HIQuad

Safety-Related Controller

HIQuad Safety Manual

SAFETY
NONSTOP

HIMA

All of the instructions and technical specifications in this manual have been written with great care and effective quality assurance measures have been implemented to ensure their validity. For questions, please contact HIMA directly. HIMA appreciates any suggestion on which information should be included in the manual.

Equipment subject to change without notice. HIMA also reserves the right to modify the written material without prior notice.

For further information, refer to the HIMA DVD and our website at http://www.hima.de and http://www.hima.com.

Contact

HIMA contact details:

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Revision index	Changes	Type of change	
		technical	editorial
1.00	New document layout, general revision	X	X
1.01	Deleted: Maintenance override, protection against manipulation, discontinued modules. Added: Cyber security. Revised: Certification, safety times, safety parameters, reload, forcing	X	X
1.02	Revised: Chapter 1.1 and Chapter 3.4.7	X	X

Table of Contents

1 Introduction

This manual contains information on how to operate the H41q and H51q safety-related automation devices from HIMA in the intended manner.

The following conditions must be met to safely install and start up the H41q/H51q automation devices, and to ensure safety during their operation and maintenance:

- Knowledge of regulations.
- Proper technical implementation of the safety instructions detailed in this manual performed by qualified personnel.

HIMA will not be held liable for severe personal injuries, damage to property or the environment caused by any of the following:

- Unqualified personnel working on or with the systems.
- De-activation or bypassing of safety functions.
- Failure to comply with the instructions detailed in this manual.

HIMA develops, manufactures and tests the H41q/H51q automation devices in compliance with the pertinent safety standards and regulations. The use of the systems is only allowed if the following conditions are met:

- They are used for the intended applications.
- They are operated under the specified environmental conditions.
- They are only connected to the approved external devices.

To provide a clearer exposition, this manual does not specify all details of all versions of the H41q/H51q automation devices.

1.1 Validity and Current Version

The most current edition of this safety manual, which is indicated by the highest revision number, is also valid for previous operating system versions. Special features of the individual versions or revisions are mentioned in this manual.

The current version is available on the current HIMA DVD or can be downloaded from the HIMA website at www.hima.de or www.hima.com.

1.2 Target Audience

This document addresses system planners, configuration engineers, programmers of automation devices and personnel authorized to implement, operate and maintain the systems and systems. Specialized knowledge of safety-related automation systems is required.

1.3 Writing Conventions

To ensure improved readability and comprehensibility, the following writing conventions are used in this document:

Bold	To highlight important parts. Names of buttons, menu functions and tabs that can be clicked and used in the programming tool.
Italics	For parameters and system variables
`Courier`	Literal user inputs.
RUN	Operating states are designated by capitals.
Chapter 1.2.3	Cross-references are hyperlinks even if they are not particularly marked. When the cursor hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are particularly marked.

1.3.1 Safety Notices

The safety notices are represented as described below.
They must be strictly observed to ensure the lowest possible operating risk. The content is structured as follows:

- Signal word: warning, caution, notice
- Type and source of risk
- Consequences arising from non-observance
- Risk prevention

⚠ SIGNAL WORD

Type and source of risk!
Consequences arising from non-observance
Risk prevention

The signal words have the following meanings:

- Warning indicates hazardous situations which, if not avoided, could result in death or serious injury.
- Caution indicates hazardous situations which, if not avoided, could result in minor or modest injury.
- Notice indicates a hazardous situation which, if not avoided, could result in property damage.

NOTICE

Type and source of damage!
Damage prevention.

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

i	The text corresponding to the additional information is located here.

Useful tips and tricks appear as follows:

TIP	The tip text is located here.

1.4 Residual Risk

No imminent risk results from a HIMA system itself.

Residual risk may result from:

- Errors related to engineering
- Errors in the user program
- Faults related to the wiring

2 Usage Notes for H41q/H51q Systems

All safety information, notes and instructions specified in this manual must be strictly observed. The product may only be used if all guidelines and safety instructions are adhered to.

2.1 Intended Use

2.1.1 Application Area

The safety-related automation devices, H41q and H51q, can be used in applications up to SIL 3 (IEC 61508), Cat. 4 or Pl e (ISO 13849-1).

All input and output modules can be used in both redundant and single-channel structure of the central modules.

When implementing safety-related communications between various systems, ensure that the overall response time does not exceed the process safety time. All calculations specified in the safety manual (HI 800 013 E) must be performed in accordance with the specified rules.

Only devices with safe electrical separation may be connected to the communications interfaces.

The H41q/H51q systems are certified for use in process controllers, protective systems, burner systems and machine controllers.

2.1.1.1 Application in Accordance with the De-Energize-to-Trip Principle

The automation devices have been designed in accordance with the de-energize-to-trip principle.

A system that operates in accordance with the **de-energize-to-trip** principle does not require any power to perform its safety function.

Thus, if a fault occurs, the input and output signals adopt a de-energized, safe state.

2.1.1.2 Application in Accordance with the Energize-to-Trip Principle

The H41q/H51q controllers can be used in applications that operate in accordance with the energize-to-trip principle.

A system operating in accordance with the **energize-to-trip** principle requires power (such as electrical or pneumatic power) to perform its safety function.

Therefore, the H41q/H51q controllers are tested and certified for use in fire alarm and fire-fighting systems in accordance with EN 54 and NFPA 72. To contain the hazard, these systems must be able to adopt an active state on demand.

2.1.1.3 Explosion Protection

The safety-related H41q and H51q automation devices are suitable for mounting in Zone 2. The declarations of conformity are contained in the corresponding data sheets.

The following operating conditions must be observed!

2.1.1.4 Use in Fire Alarm Systems

All H41q/H51q systems with analog inputs can be used in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72.

The following operating conditions must be observed!

2.1.2 Non-Intended Use

The transfer of safety-relevant data through public networks like the Internet is only permitted if additional security measures such as VPN tunnel or firewall have been implemented to increase security.

Fieldbus interfaces without safety-related fieldbus protocols cannot ensure safety-related communication.

2.2 Tasks of Operators and Machine and System Manufacturers

Operators as well as machine and system manufacturers are responsible for ensuring that H41q/H51q systems are safely operated in automated systems and plants.

The machine and system manufacturers must validate that the H41q/H51q systems are properly programmed.

2.3 ESD Protective Measures

Only personnel with knowledge of ESD protective measures may modify or extend the system or replace a module.

NOTICE

Electrostatic discharge!

Failure to comply with these instructions can damage the electronic components.

- **Prior to working with HIMA components, touch an earthed object.**
- **Make sure that the workspace is free of static and wear an ESD wrist strap.**
- **If not used, ensure that the component is protected from electrostatic discharge, e.g., by storing it in its packaging.**

Only personnel with knowledge of ESD protective measures may modify or extend the system wiring.

3 Safety Concept for Using the PES

3.1 Safety and Availability

Even as mono systems, the H41q and H51q system families are designed for use up to SIL 3 thanks to the 1oo2D microprocessor structure on one central module.

Depending on the required availability, the HIMA automation devices can be equipped with redundant modules in the central and I/O areas. Redundant modules increase availability since the redundant module maintains operation, if a module is shut down due to a failure.

3.1.1 Safety

The PFD (probability of failure on demand) and PFH (probability of failure per hour) values were calculated for the safety-related H41q and H51q systems in accordance with IEC 61508.

For SIL 3, IEC 61508-1 prescribes the following requirements:

- A PFD value of 10^{-4}...10^{-3}.
- A PFH value of 10^{-8}...10^{-7} per hour.

15 % of the limit value for PFD and PFH specified in the standard is assumed for the controller. The resulting limit values for the controller's proportion are:

- PFD = 1.5 * 10^{-4}.
- PFH = 1.5 * 10^{-8} per hour.

A proof test interval of 10 years[1] is defined for the safety-related H41q and H51q systems.

The safety functions, consisting of a safety-related loop (an input, a processing unit and an output), meet the requirements described above in all combinations.

Further information is available upon request.

3.1.2 Overview

The following table presents an overview of the system designations, safety, availability and configurations

System designation	H41q-MS H51q-MS	H41q-HS H51q-HS	H41q-HRS H51q-HRS
SIL / Category	SIL 3 / Kat. 4	SIL 3 / Kat. 4	SIL 3 / Kat. 4
Availability	Normal	High	Very high
Configuration			
Central Module	Mono	Redundant	Redundant
I/O modules	Mono[1)]	Mono[1)]	Redundant
I/O bus	Mono	Mono	Redundant[2)]

1) To increase availability, individual I/O modules can also be used redundantly or in a 2oo3 circuit (e.g., see Chapter 7.8.3).

2) When a redundant I/O bus is used, HIMA recommends configuring both the I/O modules and the peripherals (sensors and actuators within the plant) as redundant modules. Experience shows that these components have higher failure rates than the PES modules.

Table 1: System Designations, Safety, Availability and Configurations

[1] Refer to Chapter 6.5 for restrictions applying to the F 3430 relay module.

When redundant modules are used for increasing availability, three essential points must be considered:

- Faulty modules must be detected and shut down to prevent the system from being blocked.
- If a fault occurs, the operator must receive a message indicating that the module must be replaced.
- Once the module has been replaced, it must automatically start operation.

The HIMA automation systems with the corresponding configuration meet these requirements.

A PADT (programming and debugging tool, PC) with **ELOP II** in accordance with IEC 61131-3 is used to program the systems. It helps the user operate the automation devices and create safety-related programs.

3.2 Safety Times

Single faults which may lead to a dangerous operating state are detected by the self-test facilities within the safety time (≥ 1 s).

- Process safety time

  Process value which is often referred to as safety time in user guidelines.
- Safety time (within the PES)

  Value which depends on the system capability.

  Failures, which can only have a dangerous impact on safety if combined with additional faults, are detected by tests.

  The distinction between two types of tests is made:
  - Tests within the safety time

    They are carried out during the safety time (foreground tests).

    Response time: immediately or, at the latest, within the safety time.
  - Background tests

    They are distributed over multiple cycles.

    The response occurs when an error has been detected or, at the latest, within a time which is 3600-times the safety time value.

  Example of response time: a maximum of two times the cycle time. If a safety time of 1 s is required for the process, the cycle time may not exceed 500 ms.
- Fault response time

  The fault response time of an automation device corresponds to the safety time (≥ 1s), defined in the resource properties. Notice that the cycle time may not exceed half the safety time value, since a response to faults in the input modules is triggered within 2 cycles. The cycle time depends on the safety time, which defines the period within which all foreground tests are performed.

  A short safety time increases the cycle time, and vice versa. With long safety times, some tests are distributed among multiple cycles.
  - Example 1: Safety time = 1 s

    Cycle time for user program = 450 ms

    Cycle time required for tests = 100 ms

    2 cycles are possible within the safety time

    100 ms / 2 = 50 ms / cycle time required for tests

    Overall cycle time = **500 ms**
  - Example 2: Safety time = 2 s

    Cycle time for user program = 450 ms

    Cycle time required for tests = 100 ms

    4 cycles are possible within the safety time

    100 ms / 4 = 25 ms / cycle time required for tests

Overall cycle time = **475 ms**

i For operating system versions prior to (07.14), the safety time must **not** be set to 255 s! Only values within 1...254 s are allowed!

3.3 Proof Test

The proof test detects dangerous undetected faults that could otherwise affect the safe function of the system.

HIMA safety systems must be subject to a proof test in intervals of **10 years**[2]. It is often possible to extend this interval using a calculation tool to analyze the implemented safety loops.

For relay modules, the proof test must be performed in the intervals defined for the plant.

3.3.1 Proof Test Execution

The proof test execution depends on the following factors:

- Plant characteristics (EUC = equipment under control).
- Plant's intrinsic risk potential.
- The standards applicable to the plant operation and required for approval by the responsible test authority.

According to IEC 61508 1-7, IEC 61511 1-3 and VDI/VDE 2180 Sheets 1...4, the operator of the safety-related systems is responsible for performing the proof tests.

3.3.2 Frequency of Proof Tests

The HIMA PES can be proof tested by testing the full safety loop.

In practice, shorter proof test intervals are required for the input and output field devices (e.g., every 6 or 12 months) than for the HIMA controller. Testing the entire safety loop together with a field device automatically includes the test of the HIMA controller. There is therefore no need to perform additional proof tests of the HIMA controller.

If the proof test of the field devices does not include the HIMA controller, the HIMA controller must be tested at least once every 10 years. This can be achieved by restarting the HIMA controller.

Additional proof test requirements for specific devices are described in the corresponding data sheets.

3.4 Safety Requirements

The following safety requirements must be met when using the safety-related controllers of the H41q and H51q systems.

i The operating company is responsible for operating a plant safely in accordance with the relevant application standards.

3.4.1 Hardware Project Planning: Product-Independent Requirements

To ensure safety-related operation, only approved fail-safe hardware modules and software components may be used. The approved hardware modules and software components are

[2] Exception: The F 3430 module must be tested for SIL 3 in intervals of 5 years.

listed in the *Revision List of Devices and Firmware of H41q/H51q Systems of HIMA Paul Hildebrandt GmbH*.

Refer to the last valid release document for the certificate number. The latest versions can be found in the version list maintained together with the test authority.

- The operating requirements specified in this safety manual (see Chapter 3.5.1) about EMC, mechanical and climatic influences must be observed.
- Non-fail-safe, interference-free hardware modules and software components may be used for processing non-safety-relevant signals, but not for handling safety-related tasks.

3.4.2 Hardware Project Planning: Product-Dependent Requirements

- Only devices that are safely separated from the power supply may be connected to the system.
- The safe electrical power supply separation must be guaranteed within the 24 V system supply. Only power supply units of type PELV or SELV may be used.

3.4.3 Programming: Product-Independent Requirements

- In safety-related applications, ensure that the system parameters influencing safety are properly configured. The possible configuration variants are described in the following chapters. In particular, this applies to the system configuration, maximum cycle time and safety time.

3.4.4 Programming: Product-Dependent Requirements

- The system response to faults in the fail-safe input and output modules must be defined in the user program in accordance with the system-specific safety-related conditions.
- If ELOP II, rev. 3.5 and higher, is used as programming tool, the verification of the created program can be simplified in accordance with the conditions specified in this manual.
- The program, however, must be sufficiently validated.
- Function tests / verifications after a user program change can be limited to the modified program parts.
- The procedure for creating and changing the program described in Chapter 7 must be observed.

3.4.5 Communication: Product-Dependent Requirements

- When implementing safety-related communications between various systems, ensure that the overall response time does not exceed the process safety time. All calculations must be performed in accordance with the specified rules.
- The transfer of safety-relevant data through public networks like the Internet is only permitted if additional security measures such as VPN tunnel have been implemented.
- If data is transferred through company-internal networks, administrative or technical measures must be implemented to ensure sufficient protection against manipulation (e.g., using a firewall to separate the safety-relevant components of the network from other networks).
- Only devices with safe electrical separation may be connected to the communications interfaces.

3.4.6 Special Modes of Operation: Product-Independent Requirements

- Reload in safety-related applications is only permitted after receiving consent from the test authority responsible for the factory acceptance test (FAT) and using the certified tool, ELOP II.

- During the entire reload process, the person in charge must take further technical and organizational measures to ensure that the process is sufficiently monitored in terms of safety.
- Prior to performing the reload, determine the version changes compared to the user software using the C-code comparator of ELOP II.
- During the reload of a mono PES, the time needed to perform the entire change plus twice the cycle time must not exceed the process safety time.
- A static offline test of the logic may be performed with ELOP II. The offline simulation was not subject to any safety-relevant tests. For this reason, the simulation may not replace the functional test of the plant.
- Whenever necessary, the operator must consult with the test authority responsible for the factory acceptance test (FAT) and define administrative measures appropriate for regulating access to the controller.

3.4.7 Cyber Security for HIQuad Systems

Industrial controllers must be protected against IT-specific problem sources. Those problem sources are:

- Attackers inside and outside of the customer's plant
- Operating failures
- Software failures

A HIQuad installation consists of the following parts to be protected:

- HIQuad PES
- PADT
- OPC server: X-OPC DA, X-OPC AE (optional)
- Communication connections to external systems (optional)

The HIQuad system with basic settings is already a system fulfilling the requirements for cyber security.

Protective mechanisms for preventing unintentional or unapproved modifications to the safety system are integrated into the PES and the programming tool:

- Each change to the user program or configuration results in a new configuration CRC.
- Online changes of the safety parameters can be deactivated in the PES. Changes to the safety parameters are only possible by performing a download/ reload.
- The programming tool prompts the user to enter a password in order to log in to the PES.
- PES data can only be accessed if the PADT is operating with the current version of the user project (archive maintenance!).
- Connection between the PADT and PES is not required in RUN and can be interrupted.

  The PADT can be shortly connected for maintenance work or diagnostic tasks.

All requirements about protection against manipulation specified in the safety and application standards must be met. The operator is responsible for authorizing employees and implementing the required protective actions.

⚠ WARNING

Physical injury possible due to unauthorized manipulation of the controller!

The controller must be protected against unauthorized access!

For instance:

- **Changing the default settings for login and password!**
- **Controlling the physical access to the controller and PADT!**

Careful planning should identify the measure to be taken. The required measures are only to be taken after the risk analysis is completed. Such measures are, for example:

- Meaningful allocation of users.
- Maintained network maps help ensuring that secure networks are permanently separated from public networks, and if required, only a well-defined connection exists (e.g., via a firewall or a DMZ).
- Use of appropriate passwords.

A periodical review of the security measures is recommended, e.g., every year.

The user is responsible for implementing the necessary measures in a way suitable for the plant!

For more details, refer to the HIMA cyber security manual (HI 802 373 E).

3.5 Certification

The safety-related automation devices (PES = programmable electronic system) of the H41q and H51q system families are certified as follows:

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am grauen Stein
51105 Köln

Certificate and Test Report

Safety-Related Automation Devices

H41q-MS, H41q-HS, H41q-HRS

H51q-MS, H51q-HS, H51q-HRS

The safety-related automation devices of the H41q and H51q system families are tested and certified in accordance with the following relevant functional safety standards:

IEC 61508, Parts 1-7: 2010	up to SIL 3
IEC 61511, Parts 1-3: 2015	up to SIL 3
EN/ISO 13849-1: 2008 + AC: 2015	Category 4, Performance Level e
EN 50156-1: 2005	
EN 12067-2: 2004, EN 298: 2012	
NFPA 85: 2015, NFPA 86: 2015	
EN 61131-2: 2007	
EN 61000-6-2: 2005, EN 61000-6-4: 2007	
EN 54-2:1997, A1: 2007, NFPA 72: 2016	
EN 50130-4: 2011 + A1: 2014	

Chapter 3.5.1 contains a detailed list of all environmental and EMC tests performed.

3.5.1 Test Conditions

3.5.1.1 Environmental Conditions and Specifications

When using the safety-related H41q/H51q control systems, the following general conditions must be met:

Condition type	Condition content
Protection class	Protection class II in accordance with IEC/EN 61131-2
Operating temperature	Operating temperature: 0...+60 °C
Storage temperature	Storage temperature: -40...+80 °C (with battery: only -30...+75 °C)
Pollution	Pollution degree II
Altitude	< 2000 m
Enclosure	Standard: IP20 If required by the relevant application standards (e.g., EN 60204, EN 954-1), the system must be installed in an enclosure of the specified protection class (e.g., IP54).
Power supply input voltage	24 VDC

Table 2: Environmental Conditions

Refer to the relevant data sheets for various deviations.

The safety-related control systems H41q and H51q have been developed to meet the following standards for EMC, climatic and environmental requirements.

Standard	Content
IEC/EN 61131-2: 2007	Programmable controllers, Part 2 Equipment requirements and tests
IEC/EN 61000-6-2: 2005	EMC Generic standards, Parts 6-2 Immunity for industrial environments
IEC/EN 61000-6-4: 2007	Electromagnetic Compatibility (EMC) Generic emission standard, industrial environments

Table 3: Standards

3.5.1.2 Climatic Tests

The following table lists the key tests and thresholds for climatic requirements:

IEC/EN 61131-2	Climatic tests
	Dry heat and cold resistance tests: +70 °C / -40 °C, 16 h, +85 °C, 1 h Power supply not connected
	Temperature changes, withstand test: Fast temperature changes: -40 °C / +70 °C power supply not connected
	Immunity test Slow temperature changes: -10 °C / +70 °C power supply not connected
	Cyclic damp-heat withstand tests: +25 °C / +55 °C, 95 % relative humidity, Power supply not connected
EN 54-2	Damp-heat 93 % relative humidity, 40 °C, 4 days in operation 93 % relative humidity, 40 °C, 21 days, power supply not connected

Table 4: Climatic Conditions

3.5.1.3 Mechanical Tests

The following table lists the most important tests and limits for mechanical conditions:

IEC/EN 61131-2	Mechanical tests
	Vibration immunity test: 5...9 Hz / 3.5 mm 9...150 Hz / 1 g, EUT in operation, 10 cycles per axis
	Shock immunity test: 15 g, 11 ms, EUT in operation, 3 shocks per axis and direction (18 shocks)

Table 5: Mechanical Tests

3.5.1.4 EMC Tests

Refer to the EC declaration conformity to find out which test conditions are complied with.

All modules of the H41q and H51q systems meet the requirements of the EMC Directive of the European Union and are labeled with the CE mark.

The systems react safely to interferences exceeding the specified limits.

3.5.1.5 Power Supply

The following table lists the key tests and thresholds for power supply requirements:

IEC/EN 61131-2:	Verification of the DC supply characteristics
	Alternatively, the power supply unit must comply with the following standards: ▪ IEC 61131-2 or ▪ SELV (Safety Extra Low Voltage, EN 60950) or ▪ PELV (Protective Extra Low Voltage, EN 60742)
	The H41q and H51q systems must be fuse-protected as specified in the data sheets.
	Voltage range test: 24 VDC, -20...+25 % (19.2...30.0 VDC)
	Momentary external current interruption immunity test: DC, PS 2: 10 ms
	Reversal of DC power supply polarity test: Refer to corresponding chapter of the catalog or data sheet of the power supply module.
	Backup battery, withstand test: Test B, 1000 h, lithium battery as back-up battery

Table 6: Verification of the DC Supply Characteristics

4 Central Modules

The central components required for the different types of HIMA automation devices are assembled in kits. The kit of a functioning central module is composed of the following elements:

- Central subracks
- Central modules
- Power supply units
- Accessories

The detailed scope of delivery, the supply voltage wiring and the connection of the I/O level are described in the data sheets of the catalog Programmable Systems, System Families H41q/H51q (HI 800 263).

4.1 Central Modules and Kits for the H41q Systems

Module / kit	Designation	Safety-related	Interference-free
F 8652X	Central module, dual 1oo2 processor	•	•
B 4235	Central device kit H41q-MS	•	•
B 4237-1	Central device kit H41q-HS	•	•
B 4237-2	Central device kit H41q-HRS	•	•

Table 7: Central Modules and Kits for the H41q Systems

4.2 Central Modules and Kits for the H51q System

Module / kit	Designation	Safety-related	Interference-free
F 8650X	Central module, dual 1oo2 processor	•	•
B 5231	Central device kit H51q-MS	•	•
B 5233-1	Central device kit H51q-HS	•	•
B 5233-2	Central device kit H51q-HRS	•	•
B 9302	I/O subrack	•	•

Table 8: Central Modules and Kits for the H51q Systems

4.3 Additional Central Modules for the H41q and H51q Systems

Module / kit	Designation	Safety-related	Interference-free
Power distribution modules			
F 7133	4-fold power distribution modules with fuse monitoring		•
Supplementary modules			
F 7126	Power supply module		•
F 7130A	Power supply module		•
F 7131	Power supply module monitoring with back-up batteries for H51q		•
F 8621A	Co-processor module for H51q		•
F 8627X	Ethernet		•
F 8628X	Communication module for PROFIBUS DP (slave)		•
Bus connections			
F 7553	I/O bus connection module for H51q		•
Bus connection modules for configuring HIPRO			
H 7505	Interface converter RS485, V.24/20 mA 2-wire/4-wire (HIPRO)		•
H 7506	Bus terminals for configuring 2-wire busses		•

Table 9: Central Modules and Kits for the H51q Systems

4.4 General Notes on the Safety and Availability of Safety-Related Central Modules

Compliance with the following requirements concerning the equipment of the central and power supply modules and the bus components within the subrack of the H41q and H51q system families must be ensured:

H41q systems	H51q system
The following modules can be used in the H41q system subrack: ▪ 2 central modules ▪ 12 I/O modules ▪ 2 power supply modules ▪ 2 fuse modules	The following modules can be inserted in the central module subrack: ▪ 2 central modules ▪ For each central module: 3 F 8621/A co-processor modules or 5 F 8627X, F 8628X communication modules

Table 10: Differences between H41q and H51q

4.4.1 Power Supply Units

In safety-related applications, use one 24 VDC / 5 VDC power supply unit more than required by the power consumption. This applies to the central module subrack and the additional power supply module. The power supply units are decoupled via diodes and monitored by the central devices.

4.4.2 Functional Description of the Safety-Related F 8652X / F 8650X Central Modules

Each central module of type F 8652X or F 8650X is composed of the following function blocks:

- Two synchronous microprocessors
- Each microprocessor has its own memory
- The memories of one processor contain the program and the data in non-inverted form while the memories of the other processor contain the program and the data in inverted form.
- Testable hardware comparators for all external accesses of both microprocessors.
- If a fault occurs, the watchdog is set to a safe state and the processor status is reported.
- Flash EPROM as the program memory for operating systems and user programs, suitable for at least 100 000 memory cycles.
- Data storage in SRAM (static RAM)
- Multiplexer connection to I/O bus, dual port RAM (DPR) and redundant central module.
- Buffering of the SRAMs through batteries on the central module
- 2 RS485 interfaces with galvanic separation and baud rate equal to 57600 bps. The switch or software can be used to set the rate to 9600 bps and 57600 bps (other baud rates are also possible); values set with the software have priority.
- Diagnostic indicators and 2 LEDs for information from the system, I/O area and user program.
- DPR for fast, mutual memory access to the second central module
- Battery-buffered hardware clock
- I/O bus logic for connection to I/O modules.
- Safe watchdog
- Monitoring of power supply units, testable (5 V system voltage).
- Battery monitoring

4.5 General Operation of Safety-Related Central Modules

Safety-related central modules, which simultaneously process the same programs, operating systems and user programs, are composed of two microprocessors, each with its own RAM. A comparator continuously compares the data on the busses between the two microprocessors and their memories.

The operating system includes self-test routines which are periodically run. The watchdog monitors the program sequence.

4.5.1 Self-Test Routines

Table 11 explains the self-test routines run by the safety-related F 8650X and F 8652X central modules and how they are connected at the I/O level:

Test	Description
CPU test	The following is tested: ▪ Command and addressing types ▪ The writability of the flags and the commands affected by the flags. ▪ The writability and crosstalk of the registers. ▪ Arithmetic logic unit (ALU)
Memory areas test	The operating system, user program, constants and parameters as well as the variable data are stored in each central module directly and inversely and are checked for antivalence by a hardware comparator.
Fixed memory areas	The operating system, user program and parameter area are each stored in a flash EPROM and are protected by a CRC test.
RAM test	A write and read test is performed to check the RAM areas, in particular for crosstalk.
Watchdog test	The watchdog signal is switched off unless it is triggered within a determined period by both the CPUs with antivalent bit patterns or if the hardware comparator detects a difference between the two memories (directly and inversely). An additional test determines the switch-off ability of the watchdog signal.
Test of the connection to the I/O level within the central module	If the central modules in the H41q-HS and H51q-HS systems are used redundantly with a single-channel I/O bus, the reciprocal interlocking of the I/O access to the central modules is ensured. Self-tests check the interlocking circuit used to this end. For HR or HRS systems with a two-channel I/O level, the I/O access rights are read back and checked. For M or MS systems with a single-channel I/O level (single-channel I/O modules and single-channel CPU), the I/O access rights are read back and checked.
Test of the connection module in the I/O subracks	The addressing is tested cyclically after the safety-related I/O module has been processed. The addresses of all defined I/O module positions are read back and tested. The safety switches of the F 7553 modules are tested.

Table 11: Self-Test Routines

4.5.2 Response to Faults Detected in Central Modules

The test routines ensure that faults are detected and that the defective central module is switched off. At the same time, the diagnostic display reports the faults and register them in the system diagnostics.

For a central module, MS system, this means a complete shutdown of the automation device.

For redundant central modules, HS and HRS systems, the defective central module is switched off while the redundant module continues to operate.

If the defective central module of a redundant system is replaced by a functional one with the same user program and operating system, the new central module receives the current data from the running central module and the system starts again to operate redundantly.

Under certain conditions, such as the same operating system version which must be at least V7.0-8 (05.34), the running central module can load the user program in the new "empty" central module (self-education). Refer to the operating system manual (HI 800 105 E) for details.

4.5.3 Diagnostic Display

The diagnostic display is integral part of the central module. It includes the following elements:

- a 4-digit alphanumeric display for representing texts and values
- a *CPU* LED for signaling central module faults
- an *IO* LED for displaying general faults in safety-related I/O modules.

Three additional keys are also available: an acknowledgement key *ACK* and two keys for calling further system information.

If faults occur in the central module, the *CPU* LED is lit. STOP appears on the 4-digit display. The error code can be displayed through an operator's intervention. The operating system manual (HI 800 105 E) provides a list of the error codes.

If faults occur in the safety-related modules at I/O level, the *IO* LED is lit. The 4-digit display shows the module position and possibly the faulty channel.

The diagnostic system provides all error codes to be visualized in the process control system. The diagnostic system maintains an error history. The error history can be displayed in the PADT and provides support for detecting problems within the plant.

4.6 Response to Faults Detected in the I/O Bus Area

If a fault occurs in the I/O bus area between central module and connection modules, all I/O subracks affected by the fault are switched off.

If a fault in the I/O bus area only occurs within an I/O subrack, the connection module switches off the output modules in the affected I/O subrack.

4.7 Notice for Replacing Central Modules

Faulty modules in the central area or in the I/O area can be replaced during operation; the automation device needs not be shut down during replacement.

i Interruption of operation possible!
HIMA strongly recommends replacing faulty central modules.

During maintenance or if faults occur, the following steps are required for replacing the modules:

- Central modules for non-redundant automation devices with integrated back-up battery must be stored without user program if the user program contains retain variables. These variables are not set to their initial values when the system is started.
- Central modules for redundant automation devices with integrated back-up battery may be stored with the user program even if the user program contains retain variables. These variables are adopted by the running central module during start-up.

The diagnostic display on the central module displays *BATI* to signalize that the internal battery is empty.

Refer to the data sheet for recommendations on how to replace the battery on the modules.

i If the battery fails simultaneously to a voltage drop, the RETAIN variables lose the values previously stored. In such a case, the system initializes the values during start-up.

5 Input Modules

5.1 Overview of All Input Modules for the H41q and H51q Systems

Module	Designation	Safety-related	Interference-free	(Ex)i	Dedicated software function block
Digital input modules					
F 3221	Input module, 16 channels		•		
F 3222	Input module, 8 channels		•		
F 3223	Input module, 4 channels		•	•	
F 3224A	Input module, 4 channels		•	•	
F 3236	Input module, 16 channels	•	•		
F 3237	Input module, 8 channels	•	•		HB-RTE-3
F 3238	Input module, 8 channels	•	•	•	HB-RTE-3
F 3240	Input module, 8 channels	•	•		
F 3248	Input module, 16 channels	•	•		
F 5220	Counter module, 2 channels	•	•		HF-CNT-3, -4
Analog input modules					
F 6213[1)]	Analog input module, 4 channels	•	•		HA-RTE-3
F 6214[1)]	Analog input module, 4 channels	•	•		HA-RTE-3
F 6215	Analog input module, 8 channels		•		
F 6217	Analog input module, 8 channels	•	•		
F 6220	Thermocouple input module, 8 channels	•	•	•	HF-TMP-3
F 6221	Analog input module, 8 channels	•	•	•	HF-AIX-3
[1)] Discontinued module, no longer deliverable.					

Table 12: Input Modules for the H41q and H51q Systems

5.2 Safety and Availability of Safety-Related Input Modules

Due to their high complexity, some types of analog and digital input modules modules have their own 1oo2 microprocessor system that automatically performs safety-related tests during operation and provides safe data to the safe processing unit.

The safety-related input modules allow the diagnostics to be displayed and therefore the faults to be identified and located.

In safety-related systems, both safety-related and interference-free input modules can be used with mixed component configurations.

During operation, safety-related input modules automatically perform high-quality, cyclic self-tests within the H41q and H51 systems. The input modules include wiring elements ensuring that the input module function is tested with special test routines integrated in the operating system. These test routines are TÜV-tested and ensure the safe functioning of the corresponding module. If faults are detected, error messages are displayed. Detected faults automatically trigger a safety-related reaction of the system. The error messages are diagnostic information for the operator. It is thus possible to flexibly create a diagnostic system when planning and implementing the system.

To increase availability, the safety-related input modules can also be used redundantly.

The use of redundant input modules does not affect the system safety.

Safety-related input modules can be used for both safety-related signals and non-safety-related signals.

The following conditions must be observed when using the slots permitted for input modules within the system subracks, and the H41q and H51q systems within the I/O subracks:

H41q system	H51q system
The input modules are inserted into the system subrack. Kits with 12 slots (H41q) for I/O modules are available.	Each input module is inserted into the I/O subracks with 16 slots. The required basic components for I/O subracks are assembled in kits.

Table 13: Permitted Slots

5.2.1 Safety of Sensors, Detectors and Transmitters

Safety-related signals are only given if the external sensors, detectors or transmitters have a related proof of safety. If no proof of safety is available, safety of external sensors, detectors or transmitters can also be ensured by a special wiring, see the operating system manual (HI 800 105 E).

To this end, multiple sensors must be wired in a 1oo2, 2oo3 or NooM circuit. (Note: 1oo2 means 1 out of 2).

The safety and availability of the sensors can be increased through appropriate wiring. Chapter 7.8 details various implementation options for sensor wiring, taking safety and availability aspects into account. The user program must be designed accordingly.

Based on the IEC 61508 standard, various proofs of safety can be provided through the specification of proof test intervals. The detailed specifications of the proof test intervals depend on the application.

5.3 Safety-Related Digital Input Modules F 3236, F 3237, F 3238, F 3240 and F 3248

5.3.1 Test Routines

The online test routines check whether the input channels are able to forward both signal levels (low and high), irrespective of the signals actually present on the input. This functional test is performed whenever the input signals are read. Whenever a fault occurs in the input module, the low level (safe state) is processed in the user program.

The modules for proximity switches and mechanical contacts with line monitoring additionally test the line up to the sensor. A safety-related proximity switch can be connected to these modules. Self-tests ensure that all requirements for detecting thresholds in safety-related proximity switches are met.

Wiring with two resistors in accordance with the data sheet is required for the sensor current monitoring of a mechanical contact.

5.3.2 Response to Faults Detected in the F 3236, F 3237, F 3238, F 3240 and F 3248

Type of error	System reaction	Remark
Module fault (input module)	FALSE forwarded to user program for all channels	This ensures the system's safe function in accordance with the de-energize-to-trip principle.
Open-circuit in the sensor circuit	FALSE is read in the affected channel	If modules with line monitoring are used, a line fault is reported. In safety-related inputs, this signal must be evaluated with the HB-RTE-3 software function block (see Annex) to ensure a safe system reaction.
Short-circuit in the sensor circuit	TRUE is read in the affected channel	If modules with line monitoring are used, a line fault is reported. In safety-related inputs, this signal must be evaluated with the HB-RTE-3 software function block (see Annex) to ensure a safe system reaction.
General	The position of the faulty module is output to the diagnostic display. For F 3238 modules, which occupies two slots, the position of the right slot is displayed. If input modules are used and their sensor circuit is monitored for open-circuits and short-circuits, the diagnostic display also indicates the faulty module channel.	

Table 14: Response to Faults Detected in Safety-Related Digital Input Modules

5.4 Safety-Related F 5220 Counter Module

This two-channel counter module has its own dual processor system with one safety-related output for each channel. It can be used for counting the pulses, measuring the frequency or the rotational speed via an adjustable gate time and for monitoring the rotation direction.

If the gate time is modified, the correct measured value is only available at the output after three gate times.

5.4.1 Test Routines

The module has its own 1oo2 microprocessor system that automatically performs safety-related online tests and provides the safe data for safe signal processing to the HF-CNT-3 or HF-CNT-4 software function block.

5.4.2 Responses to Detected Errors

Type of error	System response in the event of faults	Remark
Module fault	The safety-related outputs are switched off.	In the event of a fault, reaction in safe direction only
Channel fault	Assigned safety-related output is switched off	In the event of a fault, reaction in safe direction only
Open-circuit, short-circuit or other type of faults within the proximity switch circuit.	Assigned safety-related output is switched off	After removing the fault, the reset signal is required on the input of the HF-CNT-3 / 4 function block.

Table 15: Response to Faults Detected in the Safety-Related Counter Module F 5220

5.5 Safety-Related Analog Input Modules F 6213, F 6214 and F 6217

If the safety-related analog input modules are functional and redundantly configured, the mean value is processed (within permitted deviations only!). The mean value is created by the corresponding function block or the user program depending on whether the F 6213 and F 6214 modules (function block) or the F 6217 (user program) are used. If faults occur, only the value of the functional module is processed.

5.5.1 Test Routines

The modules use the test D/A converter to apply test values and test these values with the A/D converter with which the input signal is digitized.

5.5.2 Responses to Faults Detected in the F 6213 and F 6214

Type of error	System response in the event of faults	Remark
Module or channel fault in single-channel analog inputs	Configured value processed in the HA-RTE-3 software function block (see Annex).	In the event of a fault, reaction in safe direction only
Module or channel fault in redundant analog input modules and redundant transmitters	If an input module fails, the value of the redundant module or the configured error value is processed.	Minimum, maximum or average determined via the HA-RTE-3 software function block (see Annex).
Short-circuit in the transmitter circuit	Module position and faulty channel output to the diagnostic display	Only if 4...20 mA is used

Table 16: Response to Faults Detected in Safety-Related Analog Input Modules F 6213, F 6214

5.5.3 Responses to Faults Detected in the F 6217

Type of error	System response in the event of faults	Remark
Channel fault	Analog value = 0000 Channel fault bit = TRUE	Channel fault bit must be safely processed in the user program
Module fault	All analog values = 0000 All channel bits = TRUE	See channel fault; concerns all channel fault bits
Measuring range exceeded (22 mA)	max. analog value = 4095 Channel fault bit = TRUE	The maximum value allowed must be defined in the user program.

Table 17: Response to Faults Detected in Safety-Related Analog Input Modules F 6217

The module has its own 1oo2 microprocessor system that automatically performs safety-related online tests and provides the safe data to the safe processing unit. Each channel has an analog value and a corresponding channel fault bit.

⚠ WARNING

Warning! Physical injury possible due to incorrect measured values!

If the channel fault bit is set, a safety-related reaction must be programmed for each safety-related analog input.

5.6 Safety-Related Analog Intrinsically Safe Thermocouple Input Module F 6220

The thermocouple module has 8 channels for connecting thermocouples of various types (according to the parameters set on the HF-TMP-3 function blocks) and one input for connecting a Pt 100 resistance thermometer as a reference temperature input. It has its own dual processor system and is configured using the HF-TMP-3 software function block (see Chapter 9.2.9 and the ELOP II online help) for each channel in use.

The inputs can also be used to measure low voltages, see data sheet.

5.6.1 Test Routines

The module has its own 1oo2 microprocessor system that automatically performs safety-related online tests and provides the safe data for safe signal processing to the HF-TMP-3 software function block. Each of the 8+1 channels provides safe input values and a safe fault status.

5.6.2 Response to Faults Detected in the F 6220

State	System reaction	Remark
Module fault	The *Channel Fault* output on the HF-TMP-3 function block is set to TRUE.	The reaction must be implemented in the user program using the *Channel Fault* output signal.
Channel fault	The *Channel Fault* output on the HF-TMP-3 function block is set to TRUE.	The reaction must be implemented in the user program.
Underflow	The *Underflow* output on the HF-TMP-3 function block is set to TRUE.	The reaction must be implemented in the user program.
Overflow	The *Overflow* output on the HF-TMP-3 function block is set to TRUE.	The reaction must be implemented in the user program.

Table 18: Response to Faults Detected in the Safety-Related Thermocouple Module F 6220

The *Underflow Threshold* and *Overflow Threshold* inputs of the HF-TMP-3 function block are used to define the limit values for underflow and overflow, respectively. If the measured value for the configured limit values is exceeded, the corresponding signal is set to TRUE, even if no fault occurred in the module.

5.6.3 Configuration Notices

- Unused inputs must be short-circuited.
- A requirement for SIL 3 is that the reference temperature must be taken from the user program or must be determined by comparing the reference temperatures of two modules.
- All possible deviations must be considered and taken into account when evaluating the measured values.
- For SIL 3, the thermocouple temperature must be determined by comparing the temperatures of two different thermocouples.

5.7 Safety-Related Analog Intrinsically Safe Input Module F 6221

The analog input module has eight channels to directly connect analog transmitters from the Ex-Zone. The transmitter supply voltage can be ensured through the F 3325 output module or another power supply in accordance with the data sheet specifications. This transmitter voltage supply must be connected to the F 6221 module for monitoring purposes.

Each channel in use is configured using a specific HF-AIX-3 software function block.

5.7.1 Test Routines

The module has its own 1oo2 microprocessor system that automatically performs safety-related online tests and provides the safe data for safe signal processing to the HF-AIX-3 software function block. Each of the 8 channels provides safe input values and a safe fault status.

5.7.2 Responses to Faults Detected in the F 6221

State	System reaction	Remark
Module fault	The *Value* output (INT) on the HF-AIX-3 function block is set to 0. The *Channel Fault* output on the HF-AIX-3 function block is set to TRUE.	The *Error Value* input signal of the function block must be used to define an error value in the user program.
Channel fault	The *Channel Fault* output on the HF-AIX-3 function block is set to TRUE.	
Underflow	The *Underflow* output on the HF-AIX-3 function block is set to TRUE.	
Overflow	The *Overflow* output on the HF-AIX-3 function block is set to TRUE.	

Table 19: Response to Faults Detected in the Safety-Related Analog Input Module F 6221

The *Underflow Threshold* and *Overflow Threshold* inputs of the HF-AIX-3 function block are used to define the limit values for underflow and overflow, respectively. If the measured value for the configured limit values is exceeded, the corresponding signal is set to TRUE, even if no fault occurred in the module.

5.7.3 Additional Configuration Notices

- Unused voltage inputs 0...1 V must be short-circuited on the terminal block.
- Unused current inputs are terminated with a shunt in the cable plug.
- Only uses specified in the data sheet of the F 6221 module are allowed.
- The Ex protection regulations and Ex connection conditions must be observed.

5.8 Notice for Replacing Input Modules

During maintenance or if faults occur, the following steps are required for replacing the modules:

To replace an input module

1. Unscrew the cable plug or remove the input module with inserted cable plug.
2. Insert the new module without cable plug and screw it in place.
3. Plug in the cable plug and screw it in place.
4. Press the acknowledgment key (ACK key on the central module).

► The replacement of the input module is complete.

i Interruption of operation possible!
HIMA strongly recommends replacing faulty input modules.

5.9 Checklists for Engineering, Programming and Starting up Safety-Related Input Modules

When engineering or starting up the system, a checklist must be filled out for each of the safety-related input modules used in the system to verify the requirements to be met. This is the only way to ensure that all requirements were considered and clearly recorded. The checklists are also documents demonstrating a thorough engineering.

The checklists associated with this safety manual are available as MS Word files on the HIMA DVD or can be downloaded from the HIMA Internet page at www.hima.de and www.hima.com.

SDIGE-F3236	For safety-related digital modules
SDIGE-F3237	For safety-related digital modules
SDIGE-F3238	For safety-related digital modules
SDIGE-F3240	For safety-related digital modules
SDIGE-F3248	For safety-related digital modules
SDIGE-F5220	For safety-related counter modules
SANAE-F6213 / F6214	For safety-related analog modules
SANAE-F6217	For safety-related analog modules
SANAE-F6220	For safety-related analog modules
SANAE-F6221	For safety-related analog modules

6 Output Modules

6.1 Overview of All Output Modules for the H41q and H51q Systems

Module	Designation	Safety-related	Interference-free	Load capacity	Dedicated software function block
Digital output modules					
F 3322	Digital output module, 16 channels		•	≤ 0.5 A	
F 3325	Supply Module (Ex), 6 channels		•	22 V ≤ 0.02 A	
F 3330	Digital output module, 8 channels	•	•	≤ 0.5 A	
F 3331	Digital output module, 8 channels	•	•	≤ 0.5 A	HB-BLD-3[1)] HB-BLD-4[1)]
F 3333	Digital output module, 4 channels	•	•	≤ 2 A	
F 3334	Digital output module, 4 channels	•	•	≤ 2 A	HB-BLD-3[1)] HB-BLD-4[1)]
F 3335	Digital output module (Ex)i, 4 channels	•	•	22 V ≤ 0.053 A	
F 3348	Digital output module, 8 channels	•	•	≤ 0.5 A	
F 3349	Digital output module, 8 channels	•	•	≤ 0.5 A ≤ 48 V	HB-BLD-3[1)] HB-BLD-4[1)]
F 3422	Digital relay module, 8 channels		•	≤ 2 A ≤ 60 V	
F 3430[2)]	Digital relay module	•	•	≤ 4 A ≤ 250 V	
Analog output modules					
F 6705	Analog output module,2 channels	•	•	0...20 mA	HZ-FAN-3[3)]
F 6706	Analog output module,2 channels		•	0...20 mA	

[1)] For displaying faults and configuring the modes of operation (de-energize-to-trip, energize-to-trip)

[2)] The F 3430 module is not certified in accordance with EN/ISO 13849-1.

[3)] Required for fault evaluation in current sink mode

Table 20: Output Modules for the H41q and H51q Systems

6.2 General Notes on the Safety and Availability of Safety-Related Output Modules

The safety-related output modules are written in each cycle, the generated output signals are read back and compared with the output data calculated by the user program.

Additionally, a background walking bit test is performed on all the outputs. During this test, the test signal is present for no longer than 200 µs. This ensures that the switchability of the outputs is verified without affecting the function of the connected actuators. As a result, the freezing of each output is detected, even if the output signal is static.

Safety-related output modules with line monitoring can detect faults in the input line to the load. The line monitoring function meets the safety requirements up to SIL 1. This is only relevant if line monitoring is used in safety-related circuits. The output signal can be used in all applications for safety requirements up to SIL 3.

H41q system	H51q system
The output modules are inserted into the system subrack. Kits with 12 slots (H41q) for I/O modules.	The output modules are inserted into specific I/O subracks equipped with a maximum of 16 slot for I/O modules. The basic components required for I/O subracks are assembled in kits (see Chapter 4.2).
Slots for output modules in the H41q and H51q systems	Slots for output modules in the H41q and H51q systems

Table 21: Slots for Output Modules in the H41q and H51q Systems

6.2.1 Safety-Related Digital Output Modules

The test routines detect faults by comparing the output signals read back with the internal output data. The operating system ensures that the module in the module position detected as defective enters the safe state, and reports this to the diagnostic display.

In modules with output circuit monitoring, a detected open-circuit is reported to the diagnostic display with indication of the faulty module channel. The faulty module is safely shut down using the integrated safety shutdown.

Additionally, the H8-STA-3 software function block can be used to define one or several shutdown groups. An output module fault causes all remaining output modules of the shut-off group to be shut down.

Depending on the system safety requirements, the I/O parameters in the resource settings can be used to configure a complete shutdown of the controller.

6.2.2 Safety-Related Analog Output Modules

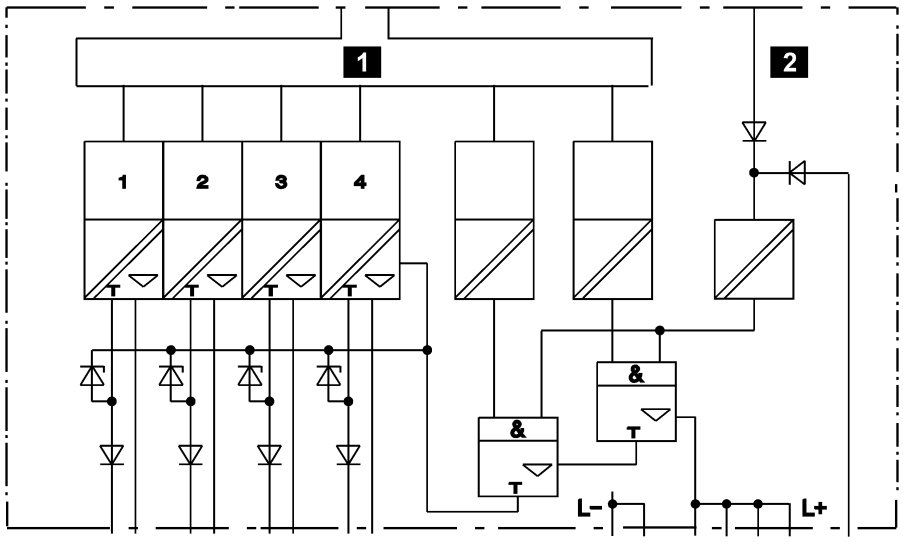
The safety-related analog output modules can be used in current source mode or in current sink mode of operation.

In current source mode, if a fault occurs, the integrated safety shutdown ensures the safe state (output current 0 mA).

In current sink mode, the module is only able to enter the safe state if additional measures are taken. The user program must safely shut down the supply voltage for the current loop. To this end, the HZ-FAN-3 software function block must be used for evaluating the faults.

6.3 General Operation of Safety-Related Output Modules

In safety-related output modules, 3 testable semiconductor switches are connected in series. Thus, a second independent switch-off function, which is a safety requirement, is integrated into the output module. If a fault occurs, this integrated safety switch-off function safely de-energizes the individual channels of the defective output module (de-energized state).



1 I/O Bus

2 Watchdog (WD) Signal

Figure 1: Principle of the Output Module Circuit with Integrated Safety Shutdown (here with 4 Output Channels)

6.4 Safety-Related Digital Output Module F 3330, F 3331, F 3333, F 3334, F 3335, F 3349

6.4.1 Test Routines

The modules are tested automatically during operation. The main test functions are:

1. Read back of the output signals from the switching amplifier. The switching threshold for a read-back low level is ≤ 6.5 V.
2. Reading the line diagnosis for the activated channels (only with F 3331, F 3334 and F 3349).
3. Applying the test patterns and testing for crosstalk (walking bit test) during the background test.
4. Reading the line diagnosis for all channels (only with F 3331, F 3334 and F 3349).
5. Checking the integrated safety shutdown.

6.4.2 Response to Faults Detected in the F 3330, F 3331, F 3333, F 3334, F 3335 and F 3349

- All faults detected in the modules cause the affected module to enter the safe, de-energized state, i.e., the module is shut down.
- External short-circuits that cannot be distinguished from internal faults, cause the module to shut down.
- Line faults are only signaled and do not lead to the module's shutdown.

6.4.3 Notices for Engineering

Prior to deleting an F 3330, F 3331, F 3333 or F 3334 module from the project configuration, the outputs must be reset, e.g., the forcing process must be stopped for outputs that are being forced to signal 1.

6.5 Safety-Related Digital F 3430 Relay Module

6.5.1 Test Routines

The module is automatically tested during operation. The main test functions are:

1. Reading the output signals back from the switching amplifier for the diversified, 3-channel relay switch.
2. Applying the test patterns and testing for crosstalk (walking bit test) during the background test.
3. Checking the integrated safety shutdown.

6.5.2 Response to Faults Detected in Safety-Related Digital Relay Modules

- All faults detected in the modules cause the affected module to enter the safe, de-energized state, i.e., the module is shut down.
- External short-circuits cause the fuse for the relevant channel to trigger. No error message is generated.

6.5.3 Notices for Engineering

Relays are electromechanical components with limited lifetime due to their construction. The lifetime of relays depends on the switching capacity of the contacts (voltage/current) and the number of switching cycles.

At nominal operating conditions, the lifetime is approx. 300 000 switching operations at 30 VDC and 4 A.

To meet the requirements in accordance with IEC 61508 (PFD/PFH, see Chapter 3.1.1), the proof-test interval is of 5 years for use in SIL 3 and 20 years for use in SIL 2.

The required tests are performed by HIMA.

6.6 Safety-Related Analog Analog F 6705 Output Module

6.6.1 Test Routines

The module is automatically tested during operation. The main test functions are:

1. Reading the output signals back.
2. Checking the D/A converter for linearity.
3. Crosstalk test between the outputs.
4. Checking the integrated safety shutdown.

6.6.2 Responses to Faults Detected in the F 6705

In current source mode, all faults detected in the modules cause the affected module to enter the safe, de-energized state, i.e., the module is shut down via the integrated safety shutdown.

An external open-circuit cannot be distinguished from internal faults and cause the module to be shut down.

In current sink mode, the module can only enter the safe, de-energized state via an external shutdown. The user program must shut down the voltage supply for the current loop safely. Therefore, the HZ-FAN-3 software function block must be used for evaluating the faults.

6.7 Notice for Replacing Output Modules

During maintenance or if faults occur, the following steps are required for replacing the modules:

To replace an output module

1. Unscrew the cable plug or remove the output module with inserted cable plug.
2. Insert the new output module without cable plug and screw it in place.
3. Plug in the cable plug and screw it in place.
4. Press the acknowledgment key (ACK key on the central module).

► The output module is replaced.

i Interruption of operation possible!
HIMA strongly recommends replacing faulty output modules.

6.8 Checklists for Engineering, Programming and Starting up Safety-Related Output Modules

When engineering or starting up the system, a checklist must be filled out for each of the safety-related output modules used in the system to verify the requirements to be met. This is the only way to ensure that all requirements were considered and clearly recorded. The checklists are also documents demonstrating a thorough engineering.

The checklists associated with this safety manual are available as MS Word files on the HIMA DVD or can be downloaded from the HIMA Internet page at www.hima.de and www.hima.com.

SDIGA-F3330	For safety-related digital modules
SDIGA-F3331	For safety-related digital modules
SDIGA-F3333	For safety-related digital modules
SDIGA-F3334	For safety-related digital modules
SDIGA-F3335	For safety-related digital modules
SDIGA-F3348	For safety-related digital modules
SDIGA-F3349	For safety-related digital modules
SDIGA-F3430	For safety-related digital modules
SANAA-F6705	For safety-related analog modules

7 Software

The software for the safety-related HIMA automation devices of the H41q and H51q system families is divided into three blocks:

- Operating systemOperating System
- User program
- Programming tool in accordance with IEC 61131-3 (ELOP II with integrated safety tool).

The operating system must be used in the current version certified by TÜV for safety-related applications. This version can be found in the document *Revision List of Devices and Firmware of H41q/H51q Systems* maintained together with the test authority. This document is created by the joint modification service from TÜV Rheinland Industrie Service GmbH and HIMA.

The user program is created using the ELOP II programming tool and contains the application-specific functions to be performed by the automation device. ELOP II is also used to configure the operating system functions. A code generator translates the user program into a machine code. ELOP II uses a serial interface or the Ethernet interface to transfer this machine code and the project configuration to the flash EPROM of the central module.

The main functions of the operating system and the resulting specifications for the user program are described in the operating system manual (HI 800 105 E).

7.1 Safety-Related Aspects of the Operating System

This chapter describes the signatures and the basic functionality of the operating system.

7.1.1 Identifying the Current Version Released for Safety-Related Applications (CRC Signature)

Each new operating system is identified by a specific release status. An additional identification option is the operating system signature, which can be output to the diagnostic display while the automation device is operating.

The valid operating system versions approved by TÜV for safety-related automation devices, and the corresponding signatures (CRCs) are specified in the *Revision List of Devices and Firmware of H41q/H51q Systems*.

7.1.2 Operation and Functions of the Operating System

The operating system executes the user program cyclically. The sequence order is represented in simplified form:

1. Reading the input data (hardware inputs)
2. Editing the logic functions in accordance with IEC 61131-3, Section 4.1.3
3. Writing the output data (hardware outputs)

The following basic functions are also executed:

- Comprehensive self-tests
- Test of I/O modules during operation
- Data transfer and comparison

A cycle is processed in seven phases. Refer to the operating system manual (HI 800 105 E) for more details on these phases.

7.2 Safety-Related Aspects of the User Program

General sequence for programming the automation devices of the H41q/H51q system families for safety-related applications:

1. Specifing the controller functionality

2. Writing the user program
3. Using the offline simulation to verify the user program
4. Compile the user program using the C-code generator.
5. The proven C compiler (GNU CC) translates the C code twice and generates the target and reference codes.
6. The target code comparator compares the target code and the reference code. It also detects and reports faults caused by the unsafe PC.
7. The operational program resulting from this error-free procedure is loaded into the H41q or H51q system. The program can then be tested from within the system.
8. Upon successful completion of the test, the PES starts safe operation.

Terms

Load	This term indicates the procedure for loading a program into the controller, either by performing a download or a reload.
Download	If a download is performed to load a program into the controller, the controller is stopped and all its outputs are reset.
Reload	If a reload is performed to load a user program into a redundant controller, the modified user program is successively loaded into the central modules. In the process, a central module is always operating in MONO mode. The controller is not stopped. If the PES only equipped with one central module, the outputs are held for the duration of the loading process. A reload can only be performed if a reloadable code was generated beforehand.

7.2.1 Requirements and Rules for Use in Safety-Related Applications (e.g., Requirements Resulting from the Type Approval Report)

The user program is created with the ELOP II programming tool. Additionally, the PC must be equipped with a hardlock module from HIMA.

The ELOP II programming tool includes the following functions:

- Input (Function Block Editor), monitoring and documentation.
- Variables with symbolic names and variable types (BOOL, UINT, etc.).
- Resource assignment (HIMA H41q/H51q automation systems).
- Code generator (for translating the user program into a machine code) with C code generator and GNU C compiler.

7.2.1.1 Programming Basics

The tasks to be performed by the controller should be defined in a specification or a requirements specification. This documentation serves as the basis for checking its proper implementation in the program. The specification format depends on the tasks to be performed. These include:

- Combinational logic:
  - Cause/effect diagram
  - Logic of the connection with functions and function blocks
  - Function blocks with specified characteristics.
- Sequential controllers (sequence control system)
  - Written description of the steps and their enabling conditions and of the actuators to be controlled.
  - Flow charts in accordance with DIN EN 60848
  - Matrix or table form of the step enabling conditions and the actuators to be controlled.
  - Definition of constraints, e.g., operating modes, EMERGENCY STOP, etc.

The automation concept of the system must include the analysis of the field circuits, i.e., the type of sensors and actuators:

- Sensors (digital or analog)
  - Signals during normal operation (de-energize-to-trip principle with digital sensors, 'life-zero' with analog sensors).
  - Signals in the event of a fault:
  - Definition of safety-related redundancies required for safety (1oo2, 2oo3).
  - Monitoring of discrepancy and reaction.
- Actuators
  - Positioning and activation during normal operation.
  - Safe reaction/positioning at shutdown or after power loss.

Programming goals for user program:

- Comprehensibility
- Traceability
- Alterability

7.2.2 Safety-Related Aspects of Programming with ELOP II

The ELOP II programming tool is used to create user programs.

Operating conditions such as supported Windows version, are specified in the documentation of the corresponding ELOP II version.

The safety concept of ELOP II ensures that:

- the programming tool operates properly, i.e., programming tool errors are detected,
- the users employ the programming tool properly, i.e., user mistakes are detected.

When commissioning a safety-related controller, a comprehensive functional test is performed to verify the safety of the entire system. So far, a complete functional test was required to ensure safety, if the user program was changed.

The safety tool included in ELOP II is in accordance with IEC 61131-3 and ensures that, if the user program has been modified, only the performed changes must be verified. This safety tool is used to detect user mistakes and programming tool errors.

The ELOP II safety tool is composed of three function blocks essential for safety:

- C code comparator
- Target code comparator
- Proven GNU C compiler

The C code comparator identifies changes performed to the user program. The target code comparator compares two target codes generated consecutively by the GNU C compiler (GNU CC). This action prevents faults due to an unsafe PC.

Non-safety-related utilities are:

- The revision management integrated in ELOP II. It can be used to uniquely identify the relevant project versions.
- The offline simulation represented in the flow diagram in Figure 2. The offline simulation verifes whether the user program complies with the specification, but has no effect on the process.

7.2.2.1 Using the ELOP II Safety Tool when Creating the Program

The reference points used in the following text are specified in the flow diagram depicted in Figure 2.

1. Creation of a user program in accordance with a binding specification (e.g., in accordance with IEC 61508, DIN V VDE 0801 or a corresponding user standard); points (1) through (4) in the flow diagram .
2. The C code generator compiles the user program into C code and generates a reference file; point (5) in the flow diagram.

⚠ WARNING

Physical injury possible due to malfunction!

A cross-reference list must be generated for the user program and checked for correct use of the variables. It must be verified that all variables are only used in the positions indicated in the specification.

3. The proven compiler (GNU CC) translates the C code and the reference file, points (6) and (13). The compiler generates the target code and the reference code.

⚠ WARNING

Physical injury possible due to malfunction!

The target code comparator must be activated, point (14). It compares the target code and the reference code. The target code comparator detects and reports the faults caused by the unsafe PC.

4. Load the resulting operational program into the H41q or H51q system, point (7). Then, the program must be completely tested and accepted; point (8).
5. Generate a backup of the target code.
6. The PES starts safe operation.

7.2.2.2 Using the ELOP II Safety Tool when Modifying the Program

1. Modification of a user program in accordance with a binding specification (e.g., IEC 61508 or a corresponding user standard); points (1) through (4) in the flow diagram.

   The modification is based on the backup of the running user program. This backup includes:
   - Reference file
   - Target code
   - Input data
2. The C code generator compiles the modified user program into C code (new), point (5).
3. The C code comparator must be activated, point (12). It compares the C code (new) with the C code (old) of the previous program version, point (11). The backup must be indicated as reference file (C code (old)).
4. The result of the comparison is documented, point (15).
5. Check whether the C code comparator displays the changes performed to the user program. Only code-relevant changes are indicated.
6. Results of the C code comparator:

   a Changes that the user does not recognize, are reported. Possible reasons:
   - The change performed by the user resulted in additional unplanned modifications.
   - An internal fault occurred.

   b Changes performed by the user are not reported. Possible reasons:
   - They are changes that are not recognized by the C code comparator such as graphical changes or changes to initial values.
   - They are changes that were not adopted correctly.

7. The compiler (GNU CC) translates the C code (new) and the reference file (new), points (6) and (13). It generates the target code and the reference code.
8. The target code comparator must be activated, point (14). It compares the target code and the reference code. Faults due to an unsafe PC are thus recognized and reported.
9. The resulting operational program is loaded into the H41q or H51q system. All program parts subject to changes are to be tested in the system. The test of the changes verifies that the target code is correct.
10. If no malfunction results, a backup of the new current program must be generated. The PES can start safe operation.

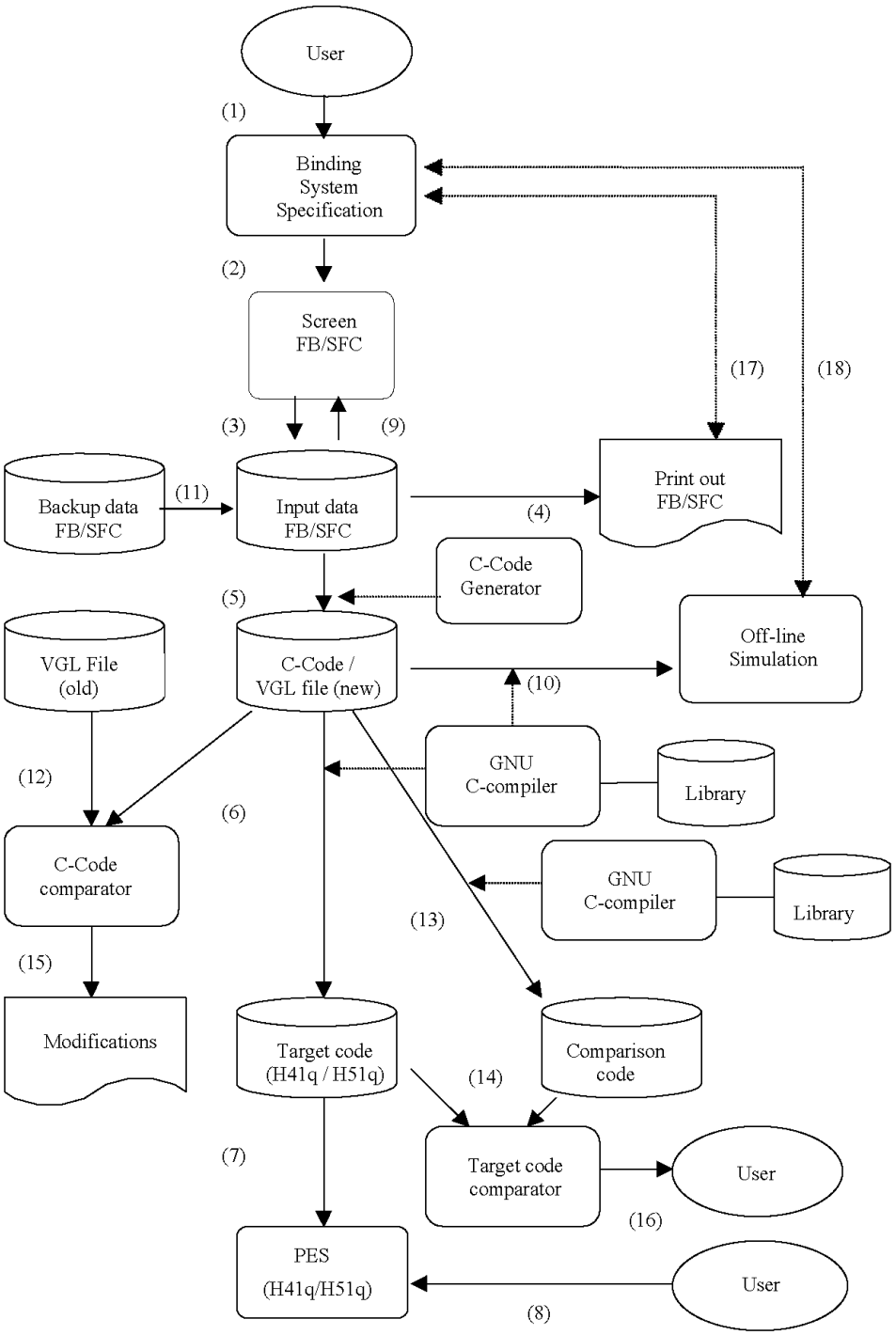


Figure 2: Flow Diagram, Function of the Safety Tool

7.2.3 Use of Variables and PCS Names

The names and data types of the variables are defined using the Variable Declaration Editor. All the user program variables are assigned symbolic names. These symbolic names may include a maximum of 256 characters.

Symbolic names are also used for physical inputs and outputs and may include up to 256 characters.

The user has two essential advantages when using symbolic names instead of physical addresses:

- The plant denominations of inputs and outputs are used in the user program.
- The modification of how the signals are assigned to the input and output channels does not affect the user program.

7.2.3.1 Assigning PCS Names to Variable Names

PCS names should be assigned to variable names in accordance with the measuring points list or a list of sensors and actuators.

Variable names are assigned to the used hardware in the dialog box for the resource, under *Edit Cabinet*. The following data must be entered:

- Subrack position (1-1 through 1-8 or 2-1 through 2-8)
- Subrack type
- Slot and type of the required module
- PCS names to be to assigned to the variable names

TIP For practical reasons, the variable name and the PCS name should be identical.

The number of channels (names) per module depends on the type of module used. The required test routines for safety-related I/O modules are automatically executed by the operating system.

HIMA recommends grouping the input and output modules used in the I/O subracks into functional units.

The functional units may be grouped in accordance with the following aspects:

- Grouping in accordance with the plant parts
- Homogeneous arrangement of the modules such as:
  - Digital/analog system components
  - Safety-related/non safety-related I/O modules
- Redundant grouping into various I/O subracks in the same order
- Spare modules or channels for later reload (reloadable code)

7.2.3.2 Types of Variables

Depending on the program organization unit (POU) – program, function block or function –, different types of variables can be defined. The following table provides an overview:

Type of variable	User program PROG	Function block FB	Function FUN	Use
VAR	X (CONST[1)], RETAIN[2)])	X (CONST, RETAIN)	X (CONST)	Local variables
VAR_INPUT	-	X	X	Input variable
VAR_OUTPUT	-	X (RETAIN)	X	Output variable
VAR_EXTERNAL	-	X (CONST)	-	Externally from / to another POU
VAR_GLOBAL	X (CONST, RETAIN)	-	-	Global from another POU
VAR_ACTION	X	X	X	In the action block of the sequential function chart

[1)] CONST: Constant that can be changed in the online test without the need to recompile the user program. It cannot be written by the user program.

[1)] RETAIN: Non-volatile variable, i.e., its value is retained after a voltage drop and resumption of power supply.

Table 22: Types of Variables in ELOP II

Not initialized variables are reset to zero or FALSE after a cold start.

7.2.3.3 Digital Inputs and Outputs for Boolean Variables

When the resource is defined, the difference is made between digital inputs and outputs and safety-related digital inputs and outputs. For safety-related functions, only safety-related I/O modules may be used. For most safety-related I/O modules, HIMA standard function blocks must be planned in the user program (see Annex).

Non-safety-related I/O modules are only read or written by the operating system and are not subject to further test routines. For this reason, a defect is not detected by the operating system and no error message appears. HIMA recommends using safety-related I/O modules only, due to the extended diagnosis.

7.2.3.4 Analog I/O Modules

Analog input modules convert analog values (voltages, currents) into digital values with 12-bit resolution.

Analog output modules convert 12-bit digital values into currents 0...20 mA or 4...20 mA.

For most analog safety-related and non safety-related I/O modules, HIMA function blocks must be used in the user program, see Annex.

7.2.3.5 Imported or Exported Variables

The data of the variables to be imported or exported are either forwarded for HIMA communication via HIPRO (PES master) or to third-party systems via the interfaces. Protocols available for third-party systems are Modbus, Modbus TCP, PROFIBUS DP and 3964R. The data can also be transmitted to an OPC server via an Ethernet protocol. The import and export variables are processed in the user program like normal input and output variables. They are defined in the variable declaration of the program instance.

Boolean variables may be assigned the Event attribute. Events are signal changes of Boolean variables with additional information about the time (date and time). The timestamp of an event corresponds to the time of the automation device in millisecond precision.

7.2.4 User Program Signatures

Unintentional or unauthorized changes to the user program, can be detected due to multiple CRC signatures. These signatures are referred to as version numbers. The following version numbers exist in ELOP II:

- Code Version Number
- Run Version Number
- Data Version Number
- Area Version Number

7.2.4.1 Code Version Number

The code version number is created using the functions of the programmed logic. The controller function can only be viewed on a PC if the code version of the program loaded in the controller and in the programming device are identical.

The following actions have no influence on the code version number:

- Writing or deleting of comments
- Setting or deleting of online test fields (OLT fields), i.e., force information
- Shifting of lines or function blocks, if the processing sequence does not change
- Changing of the SIO parameters themselves, but not activating/deactivating the SIO parameters
- Bus parameters.

Changes of the basic addresses for external/Modbus coupling may result in a change of the code version number. With all other changes, the code version number changes as well.

7.2.4.2 Run Version Number

The controller generates the run version number during operation. Its comparison with a currently valid and documented run version number shows whether the program loaded into the controller has changed (which is visible in the diagnostic display after a call action).

The run version number changes in the following cases:

- A different code version number is in use (does not apply to all changes)
- Modules were added or deleted
- Other system parameters are in use
- VAR_CONST have been added or deleted
- VAR_CONST values have changed
- The resource type has changed
- Settings have been changed online
- I/O variables have been forced in the online test field
- The position of the force main switch has changed

7.2.4.3 Data Version Number

The data version number refers to the definition of non-safety-related imported or exported variables and changes in the following case:

- If the name of a variable with attributes for HIPRO-N (non safety-related) changes.
- If these variables were compressed when generating a non-reloadable code (if memory gaps exist).

7.2.4.4 Area Version Number

The area version number records all the variables defined in a project and changes in the following cases:

- If modules are deleted or added modules within the control cabinet.
- If reloadable code generation is configured and attributes of the following types are assigned more variables than deleted:
- HIPRO-N, HIPRO-S, BUSCOM, Event, 3964R.
- If reloadable code generation is not configured and variables with attributes of the following types are added or deleted:

  HIPRO-N, HIPRO-S, BUSCOM, Event, 3964R.
- If the memory must be reorganized because the memory limit was achieved.

Changes of the basic addresses for external/Modbus coupling may result in a change of the area version number.

7.2.5 Setting the Parameters for the Automation Device

The parameters listed below define how the automation device behaves during operation and are configured in the **Properties** menu for the resource.

7.2.5.1 Safety Parameters

The following safety parameters can be set in the resource's **Properties**:

- The parameters for safety-related operation of the automation device.
- The actions allowed with the PADT during safety-related operation

Safety-related parameters		Recommended settings
Parameters that can be modified online		Reset, depending on the project
Safety parameters		
	Safety time in s	Process-dependent
	Watchdog time in ms	No more than half of the safety time value
	Requirement class	6, corresponds to SIL 3, depending on the project
Changeable values		
	Constants	Reset
	Variables	Reset
	I/O forcing	Reset
Allowed actions		
	Test Mode	Reset
	Start	Reset
	Reload	Depending on the project

Table 23: Safety-Related Parameters

i For operating system versions prior to (07.14), the safety time must **not** be set to 255 s!
Only values within **1...254 s** are allowed!

Settings that may be defined for safety-related operation are not firmly bound to any specific safety integrity levels (SIL). Instead, each of these must be agreed upon together with the competent test authority for each separate implementation of the automation device.

Changing the Safety Parameters Online

The *Change System Parameters* dialog box can be activated in the Control Panel. The **Safety** tab is used to change safety parameters during operation. If *Parameter online change* is set to

Not Changeable and is transferred to the controller, these parameters can no longer be changed online.

This, however, cannot be recognized from the tab content. For this reason, it is still possible to use the functions for changing and transferring the parameters to the controller during operation. Nevertheless, the controller ignores further online changes, if the *Parameter Online Change* was not activated.

Additional online changes can only be performed again if the *Parameter Online Change* option is activated in the user program and is loaded into the controller by performing a download.

7.2.5.2 Behavior if Faults Occur in Safety-Related Output Channels

The following table shows the setting options for *Behavior in Case of Output Faults*. This parameter is located in the **I/O Parameters** tab of a resource's *Properties* dialog box.

Setting	Description
Display only	Shutdown via safety shutdown integrated in the output amplifier. If not possible, the watchdog signal within the I/O subrack is switched off via the connection module (systems H51q only). The watchdog signal in the corresponding central module is not switched off. The user program and communication continue to run. **Only allowed up to SIL 1!**
Emergency stop	The watchdog signal of the corresponding central module is switched off, which also causes the output channels to be shut off. The user program and communication are stopped.
Normal operation	Reaction as described in *Display only*; additionally, the watchdog signal in the corresponding grouping is switched off if a group was configured beforehand using the H8-STA-3 function block; refer to Chapter 9.2.1 for details. The watchdog signal in the corresponding central module is switched off (error stop) if no group was configured beforehand or the groupe relay is faulty. In this scenario, the user program and communication are stopped. **Required with SIL 2 and higher.** **Usual and recommended setting.**

Table 24: Behavior in Case of Output Faults

7.2.6 Identifying the Program

The user program can be uniquely identified using the code version number. This also allows one to uniquely identify the corresponding backup (archive version).

If it is not clear which backup copy is the correct one, the relevant backup must be compiled with download option and its target code must be compared to the code version of the loaded program.

With reloadable codes, this may only be done if the backup copy was generated in the following way:

1. Perform the last change.
2. Generate (compile) the reloadable code, resulting in code version A.
3. Load controller with code version A.
4. Generate the reloadable code, resulting in code version B, it can be identical to A.
5. Load controller with code version B.
6. Each additional code generation without changes results in code version B.

7.2.7 Checking the Created User Program for Compliance with the Specified Safety Function

A number of suitable test cases covering the specification must be created for the verification. It is not necessary to perform 2^{20} test cases for 20-fold AND gates. The independent test of each

input and of the most important logic connections is usually sufficient. This series of test cases is sufficient since ELOP II and the measures defined in this safety manual make it sufficiently improbable that a code generated properly from a semantic and syntactic view point can still contain undetected systematic faults resulting from the code generation process.

An appropriate series of tests must also be generated for numerically evaluating formulas. Equivalence class tests are convenient which are tests within defined ranges of values, at the limits of and within invalid ranges of values. The test cases must be selected such that the calculation can be proven to be correct. The required number of test cases depends on the formula used and must include critical value pairs.

To this end, the online test can be useful, e.g., for presetting values and read intermediate values. However, the active simulation with sources must be performed since it is the only way to verify the proper wiring of the sensors and actuators. This is also the only way to verify the system configuration.

7.3 Checklist: Measures for Creating a User Program

The checklist MEAP-0001-D is available as Word file on the HIMA DVD or can be downloaded at www.hima.de and www.hima.com.

7.4 Reload (Reloadable Code)

If a reload may be performed to load the user program into the central module(s), the Reloadable Code message appears while the code generator is compiling the code.

Some user program changes cause the user program to lose the capability of reload, refer to the operating system manual (HI 800 105 E) for further details and restrictions.

i A reload is only permitted after receiving consent from the test authority responsible for the factory acceptance test (FAT). During the entire reload process, the person in charge must take further technical and organizational measures to ensure that the process is sufficiently monitored in terms of safety.

⚠ WARNING

Warning! Physical injury possible due to malfunction!

Prior to performing the reload, use the C code comparator integrated in the safety tool of ELOP II to determine the changes performed to the user program compared to the user program still running.

The changes caused by the reload must be carefully tested on simulators prior to transferring them to the PES.

7.4.1 Systems with One Central Module

While the user program is being loaded, the I/O level may not be accessed, i.e., no I/O modules are read, written to or tested.

While the user program is being loaded, the controller interfaces are not processed by the user program and imported or exported variables are not routed via the interfaces.

i **Interruption of operation possible!**

If a reload is performed in systems having only one central module, it must also be completed within the process safety time.

7.4.2 Systems with Redundant Central Modules

A reload may be performed in system having redundant central modules without the restrictions mentioned for the single-channel systems.

Reload operating sequence:

1. While the first central module is being reloaded, the second central module continues processing the user program in mono operation.
2. Afterwards, the newly loaded central module receives the current data from the operating central module and adopts mono operation with the new user program.
3. After being loaded, the second central module adopts the current data from the first one and the two central modules start to operate redundantly.

7.5 Offline Test

Changes performed to the user program may be simulated in ELOP II with the offline test. This type of simulation is helpful to evaluate the potential consequences of a change. However, it is not sufficient to validate the changes performed to safety-related controllers. To this end, a test of the actual controller or a simulator is necessary.

7.6 Forcing

The operating company is responsible for forcing.

Forcing is only permitted after receiving consent from the test authority responsible for the factory acceptance test (FAT). When forcing values, the person in charge must take further technical and organizational measures to ensure that the process is sufficiently monitored in terms of safety.

The following options are available for forcing:

- The system can be configured to not permit forcing. The PES no longer accepts force values defined by the user. In such a case, the new force values can only be set once the system has been shut down.
- When closing the Control Panel, a message appears informing on whether and how many forced values are still set.
- All forced inputs and outputs may be reset using two individual force main switches.

For further details on the forcing procedure refer to the operating system manual (HI 800 105 E) and the ELOP II online help.

⚠ WARNING

Physical injury possible due to unintended function!

All force markers must be removed from the user program prior to starting safety-related operation!

7.6.1 Deletion of Forced Variables

Prior to deleting variables, stop forcing them!

Reason

- Deleting a forced variable and loading this change into the controller causes the Force Editor to no longer display the deleted variable. This applies for all ELOP II versions, including V5.1 730 IV3. With newer ELOP II versions, forcing of deleted variables can also be stopped from within the Force Editor upon completion of the loading process.
- The reason is that the input assigned to the variable until that moment retains the Forced properties and the force value.

- Adding a given variable at a later point in time and assigning it to a forced input causes the new variable to be forced immediately after the reload process!

This may impact the safety of the plant.

7.7 Functions of the User Program

Programming is not subject to hardware restrictions. The user program functions can be freely programmed. When programming, ensure that the de-energize-to-trip principle is taken into account for the physical inputs and outputs. A line break, for instance, causes the related actuators to be switched off.

- Compared to hard-wired safety-related controllers, line breaks in the user program of programmable logic controllers need not be taken into account.
- Negations are permitted at all points within the logic.
- Active signals for triggering an action (e.g., shift clock pulse for a shift register) can be used for safety-related applications.

If an error occurs in a safety-related analog input module, a defined value is further processed. Refer to the description of the function blocks provided in chapter 9.2 for details.

If an error occurs in a safety-related digital I/O module, the input is set to the safe value 0 and the digital output module is switched off by the integrated safety shutdown. Refer to the description of the function blocks provided in chapter 9.2 for details..

Compared to hard-wired controllers, programmable logic controllers are provided with a more extensive range of functions, in particular with respect to byte and word processing.

7.7.1 Group Shut-Off

The safety-related output modules used for a specific plant area (e.g., for burners) can be arranged into a group. For each group, the H8-STA-3 software function block must be added to the user program. All the positions of the output modules belonging to a group must be set in the software function block. If an output module fails, all output modules belonging to this group are shut down. However, the safety shutdown integrated in the output modules is sufficient to ensure the system's safety.

7.7.2 Software Function Blocks for Individual Safety-Related I/O Modules

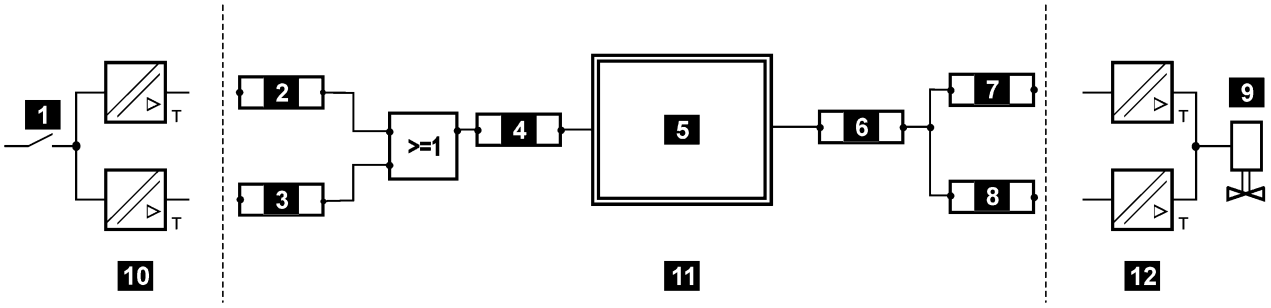
Input module		Output modules	
Digital		Digital	
Type	Software function block	Type	Software function block
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
Analog		Analog	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		
F 6221	HF-AIX-3		

Table 25: Assignment of Software Function Blocks to I/O Modules

For safety-related I/O modules, the corresponding software function blocks must be added to the user program. Refer to Chapter 9.2 or the ELOP II online help for further details.

7.8 Redundant I/O Modules

To enhance availability without impairing safety, safety-related I/O modules can be configured redundantly such as outlined below. Maximum availability is achieved if the automation devices are used with two I/O busses and the redundant I/O signals are also routed onto separated I/O modules.



1 Sensor
2 Input Signal 1
3 Input Signal 2
4 Input Variable
5 Program Logic
6 Output Variable
7 Output Signal 1
8 Output Signal 2
9 Actuator
10 Input Wiring (Hardware)
11 User Program (Software)
12 Output Wiring (Hardware)

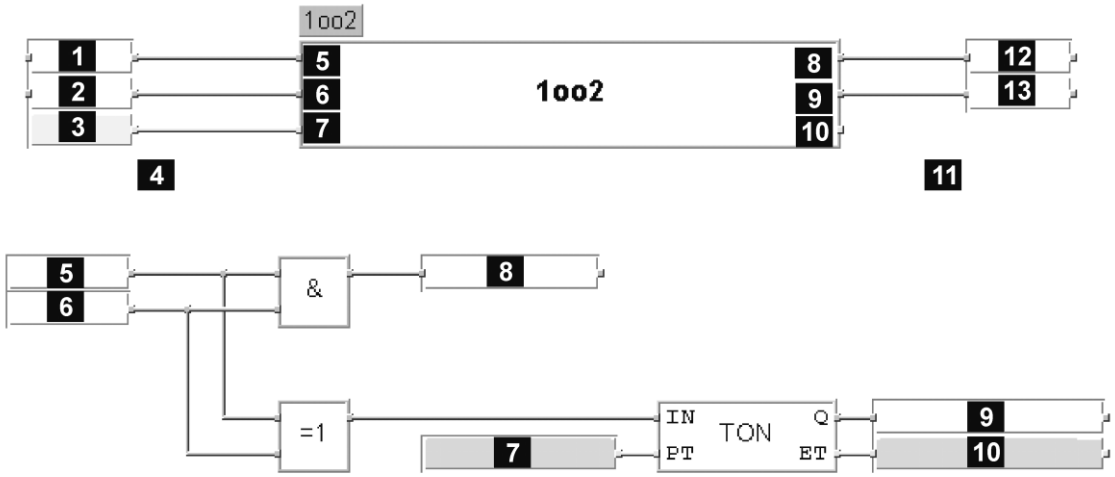
Figure 3: Redundant I/O Modules Used for Increasing Availability

7.8.1 Redundant, Non-Safety-Related Sensors

7.8.1.1 Hardware

Input modules of type F 3236, F 3237 or F 3238 must be used depending on the control signal (mechanic contact, proximity switch, intrinsically safe / not intrinsically safe). The two sensors operate in a 1oo2 structure, e. g., if one of the sensors is triggered, the safety-related circuit is immediately switched off. A discrepancy is reported upon expiration of the time previously set. This functionality can be included in a function block for the F 3236 input module. The HB-RT-3 function block with extended monitoring of proximity switch circuits is available for modules of type F 3237 and F 3238.

7.8.1.2 User Program, Input Module F 3236



1 Sensor Signal 1
2 Sensor Signal 2
3 Discrepancy Time, e. g. 1 s
4 Input Signals
5 Function Block Input: *Sensor1*
6 Function Block Input: *Sensor2*
7 Function Block Input: *Discrepancy Time*
8 Function Block Input: *Control Signal*
9 Function Block Input: *Discrepancy Signal*
10 Function Block Output: *Discrepancy Time Actual Value*
11 Signals to the Logic or Other Signaling Circuit
12 Variable for Processing the Control Signal
13 Variable for Processing the Discrepancy Signal

Figure 4: Example of a 1oo2 Function Block and Function Block Logic

The control signal has the value TRUE if both sensors have the value TRUE.

The discrepancy signal has the value TRUE if the sensor signals are different when the discrepancy time has expired.

7.8.1.3 User Program, Input Module F 3237 or F 3238

Use of the HB-RTE-3 Function Block

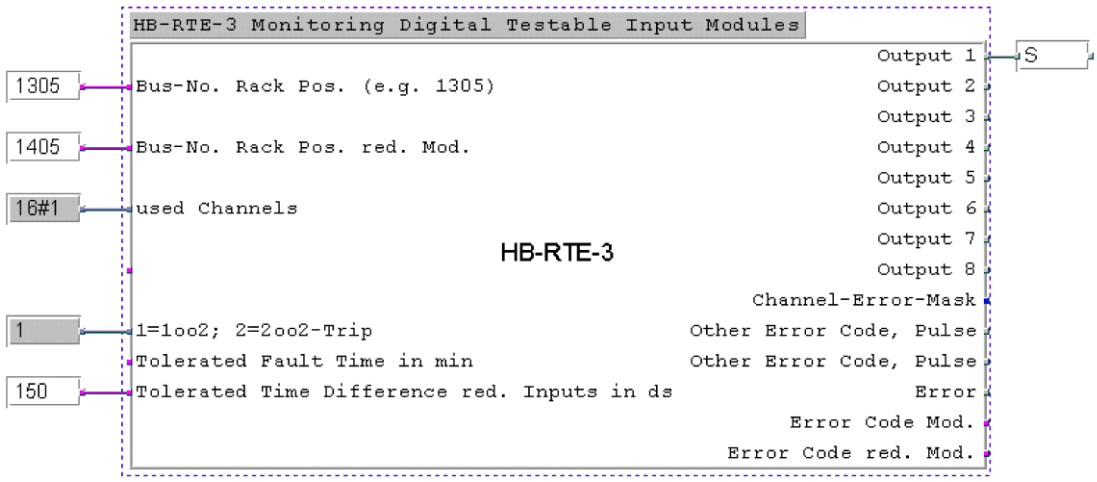


Figure 5: Use of the HB-RTE-3 Function Block

The signals S-1 and S-2 are directly connected to the first channel of the F 3237 or F 3238 module. Additional hardware is not assigned.

7.8.1.4 Safety Considerations

The output is switched off if one of the two sensors is triggered or a components fails within the system.

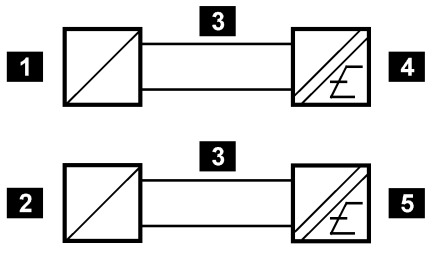
The relevant standards, e.g., IEC 61511, must be observed for sensor applications.

7.8.1.5 Availability Considerations

No availability since each component failure causes a shutdown.

7.8.2 Redundant Analog Sensors

7.8.2.1 Hardware Wiring

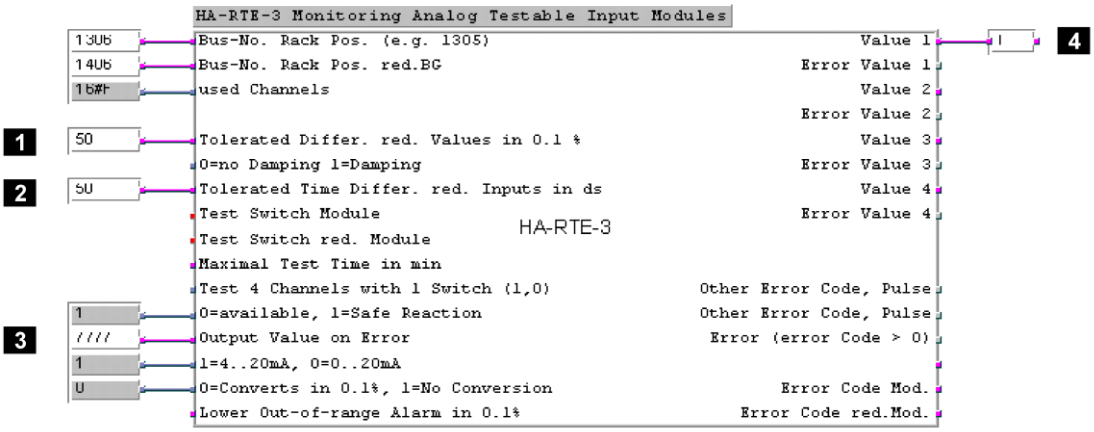


1 Transmitter 1
2 Transmitter 2
3 4…20 mA
4 T1
5 T2

Figure 6: Wiring of Redundant Sensors

7.8.2.2 User Program for the F 6213 or F 6214 Input Module

Use of the HA-RTE-3 function block, refer to Chapter 9.2.2 and the ELOP II online help for further details on the function block.



1 For instance: 50

2 For instance: 50

3 7777, if the physical size increases in dangerous situations (all four module channels),

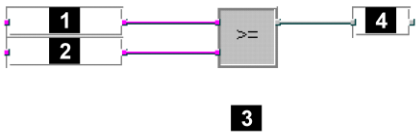
0000, if the physical size decreases in dangerous situations (all four module channels)

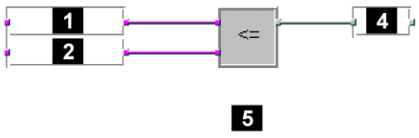
4 Values 0...1066

Figure 7: Use of the HA-RTE-3 Function Block with the F 6213 or F 6214 Module

The signals T1 and T2 are directly connected to the first channel of the F 6213 or F 6214 module. No additional hardware assignment are performed.

Two examples for a comparator element for alarming or shutting down upon achievement of the allowed threshold





1 Variable to be Compared, e. g., Measured Value

2 Reference Value

3 Reference Element for Alarming

4 Reference Result

5 Comparator Element for Shutting Down

Figure 8: Comparator Elements for Alarming or Shutting Down Upon Achievement of the Allowed Threshold

7.8.2.3 Safety Considerations

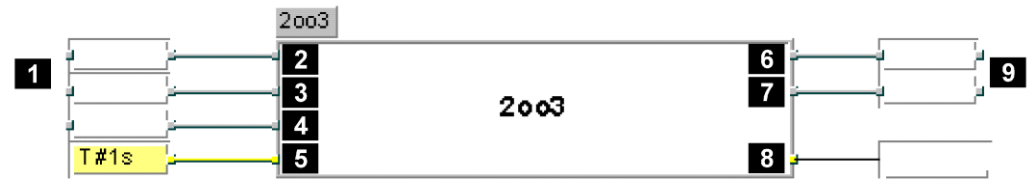
High level is present on the output A, if one of the two sensors is triggered or a component fails within the system.

The relevant standards, e.g., IEC 61511, must be observed for sensor applications.

7.8.2.4 Availability Considerations

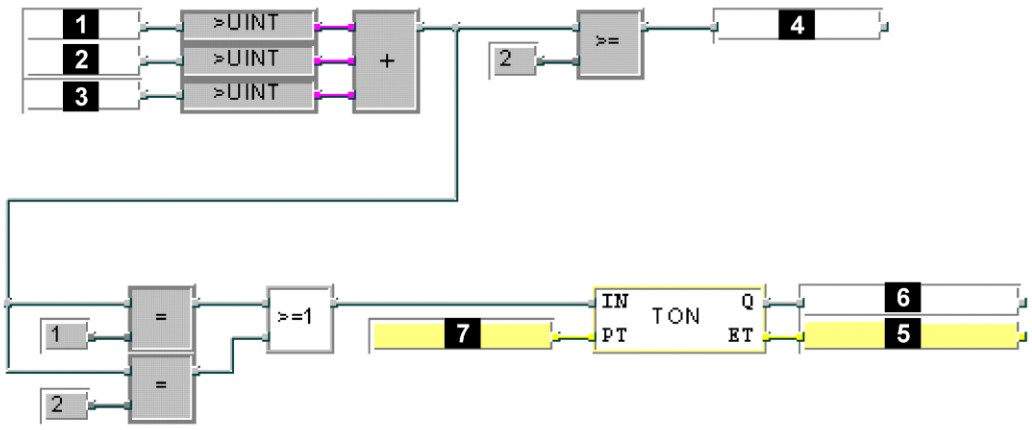
No availability since a shutdown occurs whenever a component fails or a sensor is triggered.

7.8.3 Input Modules with 2oo3 Architecture



1. Signals from 3 Different Input Modules
2. Function Block Input for Sensor1
3. Function Block Input for Sensor2
4. Function Block Input for Sensor3
5. Function Block Input for Discrepancy Time
6. Function Block Output Result Signal
7. Function Block Output for Discrepancy Signal
8. Function Block Output for the Discrepancy Time Actual Value
9. Signals to the Logic or Signaling Circuit

Figure 9: 2oo3 Function Block



1. Sensor 1
2. Sensor 2
3. Sensor 3
4. Result Signal
5. Discrepancy Time
6. Discrepancy Signal
7. Discrepancy Time Actual Value

Figure 10: Structure of a 2oo3 Function Block

Conveniently, the represented wiring is integrated in a 2oo3 function block.

The control signal has the value TRUE if two or three sensors have the value TRUE.

The discrepancy signal has the value TRUE if 1 or 2 sensors have the value TRUE when the discrepancy time has expired.

In a PES with two I/O busses, the signal of the second sensor is branched to two input channels (one to a channel on the 1st I/O bus and one to a channel of the 2nd I/O bus) and is directed to the user program via an OR function. All sensor signals can also be connected in parallel to the input channels on both I/O busses and linked to the user program via a respective OR function.

The relevant standards, e.g., IEC 61511, must be observed for sensor applications.

7.9 Project Documentation for Safety-Related Applications

The ELOP II programming tool allows the user to automatically print the documentation for a project. The most important document types include:

- Interface declaration
- List of variables
- Logic
- Description of data types
- Configurations for control cabinet, base plates, modules and system parameters
- PCS/variable cross-references
- Code generator informations

The layout of the various types of documents can be arbitrarily defined.

This documentation is required for the factory acceptance test (FAT) of a system subject to approval by a test authority (e.g., TÜV). The factory acceptance test (FAT) only applies to the user functionality, but not to the safety-related HIMA automation devices H41q-MS, H51q-MS, H41q-HS, H51q-HS, H41q-HRS, H51q-HRS that have already been approved.

HIMA recommends involving the test authority as soon as possible when designing systems that are subject to approval.

7.10 Safety-Related Communication Aspects (Safety-Related Data Transfer)

The HIPRO S protocol is certified for SIL 3.

7.10.1 Safety-Related Communication

The data transfer to resources safely assigned can be monitored via the PES master from within the resource's *Properties* dialog box (tab: **HIPRO-S**, **Edit** of the selected resource). To this end, a monitoring time can be set as *Time Interval*, and the *Reset Imported Variables* option can be activated once the monitoring time has been exceeded.

The monitoring time to be set depends on the process and must be agreed upon together with the responsible test authority.

Safety-related communication can also occur via the TÜV-certified safe**ethernet** protocol using the F 8627 X or F 8628 X Ethernet communication modules.

7.10.2 Time Requirements

To achieve a constant transmission time, HIMA recommends planning an individual PES master and an individual bus for safety-related data transmission with a baud rate of 57.6 kbit/s.

The data transmission time T_T resulting from the moment in which a sensor changes on a PES to the moment in which an output on another PES responds to the change, is:

$T_T = 2*CT_1 + 2*T_D + 2*CT_2$

CT_1 Cycle time of PES 1

CT_2 Cycle time of PES 2

T_D Time required for data transfer between two controllers. It depends on the data connection in use:

- Serial data transfer: Use the value of the bus cycle time. Refer to the operating system manual (HI 800 105 E) to determine the bus cycle time.
- Data transfer via Ethernet: Use the maximum transmission time (T_{max}), refer to the data sheet of the F 8627 X (HI 800 265 E) for details.

7.10.3 Notes for Creating the User Program

The Ethernet network is automatically configured in ELOP II for HIPRO-S. However, the following notes must be taken into account when creating the user program:

- In ELOP II, the resource name must consist of eight characters, the two last characters must be numbers. Numbers between 1 and 99 may be used. The number combination must be unique such that it can be used to determine the IP address of the communication module.
- Safety-related communication with HIPRO-S operating in NORMAL mode must be set such that safety-related data exchange with any other device is configured in every automation device (i.e., exchange of dummy data, if no user data are exchanged).
- Dummy data need not be exchanged if the HIPRO-S DIRECT mode is used. Refer to the data sheet for the F 8627X module (HI 800 265 E) for details.
- The PES master program must be compiled to verify the HIPRO-S configuration. The occurred faults must be then corrected.
- During safety-related communication, 0 must be used as safe value for transmission data.

8 Use in Fire Alarm Systems

The H41q and H51q systems may be used in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72.

In this case, the user program must fulfill the requirements specified for fire alarm systems in accordance with the standards previously mentioned.

Using the H41q and H51q systems, the requirement for a maximum cycle time of 10 s defined in the DIN EN 54-2 for fire alarm systems can be easily met since the cycle times for these systems is less than 0.5 seconds; similarly the safety time of 1 s (fault reaction time) required in certain cases.

The connection of fire alarms is performed in accordance with the energize-to-trip principle using the line short-circuit and open-circuit function. To this end, the F 3237/F 3238 input modules for Boolean connections or the F 6217/F 6221 input modules for analog connections can be used in accordance with the following wiring:

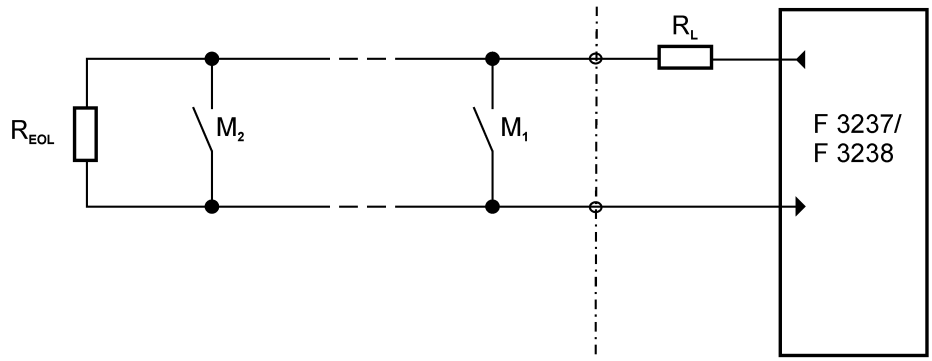
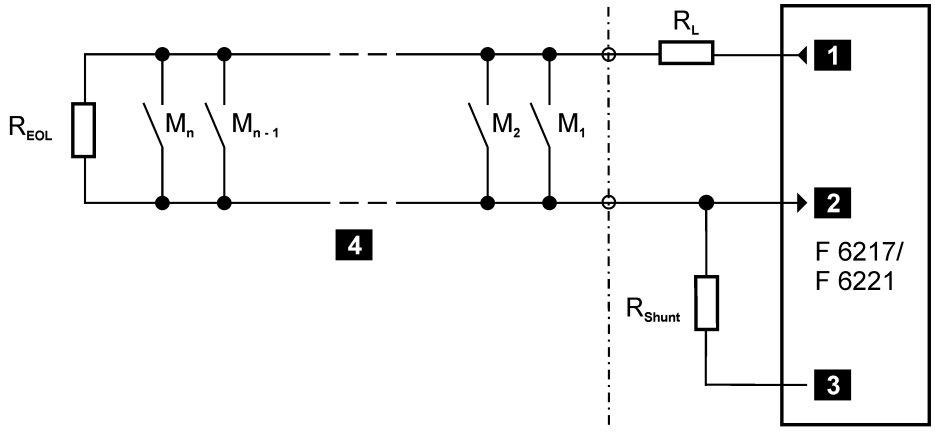


Figure 11: Wiring of Fire Alarms with Digital Inputs



1 Sensor Supply
2 Analog Input
3 Ground (L-)
4 Detection Loop

Figure 12: Wiring of Fire Alarms with Analog Inputs

Caption to Figure 11 and Figure 12:

M	Fire alarm
R_{EOL}	Terminating resistor on the last loop sensor
R_L	Limitation of the maximum permissible loop current
R_{Shunt}	Shunt

For the application, the R_{EOL}, R_L and R_{Shunt} resistors must be calculated as dictated by the sensors in use and the number of sensors per detection loop. The data sheets provided by the sensor manufacturer must also be taken into account.

Additionally, the current values specified for the F 3237 and F 3238 modules must be observed (see the corresponding data sheets). This is particularly important if the fire alarms are equipped with electronic outputs instead of mechanical contacts.

The alarm outputs for controlling lamps, sirens, horns etc. are operated in accordance with the energize-to-trip principle, which means that output modules with short-circuit and open-circuit monitoring must be used, e.g., the F 3331 or F 3334 modules.

A suitable user program can be used to control visual display systems, indicator light panels, LED indicators, alphanumeric displays, audible alarms, etc.

The routing of fault signal messages via output channels or to transmission equipment for fault signaling must occur in accordance with the de-energize-to-trip principle.

The transmission of fire alarms among HIMA systems can be implemented using the available communication standards such as Modbus, HIPRO-S, or OPC (Ethernet). Communication monitoring is an essential part of the user program. HIMA recommends configuring communication redundantly to ensure communication even if a transmission component (line, hardware fault, etc.) fails. The component failure must be reported and the replacement or repair of the faulty component during operation should be ensured.

H41q or H51q systems that are used as fire alarm systems must have a redundant power supply. Precautionary measures must also be taken against power supply drops, e.g., the use of a battery-powered horn. Switching from the main power supply to the back-up power supply must be performed as fast as possible to ensure uninterrupted operation. Voltage drops for up to 10 ms are permitted.

If a system failure occurs, the operating system writes to the system system variables that can be evaluated in the user program. This allows the user to program fault signaling for faults detected by the system. If a fault occurs, the safety-related inputs and outputs are switched off, i.e., low levels are applied to all the channels of faulty input modules and all the channels of faulty output modules are switched off.

Earth fault monitoring is required if fire detection and fire alarm systems in accordance with EN 54-2 and NFPA 72 are used.

9 Standard Function Blocks

The following table specifies the HIMA standard function blocks for safety-related applications. For a detailed description of the function blocks, refer to their respective online help.

The following text refers to the standard function blocks as function blocks».

9.1 Function Blocks Independent from I/O Modules

Standard software function blocks can be used and configured for the central module's functions.

Type	Function	TÜV Test[1)]	
		Safety-related	Interference-free
H8-UHR-3	Date and time		•
HA-LIN-3	Temperature linearization	•	•
HA-PID-3	PID controller	•	•
HA-PMU-3	Configurable transmitter	•	•
HK-AGM-3	PES master monitoring		•
HK-COM-3	Communication module monitoring		•
HK-LGP-3	LCL evaluation and configuration		•
HK-MMT-3	Modbus Master		•

[1]) In the TÜV test column, the symbol • indicates that a TÜV safety certificate exists for the corresponding function block. For the safety-related application of the function blocks, refer to their documentation.

Table 26: Standard Function Blocks not Depending on the I/O Level

The following function blocks may be used in safety-related applications, but not for safety-related actions:

- H8-UHR-3
- HK-AGM-3
- HK-LGP-3
- HK-MMT-3

9.1.1 H8-UHR-3 Function Block

This function block allows external setting or modification of the automation device's date and time.

The outputs of the function block serve informative purposes only, and no safety-related actions may be derived for the user program.

9.1.2 HA-LIN-3 Function Block

The function block is used to linearize temperatures measured using thermocouples and Pt 100 resistance thermometer. Ensure proper parameter setting if the values are used for shutting off safety-relevant circuits (see the ELOP II online help).

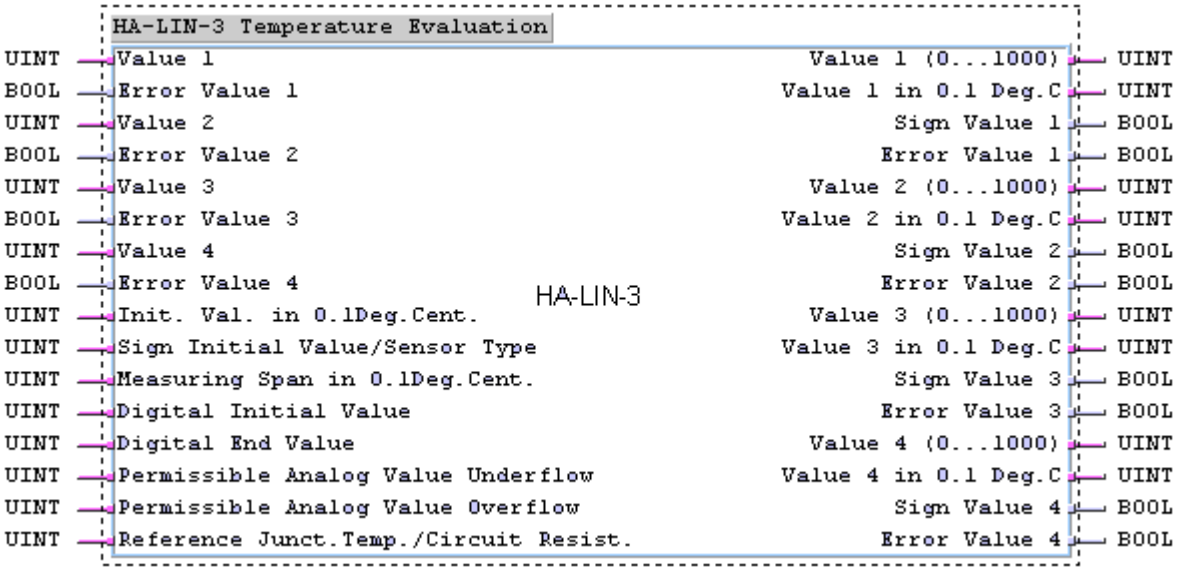


Figure 13: Connectors of the HA-LIN-3 Function Block

9.1.3 HA-PID-3 Function Block

The function block includes a digital regulator that can be configured to operate in the following operating modes: P, I, D, PI, PD and PID.

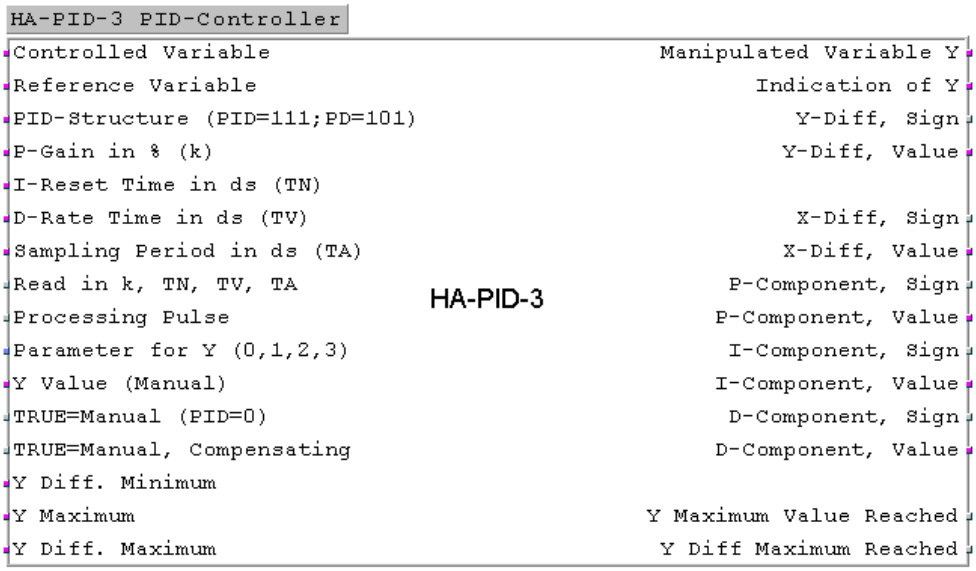


Figure 14: Connectors of the HA-PDI-3 Function Block

9.1.3.1 Inputs

True=Manual (PID=0), True=Manual, Compensating	If the control function block is safely operating, these inputs must not be used. Deviations must be approved by the responsible test authority. Parameters and constants in the function block inputs may only be changed during operation if approved by the responsible test authority and if operation is being monitored. Imported, non-safety-related variables may not be used to assign the function block inputs.

9.1.3.2 Outputs

Safety shutdowns are only allowed using the following parameters:

Maximum Value Reached and *Diff Maximum Reached*

Deviations must be approved by the responsible test authority.

i The function block control algorithm alone cannot always ensure that a system enters the safe state. Additional measures could be necessary on an individual basis.

9.1.4 HA-PMU-3 Function Block

The function block is used for converting the digitized measured values into per mille values as well as for converting per mille values into digitized analog values. Ensure proper parameter setting if the values are used for shutting off safety-relevant circuits (see the ELOP II online help).

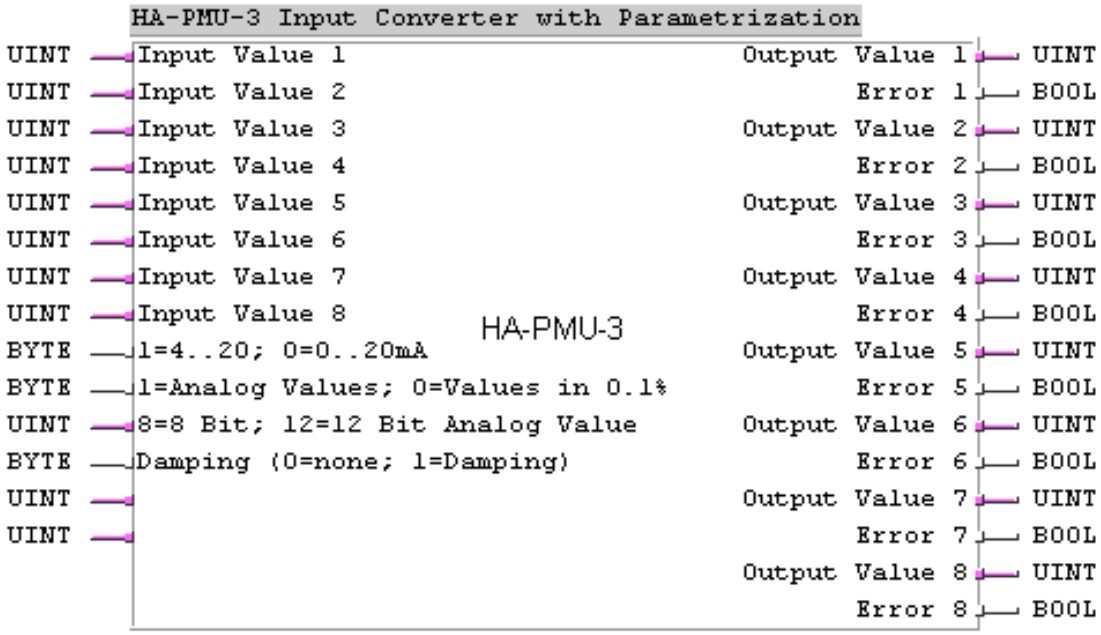


Figure 15: Connectors of the HA-PMU-3 Function Block

9.1.5 HIMA HK-AGM-3 Function Block

This function block is used to monitor the function of the H41qc or H51q automation device used as HIPRO master.

The function block is not safety-relevant. The outputs of the function block serve informative purposes only, and no safety-related actions may be derived for the user program.

9.1.6 HK-COM-3 Function Block

This function block is used to monitor the function of the communication modules within a H51qc system.

The function block is not safety-relevant. The outputs of the function block serve informative purposes only, and no safety-related actions may be derived for the user program.

9.1.7 HK-LGP-3 Function Block

The function block is used to evaluate and configure the sequence of events recording and the changeover between Modbus and LCL (logic-plan controlled logging).

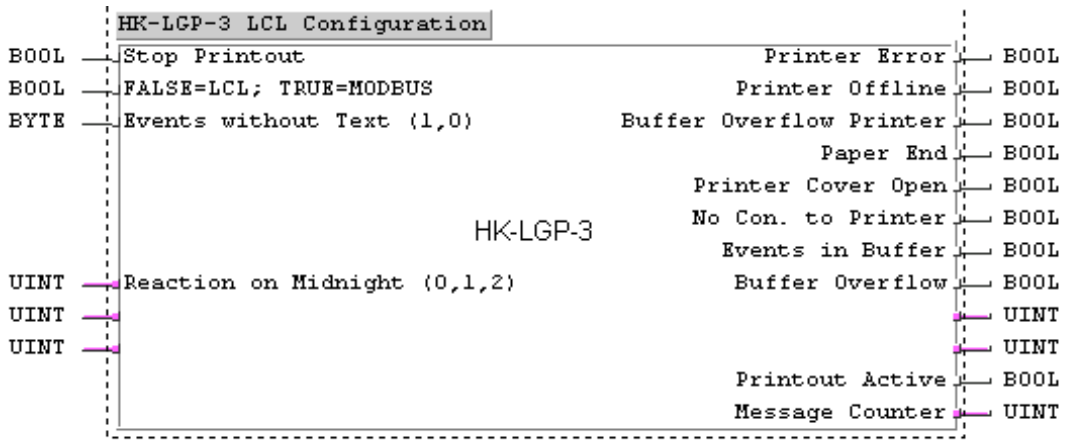


Figure 16: Connectors of the HK-LGP-3 Function Block

The function block is not safety-relevant. The function block outputs are for information purposes only. They may not be used for programming safety-related reactions in the user program.

9.1.8 HK-MMT-3 Function Block

This function block allows a H41q or H51q automation device to be used as Modbus master.

The function block is not safety-relevant. The outputs of the function block serve informative purposes only, and no safety-related actions may be derived for the user program.

9.2 Function Blocks Dependent from I/O Modules

All software function blocks described below are approved for operation in safety-related automation devices.

Type	Function	TÜV test[1)]	
		Safety-related	Interference-free
H8-STA-3	Grouping of safety-related testable outputs	•	•
HA-RTE-3	Monitoring of analog testable, F 6213 / F 6214 input modules	•	•
HB-BLD-3	Module and line diagnosis of testable outputs	•	•
HB-BLD-4	Module and line diagnosis of testable outputs	•	•
HB-RTE-3	Monitoring of binary, testable input modules	•	•
HF-AIX-3	Monitoring of analog testable F 6221 input modules	•	•
HF-CNT-3	Counter function block for the F 5220 module	•	•
HF-CNT-4	Counter function block for the F 5220 module	•	•
HF-TMP-3	Configuration function block for the F 6220 module	•	•
HZ-DOS-3	Non safety-related diagnosis		•
HZ-FAN-3	Fault indicators for testable I/O modules		•

[1]) In the TÜV test column, the symbol • indicates that a TÜV safety certificate exists for the corresponding function block. For the safety-related application of the function blocks, refer to their documentation.

Table 27: Standard Function Blocks Depending on the I/O Level

The following function blocks may be used in safety-related applications, but not for safety-related actions:

- HZ-FAN-3
- HZ-DOS-3

All specific programming instructions described in this chapter must be observed.

For details on a software function block's functions and the assignment of its inputs and outputs, refer to its online help.

9.2.1 H8-STA-3 Function Block

The function block is used to configure a group shut-off. In the user program, it is used once for each shut-off group.

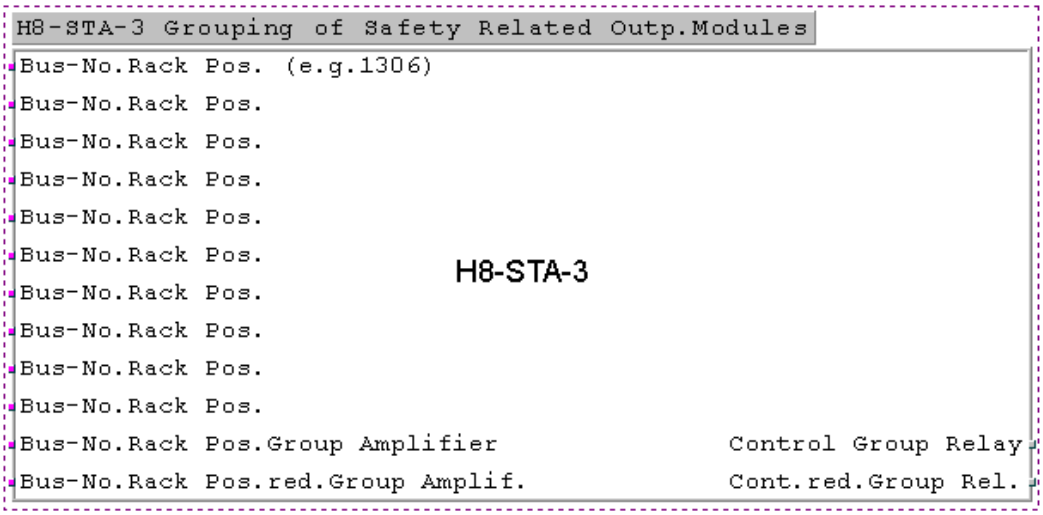


Figure 17: Connectors of the H8-STA-3 Function Block

For details on the behavior in the event of output channel faults, refer to Chapter 6.

9.2.1.1 Inputs

The positions of the modules composing the group shut-off are input as four-digit decimals in accordance with the values defined in the selected resource.

Example: 1306 means:

Cabinet 1, subrack 3, module position 06

If modules with integrated safety shutdown are used, either the *Bus-No. Rack Pos. Group Amplif.* or *Bus-No. Rack Pos. red. Group Amplif.* input must be used. To do so, specify an existing but currently unused slot.

i Output modules with integrated safety shutdown need no group shutdown. A group shut-off, however, can also be preset for this type of modules. If this is done, an output module's failure causes all modules belonging to a given group to shut down (in accordance with the specifications on the H8-STA-3 function block).

9.2.2 HA-RTE-3 Function Block

The function block is used to process values and display faults that occurred in analog safety-related modules operating in single-channel or redundant mode. In the user program, it must be used once for each safety-related analog input module (F 6213). If two redundant I/O modules are used, the function block may only exist once in the user program.

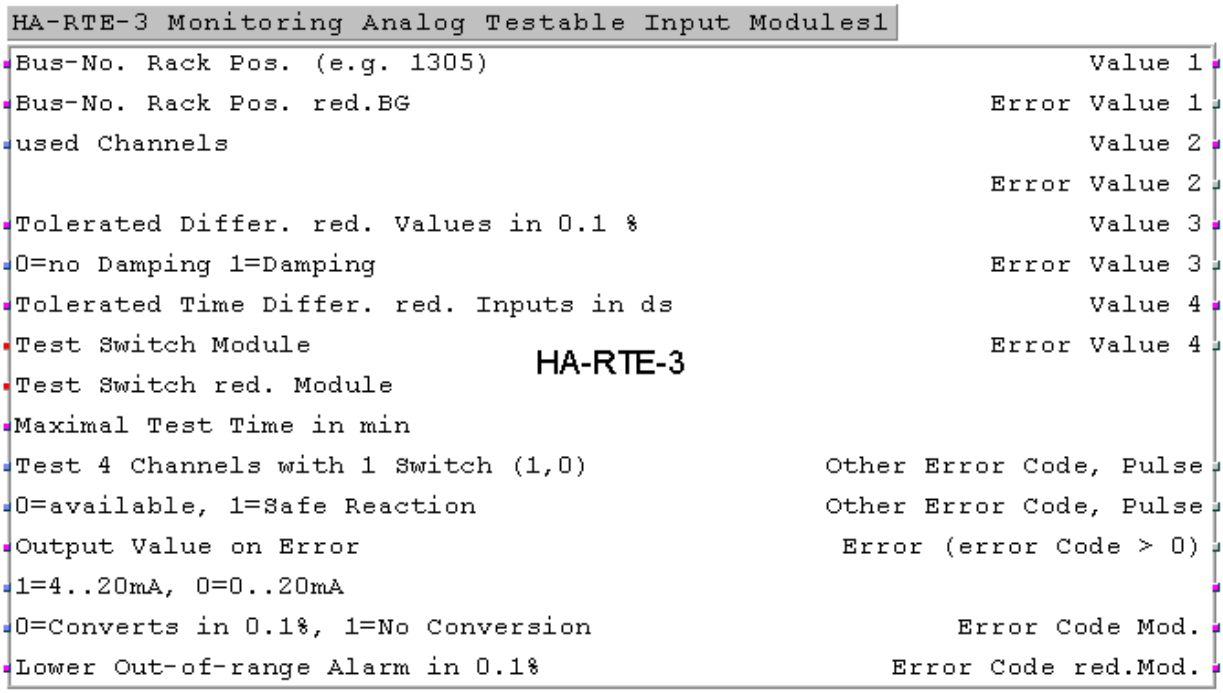


Figure 18: Connectors of the HA-RTE-3 Function Block

9.2.2.1 Inputs

Bus-No. Rack Pos. (e.g. 1305) *Bus-No. Rack Pos. red. Mod.*	Position of the safety-related analog input module and, if existing, of the redundant module as 4-digit decimal number. Example: 1305 means: Cabinet 1, subrack 3, module position 05 (for redundant operation, the redundant module must have a different position)
0 = No Damping; 1 = Damping	1 for redundant operation only. The difference between the current value and the value from the previous cycle is added to the allowed difference in ‰ (Tolerated Differ. red. Values in 0,1 %).
Maximum Test Time in min	Limitation of the test time expressed in minutes. Upon completion of the test time, the actual value is once again processed in the user logic.

9.2.2.2 Outputs

Value 1...4	The use of values must be verified if the values are used for shutting off safety-related circuits.
Error Value 1...4	The outputs must be in use to trigger a shutdown with their Boolean signal if a fault occurs.

The remaining outputs serve informative purposes only, and no safety-related actions may be derived for the user program.

9.2.3 HB-BLD-3 Function Block

The function block is used to evaluate and display channel faults that occurred in the digital safety-related output modules F 3331, F 3334 und F 3349. It may only be used once for each module in use.

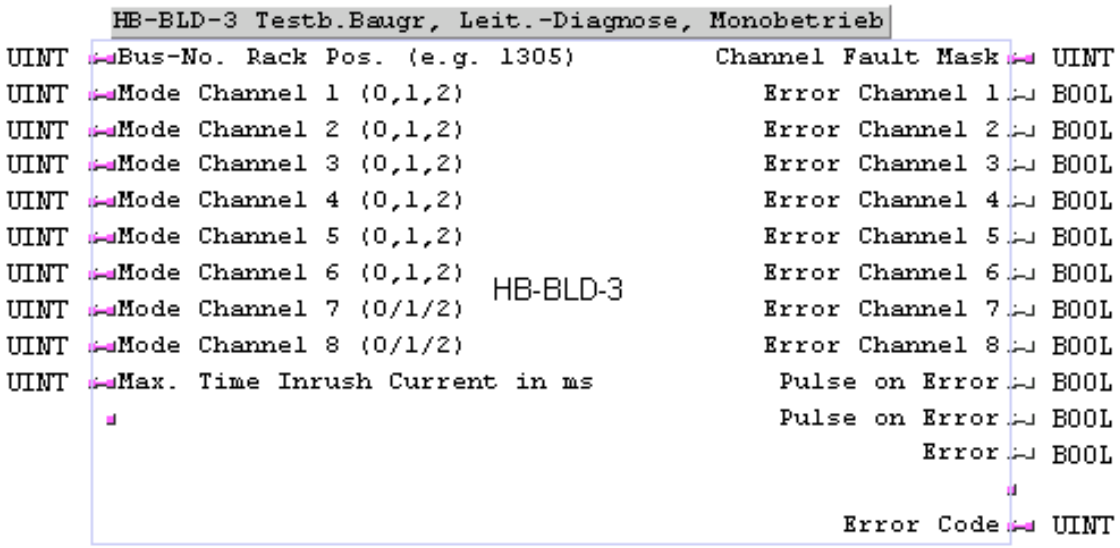


Figure 19: Connectors of the HB-BLD-3 Function Block

9.2.3.1 Inputs

Bus-No. Rack Pos. (e.g. 1305)

Position of the safety-related digital output module as four-digit decimal number,
Example: 1305 means:
Cabinet 1, subrack 3, module position 05

Mode Channel n (0/1/2)

Assignment	Description
1	Normal operation, detected errors are reported at the corresponding Error Channel n output with high level, the output circuit of the module is closed
0	Fault evaluation, error messages are suppressed
2	Only allowed depending on the plant, inverse operation, i.e., the output circuit should be open
> 2	Range of values exceeded: The channel is considered as faulty (output is TRUE) and a channel-related error message is output.

In general, the de-energize-to-trip principle must be applied to safety-related control circuits.

Max. Time Inrush Current in ms

Definition of the waiting time for detecting open-circuits or the tolerance time for current limiting. No faults are displayed during this period. Increasing the waiting time also increases the cycle time.

9.2.3.2 Outputs

The *Pulse on Error (2x), Error* and *Error Code* outputs have information purposes only, and may not be used for programming safety-related reactions in the user program.

The remaining outputs may be used for safety-related reactions.

9.2.4 HB-BLD-4 Function Block

The function block is used to evaluate and display channel faults that occurred in the digital safety-related output modules F 3331, F 3334 und F 3349 operating redundantly. It may only be used once for each redundant module pair.

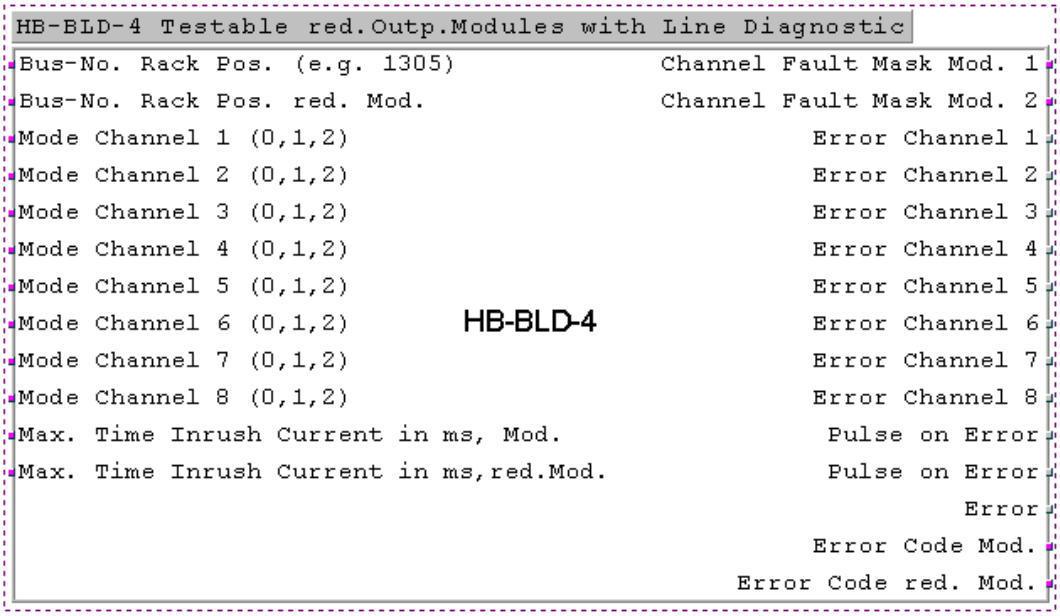


Figure 20: Connectors of the HB-BLD-4 Function Block

9.2.4.1 Inputs

Bus-No. Rack Pos. (e.g. 1305)
Bus-No. Rack Pos. red. Mod.

Position of the safety-related digital output module and, if existing, of the redundant module as 4-digit decimal number
Example: 1305 means:
Cabinet 1, subrack 3, module position 05

Mode Channel n (0/1/2)

Assignment	Description
1	Normal operation, detected errors are reported at the corresponding Error Channel n output with high level, the output circuit of the module is closed
0	Fault evaluation, error messages are suppressed
2	Only allowed depending on the plant, inverse operation, i.e., the output circuit should be open. A detected error is reported at the corresponding Error Channel n output with high level.
> 2	Range of values exceeded: The channel is considered as faulty (output is TRUE) and a channel-related error message is output.

In general, the de-energize-to-trip principle must be applied to safety-related control circuits.

Max. Time Inrush Current in ms, Mod.
Max. Time Inrush Current in ms, red. Mod.

Definition of the waiting time for detecting open-circuits or the tolerance time for current limiting. No faults are displayed during this period. Increasing the waiting time also increases the cycle time.

9.2.4.2 Outputs

The Pulse on Error (2x), Error, Error Mod. and Error Code red. Mod. outputs serve informative purposes only, and no safety-related actions may be derived for the user program.

The remaining outputs may be used for safety-related actions.

9.2.5 HB-RTE-3 Function Block

The function block is used to evaluate and display faults that occurred in digital safety-related modules in single-channel or redundant mode. In the user program, it must be used once for each input module of type F 3237 or F 3238 or for two input modules of type F 3237 or F 3238 operating redundantly.

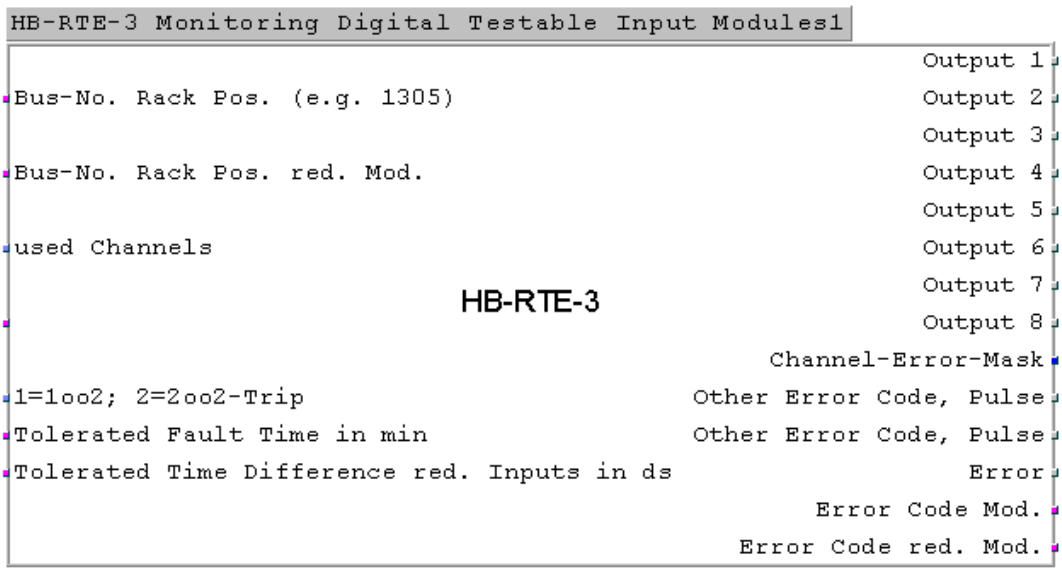


Figure 21: Connectors of the HB-RTE-3 Function Block

9.2.5.1 Inputs

Bus-No. Rack Pos. (e.g. 1305)
Bus-No. Rack Pos. red. Mod.

Position of the safety-related digital output module and, if existing, of the redundant module as 4-digit decimal number Example: 1305 means:
Cabinet 1, subrack 3, module position 05

1 = 1oo2; 2 = 2oo2 trip

Assignment	Description
0	Assignment in single-channel operation Input in accordance with IEC 61131: 16#00 or 2#00000000.
1	1oo2 trip, corresponds to an AND gate. In 1oo2 trip, the module redundancy is used to increase availability. If no faults occurred in the input modules and input circuits, the input signals of the module channels 1...8 are connected to the corresponding outputs through an AND gate. If a fault occurs in a channel, the last state is retained at the corresponding function block output; if the fault still exists after expiration of the allowed fault time, the output is set to FALSE. If another fault-free input is FALSE or faults simultaneously occur in both channels (dual fault), the function block output is immediately set to FALSE.
2	2oo2 trip, corresponds to a OR gate. In 2oo2 trip, the module redundancy is used to increase availability. If no faults occurred in the input modules and input circuits, the input signals of module channels 1...8 are connected to the corresponding outputs through an OR gate. If a fault occurs in a channel, the input signal of the other channel is transferred to the function block output. Only if faults simultaneously occur in both channels (dual fault), the last state is retained at the corresponding function block output; if the dual fault still exists after expiration of the allowed fault time, the output is set to FALSE.

In general, the de-energize-to-trip principle must be applied to safety-related control circuits.

Tolerated Fault Time in min.

No effect on the shutdown within the indicated time after a sensor test, component failure or line error.
Agreement with the test authority responsible for the final system acceptance test.

Tolerated Time Difference red. Inputs in ds

Time difference of the switching points between two redundant sensors. The time depends on the sensor; agreement with the competent test authority required.

9.2.5.2 Outputs

The *Channel Error Mask, Other Error Code, Pulse (2x), Error, Error Code Mod.* and *Error Code red. Mod.* outputs are for information purposes only. They may not be used for programming safety-related reactions in the user program.

The outputs *Output 1...Output 8* may be used for safety-related reactions.

9.2.6 HF-AIX-3 Function Block

The HF-AIX-3 function block is used to configure and evaluate one individual channel of the safety-related analog F 6221 (Ex)i input module with a resolution of 0...10 000.

The HF-AIX-3 function block must be used in the user program once for each channel of the F 6221 module.

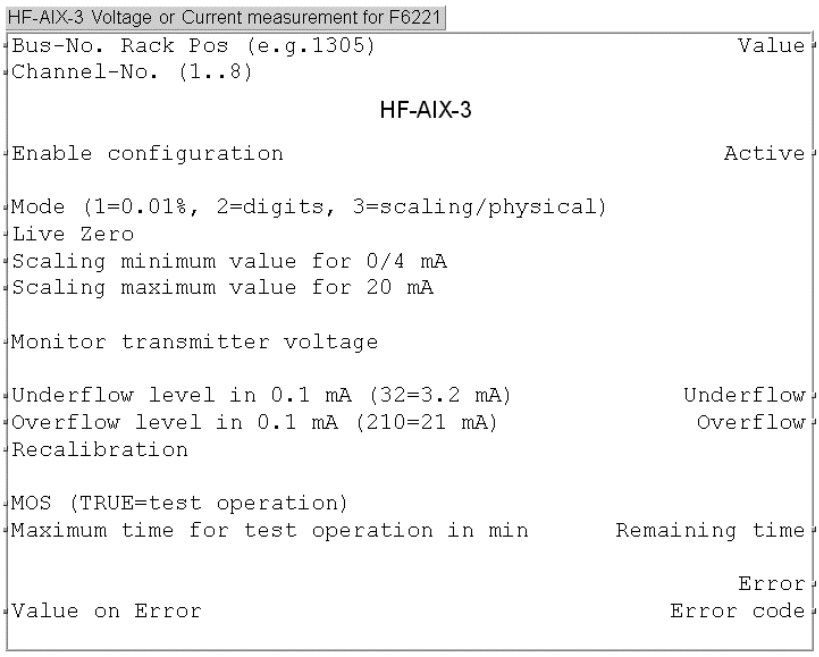


Figure 22: Connectors of the HF-AIX-3 Function Block

For each channel, the analog input module has a safety-related output that is controlled independently from the central module cycle. Its state is displayed at the HF-AIX-3 function block output and can be further processed in the user program.

The value of the analog input module can be converted and scaled through the parameter setting.

A value preset at the *Value on Error* function block input is switched to the Value output in the following cases:

- Channel faults
- Module faults
- Violation of the measurement range

In these cases, the user program processes the value of the *Value on Error* input instead of the measured value.

9.2.7 HF-CNT-3 Function Block

The HF-CNT-3 function block is used to configure and evaluate both channels of the safety-related F 5220 counter module with a resolution of 24 bits. The counter module can be used to count impulses, register frequencies or rotation speeds, and to recognize the rotation direction.

The HF-CNT-3 function block must be used in the user program once for each F 5220 counter module.

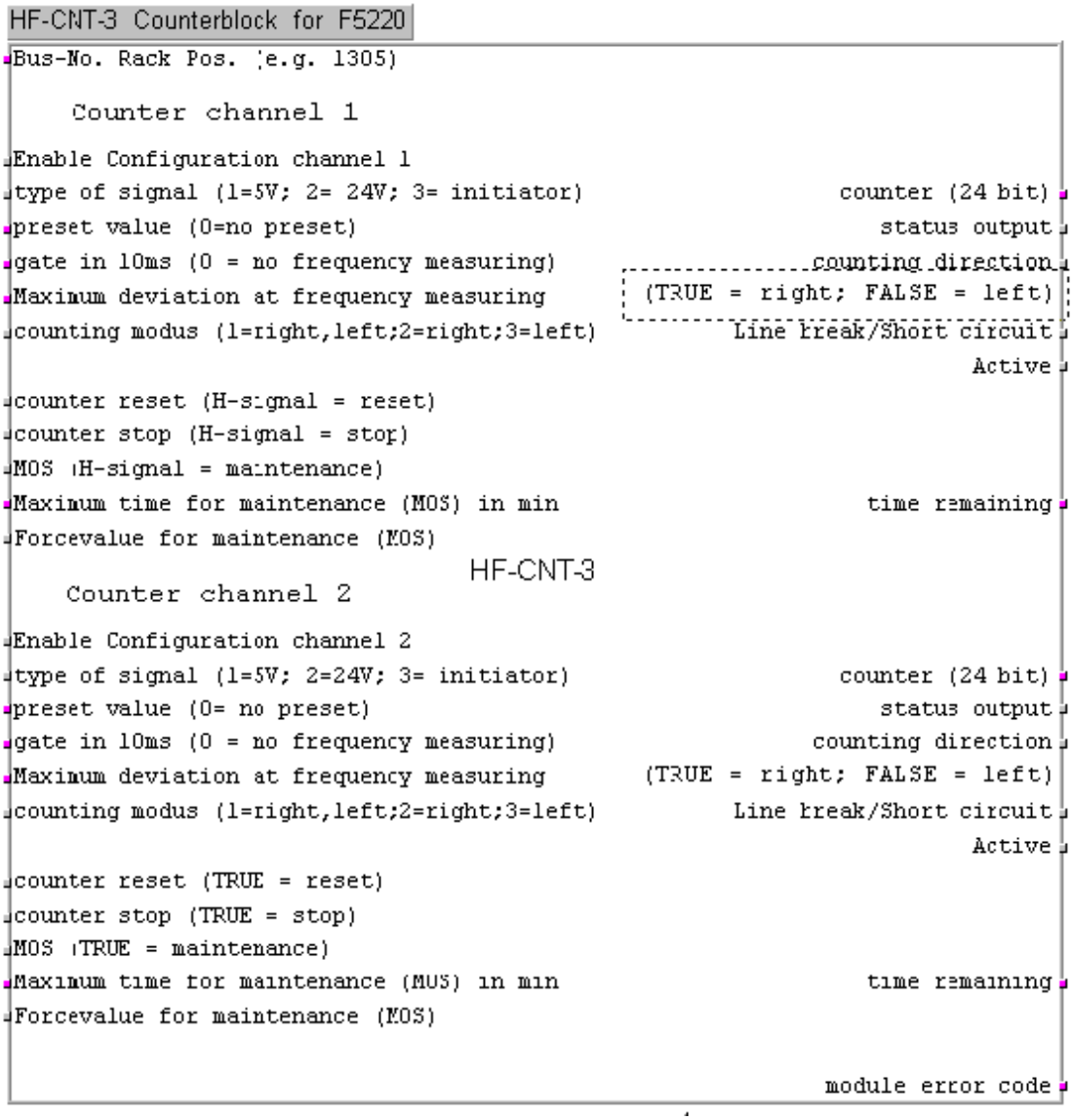


Figure 23: Connectors of the HF-CNT-3 Function Block

For each channel, the counter module has a safety-related output that is controlled independently from the central module cycle. Its *Output State* is displayed at the HF-CNT-3 counter function block output and can be further processed in the user program.

A TRUE signal at the *MOS* input (MOS: maintenance override switch) can be used to directly control the counter module output during the specified test operating time, i.e., the output has the signal specified at the *Force Value for Test Operation* input.

i If the Gate time is modified, the correct measured value is only available at the output after three Gate times (as currently set).

9.2.8 HF-CNT-4 Function Block

This function block corresponds to the HF CNT 3 function block, but also has a *Channel Error* output.

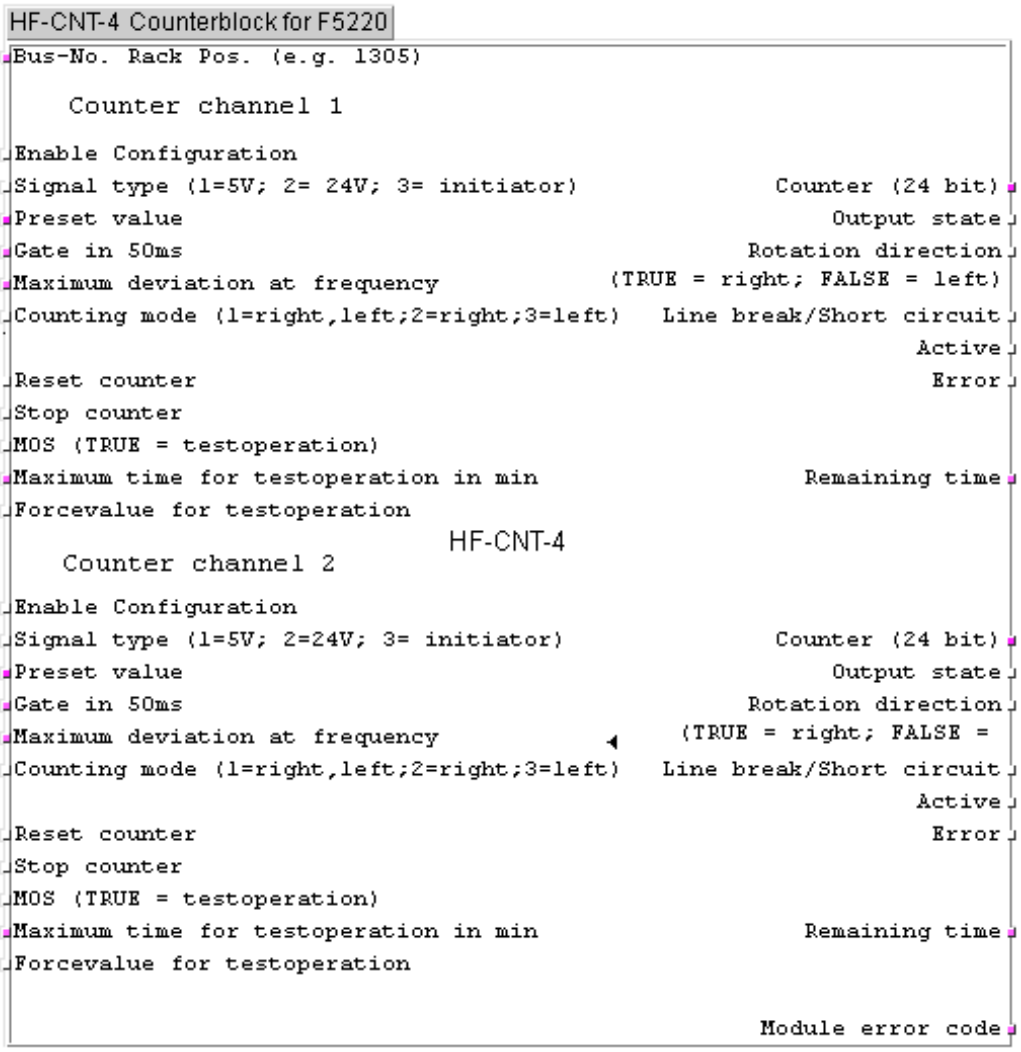


Figure 24: Connectors of the HF-CNT-4 Function Block

The *Channel Error* outputs report a channel fault.

Channel fault=

TRUE	A channel fault occurred. If a module fault occurs, both *Channel Error* outputs are set to TRUE
FALSE	The channel operates properly or has not yet been configured.

9.2.9 HF-TMP-3 Function Block

The HF-TMP-3 function block is used for each channel of the F 6220 thermocouple module. If the channel has not been properly configured with the HF-TMP-3 function block, it does not function, i.e., the output values are 0 or FALSE. No default functionality or setting exist. The sensor type 1 may only be assigned to channel 9.

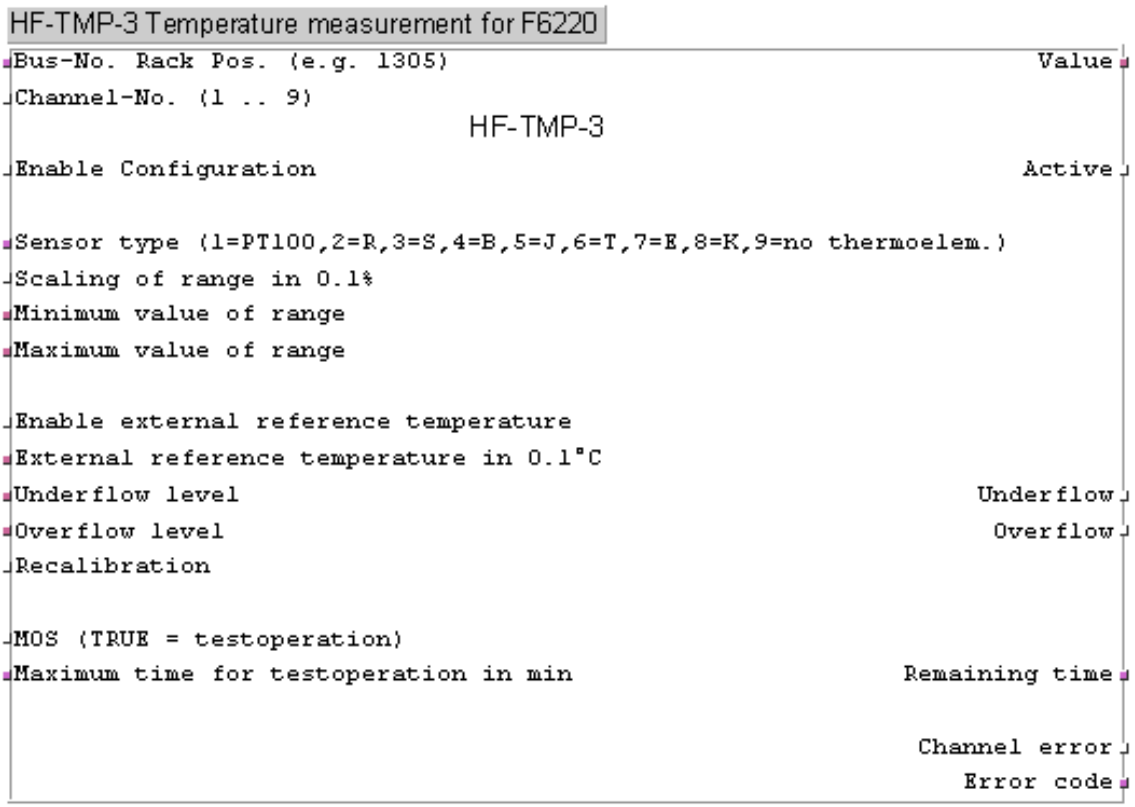


Figure 25: Connectors of the HF-TMP-3 Function Block

The *Enable External Reference Temperature* signal is only evaluated if the *Temperature Measurement* mode is set (values 2 through 8 on the *Type* input). If the input is TRUE, the temperature at the *External Reference Temperature* input is used as reference value. If this input is FALSE, the temperature value of the resistance thermometer located in the module is processed as reference temperature.

The *Value* function block output is set to 0 if the module or channel fails. The *Channel Error* function block output must be evaluated in the user program to ensure that the type of fault to be defined in the user program is processed.

In safety-related applications compliant with SIL 3, the reference temperature must be evaluated as comparison between the reference temperatures from two different modules, the same applies to the temperature of two thermocouples.

Recalibration is automatically performed every 5 minutes to ensure that environment conditions existing in the module are recorded (e.g., temperature). Recalibration can also be triggered with TRUE at the *Recalibration* output. This signal may only be present for a cycle.

The TRUE signal on the MOS input (MOS = maintenance override switch) is used to freeze the value at the Value and Channel Error function block outputs, while the time for test operation is running.

9.2.10 HZ-DOS-3 Function Block

The function block is used to determine which safety-related I/O module should be operated in diagnostic mode only. Up to sixteen modules can be monitored with a function block. The function block may be used multiple times within a user program.

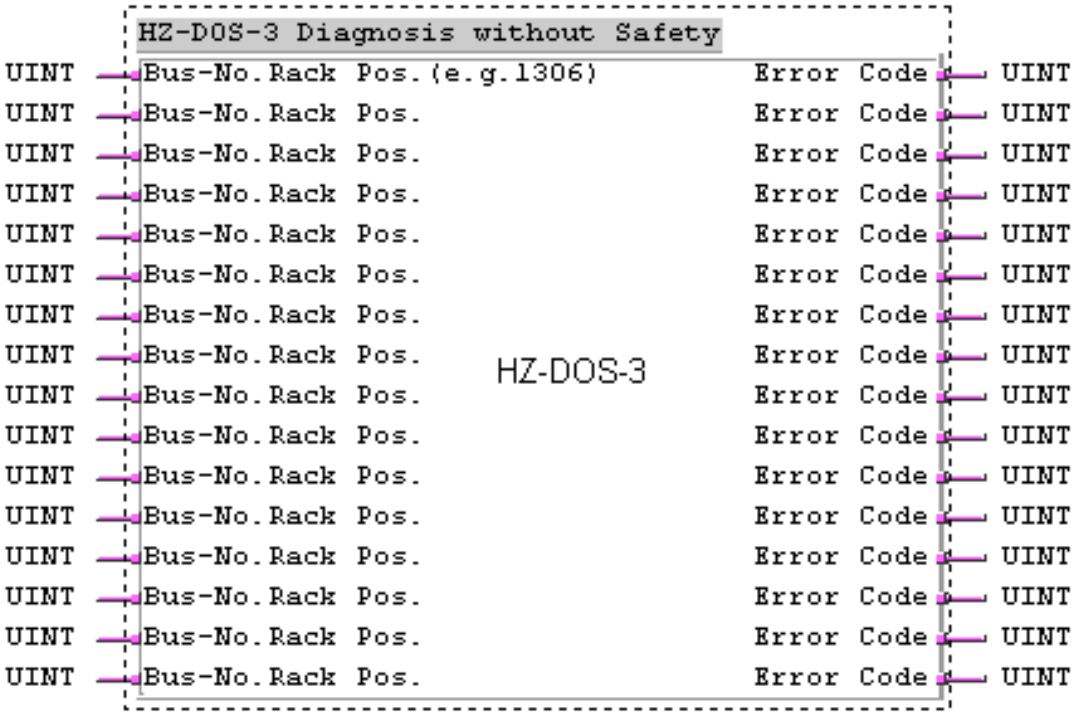


Figure 26: Connectors of the HZ-DOS-3 Function Block

The function block is not safety-relevant. The function block outputs are for information purposes only. They may not be used for programming safety-related reactions in the user program.

All safety-related I/O modules listed on the HZ-DOS-3 function block must not be used for safety functions!

9.2.11 HZ-FAN-3 Function Block

The function block is used to evaluate and display faults that occurred in safety-related I/O modules. Up to eight modules can be monitored with a function block. The function block may be used multiple times within a user program.

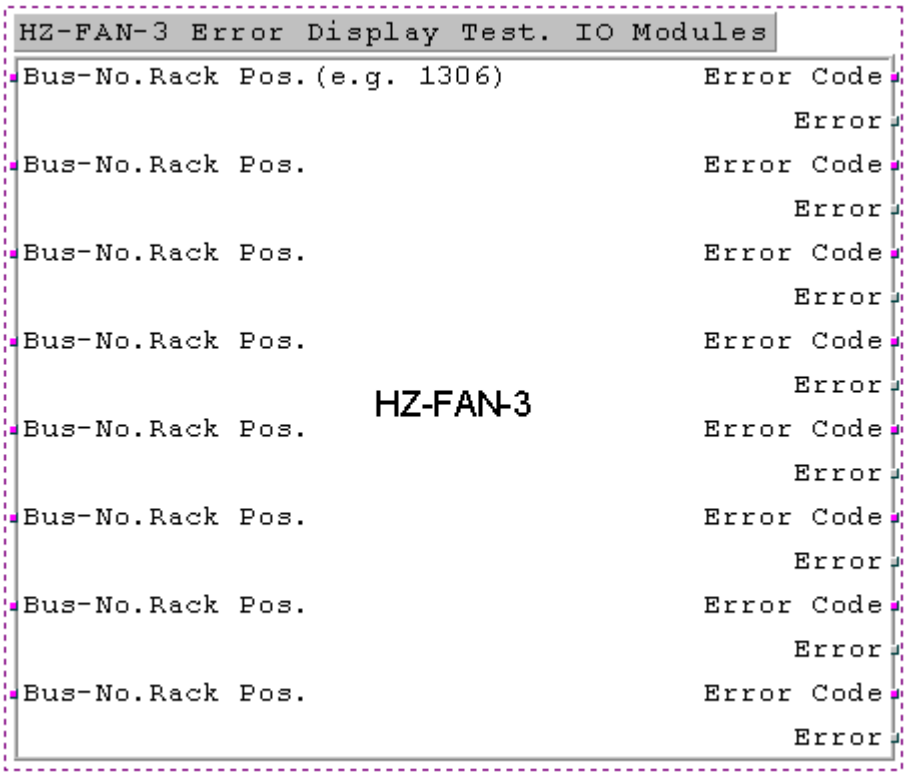


Figure 27: Connectors of the HZ-FAN-3 Function Block

9.2.11.1 Inputs

Bus-No. Rack Pos. (e.g. 1306) The positions of the safety-related I/O modules are specified as four-digit decimal numbers.
Example: 1306 means:
Cabinet 1, subrack 3, module position 06

9.2.11.2 Outputs

All function block outputs are for information purposes only. They may not be used for programming safety-related reactions in the user program.

Appendix

Glossary

Term	Description
AI	Analog Input
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CRC	Cyclic redundancy check
DI	Digital input
DO	Digital output
ELOP II	Programming tool for H41q/H51q
EMC	Electromagnetic compatibility
EN	European norm
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
ICMP	Internet control message protocol, network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Supposing that two input circuits are connected to the same source (e.g., a transmitter). An input circuit is termed interference-free if it does not distort the signals of the other input circuit.
MAC Address	Media access control address: Hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with ELOP II
PE	Protective earth
PELV	Protective extra low voltage
PES	Programmable electronic system
PFD	Probability of failure on demand, probability of failure on demand of a safety function
PFH	Probability of failure per hour, probability of a dangerous failure per hour
R	Read
R/W	Read/Write
SELV	Safety extra low voltage
SFF	Safe failure fraction, portion of faults that can be safely controlled
SIL	Safety integrity level (in accordance with IEC 61508)
SNTP	Simple network time protocol (RFC 1769)
SW	Software
TMO	Timeout
W	Write
Watchdog (WD)	Time monitoring facility for modules or programs. If the watchdog time is exceeded, the module or program enters the error stop state.
WDT	Watchdog time

Index of Figures

Index of Tables

Index

HI 800 013 E

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28 | 68782 Brühl, Germany
Phone +49 6202 709-0 | Fax +49 6202 709-107
info@hima.com | www.hima.com

SAFETY
NONSTOP

For a detailed list of all subsidiaries and representatives, refer to: www.hima.com/contact