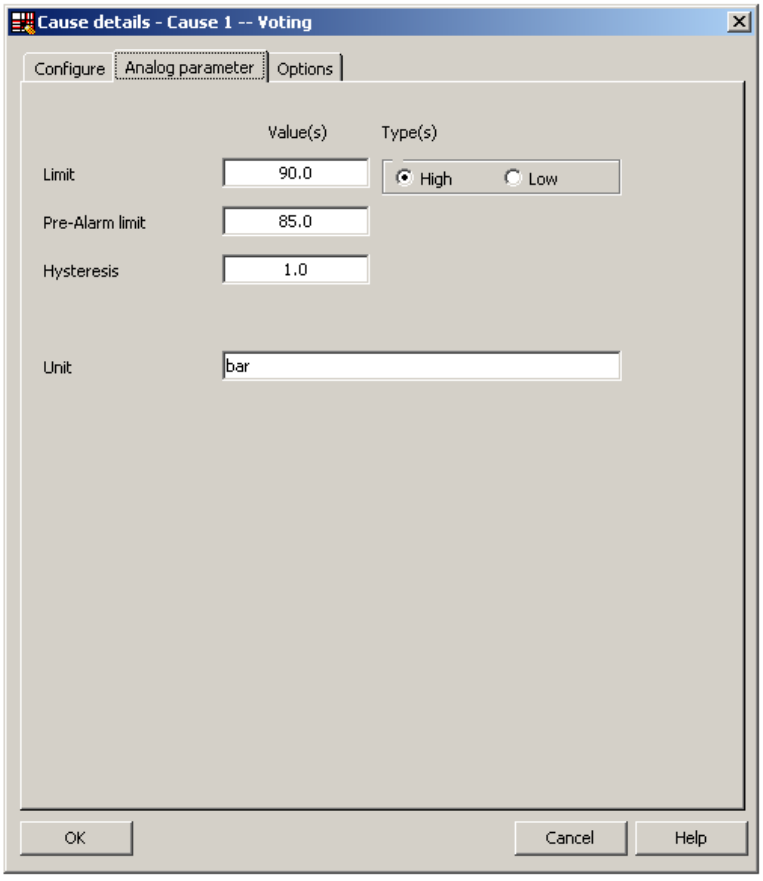
Fig. 2-9: Safety Matrix – Configure



As shown in Fig. 2-10, there are additional analog parameters that must be configured for the cause:

- Required parameters:
  - Limit type: MAX or MIN
  - Limit value
- Optional parameters:
  - Pre-alarm
  - Hysteresis
  - Units:

Fig. 2-10: Safety Matrix - Analog parameter

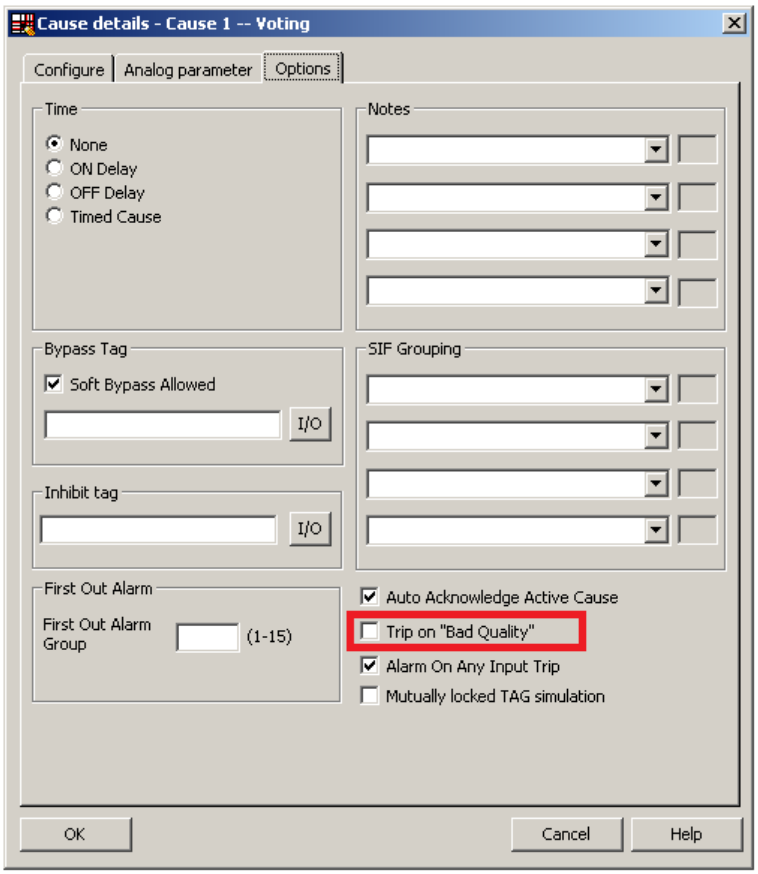


If the input TAG goes below or above the limit, the cause activates and triggers the corresponding effect(s).

You can also activate additional options (e.g. time delay and bypass option), depending on the process application.

One configuration option highlighted in Fig. 2-11 is the disconnection in case of a channel fault. If this option is activated, a channel fault will act as a violation of the limit and trigger the corresponding effect(s) on a 1oo1 (Function Type: Normal).

Fig. 2-11: Safety Matrix – Options



2.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can also implement the CPU logic for reading the input signal by means of the STEP 7 CFC Editor.

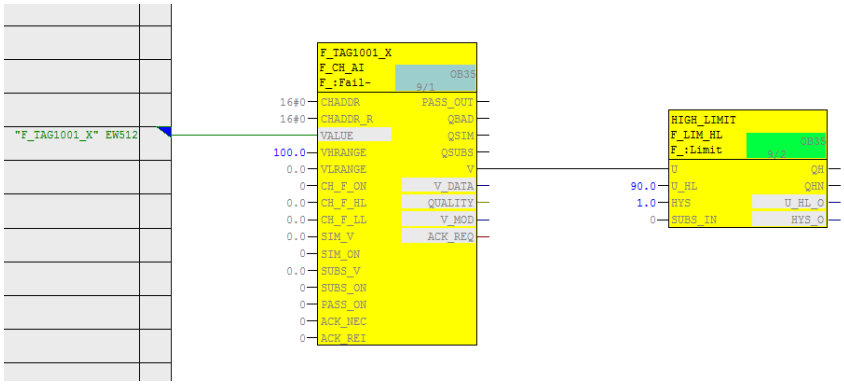
There are two ways to implement the CFC logic:

- Without channel fault evaluation
- With channel fault evaluation

Logic without channel fault evaluation (1oo1)

Fig. 2-12 illustrates an example logic created in the CFC Editor for reading an input signal that does not take a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 2-12: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the configuration shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

The example logic in Fig. 2-12 works as follows:

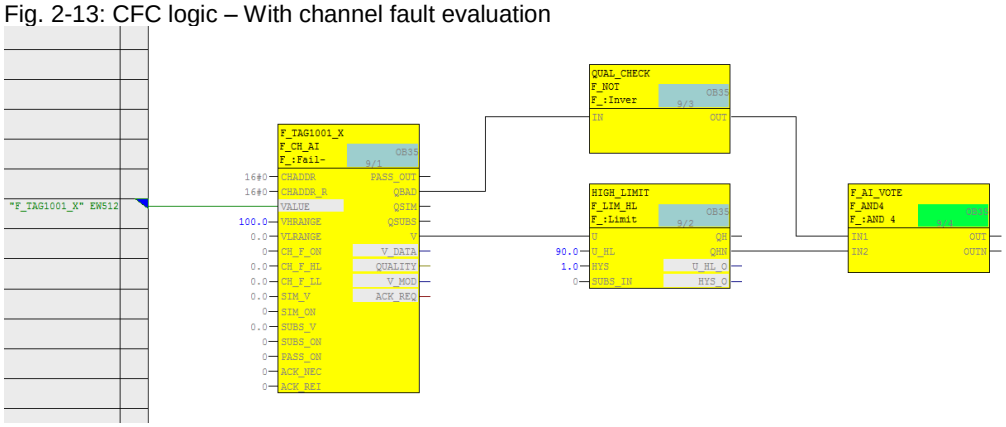
- If the process value is in the normal range (in this case, lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value exceeds the limit (in this case, greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

To create the logic, create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol or address of the sensor connected to the F-AI (e.g. F_TAG1001_X). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.

Logic with channel fault evaluation

Fig. 2-13 illustrates a sample logic created in the CFC Editor for reading a single input signal that takes a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 2-13: CFC logic – With channel fault evaluation



The example logic in

Fig. 2-13 works as follows:

- In the normal range (here: lower than 90) and with an undisturbed process value, the output of the evaluation logic is 1 (i.e., no trigger command).
- In case of upper limit violation (here: greater than or equal to 90) and with an undisturbed process value, the output of the evaluation logic is 0 (i.e., trigger command).
- If there is a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI channel driver for the analog input signal and connect it to the address of the sensor connected to the F-AI (e.g. F_TAG1001_X). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the following signals in order to generate the signal for the trigger command:
  - Negated value of the limit module (QHN or QLN)
  - Negated value of the channel fault output (QBAD) from the channel driver block

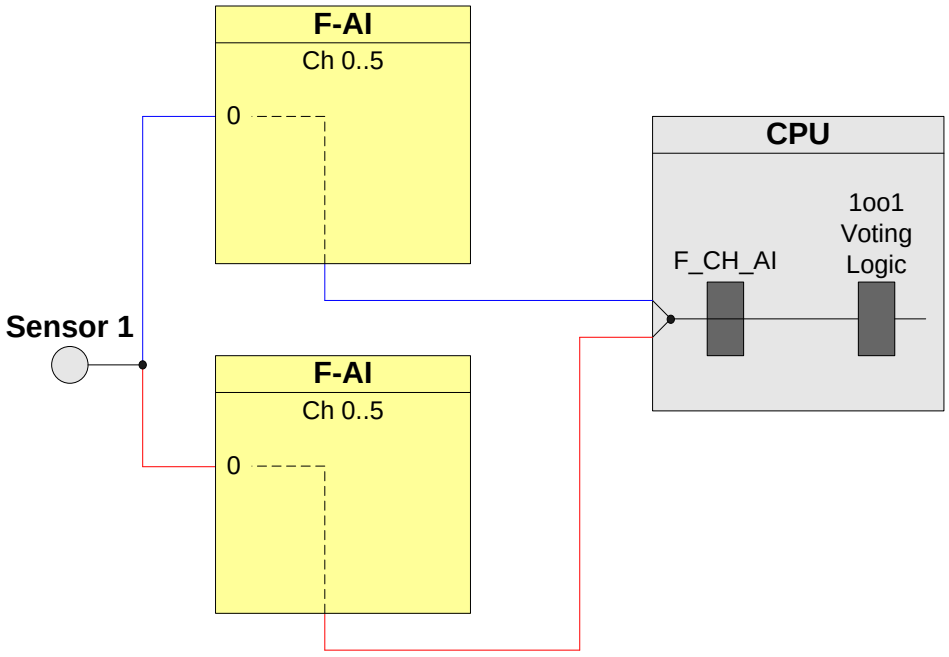
3 Hardware configuration and wiring of one sensor (1oo1) with redundant F-AI (2oo2)

This architecture increases the availability of the system by means of redundant F-AI modules. The CPU performs a 2oo2 evaluation of the signals from the F-AI.

Note The I/O modules in this architecture are certified for achieving the safety integrity level of **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

In this architecture, a single sensor is wired to a redundant F-AI. A block diagram is shown in Figure 2-17.
In Fig. 3-1, the sensor on Channel 0 is wired to both F-AIs. The F-AIs are configured as redundant in the hardware configuration. Only one analog F-channel driver is required. The F-channel driver chooses from the incoming analog signals.

Fig. 3-1: Redundant F-AI – 1oo1 architecture



With a hardware configuration according to Fig. 3-1, 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 3-1: Failure combinations

Failed component detected?			Tripping of the safety function possible?
Sensor 1	**F-AI 1**	**F-AI 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 I/O modules 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 safety function.

PFD calculation formula

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

$PFD_{In} = PFD_{Sensor} + 2\ PFD_{F\text{-}AI} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

3.2 Wiring

3.2.1 Conventional wiring

An example for the 1oo1 evaluation scheme with redundant F-AI can be found in Fig. 3-2 and in Fig. 3-3. The sensor is wired to Channel 0 (terminals 3, 4, 5) of both F-AIs.

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

Special feature

- The short-circuit between sensor supply voltage Vsn and Mn+ is controlled.
- It is possible to detect undervoltage from the transmitter by reading back the sensor supply in the F-AI.
- It is necessary to include the external elements in the application-specific safety consideration, i.e.: the external elements required for implementing the redundancy (e.g. Zener diodes) must be included in the safety consideration).

Fig. 3-2: A 2-wire transmitter, internal sensor supply with module redundancy

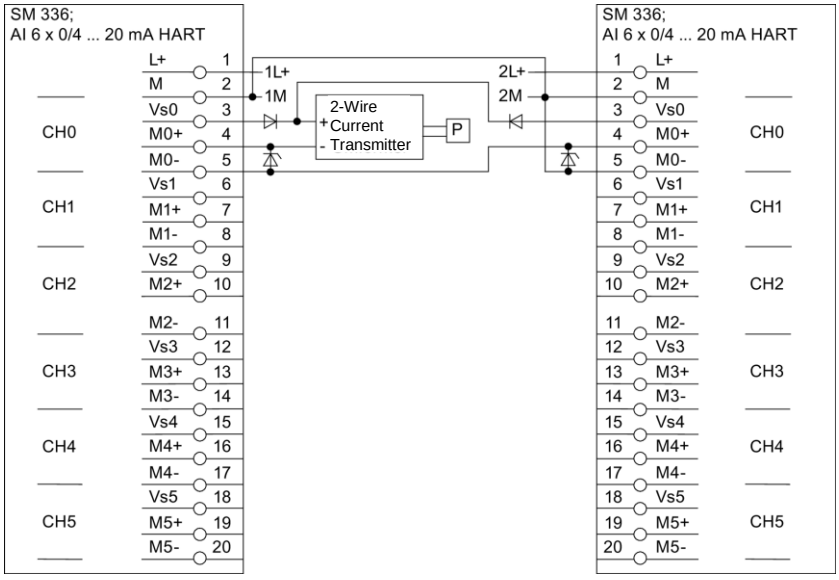
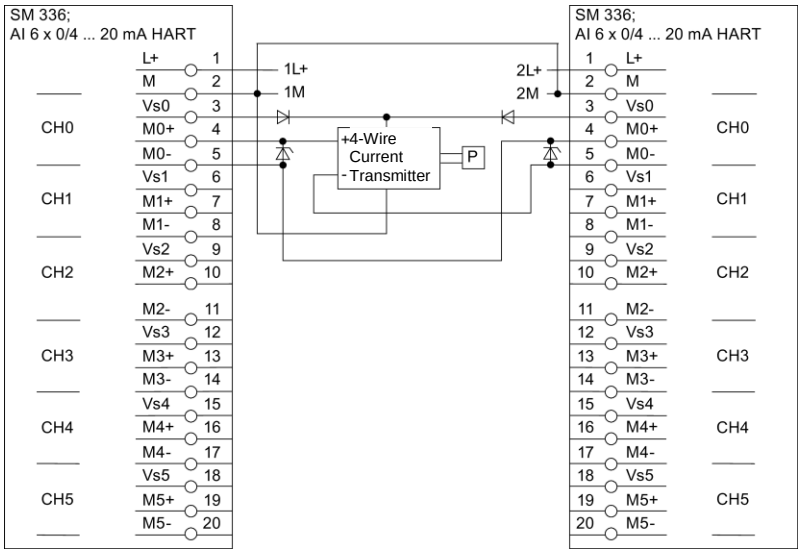


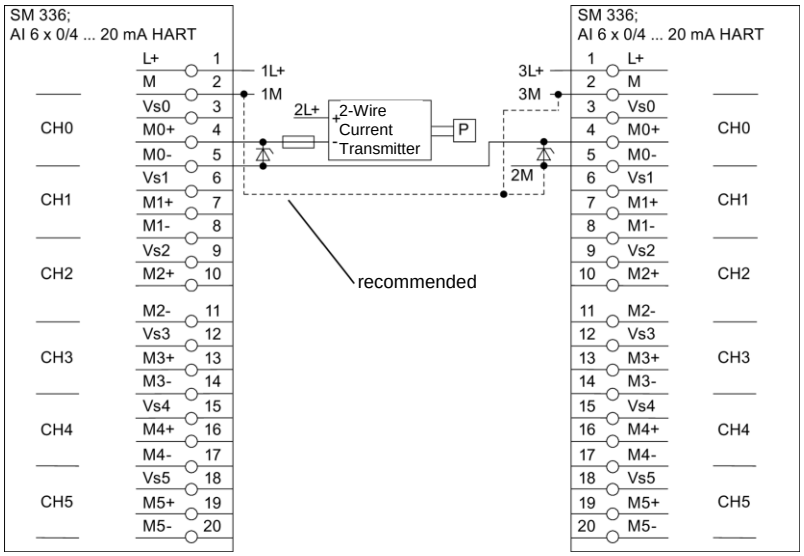
Fig. 3-3: A 4-wire transmitter, internal sensor supply with module redundancy



External power supply (2-wire transmitter)

Fig. 3-4 illustrates an external voltage source on a 2-wire transmitter. The sensor signal is looped through the Channels 0 (terminals 4, 5) of the two redundant modules.
It is recommended to connect the M potentials together.

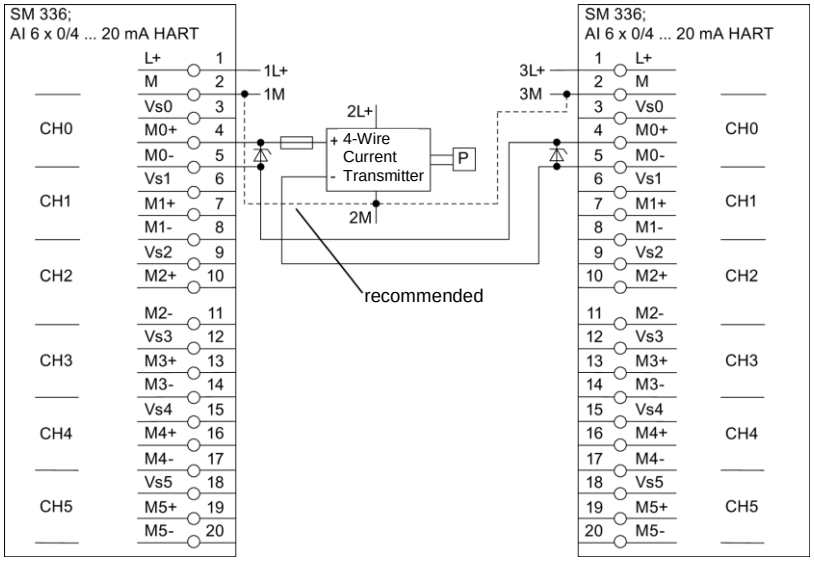
Fig. 3-4: A 2-wire transmitter, external sensor supply with module redundancy



External power supply (4-wire transmitter)

Figure 3-5 illustrates an external voltage source with a 4-wire transmitter. The sensor signal is looped through the Channels 0 (terminals 4, 5) of the two redundant modules. It is recommended to connect the M potentials together. It is recommended to connect the M potentials together.

Fig. 3-5 A 4-wire transmitter, external sensor supply with module redundancy

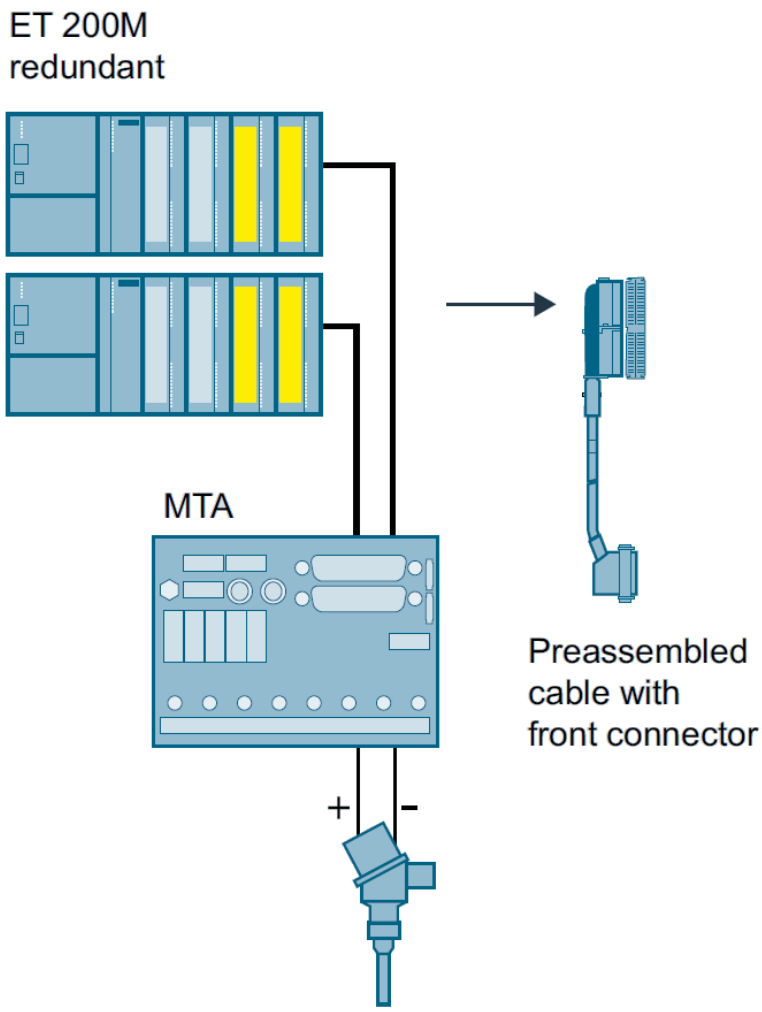


3.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

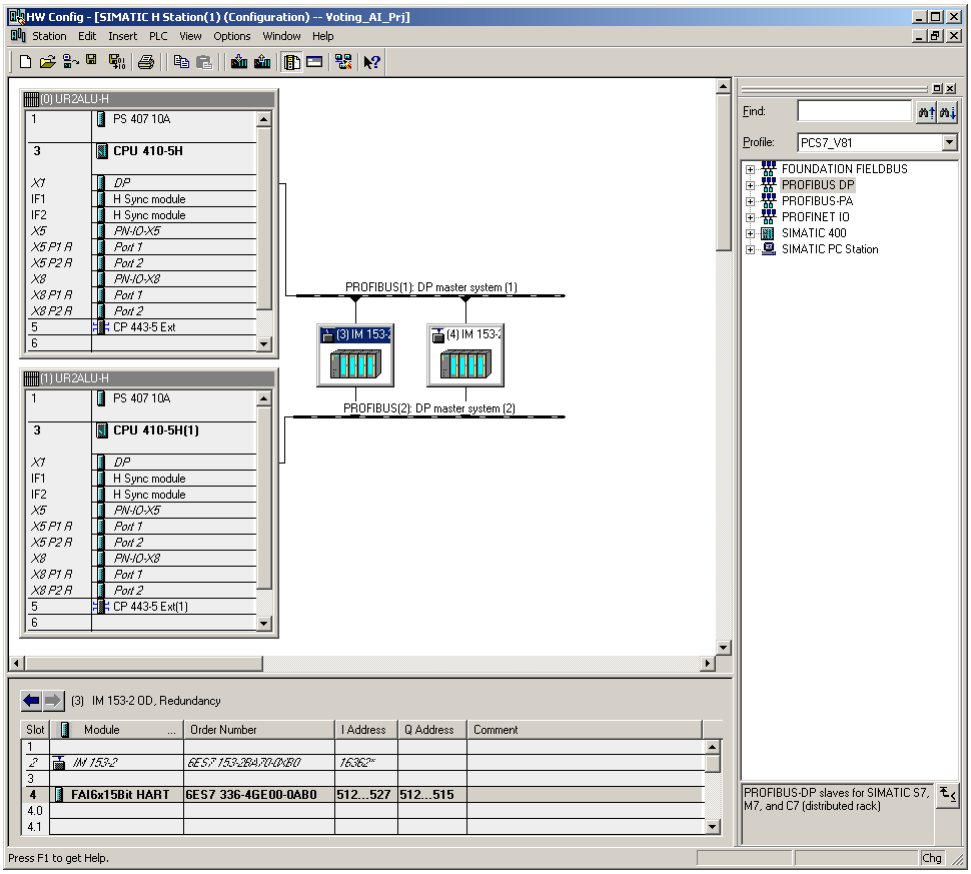
Fig. 3-6: MTA



3.3 Parameters for hardware configuration

The F-AIs are configured in STEP 7 HW Config for the 1oo1 evaluation scheme with redundant F-AI. Fig. 3-7 illustrates an example of a hardware configuration.
In this example, there is an ET 200M rack (with IM153-2 interface module for PROFIBUS) with PROFIBUS address 3 and a second ET 200M rack with PROFIBUS address 4. Each ET 200M contains one F-AI in slot 4. For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 3-7 : Redundant F-AI



The two F-AIs must be configured as a redundant pair in the HW Config. The F-AI redundancy settings can be accessed through the object properties of one of the F-AIs.

For the sake of the hardware configuration example in Fig. 3-7, the redundancy settings are made on the F-AI located in the ET 200M rack with the PROFIBUS address 3. The interface of the redundancy settings is shown in Fig. 3-8 and the settings are summarized in Table 3-2.

Fig. 3-8: Redundant F-AI - Redundancy parameters

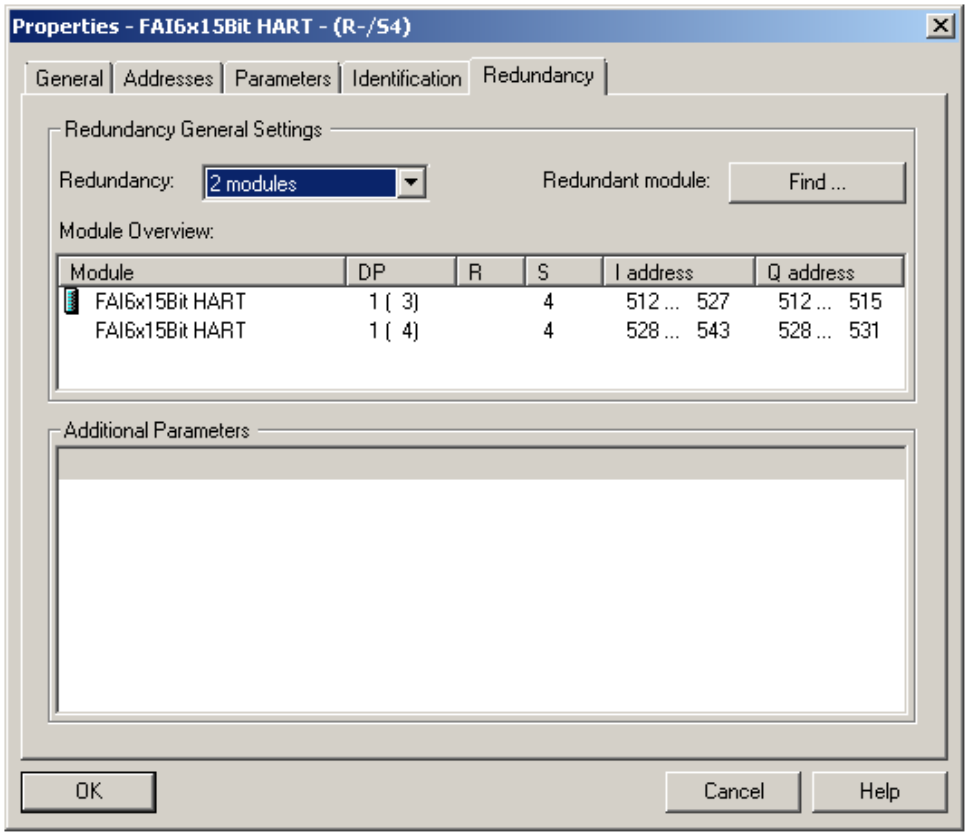


Table 3-2 : Redundant F-AI - Redundancy parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-AI is acting as part of a redundant pair or not. **Remark:** For redundancy, the parameter must be set to 2 modules.	2 modules
Redundant module	Used to select the redundant partner module.	

Note The hardware parameters and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

If the redundancy settings have been made, the other hardware parameters can be set in one of the redundant F-AIs. The settings are automatically applied to the redundant module.

3.4 Creating the Logic

Although this evaluation scheme uses redundant F-AIs, only one F_CH_AI 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 STEP 7 CFC Editor. In both cases, the F-channel driver must be connected to the analog sensor signal of the F-AI with the lowest I/O 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 enabled during compilation, the corresponding F_PS_12 module drivers are automatically added to the logic and configured during the compilation. The F-channel driver selects the valid signal and, in the event of a fault, switches to the signal of the redundant module.

3.4.1 Configuring with Safety Matrix

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

The actual evaluation logic for monitoring a single sensor with redundant F-AI is the same as that described in the Section 2.4.1 (Configuring with Safety Matrix).

3.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can also implement the CPU logic for reading the input signal by means of the STEP 7 CFC Editor.

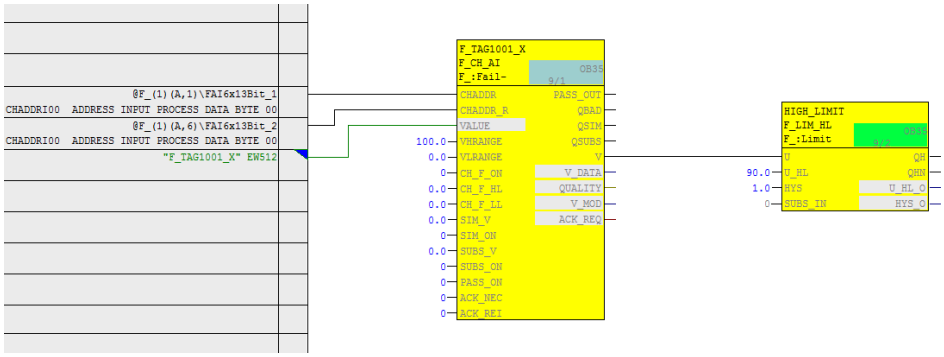
There are two ways to implement the CFC logic:

- Without channel fault evaluation
- With channel fault evaluation

Logic without channel fault evaluation

Fig. 3-9 illustrates an example logic created in the CFC Editor for reading an input signal from redundant F-modules, which does not take a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 3-9: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value of both F-AI modules is used in case of error. It is not possible to predict whether this value is above or below the limit.

Note

When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Fig. 3-9 works as follows:

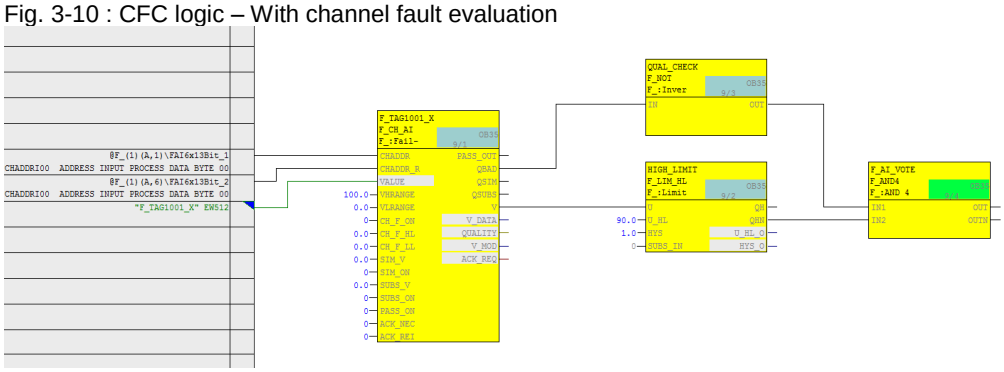
- The F_CH_AI F-channel driver evaluates the two sensor signals and sends a value to the logic for further processing.
- If the process value is in the normal range (in this case, lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value exceeds the limit (in this case, greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

To create the logic, create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.

Logic with channel fault evaluation

Fig. 2-13 illustrates a sample logic created in the CFC Editor for reading an input signal of the redundant F-AI that takes a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 3-10 : CFC logic – With channel fault evaluation



Note

When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Fig. 3-10 works as follows:

- In the normal range (here: lower than 90) and with an undisturbed process value, the output of the evaluation logic is 1 (i.e., no trigger command).
- In case of upper limit violation (here: greater than or equal to 90) and with an undisturbed process value, the output of the evaluation logic is 0 (i.e., trigger command).
- If both F-AIs report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the following signals in order to generate the signal for the trigger command:
  - Negated value of the limit module (QHN or QLN)
  - Negated value of the channel fault output (QBAD) from the F-channel driver

4 Hardware configuration and wiring of two sensors (1oo2) and one F-AI with evaluation in the module (1oo1)

The two-sensor or 1oo2 evaluation scheme refers to applications that require two sensors to achieve the required safety integrity level. 1oo2 evaluation means that only one of two sensors has to trigger, i.e., the safety logic triggers if one of the sensors indicates a trigger condition. In this evaluation scheme, the 1oo2 evaluation is done in the F-AI.

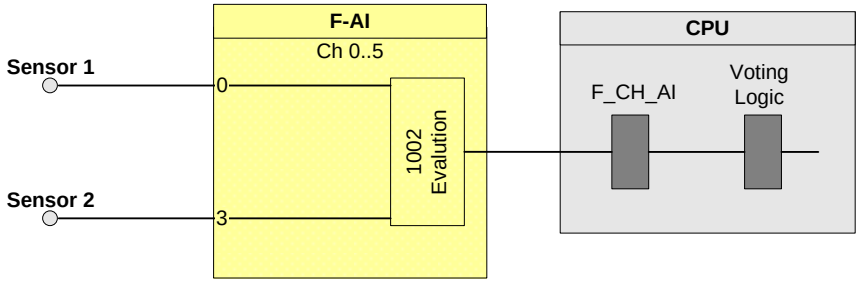
Note The I/O modules in this architecture are certified for the safety integrity level **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

In the 1oo2 architecture with evaluation in the F-AI, two sensors are wired to one F-AI. A block diagram is displayed in Fig. 4-1.

When the 1oo2 evaluation is activated for a channel pair (0/3, 1/4, 2/5), the F-AI performs a discrepancy analysis between the two input signals. One of the process values (MIN/MAX) is forwarded to the CPU depending on the parameter assignment.

The system uses the address of the channel with the lowest number. In Fig. 4-1, the first sensor on Channel 0 is wired to the F-AI. The second sensor must then be wired to Channel 3.

Fig. 4-1: 1oo2 evaluation in the F-AI – architecture



With a hardware configuration according to Fig. 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?			Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**F-AI**	
No	No	No	Yes (not required)
X	X	Yes	Yes
X	Yes	X	Yes
Yes	X	X	Yes

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 and evaluation architecture is calculated using this formula:

$$PFD_{In} = PFD_{Sensor} + PFD_{F\text{-}AI} + PFD_{CPU}$$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

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

4.2 Wiring

4.2.1 Conventional wiring

In the 1oo2 evaluation scheme, the F-AI or an external voltage source can supply the sensors with voltage.

Fig. 4-2 illustrates a wiring example for 2-wire transmitters.

The first sensor in the figure is wired to channel 0 (terminals 3 and 4) and the second sensor is wired to channel 3 (terminals 12 and 13).

Fig. 4-2: 1oo2 evaluation in the F-AI: 2-channel, 2-wire transmitter, internal supply

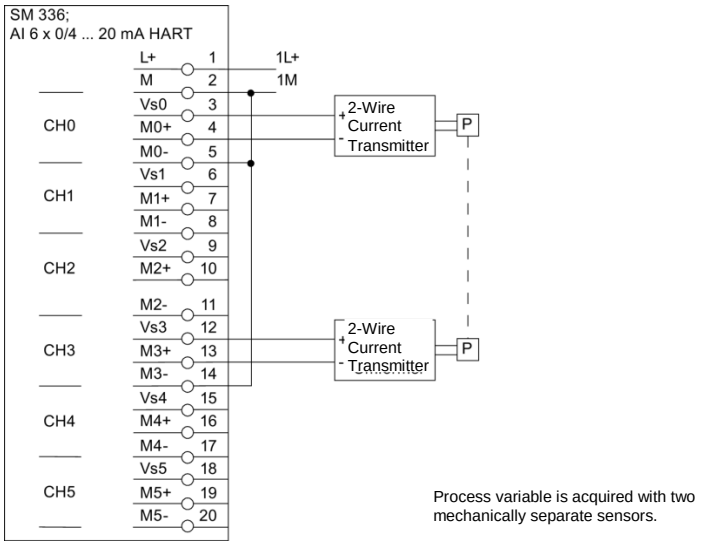


Fig. 4-3 illustrates a wiring example for 4-wire transmitters.

The first sensor in the diagram is wired to channel 0 (terminals 4 and 5) and the second sensor is wired to channel 3 (terminals 13 and 14).

Fig. 4-3: 1oo2 evaluation in the F-AI: 2-channel, 4-wire transmitter, internal supply

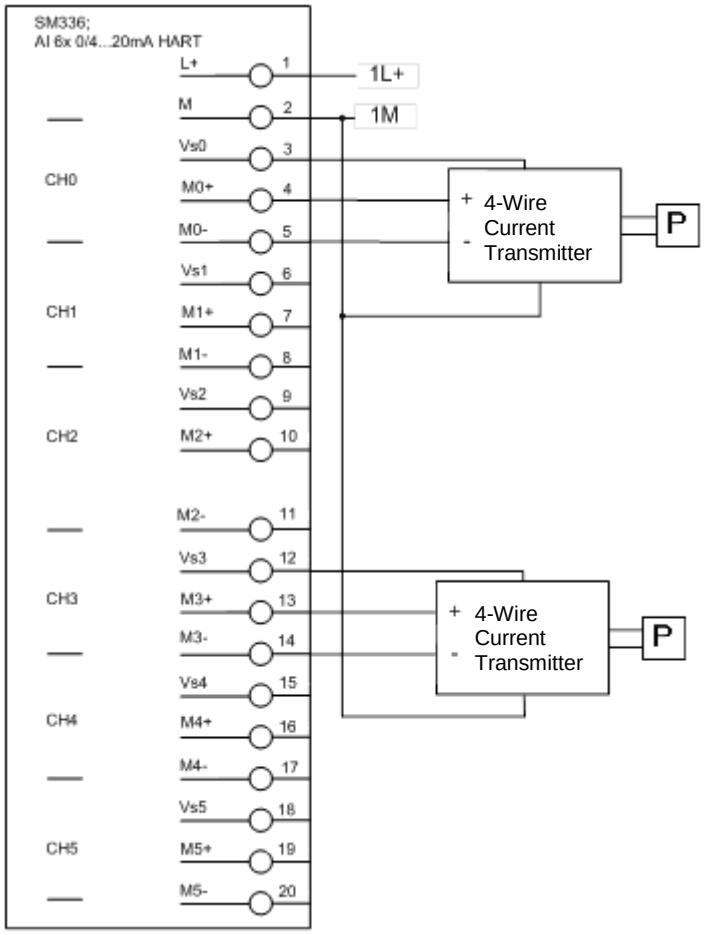


Fig. 4-4 illustrates a wiring example for 2-wire transmitters with external power supply and Fig. 4-5 illustrates a wiring example for 4-wire transmitters with external power supply.
The first sensor in both diagrams is wired to channel 0 (terminals 4 and 5) and the second sensor to channel 3 (terminals 13 and 14). It is recommended to connect the M potentials together.

Fig. 4-4: 1oo2 evaluation in the F-AI: 2-channel, 2-wire transmitter with external supply

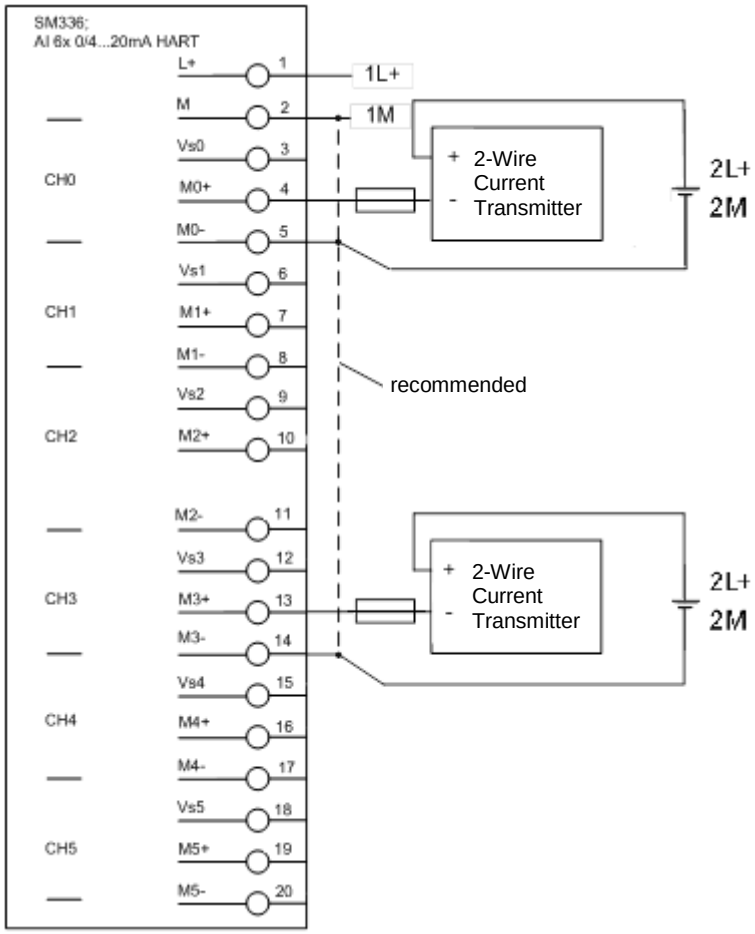
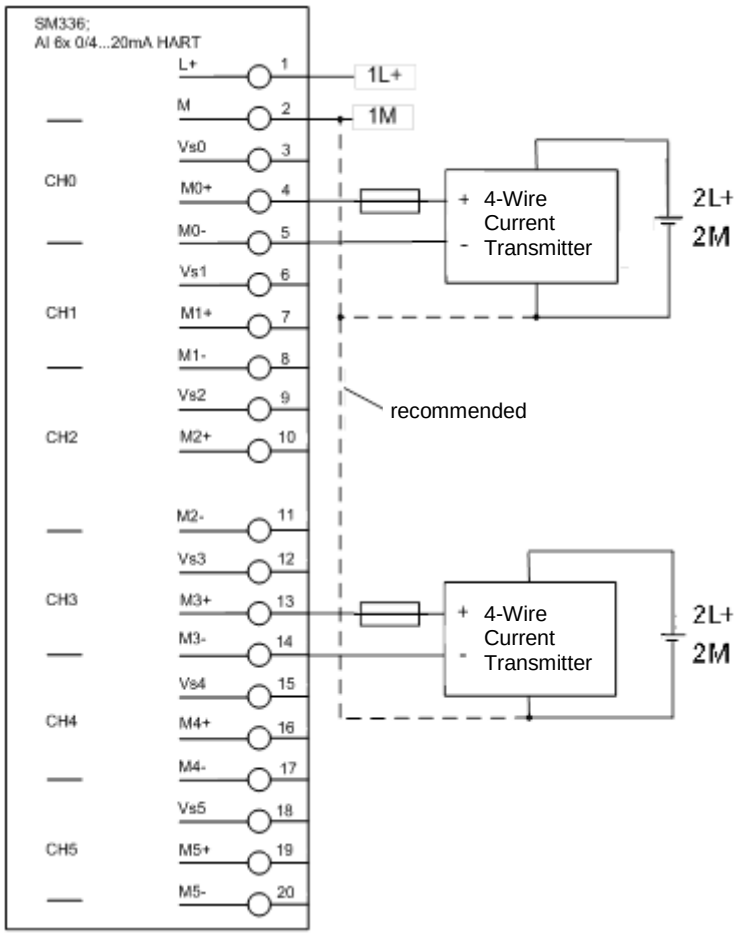


Fig. 4-5: 1oo2 evaluation in the F-AI: 2-channel, 4-wire transmitter with external supply

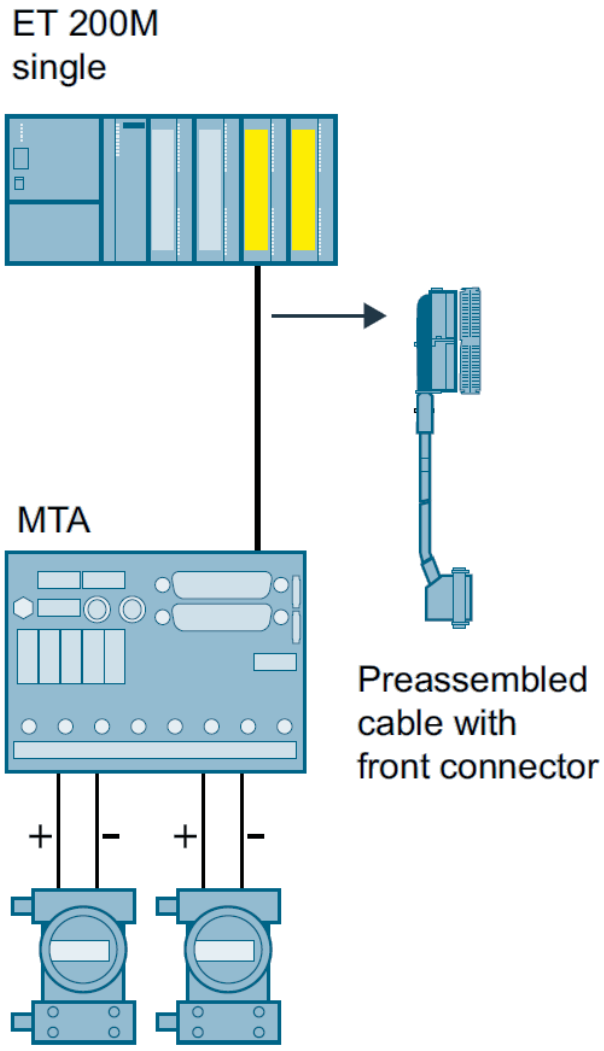


4.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

Fig. 4-6 MTA

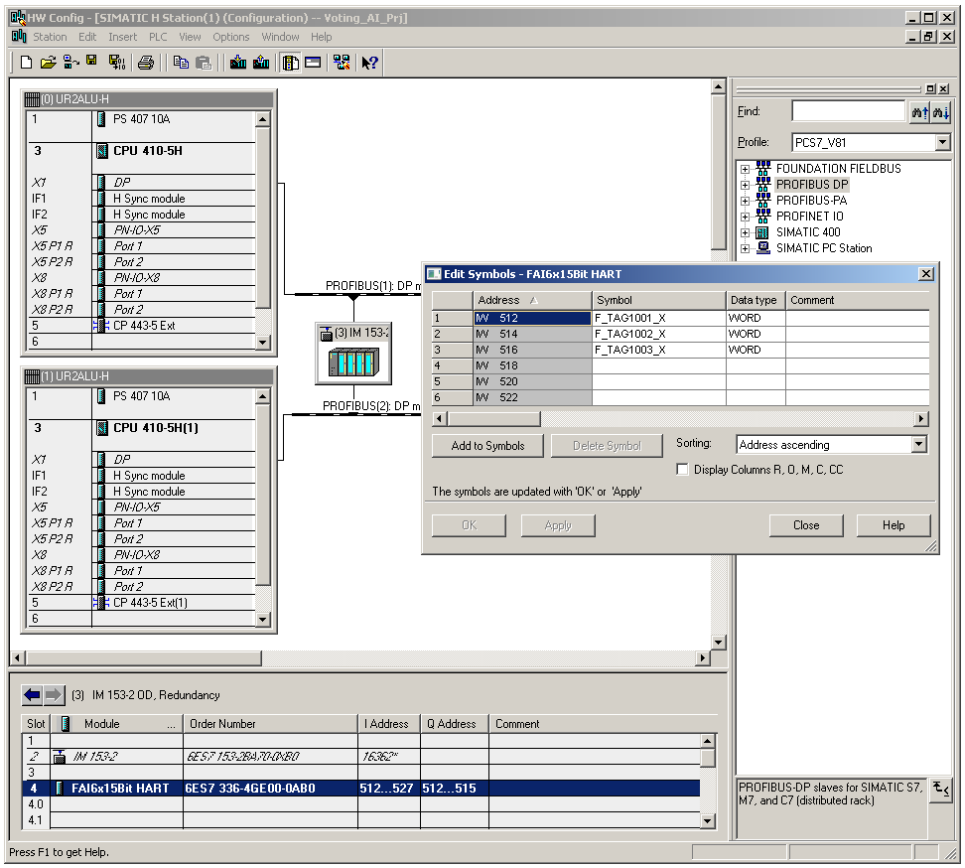


4.3 Parameters for hardware configuration

To configure, select the F-AI in the STEP 7 hardware catalog and insert it into an existing ET 200M station. Select a meaningful icon name for the analog channel in order to facilitate later configuration. When selecting the 1oo2 signal for the F-AI, make sure that only one analog sensor signal is made available to the CPU logic.

Fig. 4-7 illustrates an example of a hardware configuration with one F-AI. The signal consisting of the two sensors (channel 0 and 3) is forwarded to the CPU at the first symbol address (EW512). For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 4-7: 1oo2 evaluation in the F-AI symbol processing



The required parameters for operating the F-AI are set in the object properties of the F-AI added (see Fig. 4-8).

The parameters are summarized in Table 4-2.

Fig. 4-8: 1oo2 evaluation in the F-AI (Hardware Parameters)

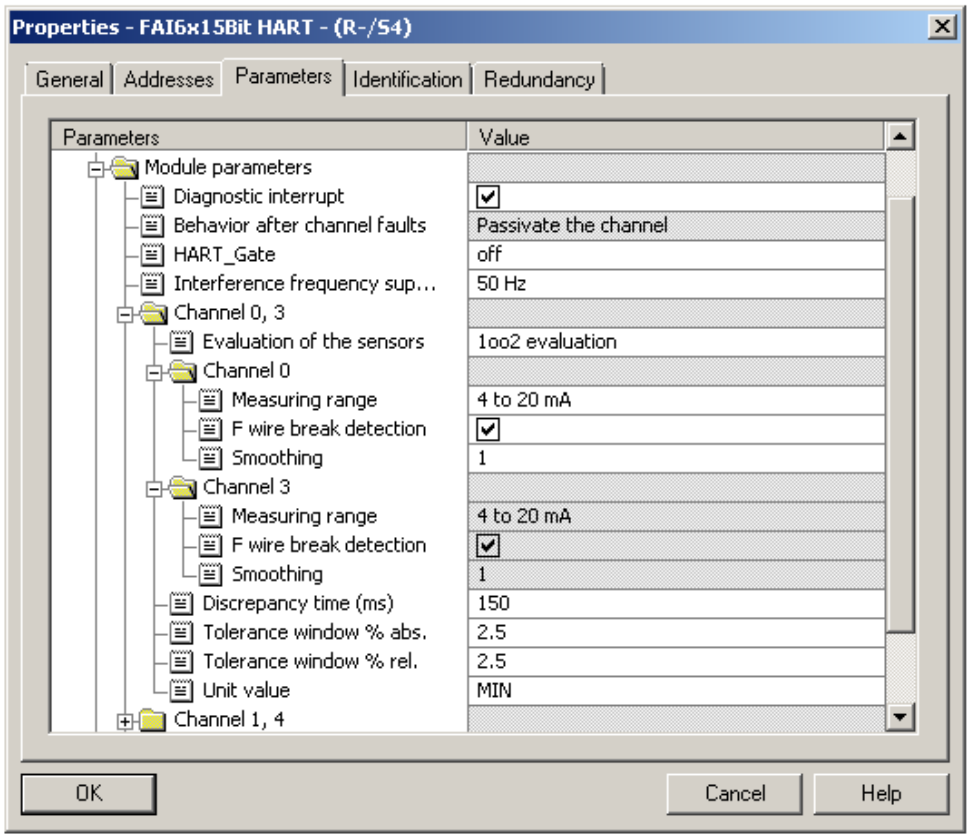


Table 4-2: 1oo2 evaluation in the F-AI Parameters for the hardware configuration

Parameter	Description / Recommendations	Desired setting or permissible value range
F-parameters		
F_destination_address	PROFIsafe address of the F-signal module (setting via DIP switch).	1-1022 or 0000000001... 1111111110
F_monitoring time (ms)	Monitoring time for safety-related communication between the CPU and the F-AI. **Remark:** A worksheet is available on the Siemens Support website to help users calculate F-monitoring times (see \10\ in the "Links and Literature" chapter).	0...65535ms Default 2500ms

Parameter	Description / Recommendations	Desired setting or permissible value range
Module parameters		
Diagnostic interrupt	A diagnostic interrupt is triggered by various error events that can be detected by the module. These events are then reported to the CPU. **Remark:** If the diagnostic interrupt is released at the module level, individual diagnostic events must be also activated at the channel level.	Release / lock
Behavior after channel fault	Passivate the entire module/ passivate the channel. **Remark:** Irrelevant for F systems	Module/ Channel
HART_Gate	Acts as a fail-safe "main switch" across the modules. HART communication is blocked with "Off". HART communication is enabled with "On". The HART modem can be switched out of the safety program for maintenance purposes with "switchable".	Off/ On/ switchable
Interference frequency suppression (Hz)	Selection for matching the integration time of the ADC to the network used. The integration time is: - 20 ms at 50 Hz - 16.66 ms at 60 Hz	50/60 Hz
Evaluation of the sensors	Channel activation by specifying the encoder evaluation. - Deactivated - 1oo1 (1v1) - 1oo2 (2v2) If 1oo1 is selected, the following parameters are not available: - Discrepancy time - Tolerance range - Unit value	1oo2 (2v2)
Measuring range	Measuring range selection for the channel.	0...20 mA 4...20 mA
F wire break detection	Select whether or not to enable wire break monitoring for the channel.	Release / lock
Smoothing	Number of measuring cycles through which smoothing is carried out.	1, 4, 16, 64
Discrepancy time (ms)	Discrepancy time selection	0…30000ms
Tolerance window % abs.	Define the maximum difference between the two signals	0.2…20.0%
Tolerance window % rel.	Define the maximum difference between the two signals	0.2…20.0%

Parameter	Description / Recommendations	Desired setting or permissible value range
Unit value	This value is forwarded to the CPU. Must be predefined depending on the series-connected limit value function.	MIN/MAX

Note The hardware parameters and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

4.4 Configuring the logic

4.4.1 Configuring with Safety Matrix

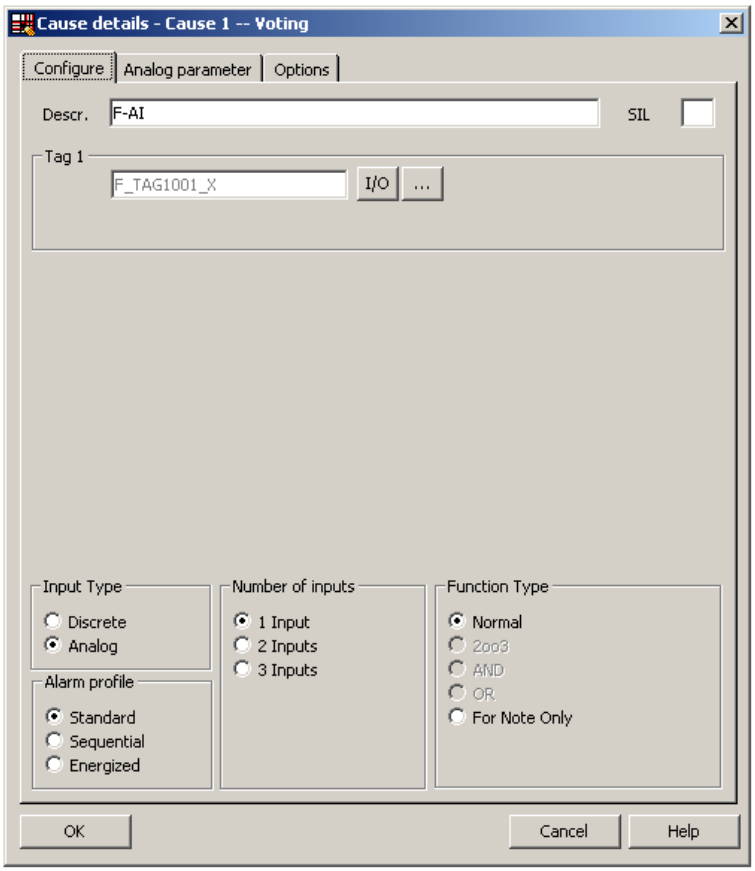
After the 1oo2 evaluation is configured in the F-AI, the CPU logic for reading a single sensor can be implemented. As pointed out earlier, a 1oo1 evaluation occurs in the user program after the F-AI handles the 1oo2 signal selection and provides only one analog sensor signal to the CPU logic. One implementation method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

Fig. 4-9 illustrates how a cause for monitoring an input TAG is configured in the Matrix. The following settings must be used:

- Input Type: Analog
- 1 input
- Function type: Normal (1oo1 evaluation)
- Enter the signal name in Tag 1 (e.g. F_TAG1001_X) or press the "I/O" button to select the symbol from the symbol table.

The cause is configured with the "Normal" function type.

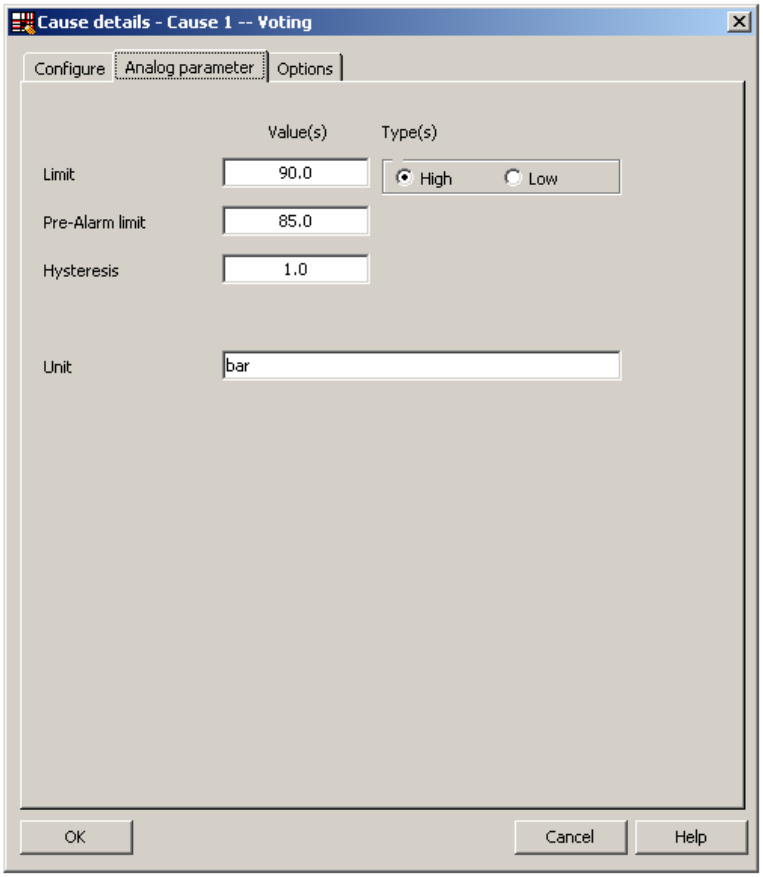
Fig. 4-9: Safety Matrix – Configure



As shown in Fig. 4-10, there are additional analog parameters that must be configured for the cause:

- Required parameters:
  - Limit type: MAX or MIN
  - Limit value
- Optional parameters:
  - Pre-alarm
  - Hysteresis
  - Units:

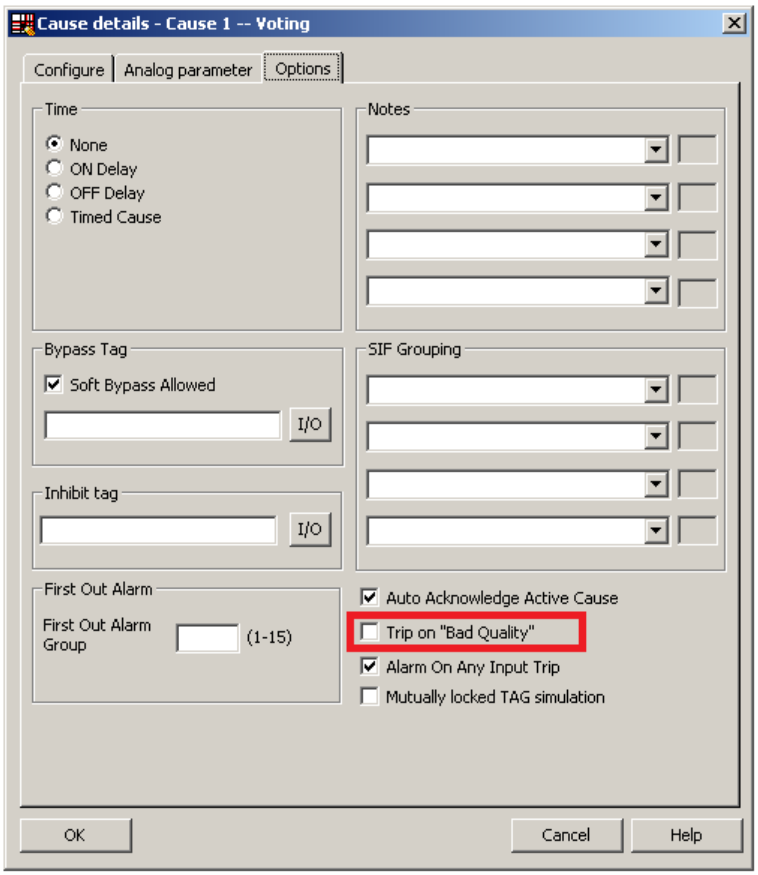
Fig. 4-10: Safety Matrix - Analog parameter



If the input TAG goes below or above the limit, the cause activates and triggers the corresponding effect(s).

You can also activate additional options (e.g. time delay and bypass option), depending on the process application.
One configuration option highlighted in Fig. 4-11 is the disconnection in case of a channel fault. If this option is activated, a channel fault at one of the sensor inputs is evaluated as a trigger signal. Depending on the number of signals and the function type, the cause can activate and trigger the corresponding effect(s).

Fig. 4-11: Safety Matrix – Options



4.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for reading the input signal by means of the STEP 7 CFC Editor. The evaluation logic can be generated in the CFC editor after the two sensor signals have been added to the hardware configuration and the F-AI performs the 1oo2 evaluation.

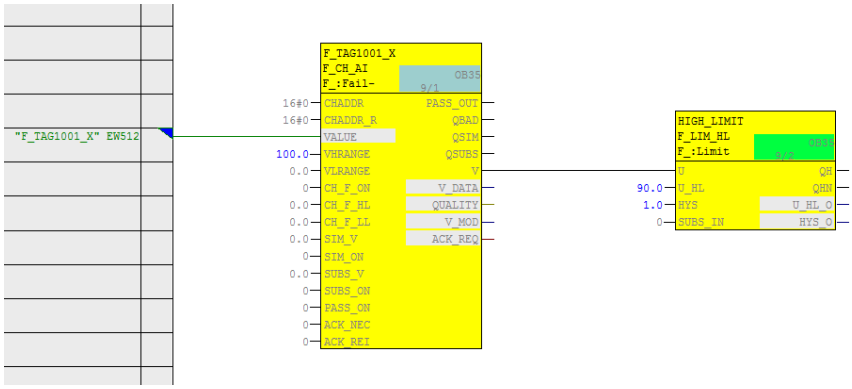
There are two ways to implement the CFC logic:

- Without channel fault evaluation
- With channel fault evaluation

Logic without channel fault evaluation

Fig. 4-12 illustrates a sample logic for reading a single input signal in the CFC Editor, which does not take a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 4-12: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

The example logic in Fig. 4-12 works as follows:

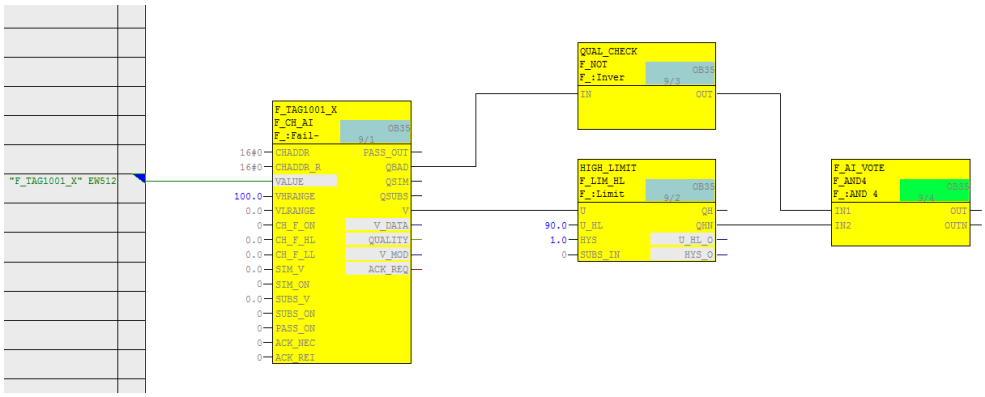
- The F-AI evaluates the two sensor signals and sends a value to the F-channel driver for further processing. Depending on how the "Unit value" parameter is set in the hardware configuration, this value corresponds to either the larger or the smaller sensor signal or to &H7FFF in case of a discrepancy.
- If the process value is in the normal range (here: lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value exceeds the limit (here: greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic must be connected to the corresponding shutdown logic.

To create the configuration, create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the address with the lowest channel number (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.

Logic with channel fault evaluation

Fig. 4-13 illustrates a sample logic created in the CFC Editor for reading a single input signal that takes a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 4-13: CFC logic – With channel fault evaluation



The example logic in Fig. 4-13 works as follows:

- The F-AI evaluates the two sensor signals and sends a value to the F-channel driver for further processing. Depending on how the "Unit value" parameter is set in the hardware configuration, this value corresponds to either the larger or the smaller sensor signal or to &H7FFF in case of discrepancies.
- If the undisturbed process value is in the normal range (here: lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the undisturbed process value exceeds the limit (here: greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- If the F-AI reports a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic must be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the address with the lowest channel number (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the following signals in order to generate the signal for the trigger command:
  - Negated value of the limit module (QHN or QLN)
  - Negated value of the channel fault output (QBAD) from the F-channel driver

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

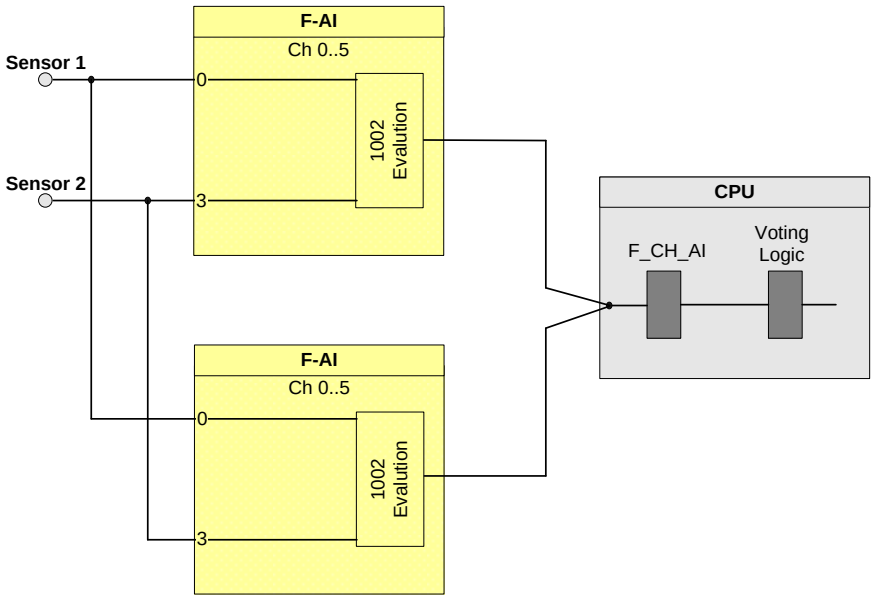
To increase the availability of the system, an architecture with two sensors can be realized with redundant modules in order to achieve the required SIL.
Each F-AI performs a 1oo2 evaluation of the two sensors and the CPU performs a 2oo2 evaluation of the signals.

Note The I/O modules in this architecture are certified for achieving the safety integrity level of **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

In this architecture, two sensors are wired to a redundant F-AI pair. A block diagram can be found in Fig. 5-1.

The first sensor in the diagram is wired to channel 0 and the second sensor is wired to channel 3 of both modules. The modules are configured as redundant modules in HW Config. Each F-AI performs a 1oo2 evaluation of the two sensors. Only one analog F-channel driver is required. The F-channel driver chooses from the incoming analog signals.

Fig. 5-1: 1oo2 evaluation in the redundant F-AI architecture



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

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

Table 5-1: Failure combinations

Failed component detected?				Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**F-AI 1**	**F-AI 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 I/O modules 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 and evaluation architecture is calculated using this formula:

$PFD_{In} = PFD_{Sensor} + 2\ PFD_{F\text{-}AI} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

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

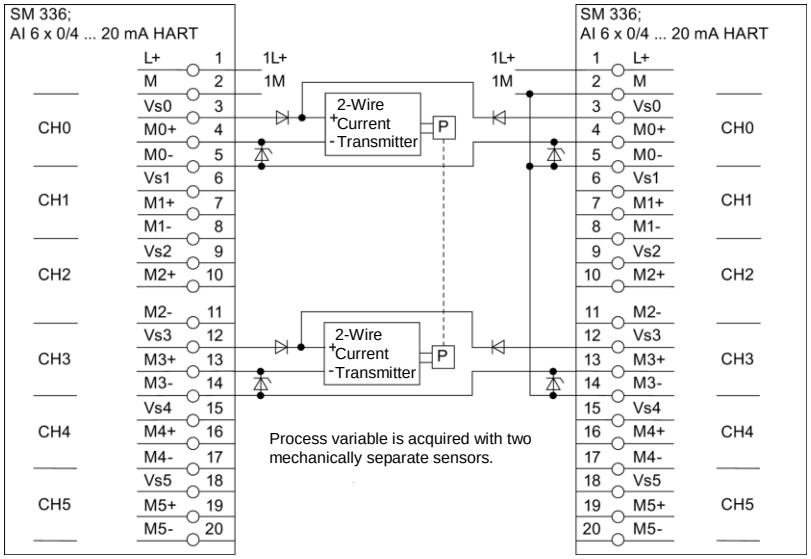
5.2 Wiring

5.2.1 Conventional wiring

An example for the 1oo2 evaluation scheme with evaluation in the F-AI and redundant F-AI is illustrated in Fig. 5-2.
The first sensor is wired to channel 0 (terminals 3, 4, 5) and the second sensor is wired to channel 3 (terminals 12, 13, 14) of both F-AIs.

Please note that this architecture also requires two Zener diodes for each sensor. The first Zener diode has an avalanche voltage of 6.2 V and the second one has an avalanche voltage of 5.6 V. Another two diodes are also used for decoupling the voltage supply. The diodes and Zener diodes are needed in case an F-AI is out of service (e.g. module failure, routine maintenance, etc.).

Fig. 5-2: 1oo2 evaluation in the redundant F-AI , 2-channel, 2-wire transmitter, internal supply

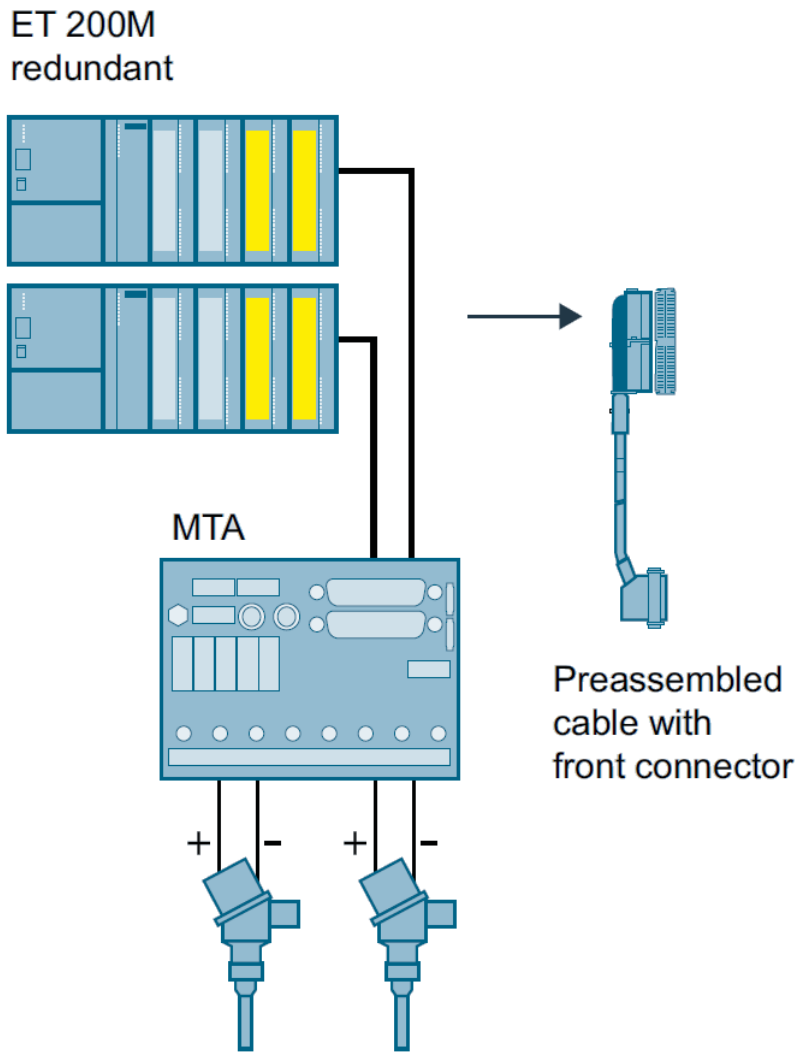


5.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

Fig. 5-3: MTA

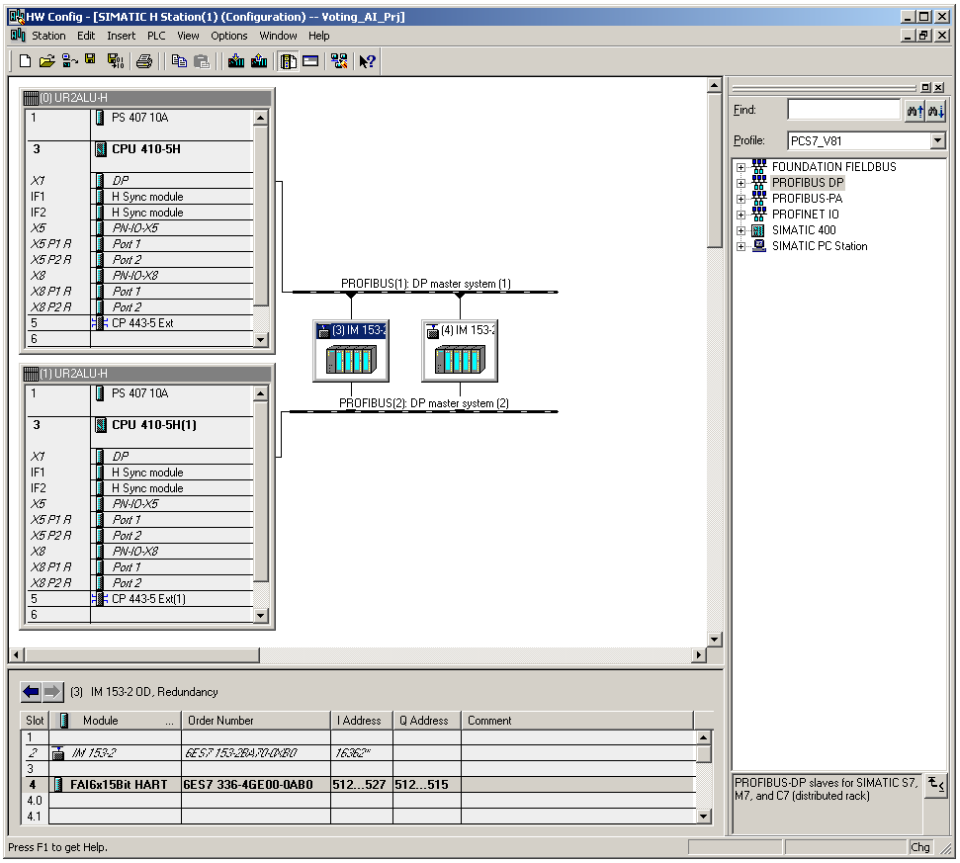


5.3 Parameters for hardware configuration

For the 1oo2 evaluation scheme with evaluation in the redundant F-AI, the F-AIs are configured in STEP 7 HW Config.

Fig. 5-4 illustrates an example of a hardware configuration. An ET 200M with PROFIBUS address 3 and a second ET 200M with PROFIBUS address 4 are used. Each ET 200M contains one F-AI in slot 4. For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 5-4: 1oo2 evaluation in the redundant F-AI HW Config



The two F-AIs must be configured as a redundant pair in the HW Config. Each of the F-AI redundancy settings can be accessed through the object properties of the F-AIs.

For the sake of the hardware configuration example in Fig. 5-4, the redundancy settings are made with PROFIBUS address 3 using the F-AI in the ET 200M.

The interface of the redundancy settings is shown in Fig. 5-5 and the settings are summarized in Table 5-2.

Fig. 5-5: 1oo2 evaluation in the redundant F-AI, redundancy parameters

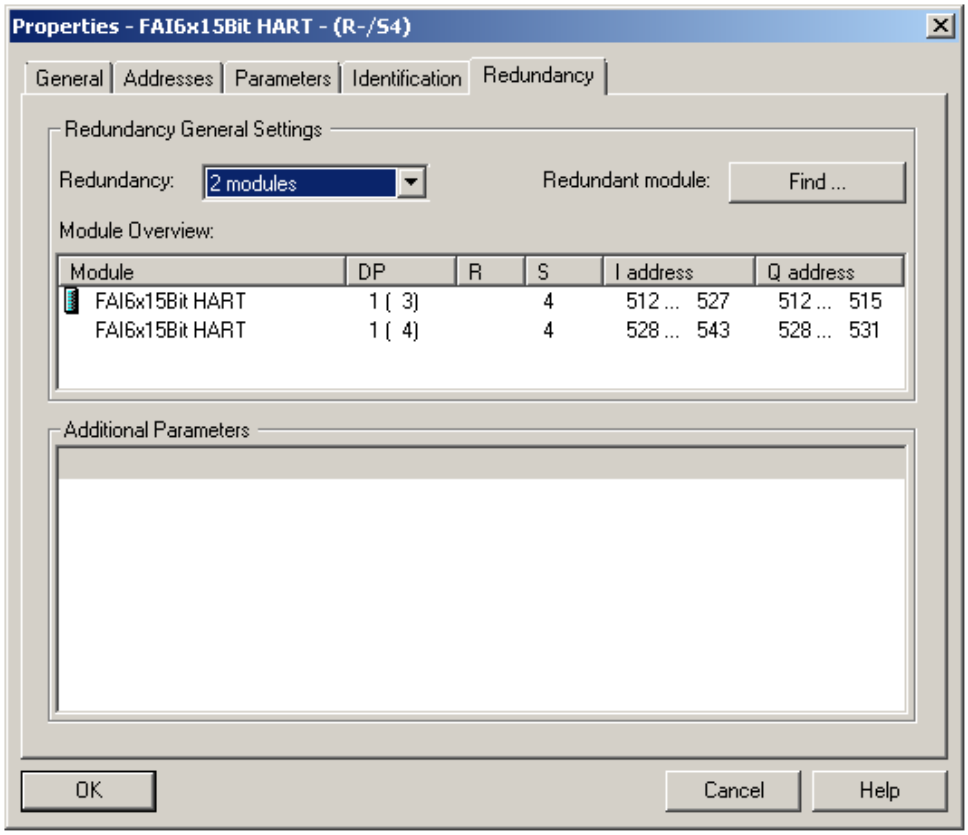


Table 5-2: 1oo2 evaluation in the redundant F-AI, redundancy parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-AI is acting as part of a redundant pair or not. **Remark:** For redundancy, the parameter must be set to 2 modules.	2 modules
Redundant module	Used to select the redundant partner module.	

Note The parameter names and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

After adjusting the redundancy settings, the remaining hardware parameters for the redundant F-AI can be set as described at the end of section 4.3. The settings are applied automatically to the redundant partner.

5.4 Creating the Logic

Although this evaluation scheme uses redundant F-AIs, only one F_CH_AI F-channel driver is needed in the logic configuration. The F-channel driver can be added and configured automatically from the SIMATIC Safety Matrix or manually using the STEP 7 CFC Editor. In both cases, the F-channel driver must be connected to the analog sensor signal of the F-AI with the lowest I/O address.

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

5.4.1 Configuring with Safety Matrix

After the 1oo2 evaluation is configured in the F-AI, the CPU logic for reading a single sensor can be implemented. One implementation method is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

The actual evaluation logic for the 1oo2 evaluation scheme with redundant F-AI is the same as that described in the Section 4.4.1 (Configuring with Safety Matrix).

5.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the CPU logic for reading the input signal by means of the STEP 7 CFC Editor. The evaluation logic can be generated in the CFC Editor after the F-AI performs the 1oo2 evaluation.

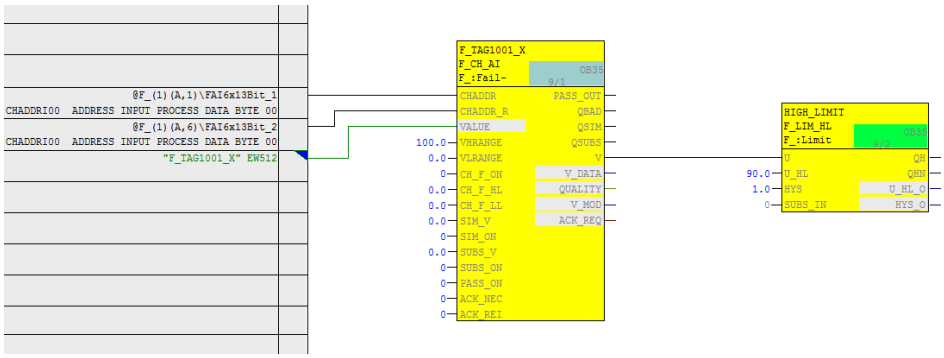
There are two ways to implement the CFC logic:

- Without channel fault evaluation
- With channel fault evaluation

Logic without channel fault evaluation (1oo2 in the F-AI)

Fig. 5-6 illustrates a sample logic for reading a single input signal in the CFC Editor, which does not take a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 5-6: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

Note

When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Fig. 5-6 works as follows:

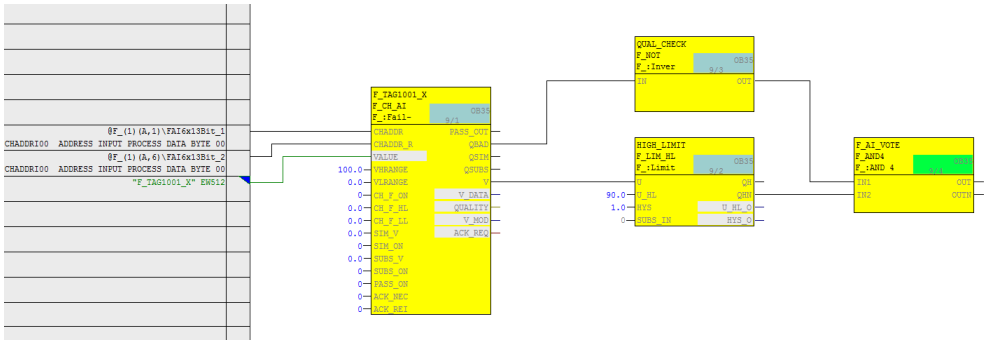
- The redundant F-AI evaluates the two sensor signals and sends a value to the CPU for further processing. This value reflects the value of one of the sensors. Depending on how the "Unit value" parameter is set in the hardware configuration, the value corresponds to either the larger or the smaller one or to &H7FFF in case of a discrepancy.
- The F_CH_AI F-channel driver evaluates the two sensor signals and sends a value to the logic for further processing.
- If the process value is in the normal range (here: lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value exceeds the limit (here: greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic must be connected to the corresponding shutdown logic.

To create the configuration, create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the F-AI with the lowest address and with the lowest channel number (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.

Logic with channel fault evaluation

Fig. 5-7 illustrates a sample logic created in the CFC Editor for reading an input signal that takes a channel fault into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 5-7: CFC logic – Channel fault evaluation



Note

When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Fig. 5-7 works as follows:

- The F-AI evaluates the two sensor signals and sends a value to the CPU for further processing. This value reflects the value of one of the sensors. Depending on how the "Unit value" parameter is set in the hardware configuration, the value corresponds to either the larger or the smaller one or to &H7FFF in case of discrepancy.
- If the undisturbed process value is in the normal range (here: lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the undisturbed process value exceeds the limit (here: greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- If both F_AIs report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic must be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the analog input signal and connect it to the symbol on the F-AI with the lowest address and with the lowest channel number (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the following signals in order to generate the signal for the trigger command:
  - Negated value of the limit module (QHN or QLN)

Negated value of the channel fault output (QBAD) from the F-channel driver

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

The two-sensor or 1oo2 evaluation scheme refers to applications that need two sensors to achieve the required safety integrity level. 1oo2 evaluation means that only one of two sensors must fail to trigger the safety function.

In contrast to the evaluation in the F-AI, in this case the evaluation is carried out in the user program in order to have the visibility of both signals and their quality in the application logic - which allows more flexible evaluation schemes (e.g. 1oo2D or 2oo2).

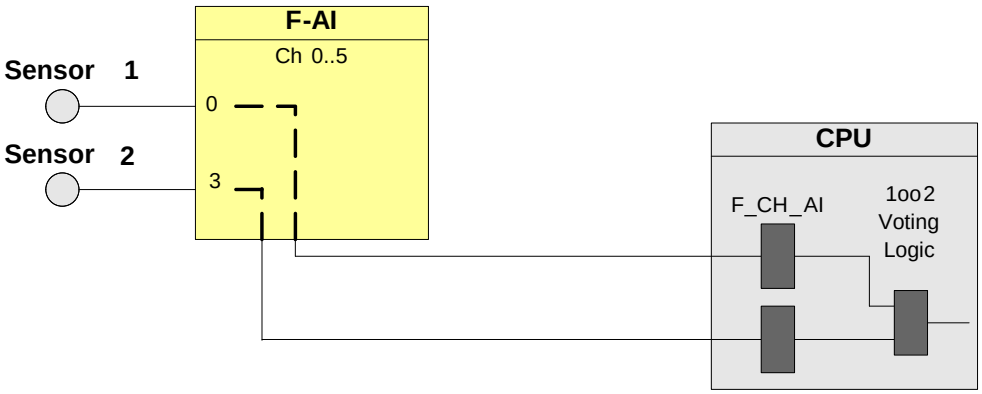
Note This architecture can achieve the safety integrity level **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

For this scheme, one can choose between two design variants, which differ in their PFD and availability.

- **Option 1:** with one module
  Both sensors are wired to one F-AI as illustrated in Fig. 6-1. In this diagram, one sensor is wired to channel 0 and the other to channel 3 of the F-AI.
- **Option 2:** with two modules
  Both sensors are wired to two F-AIs as illustrated in Fig. 6-2. In this diagram, one sensor is wired to channel 0 of the first F-AI whereas the second sensor to channel 0 of the second F-AI.

6.1 Option 1: with one module

Fig. 6-1: 1oo2 evaluation in the user program



The hardware configuration according to Fig. 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?			Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**F-AI**	
No	No	No	Yes (not required)
X	X	Yes	Yes
X	Yes	X	Yes
Yes	X	X	Yes

6.1.1 PFD calculation (option 1)

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 & evaluation architecture is calculated using this formula:

$PFD_{In} = PFD_{Sensor} + PFD_{F\text{-}AI} + PFD_{CPU}$

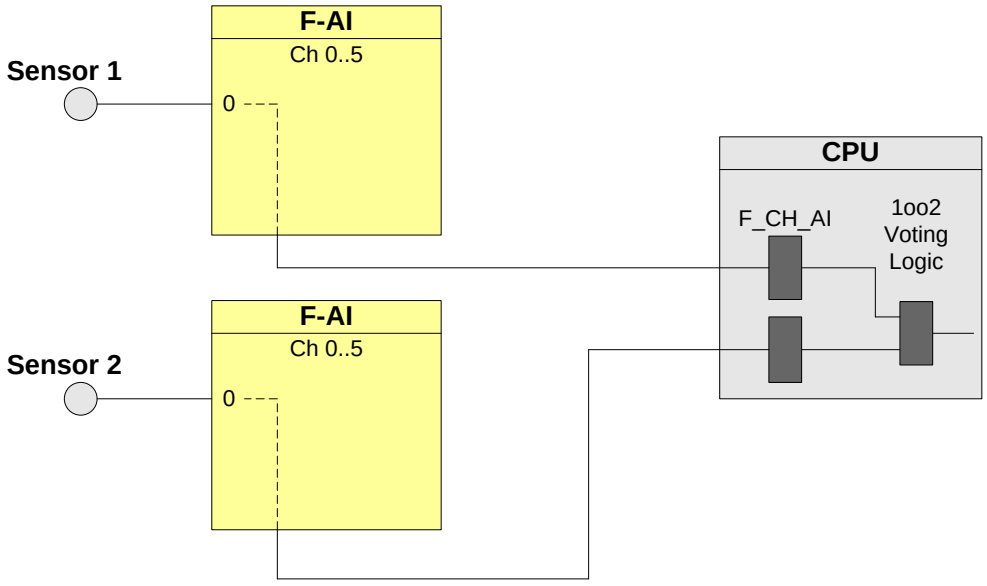
The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

6.2 Option 2: with two modules

Fig. 6-2: 1oo2 evaluation in the user program



The hardware configuration according to Figure 4-2 is suitable for achieving **SIL3**.

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

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

Table 6-2: Failure combinations

Failed component detected?				Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**F-AI 1**	**F-AI 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

6.2.1 PFD calculation (option 2)

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 and evaluation architecture is calculated using this formula:

$PFD_{In} = PFD_{1oo2} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

The *PFD* for one 1oo2 input circuit is calculated using the following [6]formula:

$$PFD_{1oo2} \approx \frac{4}{3} {PFD_{1oo1}}^2 + \beta \cdot PFD_{1oo1}$$

With: $PFD_{1oo1} = PFD_{Sensor} + PFD_{F-AI}$

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

6.3 Wiring

6.3.1 Conventional wiring

In the 1oo2 evaluation scheme, the sensors can be powered from the F-AI or an external voltage source.

The following diagrams show the wiring for 2-wire and 4-wire transmitters powered from the F-AI or an external voltage source.

The transmitters in the following diagrams are wired to two channels of an F-AI. The first sensor is wired to channel 0 (terminals 3, 4, 5 - jumper to 1M) and the second sensor to channel 3 (terminals 12, 13, 14 - jumper to 1M).

The F-AI is supplied with power via 1L+/1M (terminals 1 and 2), and the sensors via $V_{s0...}$ V_{s5} (terminal 3, 6, 9, 12, 15, 18), depending on the channel, or from an external voltage source.

Fig. 6-3: 1oo2 evaluation in the user program, 2-wire transmitter, 2-channel connection, internal supply

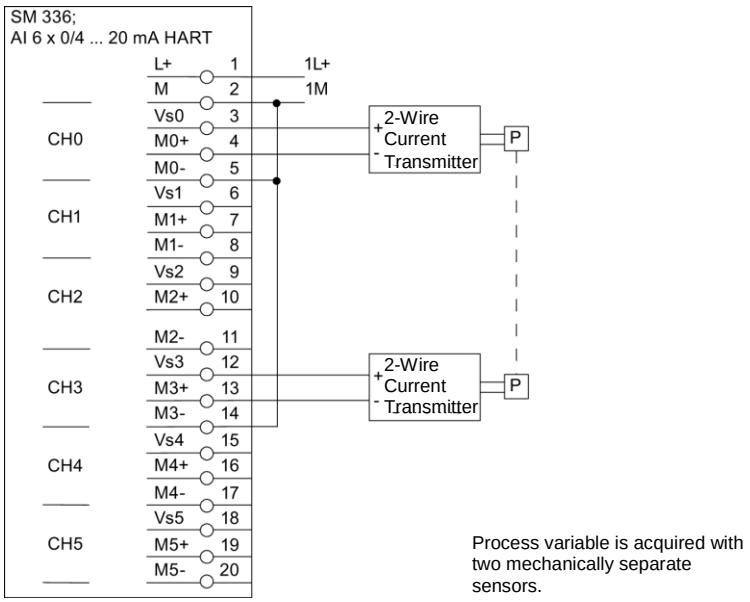
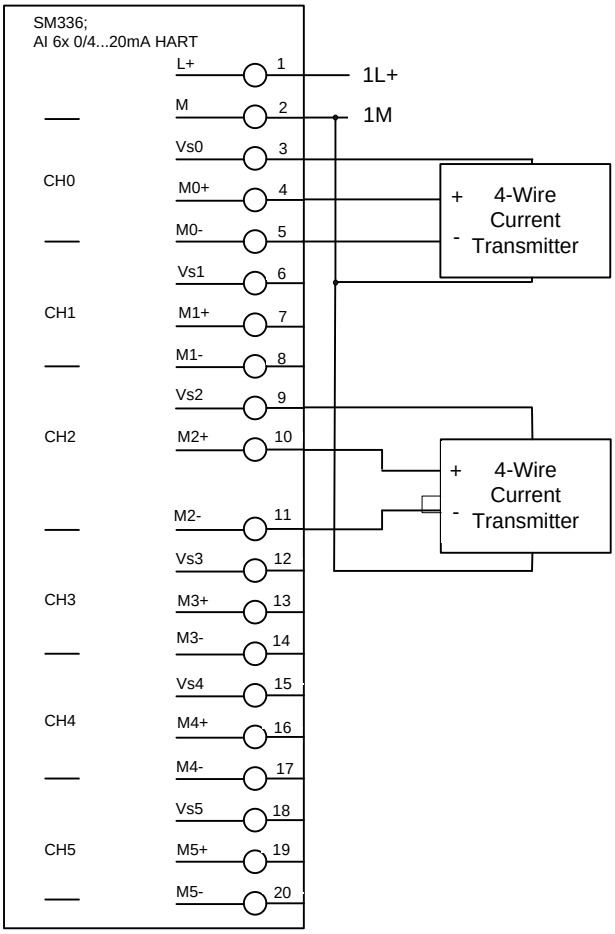


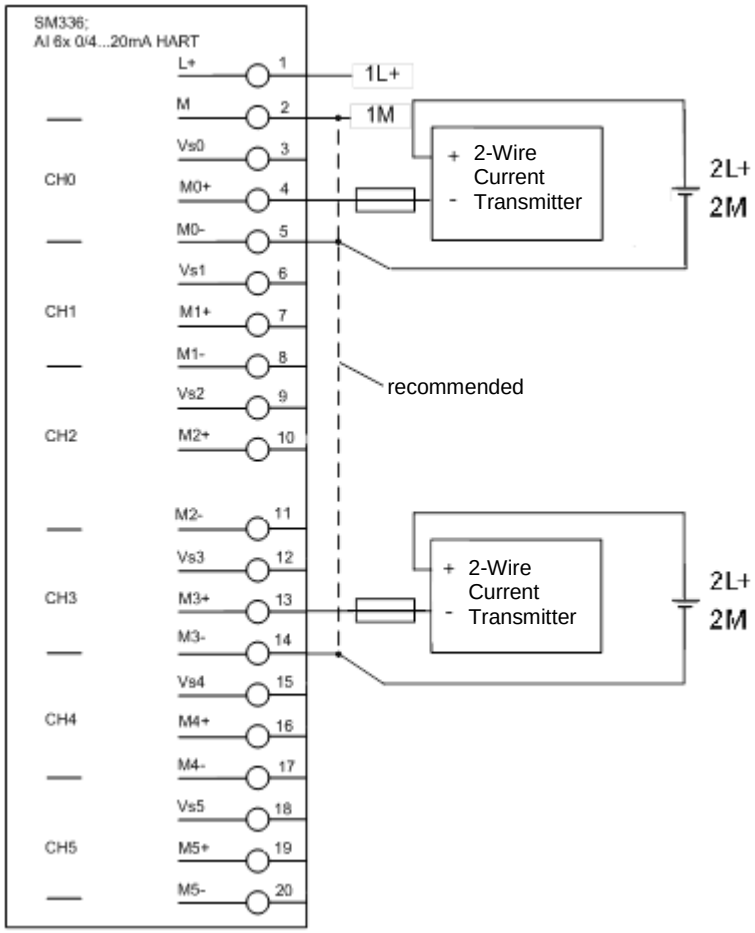
Fig. 6-4: 1oo2 evaluation in the user program, 4-wire transmitter, 2-channel connection, internal supply



The

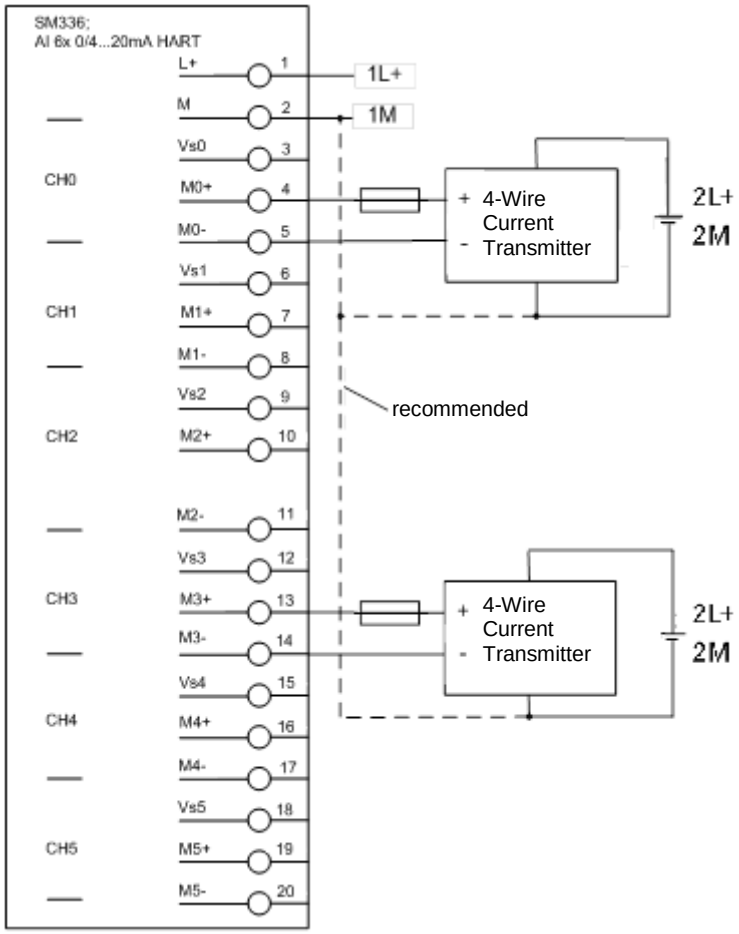
Fig. 6-5 shows an example where an external voltage source with 2-wire transmitters is used:

Fig. 6-5: 1oo2 evaluation in the user program, 2-wire transmitter, 2-channel connection, external supply



The Fig. 6-6 illustrates an external voltage source with a 4-wire transmitter.

Fig. 6-6: 1oo2 evaluation in the user program, 4-wire transmitter, 2-channel connection, external supply

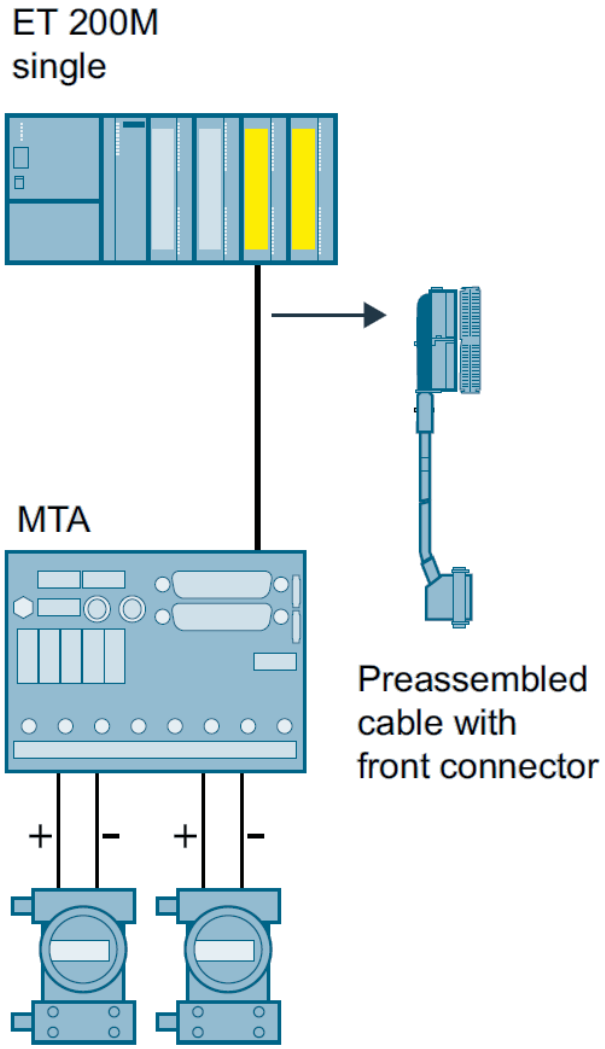


6.3.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

Fig. 6-7: MTA



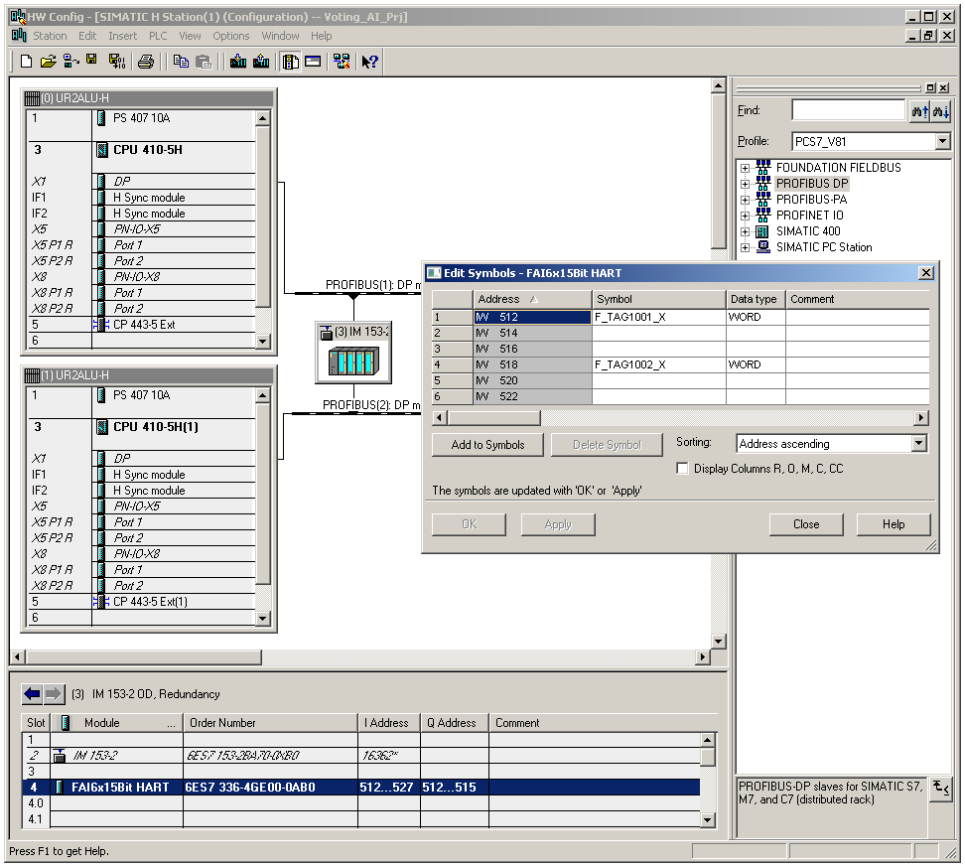
6.4 Parameters for hardware configuration

To configure, select the F-AI in the hardware catalog off the HW Config and insert it into an existing ET 200M station. Select meaningful icon names for the channels in order to facilitate later configuration.

Fig. 6-8 illustrates an example of a hardware configuration with one F-AI. The two sensor signals in this example are wired to the first two channels of the F-AI. For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Please note that you do not need to perform any particular hardware configuration to use an F-AI MTA.

Fig. 6-8 1oo2 Evaluation in the user program, Symbol editing



The required parameters for operating the F-AI are set in the object properties of the F-AI added (see Fig. 6-9 and Fig. 6-10).

The parameters are summarized in Table 6-3.

Fig. 6-9: 1oo2 Evaluation in the user program, Parameters – part 1

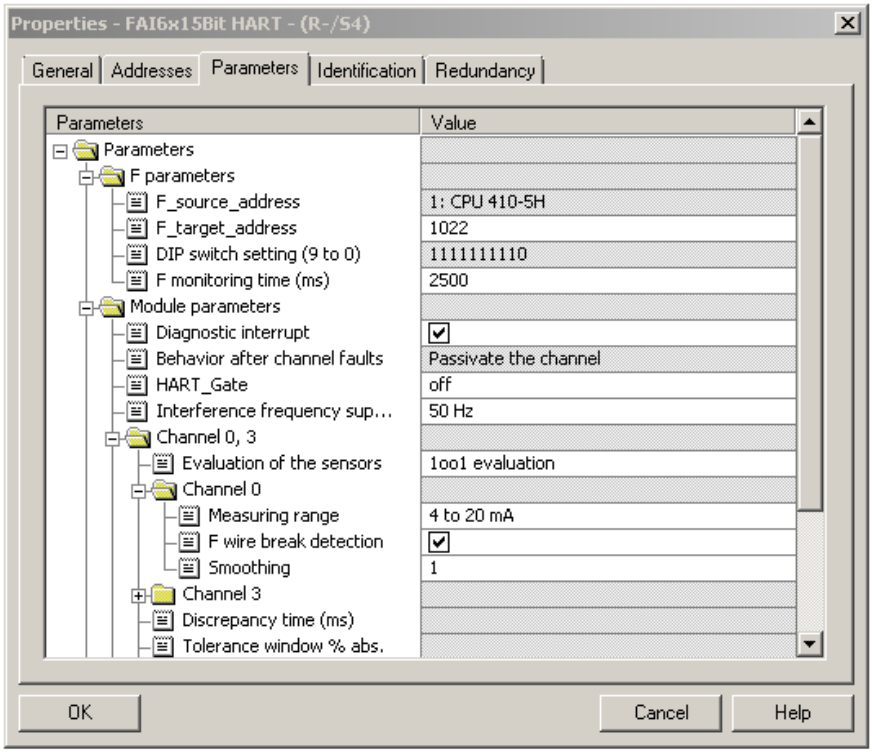


Fig. 6-10: 1oo2 Evaluation in the user program, Parameters – part 2

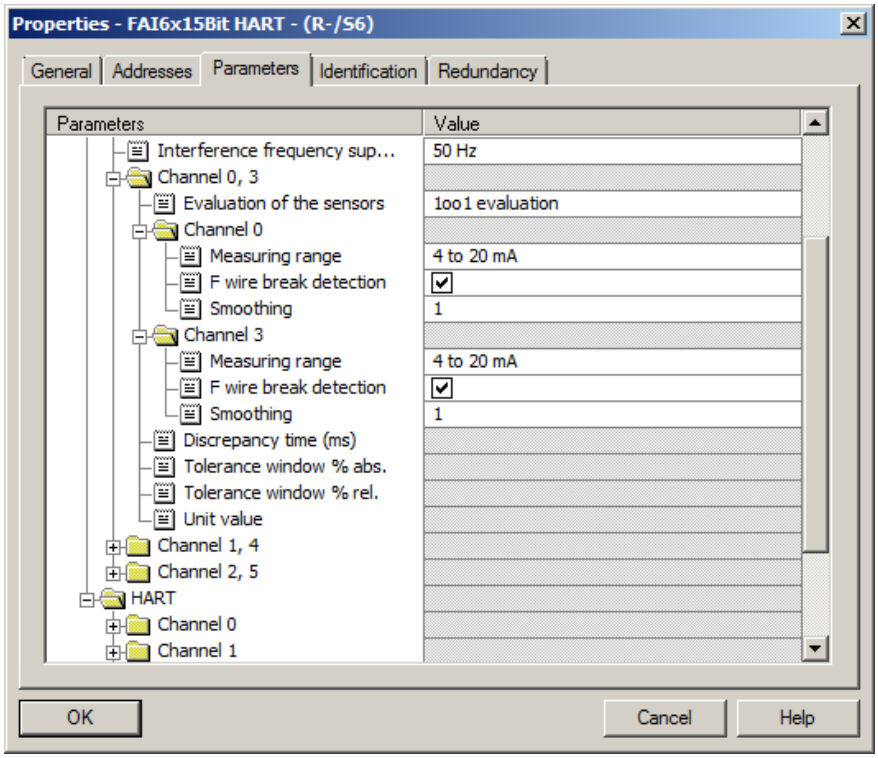


Table 6-3: 1oo2 evaluation in the user program. Hardware configuration parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
F-parameters		
F_destination_address	PROFIsafe address of the F-signal module (setting via DIP switch).	1-1022 or 0000000001... 1111111110
F_monitoring time (ms)	Monitoring time for safety-related communication between the CPU and the F-AI. **Remark:** A worksheet is available on the Siemens Support website to help users calculate F-monitoring times (see \10\ in the "Links and Literature" chapter).	0...65535ms Default 2500ms
Module parameters		
Diagnostic interrupt	A diagnostic interrupt is triggered by various error events that can be detected by the module. These events are then reported to the CPU. **Remark:** If the diagnostic interrupt is released at the module level, individual diagnostic events must be also activated at the channel level.	Release / lock
Behavior after channel faults	Passivate the entire module/ passivate the channel. **Remark:** Irrelevant for F systems	Module/ Channel
HART_Gate	Acts as a fail-safe "main switch" across the modules. HART communication is blocked with "Off". HART communication is enabled with "On". The HART modem can be switched out of the safety program for maintenance purposes with "switchable".	Off/ On/ switchable
Interference frequency suppression (Hz)	Selection for matching the integration time of the ADC to the network used. The integration time is: - 20 ms at 50 Hz - 16.66 ms at 60 Hz	50/60 Hz
Evaluation of the sensors	Channel activation by specifying the encoder evaluation. - Deactivated - 1oo1 (1v1) - 1oo21 (2v2) If 1oo1 is selected, the following parameters are not available: - Discrepancy time - Tolerance range - Unit value	1oo1 (1v1)
Measuring range	Measuring range selection for the channel.	0...20 mA 4...20 mA

Parameter	Description / Recommendations	Desired setting or permissible value range
F wire break detection	Select whether or not to enable wire break monitoring for the channel.	Release / lock
Smoothing	Number of measuring cycles through which smoothing is carried out.	1, 4, 16, 64

Note The hardware parameters and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

6.5 Configuring the logic

6.5.1 Configuring with Safety Matrix

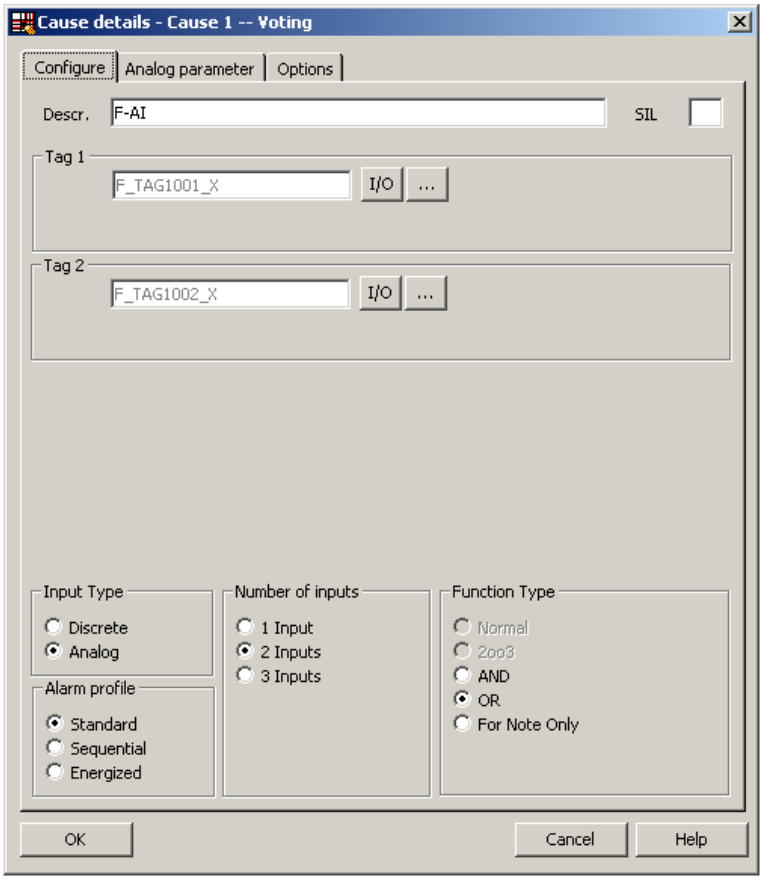
After the sensor signals have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented in the user program. One option is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

Fig. 6-11 illustrates how a cause for the 1oo2 evaluation of the sensor signals is configured in the matrix. The following settings must be used:

- Input Type: Analog
- 2 inputs
- Function type: OR (1oo2)
- Tag 1 and Tag 2 must be entered and should correspond to the symbolic I/O name of the encoder (e.g. F_TAG1001_X and F_TAG1002_X). The input can be added by selecting the signal from the symbol table. To do this, use the "I/O" button.

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

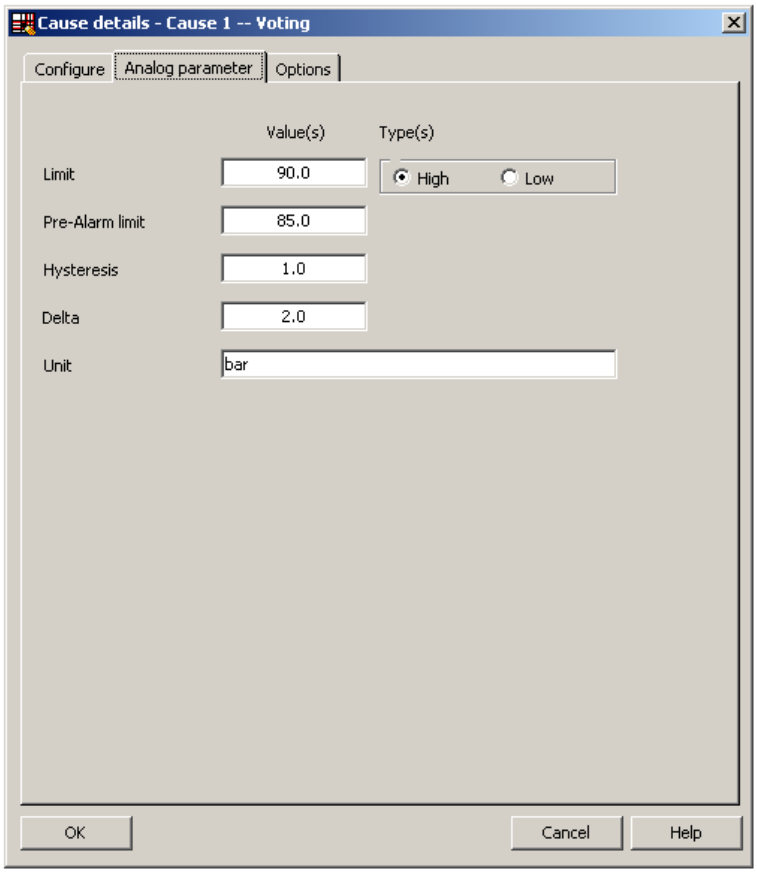
Fig. 6-11: 1oo2 evaluation in the user program (Safety Matrix – Configure)



As shown in Fig. 6-12, there are additional analog parameters that must be configured for the cause:

- Required parameters:
  - Limit type: MAX or MIN
  - Limit value
- Optional parameters:
  - Pre-alarm
  - Hysteresis
  - Delta
  - Units:

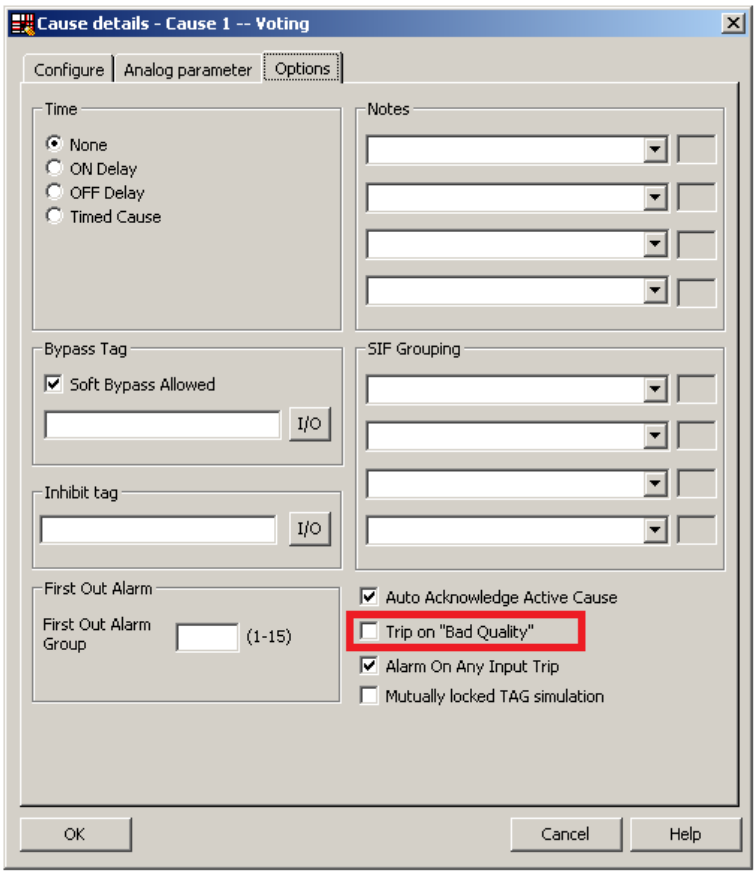
Fig. 6-12: 1oo2 evaluation in the user program (Safety Matrix – Analog parameter)



Additional attributes are available (e.g. time delay and bypass option), depending on the process application.

One configuration option highlighted in Fig. 6-13 is the shutdown behavior in case of a channel fault. If this option is activated, a channel fault will act as a violation of the limit on a sensor input. in the case of OR (1oo2), if there is a channel error and the option is enabled, the cause activates and triggers the corresponding effect(s).

Fig. 6-13: 1oo2 evaluation in the user program (Safety Matrix – Options)



6.5.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the 1oo2 evaluation logic for the input signals by means of the STEP 7 CFC Editor. After the sensor signals have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented with the CFC Editor.

There are two ways to implement the CFC logic:

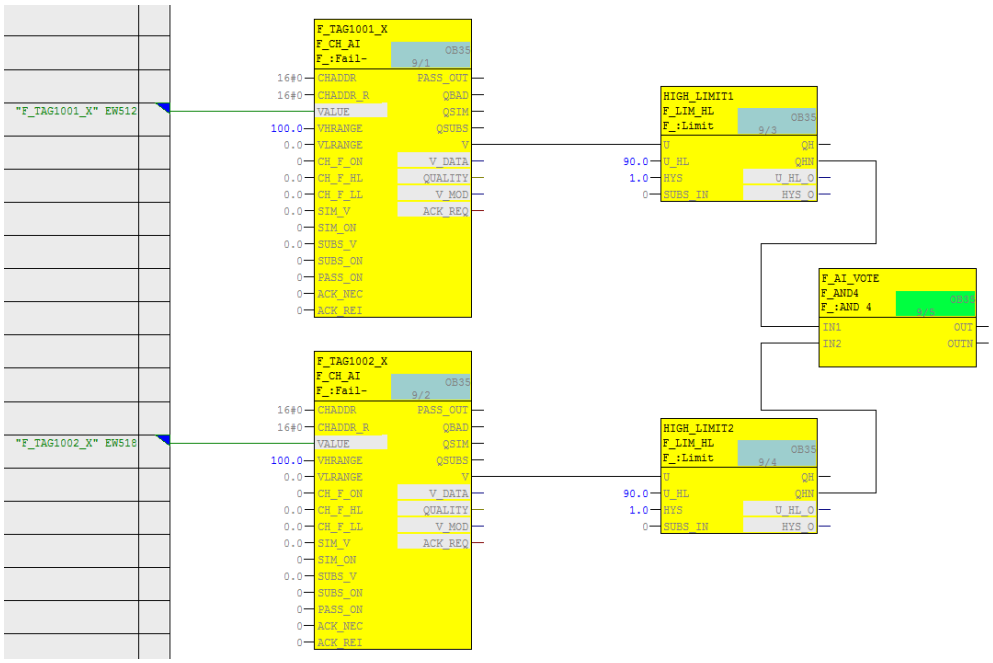
- Without channel fault evaluation
- With channel fault evaluation

Please note that by using the appropriate logic blocks, you can also implement a 2oo2 evaluation in the user program.

Logic without channel fault evaluation

Fig. 6-14 illustrates an example logic created in the CFC Editor for 1oo2 evaluation that does not take channel faults into account.
Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 6-14: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

The example logic in

Fig. 6-14 works as follows:

- If both analog sensors send a process value in the normal range (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value of one or both analog sensors exceeds the limit (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

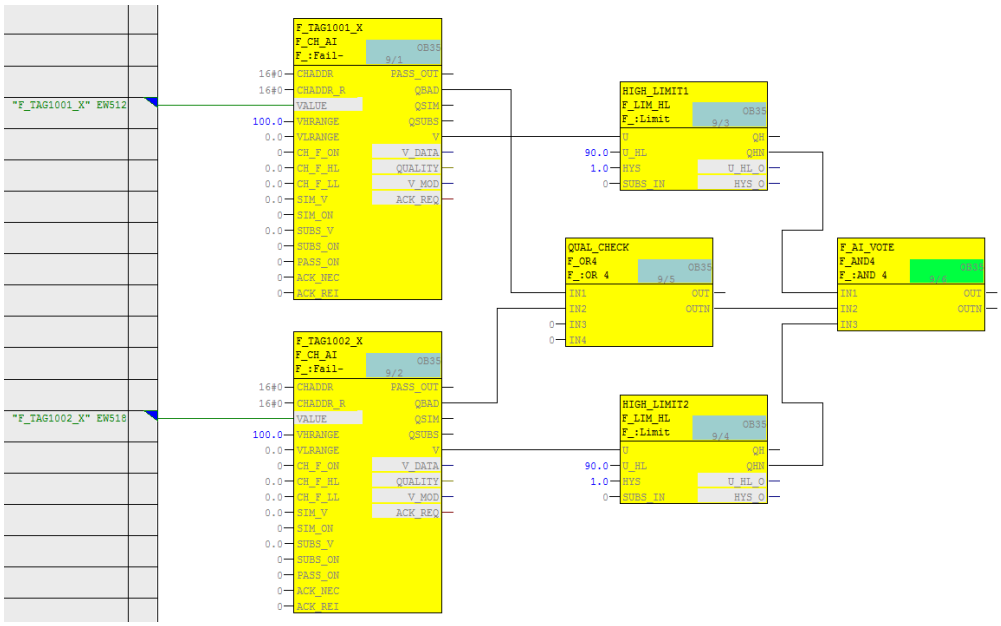
The necessary steps to create the logic are described below:

- Create an F_CH_AI channel driver for the first analog sensor and connect it to the address of the sensor connected to the F-AI (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI channel driver for the second analog sensor and connect it to the address of the sensor connected to the F-AI (e.g. F_TAG1002_X to EW518). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the negated output values of the limit blocks (QHN or QLN).

Logic with channel fault evaluation

Fig. 6-15 illustrates an example logic created in the CFC Editor for 1oo2 evaluation that takes channel faults into account.
Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 6-15: CFC logic – With channel fault evaluation



The example logic in

Fig. 6-15 works as follows:

- If both analog sensors send a process value in the normal range without channel fault (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value of one or both analog sensors exceeds the limit (here: a process value greater than or equal to 90) and the sensor does not report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- If at least one of the two analog sensors reports a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the first analog sensor and connect it to the address of the sensor connected to the F-AI (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the second analog sensor and connect it to the address of the sensor connected to the F-AI (e.g. F_TAG1002_X to EW518). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation of the 3 outputs for the following logic in order to generate the signal for the trigger command:
  - Use the negated output of the first F-channel driver's limit block (QHN or QLM).
  - Use the negated output of the second F-channel driver's limit block (QHN or QLM).
  - Use an OR block to connect the QBAD outputs of both F-channel drivers and use the output signal (OUTN) of the OR block.

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

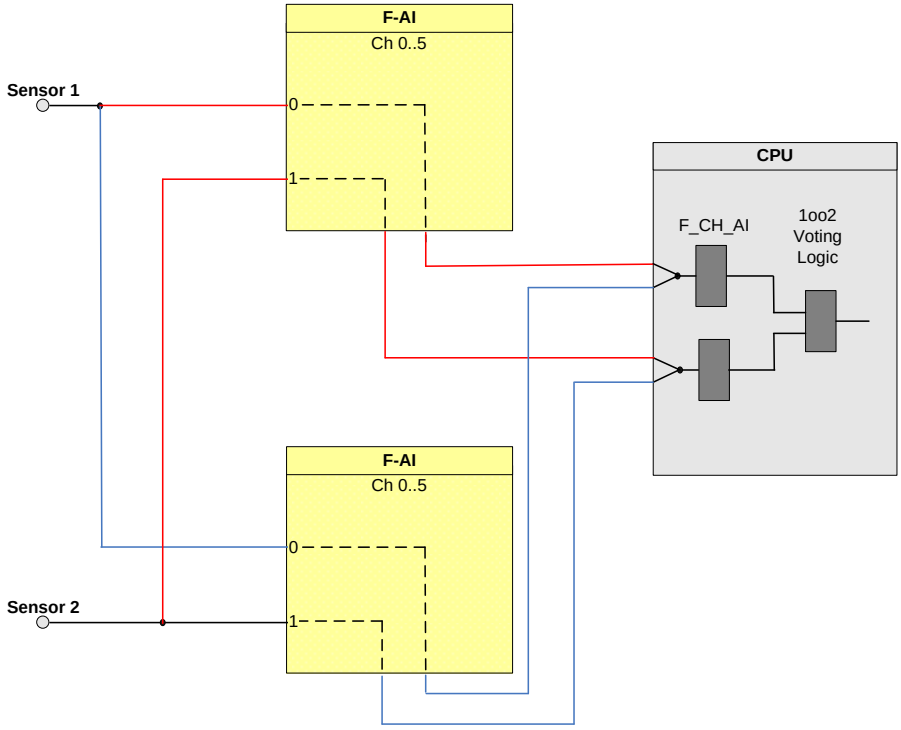
To increase the availability of the system, an architecture that requires two sensors can be realized with redundant modules in order to achieve the required SIL. Both evaluations are carried out in the user program.

Note The I/O modules in this architecture are certified for achieving the safety integrity levels of SIL3. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

In this architecture, two sensors are wired to a pair of redundant F-AIs. A block diagram can be found in Fig. 7-1.

In the diagram, the first sensor on Channel 0 is wired to both F-AIs. The second sensor is wired to Channel 1 of both F-AIs. The F-AIs are configured as redundant modules in the HW Config. Only one analog input channel driver block per sensor is required. The driver block selects a signal from the incoming signals of the redundant F-AI.

Fig. 7-1: 1oo2 evaluation in the user program – redundant F-AIs



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

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

Table 7-1: Failure combinations

Failed component detected?				Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**F-AI 1**	**F-AI 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 I/O modules does not increase the safety integrity 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 & evaluation architecture is calculated using this formula:

$PFD_{In} = PFD_{Sensor} + 2\ PFD_{F\text{-}AI} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

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

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

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

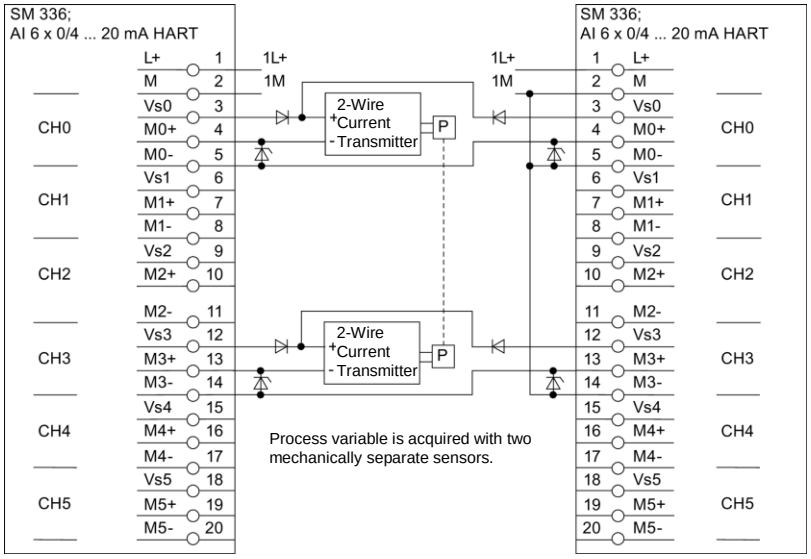
7.2 Wiring

7.2.1 Conventional wiring

A simplified example of the 2(1oo2) evaluation scheme with evaluation in the user program and redundant F-AI is illustrated in Fig. 7-2. The first sensor is wired to channel 0 (terminals 3, 4, 5) of both F-AIs and the second sensor is wired to channel 1 (terminals 6, 7, 8) of both F-AIs.

Please note that this architecture also requires two Zener diodes for each sensor. The first Zener diode has an avalanche voltage of 6.2 V and the second one has a avalanche voltage of 5.6V. Another two diodes are also used for decoupling the voltage supply. The diodes and Zener diodes are needed in case one of the F-AIs is out of service (e.g. module failure, routine maintenance, etc.).

Fig. 7-2: 1oo2 evaluation in the user program, redundant F-AI, 2-wire, 2-channel transmitter, internal supply

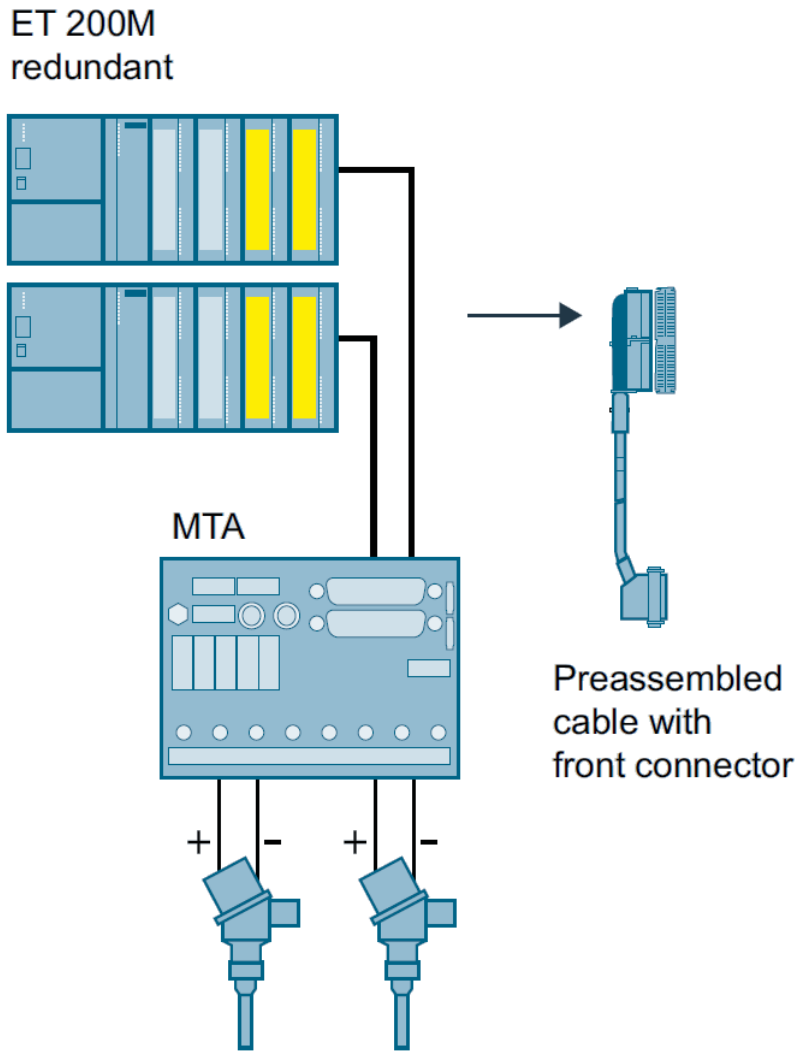


7.2.2 Wiring using an MTA (Marshalled Termination Assembly)

Siemens provides MTAs (Marshalled Termination Assemblies). By using an F-AI MTA for this evaluation scheme, the wiring between the sensors and the ET 200M signal modules is greatly simplified as it already includes the necessary diodes and Zener diodes.

You can find further relevant information in the Chapter "MTA (Marshalled Termination Assembly)".

Fig. 7-3: MTA



7.3 Parameters for hardware configuration

For the 2(1oo2) evaluation scheme with evaluation in the user program and redundant F-AIs, the F-AIs themselves are configured in the STEP 7 HW Config.

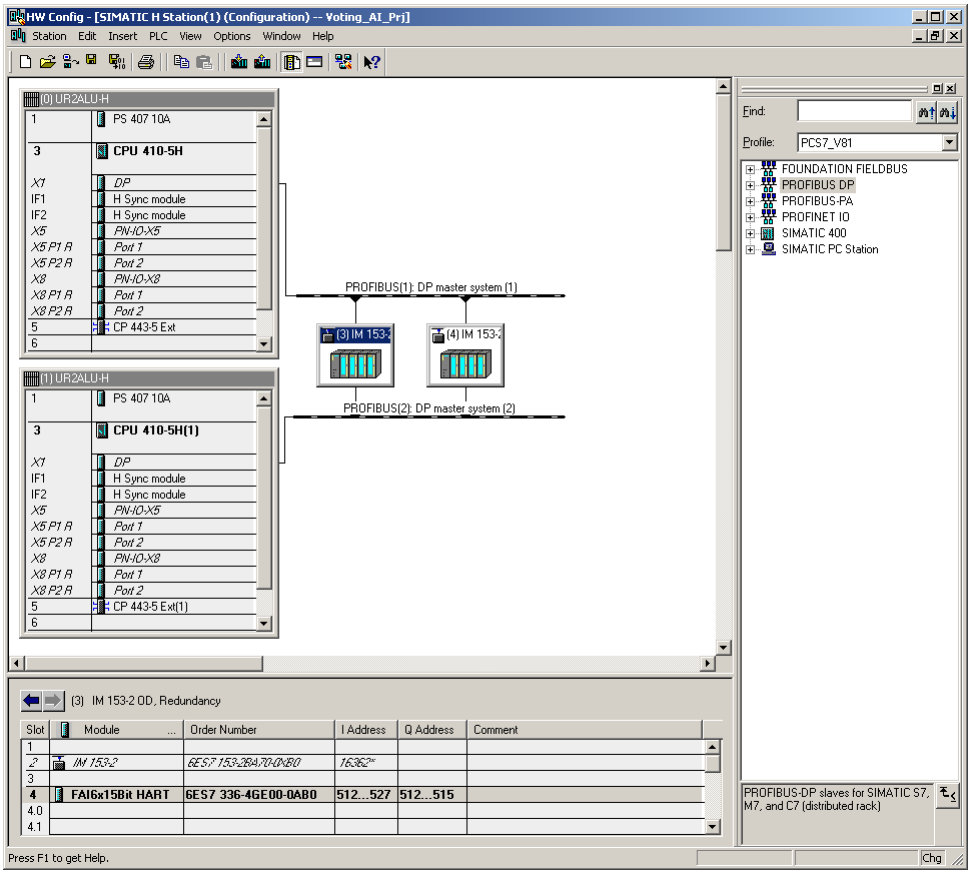
For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 7-4 illustrates a hardware configuration as an example.

In this example, there is an ET 200M (with PROFIBUS connection IM153-2) with PROFIBUS address 3 and a second ET 200M with PROFIBUS address 4. Each ET 200M contains one F-AI in slot 4.

For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 7-4: 1oo2 evaluation in the user program – redundant F-AI hardware configuration plan



The two F-AIs must be configured as a redundant pair in the HW Config. Each of the F-AI redundancy settings can be accessed through the object properties of the F-AIs.

For further information on hardware, see \4\ in the "Links and Literature" chapter.

In Fig. 7-4, the redundancy settings are made with PROFIBUS address 3 using the F-AI in the ET 200M. The settings are summarized in Table 7-2.

Fig. 7-5: 1oo2 evaluation in the user program – redundant F-AI Redundancy parameters

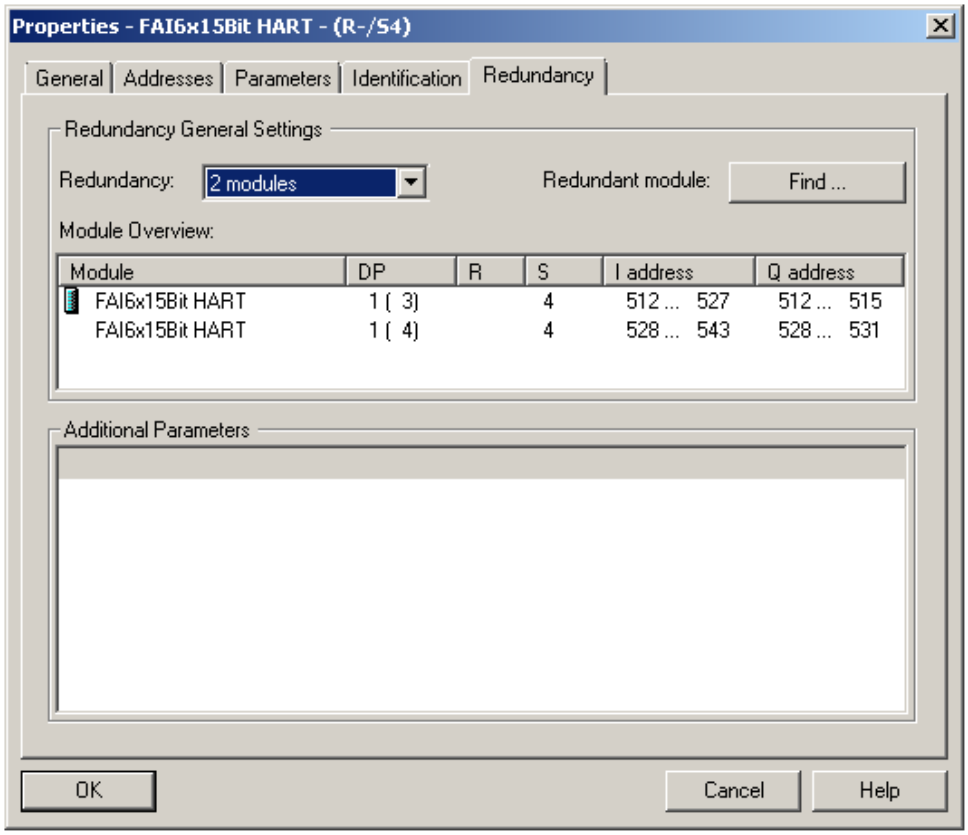


Table 7-2: 2 1oo2 evaluation in the user program – redundant F-AI - Redundancy parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-AI is acting as part of a redundant pair or not. **Remark:** For redundancy, the parameter must be set to 2 modules.	Two (2) modules
Redundant module	Used for selecting the redundant partner module.	

Note The parameter names and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

If the redundancy settings have been made, the other hardware parameters can be set in one of the redundant F-AIs. The settings are automatically applied to the redundant module.

7.4 Creating the Logic

Although this evaluation scheme uses redundant F-AIs, only two F_CH_AI F-channel driver blocks are needed in the logic configuration (one F-channel driver for each of the two sensors). The F-channel drivers can be added and configured automatically from the SIMATIC Safety Matrix or manually using the STEP 7 CFC Editor. In both cases, the drivers must be connected to the analog sensor signal of the F-AI with the lowest I/O address.

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

7.4.1 Configuring with Safety Matrix

After the sensor signals have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented in the user program. One option is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

The actual evaluation logic of the 2(1oo2) evaluation scheme with evaluation in the user program and redundant F-AI is identical to the one described in Section 6.5.1 (Configuring with Safety Matrix).

7.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the 1oo2 evaluation logic for the input signals by means of the STEP 7 CFC Editor. After the sensor signals have been added to the hardware configuration, the 1oo2 evaluation logic can be implemented with the CFC Editor.

There are two ways to implement the CFC logic:

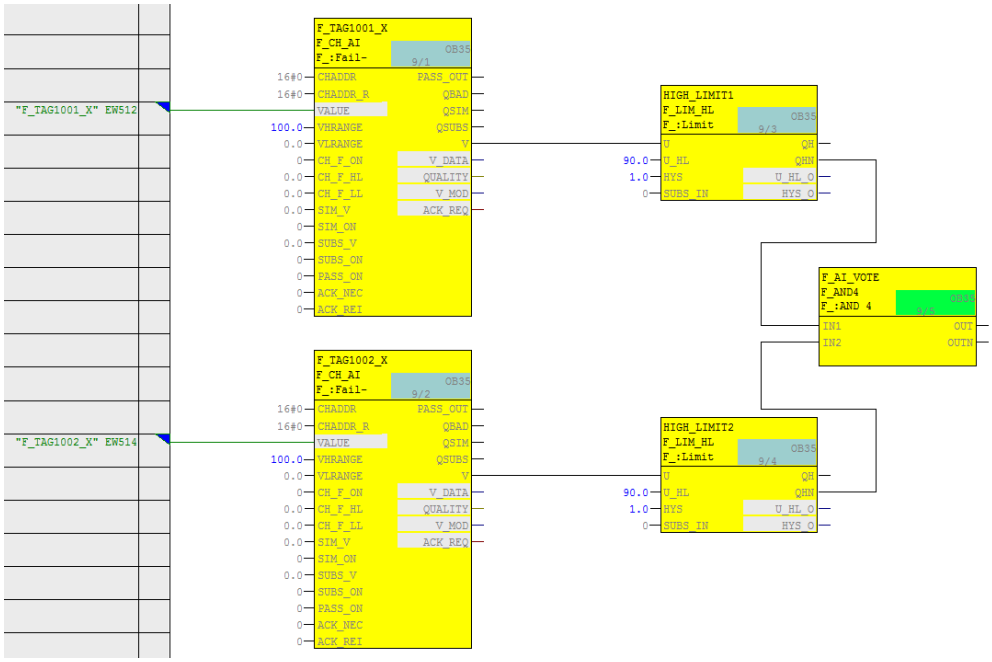
- Without channel fault evaluation
- With channel fault evaluation

Please note that by using the appropriate
logic blocks, you can also implement a 2oo2 evaluation in the user program.

Logic without channel fault evaluation

Fig. 6-14 illustrates an example logic created in the CFC Editor for 1oo2 evaluation that does not take channel faults into account.
Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 7-6: CFC Logic – Without channel fault evaluation



Note Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

The example logic in Fig. 7-6 works as follows:

- If both analog sensors send a process value in the normal range (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value of one or both analog sensors exceeds the limit (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

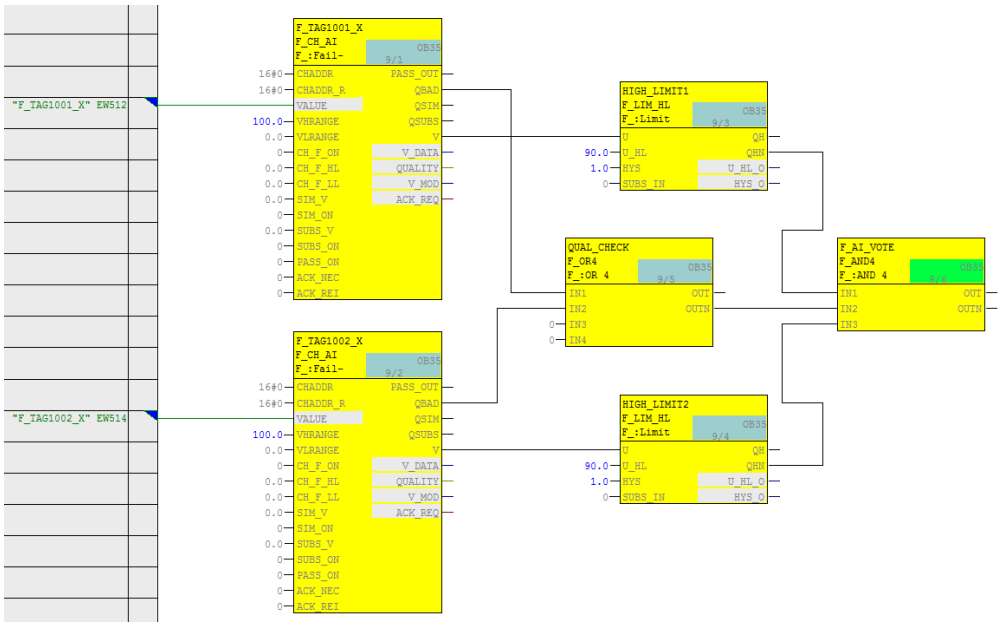
- Create an F_CH_AI channel driver for the first analog sensor and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI channel driver for the second analog sensor and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1002_X to EW514). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation for the negated output values of the limit blocks (QHN or QLN).

Logic with channel fault evaluation

Figure 7-7 illustrates an example logic created in the CFC Editor for 1oo2 evaluation that takes a channel fault into account.

Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Figure 7-7: CFC logic – With channel fault evaluation



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

- If both analog sensors send a process value in the normal range without channel fault (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If the process value of one or both analog sensors exceeds the limit (here: a process value greater than or equal to 90) and the sensor does not report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- If at least one of the two analog sensors reports a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI channel driver for the first analog sensor and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1001_X to EW512). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI channel driver for the second analog sensor and connect it to the symbol on the F-AI with the lowest address (e.g. F_TAG1002_X to EW514). Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an AND operation of the 3 outputs for the following logic in order to generate the signal for the trigger command:
  - Use the negated output of the limit block (QHN or QLM) of the first channel driver block.
  - Use the negated output of the limit block (QHN or QLM) of the second channel driver block.
  - Use an OR block to connect the QBAD outputs of both channel driver blocks and use the output signal (OUTN) of the OR block.

8 Hardware configuration and wiring of three sensors and three F-AIs (2oo3) with evaluation in the user program

The three-sensors (or 2oo3 evaluation scheme) refers to applications that require two sensors to achieve the Safety Integrity Level and a third sensor for higher availability. 2oo3 evaluation means that two out of three sensors have to trigger.

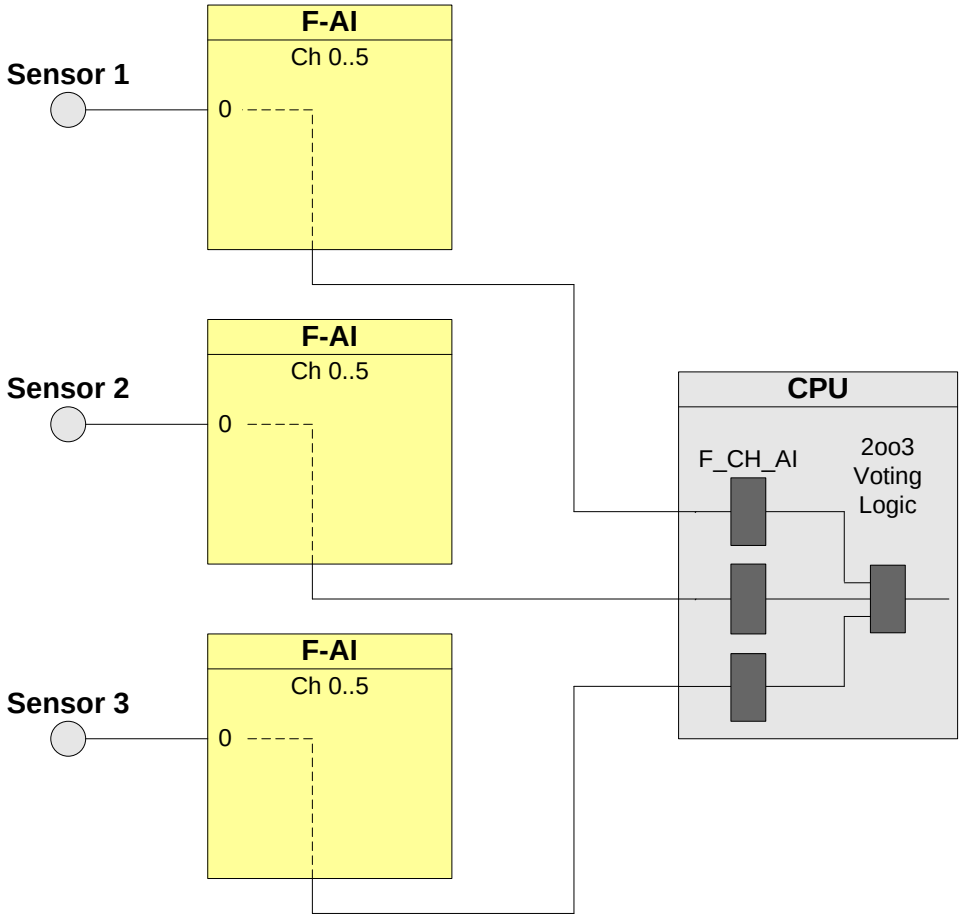
Note The I/O modules in this architecture are certified for the safety integrity level **SIL3**. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

The 2oo3 base architecture with evaluation in the user program uses three sensors and three F-AI. A block diagram can be found in Fig. 8-1. In the diagram, each sensor on Channel 0 is wired to one F-AI. In this example, the F-AI are integrated into an ET 200M.

Please note that due to the system flexibility, there could be also other architectures that differ to the variant described in terms of the availability of the modules and ET 200M racks, e.g.:

- **Low availability:**
  All three sensors are connected to one module.
- **Similar availability of the modules:**
  All three sensors are connected to two mutually redundant modules. The two modules are integrated in the same ET 200M rack.
- **Higher availability of modules and ET 200M racks:**
  All three sensors are connected to two mutually redundant modules. The two modules are integrated in various ET 200M racks (see Chapter 9).
- **Higher availability of modules and ET 200M racks:**
  Each sensor is connected to a module. The modules are integrated in various ET 200M racks.

Fig. 8-1: 2oo3 – architecture



The hardware configuration according to Figure 8-1 is suitable for achieving **SIL3**.

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

Failed component detected?						Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**Sensor 3**	**F-AI 1**	**F-AI 2**	**F-AI 3**	
Yes	No	No	Yes	No	No	Yes (not required)
			No	Yes	No	Yes
			No	No	Yes	Yes
No	Yes	No	Yes	No	No	Yes
			No	Yes	No	Yes (not required)
			No	No	Yes	Yes
No	No	Yes	Yes	No	No	Yes
			No	Yes	No	Yes
			No	No	Yes	Yes (not required)
X	Yes	Yes	X	X	X	Yes
Yes	X	Yes				
Yes	Yes	X				
X	X	X	X	Yes	Yes	
			Yes	X	Yes	
			Yes	Yes	X	

8.1 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 and evaluation architecture is calculated using this formula:

$PFD_{In} = PFD_{2oo3} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

The *PFD* value for one 2oo3 input circuit is calculated using the following [8] formula:

$$PFD_{2oo3} \approx 4 \cdot {PFD_{1oo1}}^2 + 1.5 \cdot \beta \cdot PFD_{1oo1}$$

With: $PFD_{1oo1} = PFD_{Sensor} + PFD_{F-AI}$

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

8.2 Wiring

8.2.1 Conventional wiring

In the 2oo3 evaluation scheme, the F-AI or an external voltage source can supply the sensors with voltage.

Fig. 8-2 illustrates a wiring example for 2-wire transmitters and
Fig. 8-3 illustrates a wiring example for 4-wire transmitters.

In both diagrams, each transmitter on Channel 0 is wired to one F-AI.

Fig. 8-2: 2oo3, evaluation in the user program with 3 F-AIs and 3 transmitters, 2-wire, internal supply.

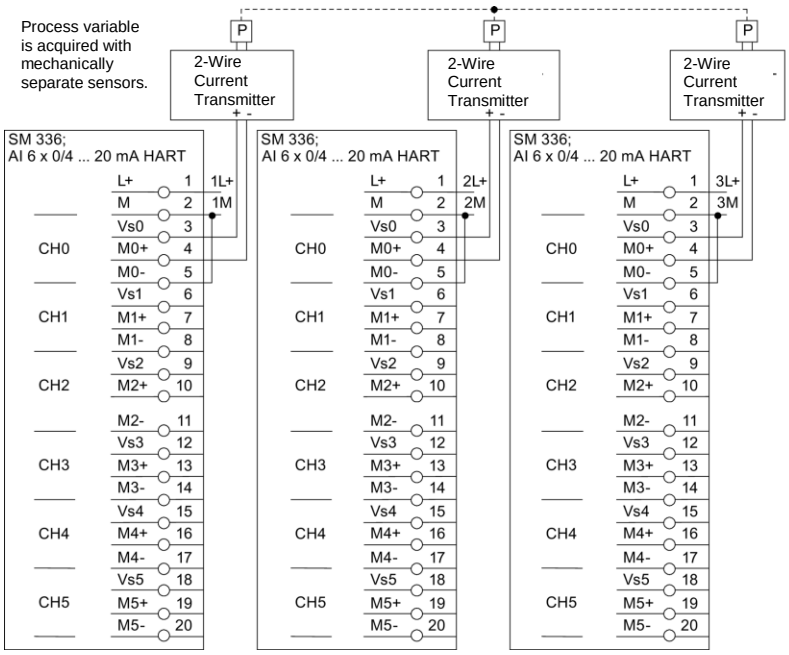


Fig. 8-3: 2oo3 evaluation in the user program with 3 F-AIs and 3 transmitters, 4-wire, internal supply.

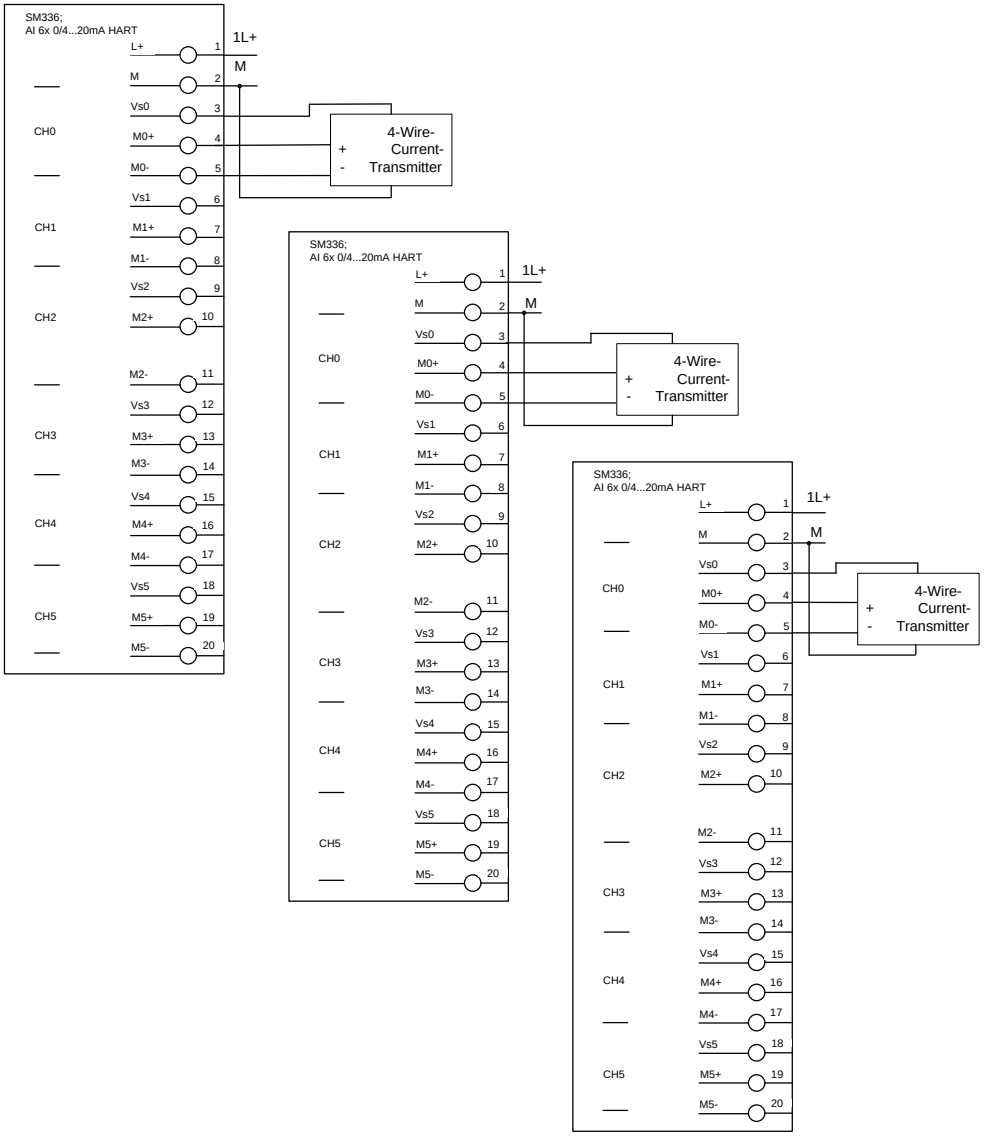


Fig. 8-4 illustrates a wiring example for 2-wire transmitters with one external voltage source and Fig. 8-5 shows a wiring example for 4-wire transmitters with one external voltage source.

In both diagrams, each transmitter on Channel 0 is wired to one F-AI.

Fig. 8-4: 2oo3 evaluation in the user program with 3 F-AIs and 3 transmitters, 2-wire, external supply.

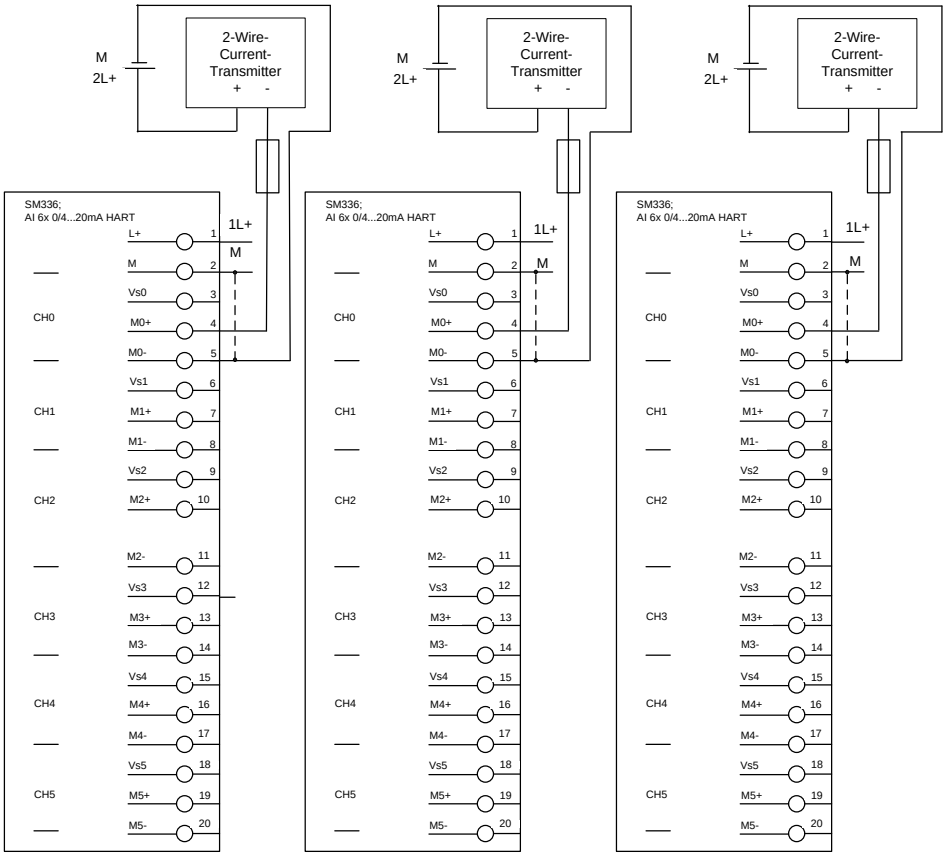
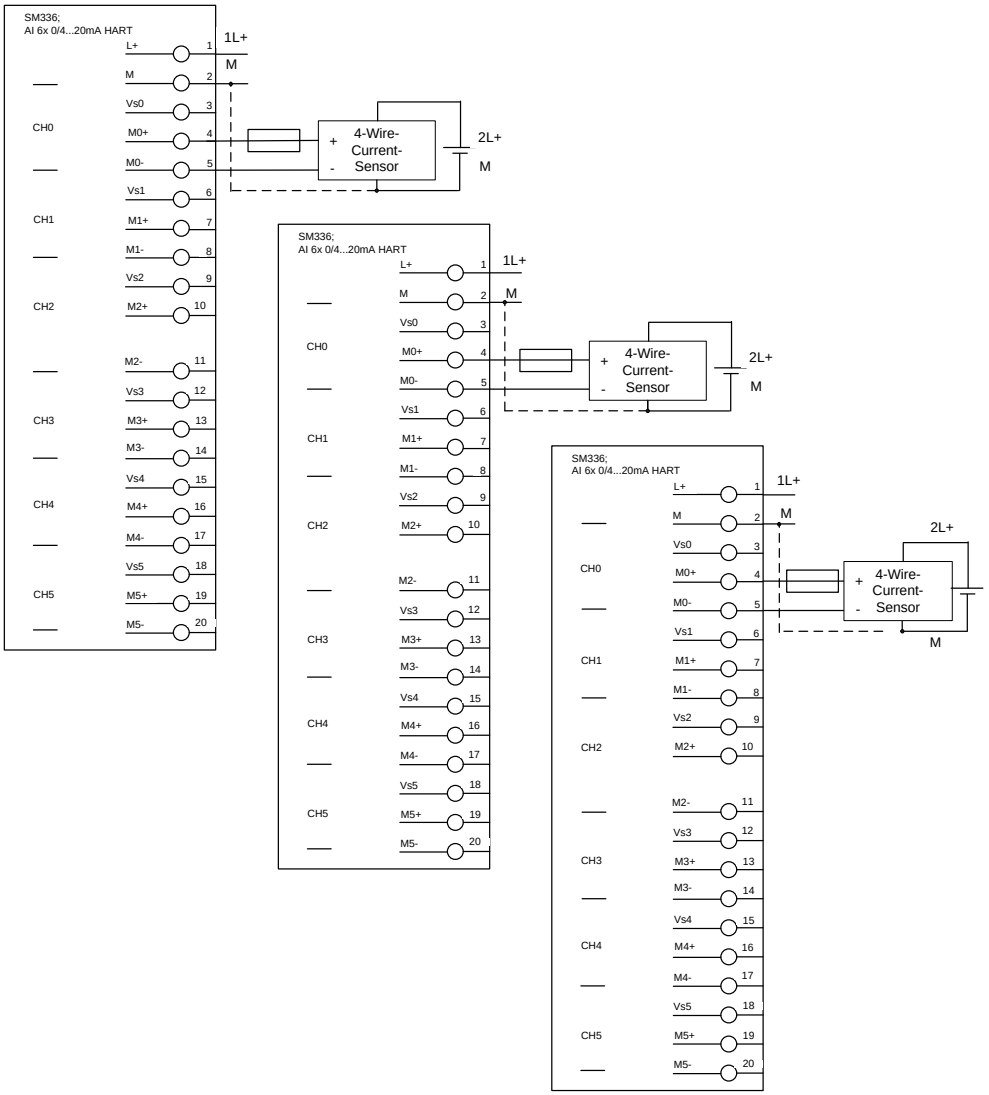


Fig. 8-5: 2oo3 evaluation in the user program with 3 F-AIs and 3 transmitters, 4-wire, external supply.



8.3 Parameters for hardware configuration

The three F-AIs required for the 2oo3 evaluation scheme are configured in STEP 7 HW Config. For configuration, select the F-AI in the STEP 7 hardware catalog. Add this to the existing hardware configuration once. Configure the channels used and assign meaningful symbol names.

Fig. 8-6: 2oo3 evaluation in the user program – symbol editing

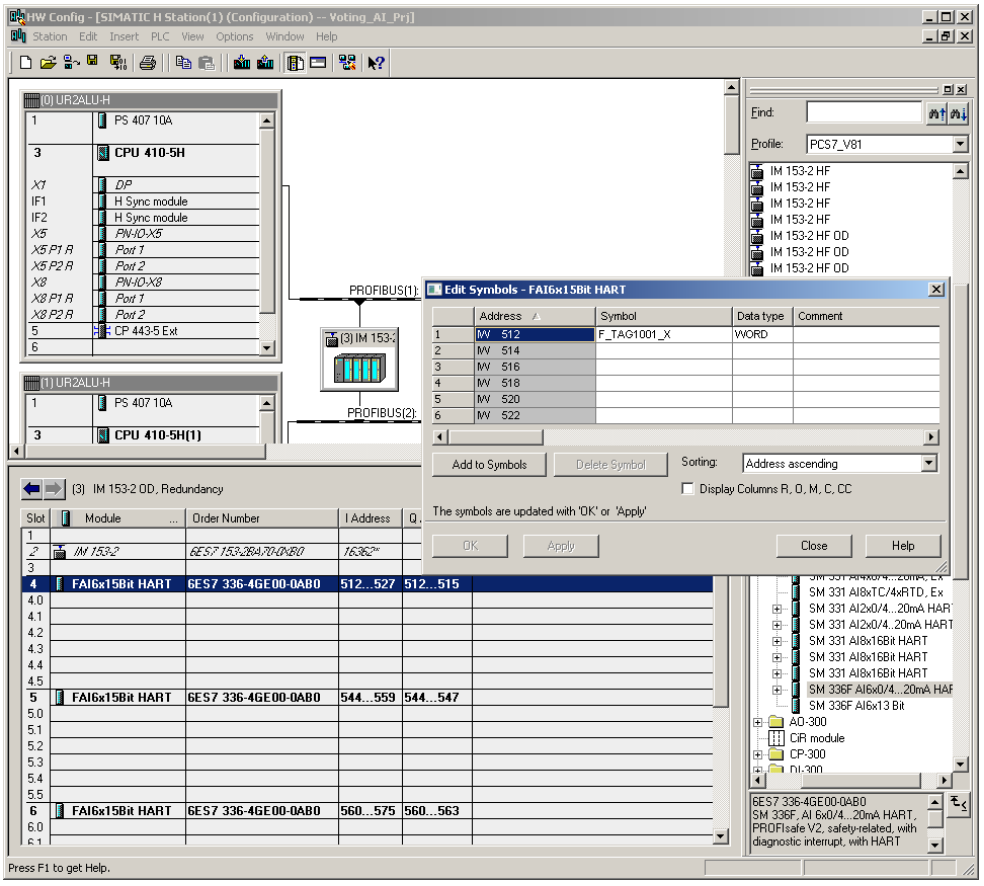


Fig. 8-6 shows an example of a hardware configuration with three F-AIs. In this example, the ET 200M (IM153-2) contains an F-AI in each of slots 4, 5 and 6. Each of the three sensor signals is wired to the first channel of an F-AI. For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

The required parameters for operating the F-AI are set in the object properties of the F-AI added (see Fig. 8-7).
The parameters themselves are summarized in Table 8-1.

Fig. 8-7: 2oo3 evaluation in the user program – Parameters

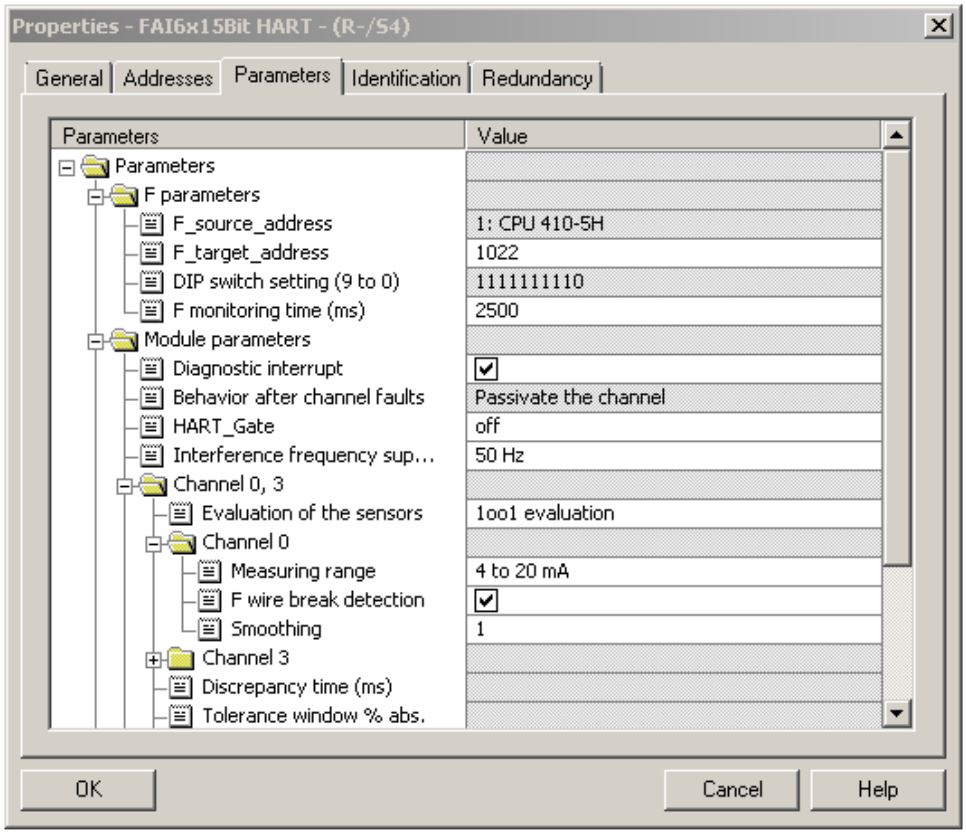


Table 8-1: 2oo3 evaluation in the user program – Parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
F-parameters		
F_destination_address	PROFIsafe address of the F-signal module (setting via DIP switch).	1-1022 0000000001... 1111111110
F_monitoring_time (ms)	Monitoring time for safety-related communication between the CPU and the F-AI. **Remark:** A worksheet is available on the Siemens Support website to help users calculate F-monitoring times (see \10\ in the "Links and Literature" chapter).	0...65535 ms Default 2500 ms

Parameter	Description / Recommendations	Desired setting or permissible value range
Module parameters		
Diagnostic interrupt	A diagnostic interrupt is triggered by various error events that can be detected by the module. These events are then reported to the CPU. **Remark:** If the diagnostic interrupt is released at the module level, individual diagnostic events must be also activated at the channel level.	Release / lock
Behavior after channel faults	Passivate the entire module/ passivate the channel. **Remark:** Irrelevant for F systems	Module/ Channel
HART_Gate	Acts as a fail-safe "main switch" across the modules. HART communication is blocked with "Off". HART communication is enabled with "On". The HART modem can be switched out of the safety program for maintenance purposes with "switchable".	Off/ On/ switchable
Interference frequency suppression (Hz)	Selection for matching the integration time of the ADC to the network used. The integration time is: - 20 ms at 50 Hz - 16.66 ms at 60 Hz	50/60 Hz
Evaluation of the sensors	Channel activation by specifying the encoder evaluation. - Deactivated - 1oo1 (1v1) - 1oo2 (2v2) If 1oo1 is selected, the following parameters are not available: - Discrepancy time - Tolerance range - Unit value	1oo1 (1v1)
Measuring range	Measuring range selection for the channel.	0...20 mA 4...20 mA
F_wire-break detection	Select whether or not to enable wire break monitoring for the channel.	Release / lock
Smoothing	Number of measuring cycles through which smoothing is carried out.	1, 4, 16, 64

Note The hardware parameters and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

8.4 Creating the Logic

8.4.1 Configuring with Safety Matrix

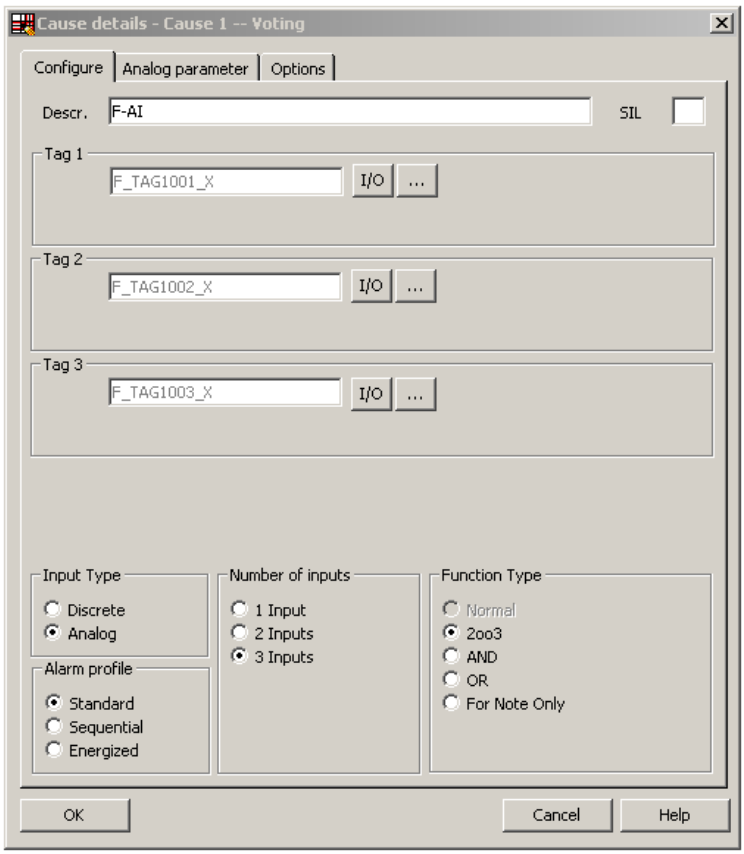
After the three sensor signals have been added to the hardware configuration, the 2oo3 evaluation logic can be implemented in the user program. One option is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

Figure 8-8 illustrates how a cause is configured in the Matrix for 2oo3 evaluation. The following settings must be used:

- Input Type: Analog
- 3 inputs
- Function type: Majority Evaluation (2oo3 evaluation)
- Tag 1, Tag 2 and Tag 3 must be entered and should correspond to the symbolic I/O name of the encoder (e.g. F_TAG1001_X, F_TAG1002_X and F_TAG 1003_X). The input can be added by selecting the signal from the symbol table. To do this, use the "I/O" button.

The cause is configured with a Majority Evaluation (2oo3 evaluation) function type. If at least two of the three encoders are released for triggering, the cause activates and triggers the corresponding effect(s). Please note that it is also possible to configure other evaluation architectures – 1oo3 (OR) or 3oo3 (AND) – in the "Function Type" field.

Figure 8-8: Safety Matrix – Configure

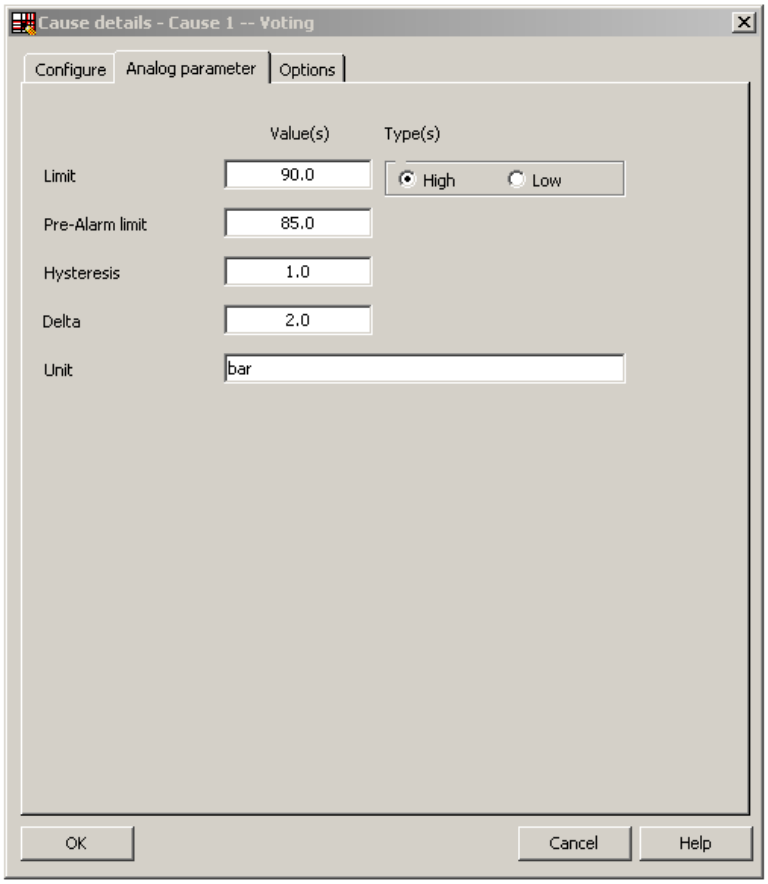


As shown in Fig. 8-9, there are additional analog parameters that must be set for the cause:

- Required parameters:
  - Limit type: MAX or MIN
  - Limit value
- Optional parameters:
  - Pre-alarm
  - Hysteresis
  - Delta
  - Unit of measurement

Exceeding the delta value is reported. It is not considered a shutdown criterion.

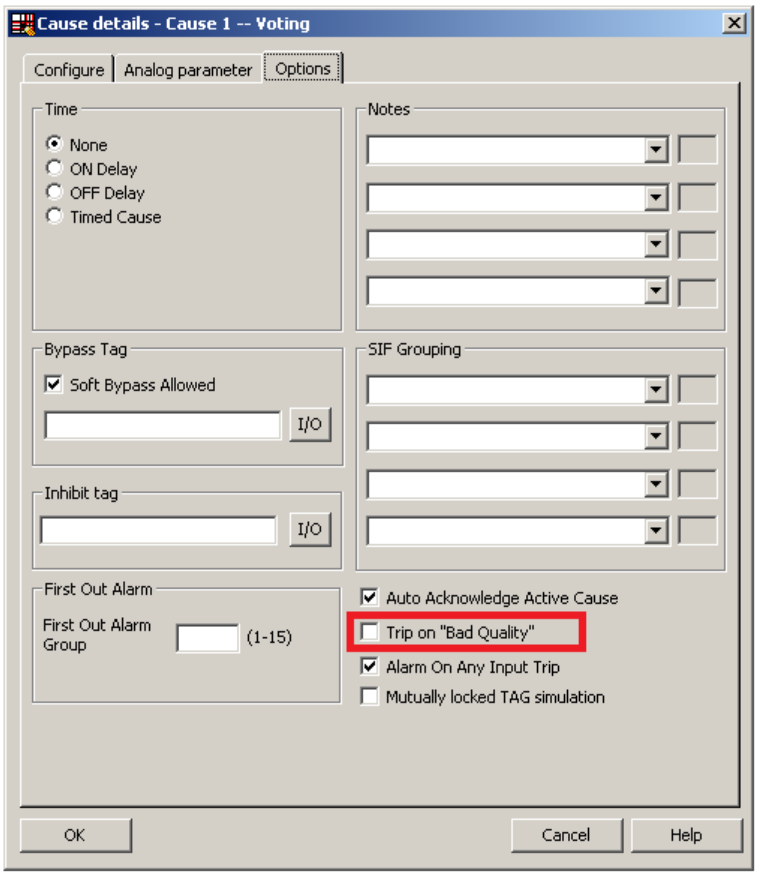
Fig. 8-9: Safety Matrix - Analog parameter



Additional attributes are available (e.g. time delay and bypass option), depending on the process application.

One configuration option highlighted in Fig. 8-10 is the shutdown behavior in case of a channel fault.
If this option is activated, a channel fault at one of the sensor inputs is evaluated as a trigger signal. In a Majority Evaluation (2oo3) (if this option is enabled), the cause is activated and the relevant effect(s) are triggered on the occurrence of two channel faults, or a channel fault and a channel limit violation.

Fig. 8-10: Safety Matrix – Options



8.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the 2oo3 evaluation logic for the CPU by means of the STEP 7 CFC Editor. After the three sensor signals have been added to the hardware configuration, the 2oo3 evaluation logic can be made with the CFC Editor.

There are two ways to implement the CFC logic:

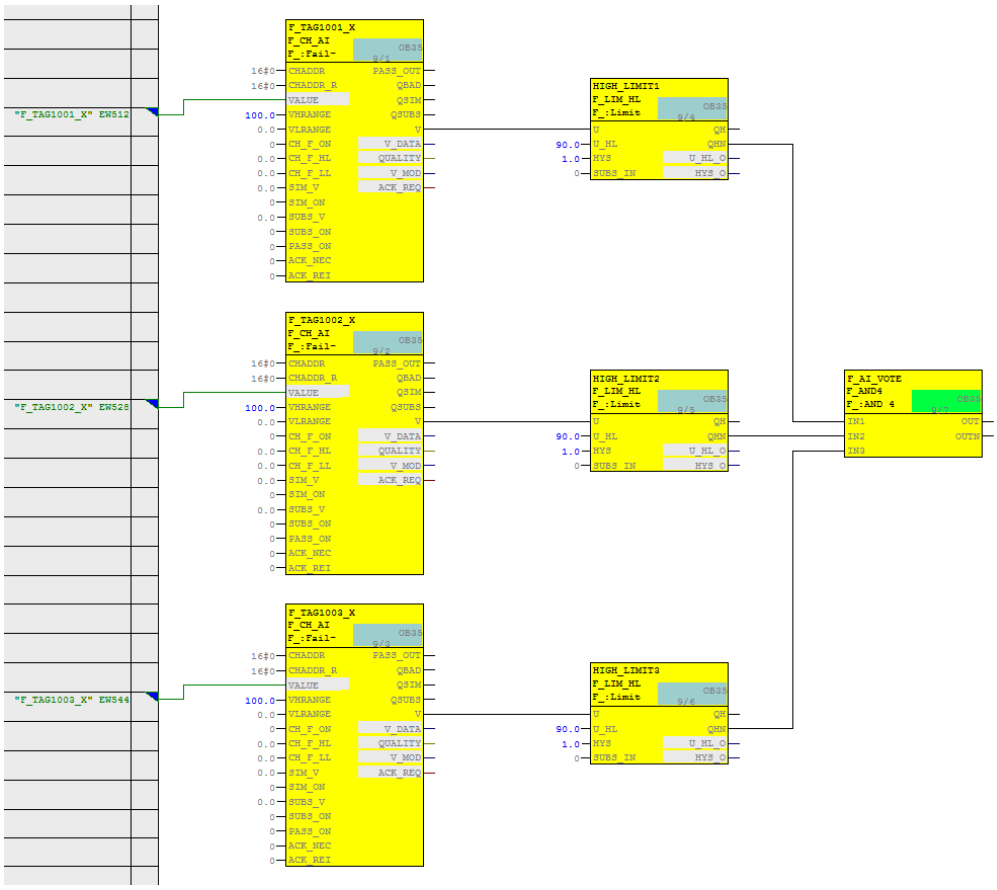
- Without channel fault evaluation
- With channel fault evaluation

Logic without channel fault evaluation

The logic corresponds to the Safety Matrix configuration, in which the function "Trip on bad quality" is not enabled. The input signals are not monitored for a maximum delta.

Figure 8-11 shows an example logic for 2oo3 evaluation in the CFC Editor, which does not take channel faults into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state
(Normal State = 1, Safe State = 0).

Figure 8-11: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.

In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

Figure 8-11 works as follows:

- If at least two of the three analog sensors report a normal value (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If at least two analog sensors report an upper limit violation (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the first analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the second analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the third analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Connect the negated outputs of the limit value blocks (QHN or QLN) with the inputs of an F_2OUT3 block in order to generate the signal for the trigger command.

Logic with channel fault evaluation

The logic corresponds to the Safety Matrix configuration, in which the function "Trip on bad quality" is enabled. The input signals are not monitored for a maximum delta.

Fig. 8-12 shows an example logic for 2oo3 evaluation in the CFC Editor, which takes channel faults into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 8-12: CFC logic – With channel fault evaluation

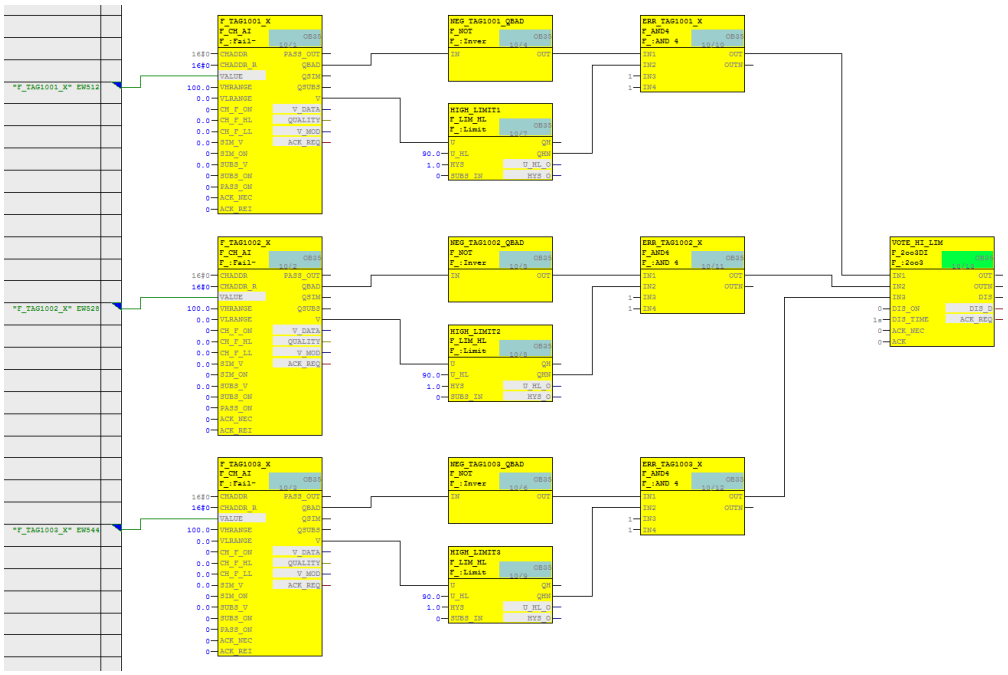


Fig. 8-12 works as follows:

- If at least two of the three analog sensors report a normal value without channel faults (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If two or more analog sensors report an upper limit violation without channel fault (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- If two or more analog sensors report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- If one sensor reports a channel fault and the other two sensors do not report a channel fault, only the values of the sensors without channel faults are used for the evaluation logic.
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI channel driver for the first analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI channel driver for the second analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI channel driver for the third analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Implement the evaluation logic by interconnecting the inputs of an F_2OUT3 block with the outputs of the following AND operations:
  - The negated output QBAD (F_NOT) of the first channel driver with the negated value of the first limit module output (QHN or QLN).
  - The negated output QBAD (F_NOT) of the second channel driver with the negated value of the second limit module output (QHN or QLN).
  - The negated output QBAD (F_NOT) of the third channel driver with the negated value of the third limit module output (QHN or QLN).

9 Hardware configuration and wiring of three sensors (2oo3) with redundant F-AI (2oo2) and evaluation in the user program

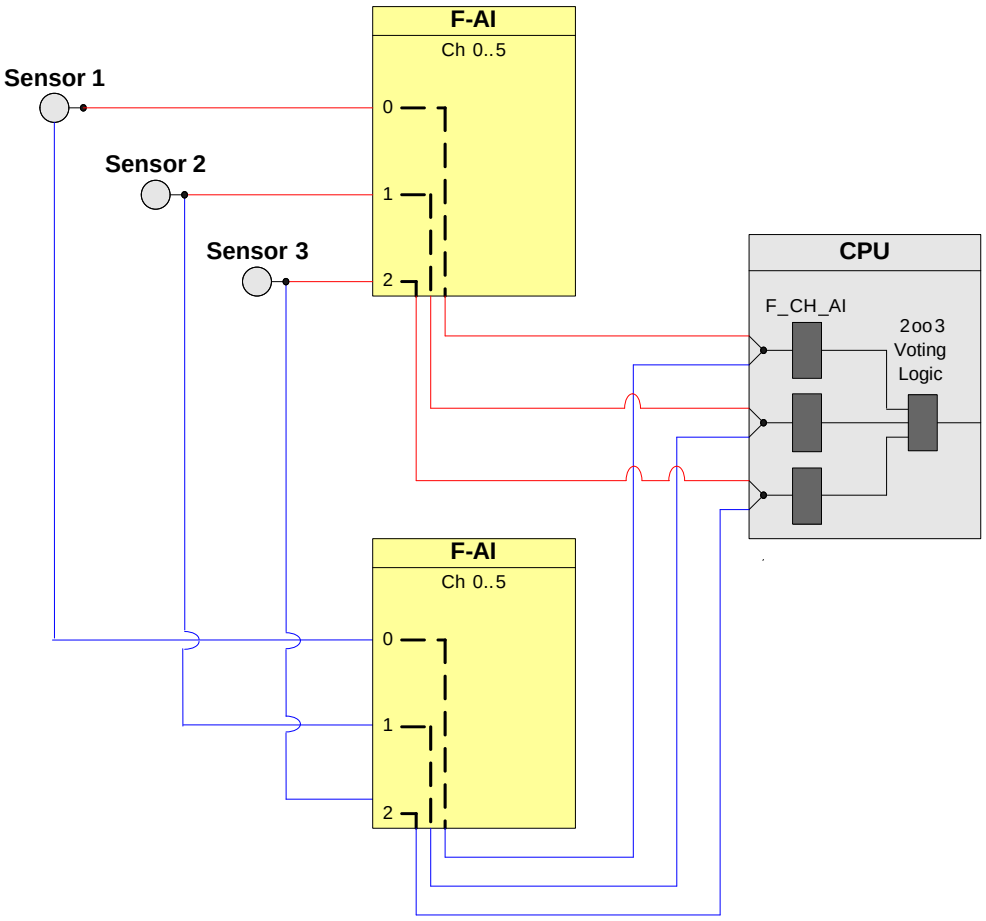
There are additional 2oo3 evaluation architectures in which the three sensors are wired to redundant F-AIs.

As with previous architectures, this 2oo3 evaluation scheme refers to applications that require two sensors to achieve the required security level. In this architecture, the third sensor increases the availability. Two of three sensors have to function. If at least two sensors indicate a trigger condition, the safety logic is triggered.

Note These architectures are able to achieve the safety integrity level SIL3 because the three signals are evaluated in the user program. However, to be SIL-compliant, the entire safety function – including the field devices – must be assessed according to IEC 61508/IEC 61511.

Figure 9-1 illustrates a block diagram with redundant F-AI. This optional 2oo3 architecture uses three sensors and two redundant F-AIs in two ET 200M racks. The three sensors in the diagram are wired to channels 0, 1 and 2 of both F-AIs.

Figure 9-1: 2oo3 optional architecture with redundant modules



The hardware configuration according to Figure 9-1 is suitable for achieving **SIL3**.

This redundant 2oo3 architecture is one possible variant.

Although it uses an F-AI less than the previously described architecture, it has similar availability. If only a few fail-safe analog inputs are needed, this variant is a more cost-effective alternative.

The non-redundant version is also a possible option when only one F-AI is available. It allows for high sensor availability, but compromises the higher availability of the F-AI.

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

Table 9-1: Failure combinations

Failed component detected?					Tripping of the safety function possible?
Sensor 1	**Sensor 2**	**Sensor 3**	**F-AI 1**	**F-AI 2**	
X	No	No	X	No	Yes (not required)
No	X	No			
No	No	X			
X	No	No	No	X	
No	X	No			
No	No	X			
X	X	X	Yes	Yes	Yes
X	Yes	Yes	X	X	
Yes	X	Yes			
Yes	Yes	X			

Note The redundancy of the I/O modules does not increase the safety integrity level.

9.1 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 & evaluation architecture is calculated using this formula:

$PFD_{2oo3} = PFD_{Sensor} + 2\ PFD_{F\text{-}AI} + PFD_{CPU}$

The $PFD_{F\text{-}AI}$ and PFD_{CPU} values are located in Section 10.

The PFD_{Sensor} value for one 2oo3 sensor is calculated using the following formula [9]:

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

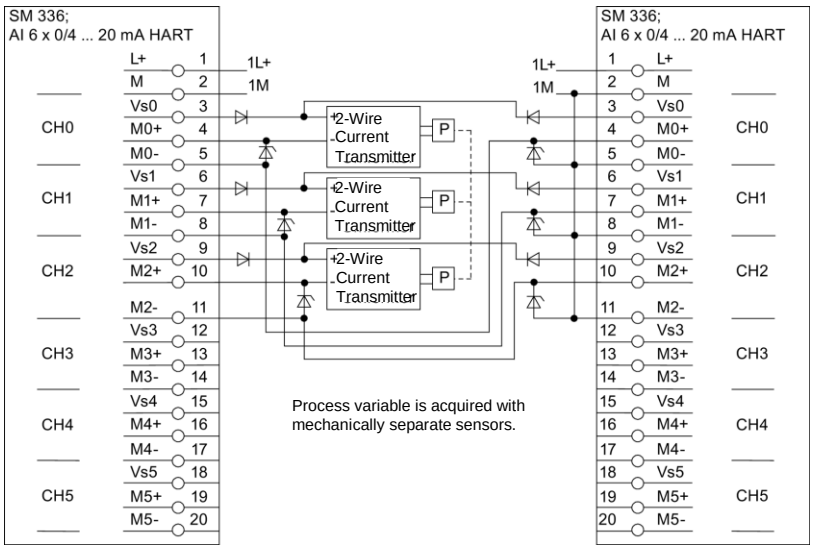
[9] The formula was taken from IEC61508, IEC 61511 and VDI 2180 sheet 4, see Appendix

9.2 Wiring

9.2.1 Conventional wiring

A simplified example of the 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program is illustrated in Fig. 9-2. The first sensor is wired to channel 0 (terminals 3, 4, 5) of both F-AIs, the second sensor is wired to channel 1 (terminals 6, 7, 8) and the third sensor to channel 2 (terminals 9, 10, 11) of both F-AIs. Please note that this architecture also requires two Zener diodes for each sensor. The first Zener diode has an avalanche voltage of 6.2 V and the second one has an avalanche voltage of 5.6 V. Another two diodes are also used for decoupling the voltage supply. The diodes and Zener diodes are needed in case one of the F-AIs is out of service (e.g. module failure).

Fig. 9-2: 2oo3 evaluation in the user program, redundant F-AI, 3-channel transmitter, 2-wire, internal supply



9.3 Parameters for hardware configuration

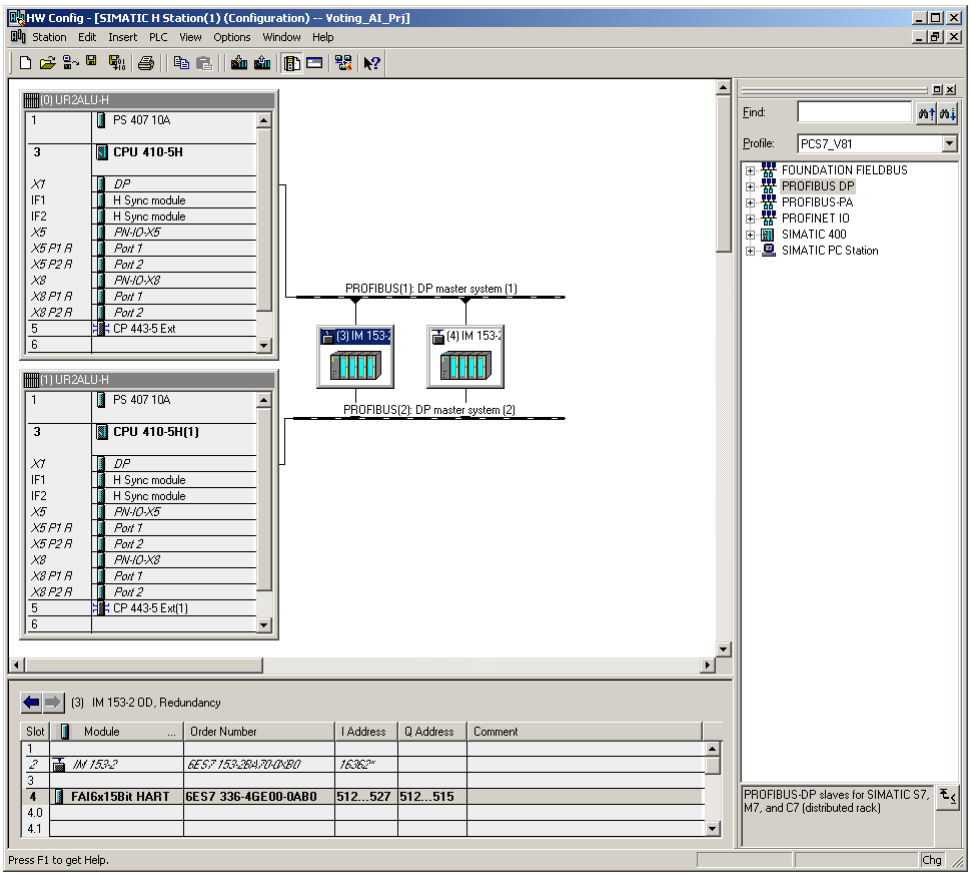
For the 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program, the F-AIs are configured in the STEP 7 HW Config.

Fig. 9-3 illustrates the example of a hardware configuration.

In this example, there is an ET 200M (IM153-2) with PROFIBUS address 3 and a second ET 200M with PROFIBUS address 4. Each ET 200M contains one F-AI in slot 4.

For further information on hardware configuration, see \4\ in the "Links and Literature" chapter.

Fig. 9-3: 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program - hardware configuration plan



The two F-AIs must be configured as a redundant pair in the HW Config. Each of the F-AI redundancy settings can be accessed through the object properties of the F-AIs.

For the sake of the hardware configuration example in Fig. 9-4, the redundancy settings are made with PROFIBUS address 3 using the F-AI in the ET 200M. The settings are summarized in Table 9-2.

Fig. 9-4: 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program - Redundancy parameters

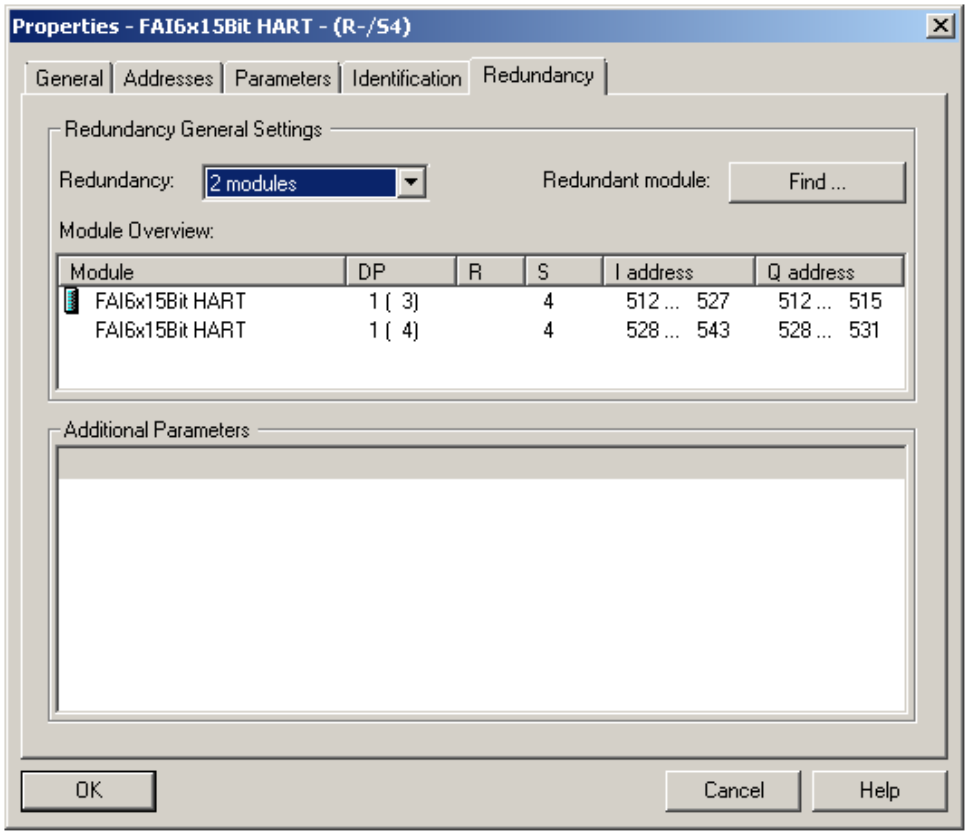


Table 9-2: 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program Redundancy parameters

Parameter	Description / Recommendations	Desired setting or permissible value range
Redundancy	Shows whether the F-AI is acting as part of a redundant pair or not. **Remark:** For redundancy, the parameter must be set to 2 modules.	Two (2) modules
Redundant module	Used for selecting the redundant partner module.	

Note The parameter names and configuration window may differ from those in this section due to the version of the module and hardware configuration pack. You can find further information in the module's documentation.

If the redundancy settings have been made, the other hardware parameters can be set in one of the redundant F-AIs. The settings are automatically applied to the redundant module.
You can find a description of the hardware parameters at the end of section 0.

9.4 Creating the Logic

Although this evaluation scheme uses redundant F-AIs, only three F_CH_AI F-channel drivers are needed in the logic. The F-channel drivers can be added and configured automatically from the SIMATIC Safety Matrix or manually using the STEP 7 CFC Editor. In both cases, the F-channel drivers must be connected to the analog sensor signal of the F-AI with the lowest I/O address.

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

9.4.1 Configuring with Safety Matrix

After the three sensor signals have been added to the hardware configuration, the 2oo3 evaluation logic can be implemented in the user program. One option is to use the SIMATIC Safety Matrix Engineering Tool (for further relevant information, see \5\ in the "Links and Literature" chapter).

The actual evaluation logic for the 2oo3 evaluation scheme with redundant F-AI and evaluation in the user program is the same as that described in the Section 8.4.1 (Configuring with Safety Matrix).

9.4.2 Configuring with CFCs

As an alternative to using the Safety Matrix Tool, you can implement the 2oo3 evaluation logic for the CPU by means of the STEP 7 CFC Editor. There are two ways to implement the CFC logic:

- Without channel fault evaluation
- With channel fault evaluation

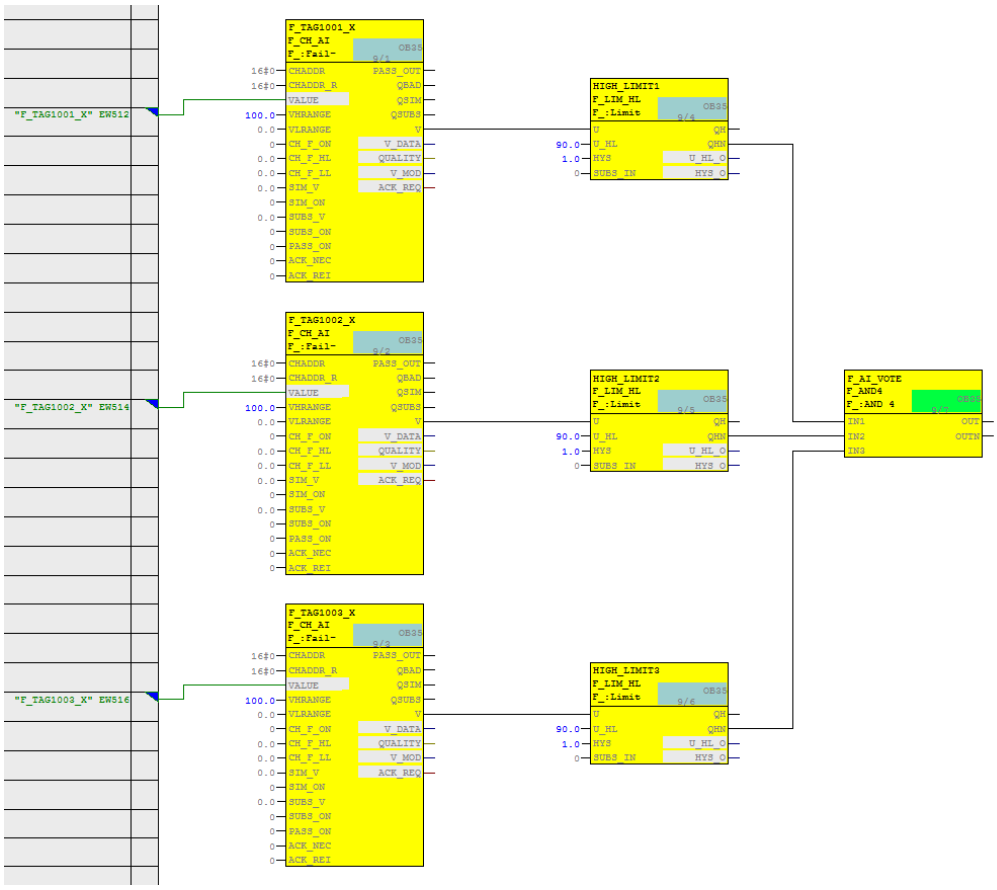
The logic for both options corresponds to the solutions described in Chapter 8.4.2.

Logic without channel fault evaluation

The logic corresponds to the Safety Matrix configuration, in which the function "Trip on bad quality" is not enabled. The input signals are not monitored for a maximum delta.

Figure 9-5 shows an example logic for 2oo3 evaluation in the CFC Editor, which does not take channel faults into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state
(Normal State = 1, Safe State = 0).

Figure 9-5: CFC Logic – Without channel fault evaluation



Note

Depending on the parameter assignment of the "SUBS_ON" block input, the F_CH_AI block outputs the substitute value or the last valid process value set at the "SUBS_V" input in the event of a channel fault at the "V" output.
In the logic shown (SUBS_ON = 0 on the F-channel driver), the last valid value is used in case of error. It is not possible to predict whether this value is above or below the limit.

Note

When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Figure 9-5 works as follows:

- If at least two of the three analog sensors report a normal value (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If at least two analog sensors report an upper limit violation (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

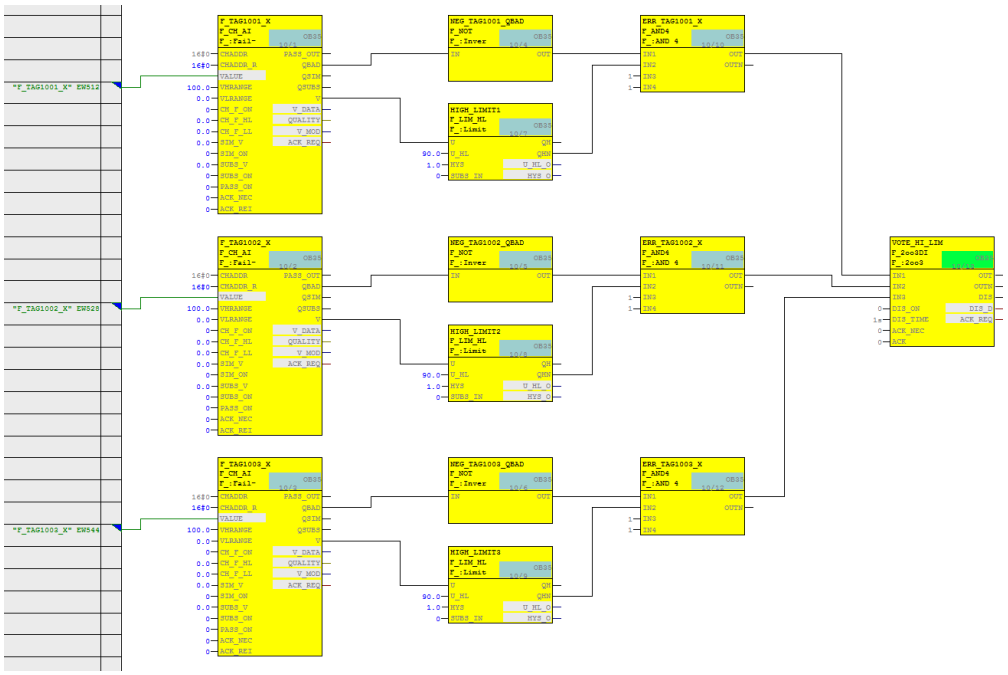
- Create an F_CH_AI F-channel driver for the first analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the second analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the third analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Connect the negated outputs of the limit value blocks (QHN or QLN) with the inputs of an F_2OUT3 block in order to generate the signal for the trigger command.

Logic with channel fault evaluation

The logic corresponds to the Safety Matrix configuration, in which the function "Trip on bad quality" is enabled. The input signals are not monitored for a maximum delta.

Fig. 9-6 shows an example logic for 2oo3 evaluation in the CFC Editor, which takes channel faults into account. Please note that this example starts from a MAX limit and that the output of the evaluation logic is switched off to reach the safe state (Normal State = 1, Safe State = 0).

Fig. 9-6: CFC logic – With channel fault evaluation



Note When redundant F-AIs are used, activate the discrepancy evaluation on F_CH_AI by setting the input "DISC_ON" to 1, "DISC_TIM" with a delay time, and "DELTA" to a max. deviation. Interconnect the "DISCF" output to a message block to alert the operator when there is a deviation between the redundant signals.

The example logic in Fig. 9-6 works as follows:

- If at least two of the three analog sensors report a normal value without channel faults (here: a process value lower than 90), the output of the evaluation logic is 1 (i.e., no trigger command).
- If two or more analog sensors report an upper limit violation without channel fault (here: a process value greater than or equal to 90), the output of the evaluation logic is 0 (i.e., trigger command).
- If two or more analog sensors report a channel fault, the output of the evaluation logic is 0 (i.e., trigger command).
- If one sensor reports a channel fault and two sensors do not report a channel fault, only the values of the sensors without channel faults are used for the evaluation logic.
- The output of the logic should be connected to the corresponding shutdown logic.

The necessary steps to create the logic are described below:

- Create an F_CH_AI F-channel driver for the first analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the second analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Create an F_CH_AI F-channel driver for the third analog sensor and connect the corresponding I/O signal to the block. Use a limit block (F_LIM_HL or F_LIM_LL) to compare the signal with the tripping limit value.
- Implement the evaluation logic by interconnecting the inputs of an F_2OUT3 block with the outputs of the following AND operations:
  - The negated output QBAD (F_NOT) of the first channel driver with the negated value of the first limit module output (QHN or QLN).
  - The negated output QBAD (F_NOT) of the second channel driver with the negated value of the second limit module output (QHN or QLN).
  - The negated output QBAD (F_NOT) of the third channel driver with the negated value of the third limit module output (QHN or QLN).

APPENDIX

10 Calculating the PFD value

The PFD value for the F-AI can be found in the "S7-300 Programmable Controller, Fail-Safe Signal Modules" manual (see \6\ in the "Links and Literature" chapter). In the technical data of the SM 336; F-AI 6 x 0/4 ... 20 mA HART or as a download on the Internet (see \11\ in the in the "Links and Literature" chapter).

The PFD values apply for the specified service lives. It is not necessary and impossible to proof test the hardware within this time. A replacement must take place at the end of the service life.

Table 10-1: PFD value for the F-AI

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

You can find the PFD value for the F-CPU in the manual "Safety Engineering in SIMATIC S7" (see \8\ in the "Links and Literature" chapter) or as a download on the Internet (see \11\ in the "Links and Literature" chapter).

Table 10-2: PFD value for F-CPUs

CPU	**Order number**	Low demand mode (average **p**robability of **f**ailure on **d**emand)	
Proof test interval		10 years	20 years
CPU 410-5H	6ES7 410-5HX08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 410E	6ES7 410-5HM08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 410SIS	6ES7 410-5FM08-0AB0	< 1.9 E-04	< 3.8 E-04
		< 2.8 E-04*	< 5.6 E-04*
CPU 412-5H PN/DP	6ES7 412-5HK06-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 414-5H PN/DP	6ES7 414-5HM06-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 416-5H PN/DP	6ES7 416-5HS06-0AB0	< 1.9 E-04	< 3.8 E-04
CPU 417-5H PN/DP	6ES7 417-5HT06-0AB0	< 1.9 E-04	< 3.8 E-04

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

When calculating the PFDavg for a safety function, an additional PFD value must be added for the safety-related communication.

Table 10-3

Safety-related communication	Low demand mode (average **p**robability of **f**ailure on **d**emand)	After a service life of
	< 1E-05*	20 years

*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 also add 3.5E-7 fail-safe I/O for this safety function.

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. For further relevant information, please see \9\, \6\ and \7\ in the "Links and Literature" chapter.

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. Please 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.

11.1.2 System power supply

The system power supply outputs cabinet-specific 24 V DC for the cabinet loads. 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 supplied 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 supplies the controllers and I/O modules with 24 V DC. The power supply for the communication modules, as well as the communication itself pass over 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 overvoltages

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 controls 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.

11.2.2 Implementation

The grounding recommendations given in this section are specific to cabinets with power supplies that supply system components with 24 V DC. 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), you have to use independent power feed units, and each current source should have its own cabinet ground connection.

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 shield collection. The shield collection should be isolated from mounting plates or rail assemblies within cabinets. Shield collections must accommodate a ground connection. The ground connection connects a shield collection 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

Please 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 setup

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 design 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 hardware module (see Figure 11-1) or of the system backplane (see Figure 11-2).

Figure 11-1: Installation location of the bridge with IM-153 (ET 200M interface module)

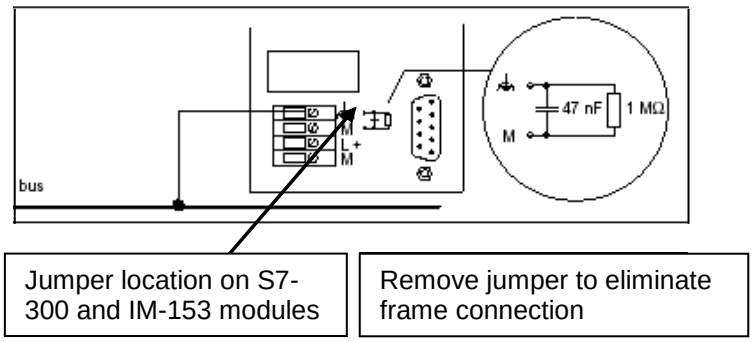
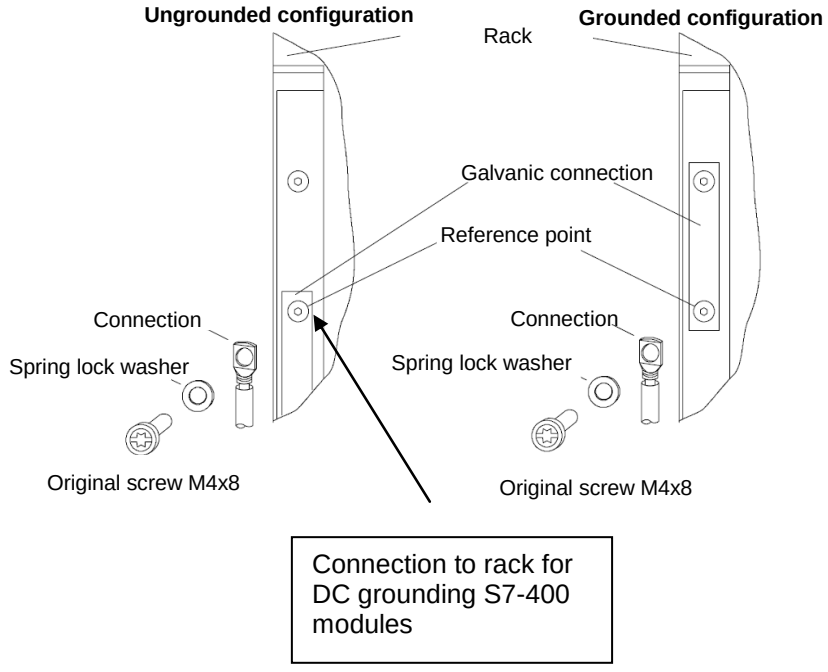


Figure 11-2: Location of grounding for S7-400 modules



12 MTA (Marshalled Termination Assembly)

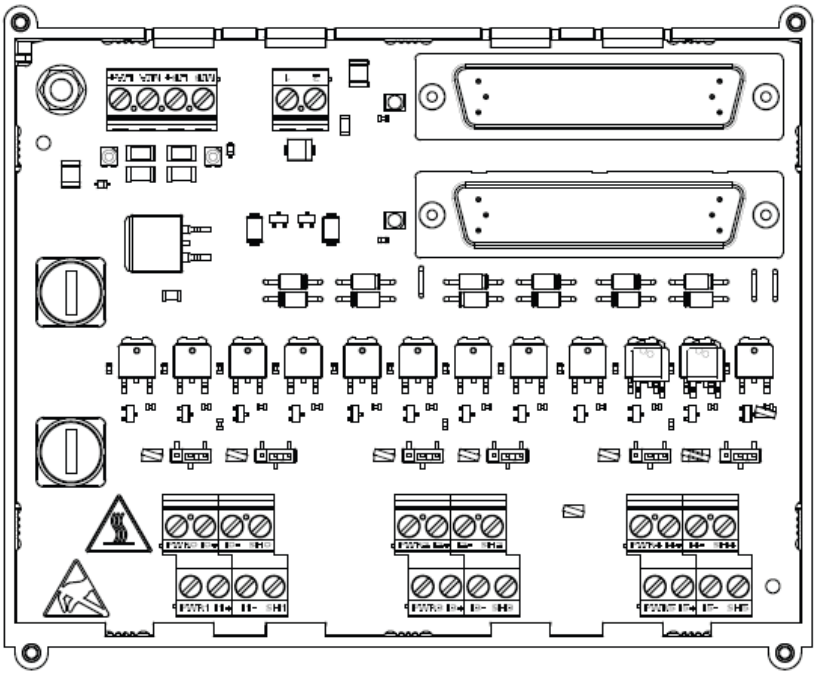
The MTA terminal modules (Marshalled Termination Assemblies) offer the possibility of connecting field devices, sensors and actuators in a simple, quick and safe manner to the signal modules of the ET 200M. They can be used to significantly reduce the required work for cabling and commissioning, and prevent wiring errors. The individual MTA terminal modules are each tailored to specific I/O modules from the ET 200M range.
The F-AI HART module described in this documentation can be combined with the "6 Channel F-Analog Input HART MTA" (6ES7650-1AH62-5XX0). This MTA can be used for redundant and safety-oriented applications.

Properties

MTAs are characterized by the following properties:

- Redundant 24 V DC power supply with LED display
- Screw-type terminals for direct (1:1) connection of field devices, sensors and actuators
- Fuse with LED indicator for each I/O channel
- Pre-assembled cables to connect the MTA with the I/O module
- With 50/25-pole D-sub connector on the MTA side
- and 40/20-pole Siemens front panel connector for ET 200M module
- On-board simulation capabilities (wire break, to switch ON/OFF a channel)
- Tested as a PCS 7 system component and approved with appropriate approvals (FM, UL, CE, ATEX, TÜV (German Technical Inspectorate)).

Fig. 12-1: F-AI MTA - Layout



The F-AI MTA and the F-AI module are connected to each other over a pre-assembled connecting cable. The custom length cable is shown below in Fig. 12-2.

Fig. 12-2: F-AI MTA - connecting cable

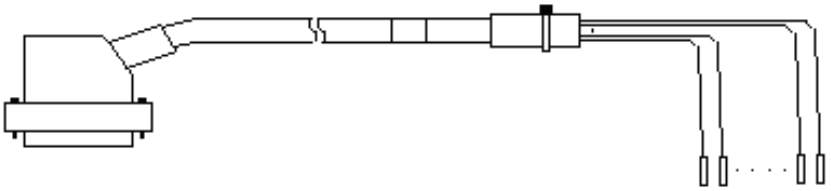


Fig. 12-3 illustrates an example of how to wire a 4-wire transmitter (self-powered) to the F-AI MTA.

Fig. 12-3: four-wire transmitter (self-powered)

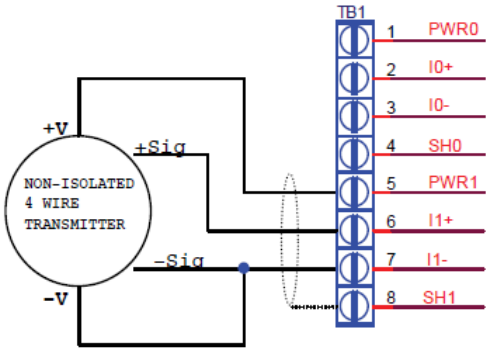


Fig. 12-4 illustrates an example of how to wire a 4-wire transmitter (with external power supply) to the F-AI MTA.

Fig. 12-4: Four-wire transmitter (with external power supply)

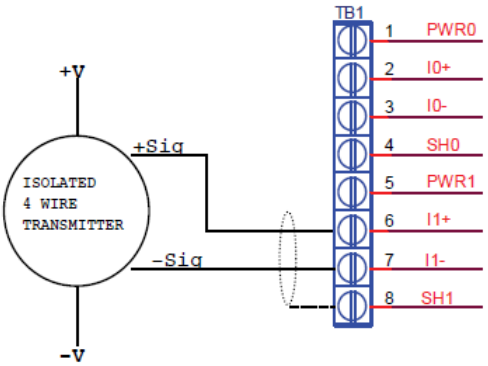
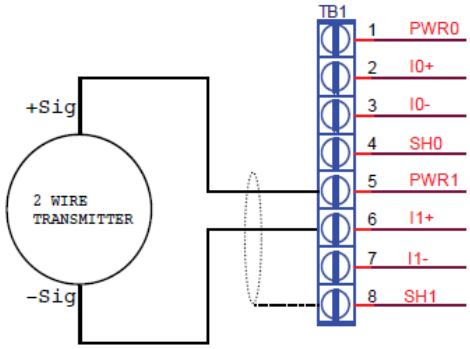


Fig. 12-5 illustrates an example of how to wire a 2-wire transmitter to the F-AI MTA.

Fig. 12-5: two-wire transmitter



An additional connecting cable is connected to the additional module connection on the MTA for voting architectures that contain a redundant module.

You can find further information under \3\ in the "Links and Literature" chapter.

13 Glossary

The following table shows the abbreviations used in the document.

Table 13-1 Glossary

Abbreviation	Meaning
MooN	M-out-of-N channel system
MooND	M-out-of-N channel system, extended diagnostics
1oo1	Architecture type: 1 channel system, loss of safety if a channel is faulty. (1-out-of-1)
1oo1D	Architecture type: 1 channel system, loss of safety if a channel is faulty; extended diagnostics
1oo2	Architecture type: 2 channel system, safety maintained if a channel is faulty.
1oo2D	Architecture type: 2 channel system, safety maintained if a channel is faulty; extended diagnostics.
β	CCF factor - The relationship between the probability of occurrence of a CCF and the probability of any fault. β is dependent on the system components, typical values for β are in the range of 1 % and 5 %.
CCF	Common Cause Failure – These are errors that affect two or more separate channels or components in a system. A CCF causes the system to fail
CPU	Central processing unit
IEC61508	Basic standard and basis for safety standardization
IEC61511	Based on the IEC61508, sector-specific standard for the process industry
MTA	Marshalled Termination Assemblies
PFD	Probability of Failure on Demand, Failure probability upon usage request of the safety function (requested less than once a year) Probability of a safety function failure upon request
SIL	Safety Integrity Level: safety level; level of risk reduction
SIS	Safety Instrumented System

14 Links andLiterature

Table 14-1

	Topic
\1\	Siemens Industry Online Support http://support.industry.siemens.com
\2\	Link to this entry https://support.industry.siemens.com/cs/ww/en/view/24690377
\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 V5.5 https://support.industry.siemens.com/cs/ww/en/view/45531110
\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\	SIMATIC PCS 7 Engineering System (V9.0) https://support.industry.siemens.com/cs/ww/en/view/109746533
\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\	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
\12\	SIMATIC Industrial software S7 F/FH Systems - Configuring and Programming https://support.industry.siemens.com/cs/ww/en/view/101509838

15 Change documentation

Table 15-1

Version	Date	Modifications
V1.0	04/2007	First version
V2.0	12/2007	New hardware and software considered, supplemented by MTA
V2.1	05/2009	Update
V3.0	08/2015	Complete revision
V3.1	08/2017	Update
V3.2	09/2017	Update
V3.3	12/2017	Improved wording and expansion