

Programmable Systems

Safety Manual

Systems H41q, H41qc and H51q

Operating System BS 41q/51q V7.0-8



HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation

HI 800 013 FEA

Important Note

All HIMA products mentioned in this manual are protected with the HIMA trade-mark. As not differently noted down this is possibly also valid for other mentioned manufactueres and their products.

The technology is subject to changes without notice.

All technical statements and data in this manual have been worked out very carefully, and effective checks and inspections have been applied. This manual may however contain flaws or typesetting errors. Therefore HIMA does not offer any warranties nor assume legal reponsibility nor any liability for the possible consequences of any errors in this manual. HIMA would appreciate being informed on possible errors.

About this Manual

This manual contains Information for proper application of the safety-related HIMA Automation Devices H41q and H51q.

The knowledge of regulations and the technically perfect transfer of the safety advices contained in this manual carried out by qualified staff are prerequisites for the safe installation, start-up and for the safety during operation and maintenance of the HIMA Automation Devices.

In case of unqualified interventions into the automation devices, de-activating or bypassing safety functions, or if advices of this manual are neglected (causing disturbances or impairments of safety functions), severe personal injuries, property or environmental damage may occur for which we cannot take liability.

HIMA Automation Devices are developed, manufactured and tested according to the relevant safety standards. They must only be used for the applications described in the instructions and with specified environmental conditions, and only in connection with approved external devices.

Intended readership

This manual addresses on system planners, configuration engineers and programmers as well as persons authorized for the start-up and for operation of the devices and systems. Presupposed is knowledge in the area of the safety technology.

The reproduction of the contents of this publication (either in its entirety or in a part) is not permitted without the written permission of HIMA.

All rights and technical modifications reserved:

© **HIMA Paul Hildebrandt GmbH + Co KG**

P. O. Box 1261

D - 68777 Bruehl near Mannheim

Phone +49 6202 709-0

Fax +49 6202 709-107

E-mail info@hima.com

Internet <http://www.hima.com>

Table of Contents

Chapter 1 The Safety Philosophy and Conditions

1	Introduction	1
1.1	Definitions	1
1.2	Certification	1
1.3	Safety and Availability	2
1.4	Safety Times	3
1.5	Offline Proof-Test.	4
1.5.1	Execution of the Offline Proof Test	4
1.5.2	Periodic Proof Testing	4
2	Safety Conditions	5
2.1	Hardware Project Planning; Product Independent Conditions	5
2.2	Hardware Project Planning;	Product Dependent Conditions5
2.3	Programming; Product Independent Conditions	5
2.4	Programming; Product Dependent Conditions	5
2.5	Communication; Product Dependent Conditions	6
2.6	Special Operating Modes; Product Independent Conditions	6

Chapter 2 Central Modules

1	Overview of the Modules in the Central Area of the H41q, H41qc and H51q Systems	7
1.1	Central Area of HIMA Automation Devices of the H41q, H41qc and H51q Systems	7
1.2	Overview of the Central Modules for the H41q, H41qc and H51q Systems	8
1.2.1	Other Modules for the H41q, H41qc and H51q Systems in the Central Device Area.	9
2	General Notes on the Safety and Availability of safety-related Central Modules	10
2.1	Power Supply Modules	10
2.2	Functional Description of the Safety-related F 8652 (A, E) / F 8650 (A, E) Central Modules for the H41q, H41qc and H51q Systems	11
3	The Principles of Function of Safety-related Central Modules	13
3.1	Self Test Routines	13
3.2	Response on Errors Detected in Central Modules	13
3.3	Diagnostic Display	14
4	Response on Errors Detected in the IO Bus Area	15
5	Instructions for the Replacement of Central Modules	16

Chapter 3	Input Modules	
1	Overview of the Input Modules for the H41q, H41qc and H51q Systems	17
2	Safety and Availability of Safety-related Input Modules	18
2.1	General notes on safety-related input modules	18
2.1.1	Safety of Sensors, Detectors, Transmitters	19
2.2	The F 3236, F 3237, F 3238, F 3240 and F 3248 Safety-related Digital Input Modules	19
2.2.1	Test Routines	19
2.2.2	Response of the System on Failures Detected at Safety-related Digital Input Modules	20
2.3	The F 5220 Safety-related Counter Module	21
2.3.1	Test Routines	21
2.3.2	Response of the System on Failures Detected at Safety-related F 5220 Counter Modules	21
2.4	The F 6213, F 6214 and F 6217 Safety-related Analogue Input Modules	21
2.4.1	Test Routines	21
2.4.2	Response of the System on Failures Detected at Safety-related F 6213, F 6214 Analogue Input Modules	22
2.4.3	Response of the System on Failures Detected at Safety-related F 6217 Analogue Input Modules	22
2.5	The F 6220 Safety-related and Intrinsically Safe Thermocouple Input Module	23
2.5.1	Test Routines	23
2.5.2	Response of the System on Failures Detected at Safety-related F 6220 Thermocouple Input Modules	23
2.6	The F 6221 Safety-related Analogue and Intrinsically Safe Input Module	24
2.6.1	Test Routines	24
2.6.2	Response of the System on Failures Detected at Safety-related F 6221 Analogue Input Modules	24
3	Instructions for the Replacement of Input Modules	25
4	Check Lists for Project Planning, Programming and Commissioning safety-related Input Modules	26
4.1	F 3236 Safety-related Digital Input Module (16-channel)	27
4.2	F 3237 Safety-related Digital Input Module (8-channel)	28
4.3	F 3238 (Ex)i Safety-related Digital Input Module (8-channel)	29
4.4	F 3240 Safety-related Digital Input Module (16-channel)	30
4.5	F 3248 Safety-related Digital Input Module (16-channel)	31
4.6	F 5220 Safety-related Counter Module (2-channel)	32
4.7	F 6213 / F 6214 Safety-related Analogue Input Module (4-channel)	33
4.8	F 6217 Safety-related Analog Input Module (8-channel)	34
4.9	F 6220 (Ex)i Safety-related Analog Thermocouple Input Module (8-channel)	35
4.10	F 6221 (Ex)i Safety-related analogue input module (8-channel)	36
Chapter 4	Output Modules	
1	Overview of Output Modules for the H41q/H41qc and H51q Systems	37

Table of Contents

2	General Notes on the Safety and Availability of Safety-related Output Modules	38
2.1	Safety-related Digital Output Modules	38
2.2	Safety-related Analog Output Modules	39
3	The Principles of Function of Safety-related Output Modules	40
3.1	The F 3330, F 3331, F 3333, F 3334, F3335, F 3348, F3349 Safety-related, Digital Output Modules	40
3.1.1	Test routines	40
3.1.2	Response of the System on Failures Detected at Safety-related Digital Output Modules	41
3.2	The F 3430 Safety-related Digital Relay Output Module	41
3.2.1	Test Routines	41
3.2.2	Response of the System on Failures Detected at Safety-related Digital Relay Output Modules	41
3.2.3	Notes for Projecting with F 3430	41
3.3	The F 6705 Safety-related Analog Output Module	42
3.3.1	Test Routines	42
3.3.2	Response of the System on Failures Detected at Safety-related Analogue Output Modules	42
4	Instructions for the Replacement of Output Modules	43
5	Check Lists for Project Planning, Programming and Commissioning Safety-related Output Modules	44
5.1	F 3330 Safety-related Digital Output Module	45
5.2	F 3331 Safety-related Digital Output Module	46
5.3	F 3333 Safety-related Digital Output Module	47
5.4	F 3334 Safety-related Digital Output Module	48
5.5	F 3335 Safety-related Digital Output Module	49
5.6	F 3348 Safety-related Digital Output Module	50
5.7	F 3349 Safety-related Digital Output Module	51
5.8	F 3430 Safety-related Digital Output Module	52
5.9	F 6705 Safety-related Analogue Output Module	53
Chapter 5	Software	
1	Software for Safety-related HIMA H41q/H41qc and H51q Automation Devices	55
2	Safety Aspects concerning the Operating System	57
2.1	Designation, Current Approved Version for Safety-related Applications (CRC Signature)	57
2.2	Signatures of the User Program	57
2.3	Procedures and Functions of the Operating System	58

3	Safety Aspects Concerning Programming with ELOP II	59
3.1	The ELOP II Safety Concept	59
3.1.1	Application of the Safety Tool of ELOP II for the Creation of the Program	60
3.1.2	Application of the Safety Tool of ELOP II for Program Modifications	60
3.1.3	Program Identification Possibilities	62
3.1.4	Check of the User Program to Meet the Specified Safety-related Function	64
3.2	Guidelines for the ELOP II User	64
3.3	Parameterization of the Automation Device	64
3.3.1	Safety	64
3.3.2	Failures in Safety-related Output Amplifiers	65
3.4	Check list: Measures Required for the Creation of a User Program	66
3.5	Reload (Reloadable Code)	68
3.5.1	Systems with one Central Module	69
3.5.2	Systems with Redundant Central Modules	69
3.6	Offline Test	69
3.7	Forcing	69
3.8	Protection against Manipulations	70
4	Safety Aspects Concerning the User Program	71
4.1	General Programming Procedure for Automation Systems of the H41q/H51q Families for Safety-related Applications	71
4.2	Use of Standard Function Blocks for Safety-related Applications	71
4.2.1	Standard Function Blocks Independent of the IO Level	71
4.2.2	Standard Function Blocks Depending on the IO Level	72
4.3	Prerequisites and Rules for the Use in Safety Applications (Requirements from Prototype Certificates etc.)	72
4.3.1	Basic Programming	73
4.3.2	Variable Declaration and Entering of Process I&C Names	73
4.3.2.1	Allocation of Process I&C Names with Variable Names	74
4.3.2.2	Types of Variables	75
4.3.2.3	Digital Inputs and Outputs for Boolean Variables	75
4.3.2.4	Analogue IO Modules	75
4.3.2.5	Imported or Exported Variables	75
4.3.3	Functions of the User Program	76
4.3.3.1	Group Shutdown	76
4.3.3.2	Function Blocks for Individual Safety-related IO Modules	76
4.3.3.3	Redundant IO Modules	77
4.3.3.4	Redundant, Non-safety-related Sensors	77
4.3.3.5	Analog Redundant Transmitters	79
4.3.3.6	Input Modules with 2oo3 Circuit	81
4.4	Program Documentation for Safety-related Applications	82
5	Safety Aspects for Communication (Safety-related Data Transmission)	83
5.1	Safety-related Communication	83
5.2	Time Requirements	83
5.3	Instructions for the Creation of the User Program	84
6	Use for Central Fire Alarm Systems according to DIN EN 54-2 and NFPA 72	85
Chapter 6	Operating Conditions	
1	Climatic Conditions	88

Table of Contents

2	Mechanical Conditions	89
3	EMC Conditions	89
4	Power Supply Conditions	90

Appendix

1	Standard Function Blocks for the Central Area	92
1.1	Function Block HK-AGM-3	92
1.2	Function Block HK-COM-3	92
1.3	Function Block HK-MMT-3	92
1.4	Function Block H8-UHR-3	92
2	Allocation of Standard Function Blocks for the IO Area	93
2.1	Function Block H8-STA-3	93
2.2	Function Block HA-LIN-3	94
2.3	Function Block HA-PID-3	94
2.4	Function Block HA-PMU-3	95
2.5	Function Block HA-RTE-3	96
2.6	Function Block HB-BLD-3	97
2.7	Function Block HB-BLD-4	98
2.8	Function Block HB-RTE-3	99
2.9	Function Block HF-AIX-3	100
2.10	Function Block HF-CNT-3	101
2.11	Function Block HF-CNT-4	102
2.12	Function Block HF-TMP-3	103
2.13	Function Block HK-LGP-3	104
2.14	Function Block HZ-DOS-3	104
2.15	Function Block HZ-FAN-3	105

Chapter 1 The Safety Philosophy and Conditions

1 Introduction

1.1 Definitions

Closed circuit principle: A system operating in "deenergize to trip" mode does not need energy to perform its safety function.

Open circuit principle: A system operating in "energize to trip" mode needs energy, for example electrical or pneumatic energy, to perform its safety function.

1.2 Certification

The safety-related automation devices (PES = Programmable Electronic System) of the H41q, H41qc and H51q system families are certified as follows:



TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie
Am grauen Stein
D - 51105 Köln

Certificate and Test Report No. 968/EZ 129.06/05

Safety-related Automation Systems
H41q-MS, H41q-HS, H41q-HRS
H41qc-MS, H41qc-HS, H41qc-HRS
H51q-MS, H51q-HS, H51q-HRS

The safety-related HIMA automation devices of the H41q, H41qc and H51q system families are tested and certified for their functional safety according to the important standards as listed below:

IEC 61508: Parts 1-7: 2000	up to SIL 3
IEC 61511: 2004	
EN 954-1: 1996	up to Category 4
DIN VDE 0116: 1989, EN 50156-1: 2004	
EN 120672: 2004, EN 298: 2003, EN 230: 1990	
NFPA 85: 2001	
EN 61131-2: 2003	
EN 61000-6-2: 2001, EN 61000-6-4: 2001	
EN 54-2:1997, NFPA 72: 2002	

The **Chapter 6 Operating Conditions** contains a detailed listing of all applied environment and EMC tests.

1.3 Safety and Availability

Due to the 1oo2D microprocessor structure on one central module, already as mono systems the system families H41q, H41qc and H51q are designed for use up to SIL 3 (Cat 4).

Depending on the required availability, the HIMA Automation devices can be equipped with redundant modules in the central and IO areas. Redundant modules increase availability, as in the event of the failure of one module the failed module is automatically switched off, and the redundant module maintains operation without interruption.

According to IEC 61508 the PFD (Probability of Failure on Demand) and PFH (Probability of Failure per Hour) calculations were made for the safety-related systems H41q, H41qc and H51q.

IEC 61508-1 defines for SIL 3

a PFD of 10^{-4} ... 10^{-3} and

a PFH of 10^{-8} ... 10^{-7} per hour.

For the control (PES) are estimated 15 % of the standard limit value for PFD and PFH. This results in the following limit values for the control part

$$\text{PFD} = 1,5 \cdot 10^{-4}$$

$$\text{PFH} = 1,5 \cdot 10^{-8} \text{ per hour}$$

The offline proof-test intervals for the for the safety-related systems H41q, H41qc and H51q is determined to 10 years ¹.

The safety functions each consisting of a loop (input, processing stage, output) meet the requirements in all configurations.

Further information is available on request.

Overview: system designations, safety, availability and system configurations

System designation	H41qc-MS H41q-MS H51q-MS	H41qc-HS H41q-HS H51q-HS	H41qc-HRS H41q-HRS H51q-HRS
SIL / Category	SIL 3 / Cat 4	SIL 3 / Cat 4	SIL 3 / Cat 4
Availability	normal	high	very high
Configuration			
Central module	mono	redundant	redundant
IO modules	mono ¹	mono ¹	redundant
IO bus	mono	mono	redundant ²

1. To increase availability, individual IO modules may be used as redundant modules or in a 2oo3 circuit.
2. When using a redundant IO bus, we recommend using not only the IO modules but also the peripherals (sensors and actuators) as redundant modules. Experience shows that these components have higher failure rates than the modules of the PES.

1. Restrictions for the relay output module F 3430 (cf. **chapter 4, item 3.2**)

To increase the availability by using redundant modules, three essential points must be considered:

- Defective modules must be detected and switched off so that they do not block the system.
- In the event of an fault, the operator must receive a message indicating that the module must be replaced.
- Automatic restart of operation after the replacement of a module must be ensured.

The HIMA Automation devices meet all these requirements in the respective configurations.

To program the devices, a PADT (programmer unit, PC) is used running with the programming tool

ELOP II

according to IEC 61131-3. It supports the user during creating safety-related programs and operation of the automation devices.

The automation devices are designed for the closed-circuit principle, i.e. for the peripheral equipment and for the function of the control the de-energized state is to see as the safe state. In case of faults input and output signals are switched to the safe state, they are free of voltage or current.

1.4 Safety Times

Single faults which may lead to a dangerous state of operation are detected by the self-test equipment within the fault tolerance time (min. 1 s). The fault tolerance time is preset as safety time in the menu properties in the resource.

Fault tolerance time

Process value which is very often called safety time in guidelines for users

Safety time (in the PES)

Value depending on the system capability

Failures whose effects may be critical for safety only in combination with additional faults are detected by background tests within the Multiple Fault Occurrence Time. The Multiple Fault Occurrence Time is determined with the setting of the safety time (fault tolerance time). In the operating system it is defined as 3600 times that value.

Two types of tests are distinguished:

- Tests performed during the safety time
They are performed within the safety time (foreground tests);
Response time: immediate response, at the latest within the safety time
- Tests performed during the multiple fault occurrence time
They are performed during the multiple fault occurrence time and are subdivided into many cycles (background test);
Response time: immediate response upon detection of the fault, at the latest within the multiple fault occurrence time.

Example for the response time: maximum double the cycle time. If a fault tolerance time (safety time) of 1s 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 (Š 1s) defined in the properties for the resource. Special attention should be paid to the fact that the cycle time does not exceed half of the safety time, as the response to faults in the input modules comes within max. 2 cycles. The cycle itself depends on the safety time which determines the period of time during which all foreground tests are performed.



A short safety time therefore increases the cycle time and vice versa.
With long safety times, some tests are distributed to several cycles.

Example 1: safety time = 1 s
 Cycle time for user program = 450 ms
 Time required for tests = 100 ms
 Two cycles are possible during the safety time
 $100 \text{ ms} / 2 = 50 \text{ ms} / \text{cycle}$ - time required for tests
 Total cycle time = **500 ms**

Example 2: safety time = 2 s
 Cycle time for user program = 450 ms
 Time required for tests = 100 ms
 Four cycles are possible during the safety time
 $100 \text{ ms} / 4 = 25 \text{ ms} / \text{cycle}$ - time required for tests
 Total cycle time = **475 ms**



**The safety time must not be set to the value 255 s!
 Only the value range 1 to 254 is permitted!**

1.5 Offline Proof-Test

The offline proof-test recognizes dangerous concealed faults that would affect the safe function of the plant.

HIMA safety systems have to be subjected to an **offline proof test in intervals of 10 years**. By an analysis using the HIMA calculation tool SILence, the interval often may be extended. For relay modules, the proof test for the relays has to be carried out in intervals defined for the respective plant.

1.5.1 Execution of the Offline Proof Test

The execution of the offline proof test depend on the configuration of the plant (EUC = equipment under control), which risk potential it has, and which standards for operation are applied and form the bases for the approval by the test authority in charge.

According to the standards IEC 61508 1-7, IEC 61511 1-3, IEC 62061, and VDI/VDE 2180 sheet 1 to 4, in case of safety-related systems the operating company has to arrange for proof tests.

1.5.2 Periodic Proof Testing

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

In practice the input and output field devices have a more frequent proof test interval (e.g., every 6 or 12 months) than the HIMA PES. If the end-user tests the complete safety loop because of the field devices then the HIMA PES is automatically included in these tests. No additional periodic tests are required for the HIMA PES.

If the proof test of the field devices does not include the HIMA PES then the PES needs to be tested as a minimum once in 10 year. This can be done by executing a reset of the HIMA PES.

In case there are periodic proof test requirements for specific modules then the end-user should refer to the data sheets of these modules.

2 Safety Conditions



The operating company is responsible for operating a plant safely according to the relevant application standards.

For use of the safety-related PES of the systems H41q, H41qc and H51q the following safety requirements are valid:

2.1 Hardware Project Planning; Product Independent Conditions

- For safety-related operation, only the fail-safe hardware modules and software components approved for such use are to be used. The approved hardware modules and software components are listed in the
List for tracing the version releases pertaining to the modules and
Firmware of the Company HIMA Paul Hildebrandt GmbH + Co KG,
Certificate No. 968/EZ/129.00/02
Each running version is to take from this list which is commonly managed with the certification authority.
- The conditions of use (specified in chapter 6) regarding EMC, mechanical and climatic effects must be observed.
- Non-fail-safe, but interaction-free hardware modules and software components may only be used for the processing of signals not relevant to safety but not for the processing of safety-related tasks.
- The closed circuit principle has to be applied to all safety circuits connected externally to the system.

2.2 Hardware Project Planning; Product Dependent Conditions

- Safe electrical isolation from the mains supply must be ensured for all devices connected to the system.
- The safe electrical isolation of the power supply must be performed in the 24 V supply of the system. Only PELV or SELV version power supplies may be used.

2.3 Programming; Product Independent Conditions

- In safety-relevant applications there must be regarded carefully the correct setting of the system parameters which have an effect on safety. Possible parameterization is described in this Safety Manual.
In particular, the definition of the system configuration, the maximum cycle time and the safety time must be regarded.

2.4 Programming; Product Dependent Conditions

- The error reaction of the system in the case of errors in the fail-safe input and output modules must be defined in accordance with the specific safety aspects of the plant by the user program.
- In case of the use of a not certified tool¹ for the user program, the correct compilation and implementation of the program after initial set up or after modifications of the application is

to be verified by full functional testing.

- By using ELOP II, from version 3.5 on, the verification of the program can be simplified according to the conditions of this safety manual.
- However, a sufficient validation of the program is required.
- Function checks / verifications after a modification of the user program can be limited to the modified parts.
- The procedure of programming and modification of programming is described in Chapter 5 Software. The requirements mentioned there must be regarded.

2.5 Communication; Product Dependent Conditions

- Using the safety-related communication between the different devices it must be regarded, that the total reaction time of a system does not exceed the fault tolerance time. The calculation elements mentioned in this Safety Manual must be applied.
- At present the transfer of safety-related data via public networks (e. g. Internet) is not admissible.
- If the data are transferred via internal networks (of a company or factory), a sufficient protection against manipulation must be reached by administrative or technical actions (e. g. blocking of the safety-related part of the network against access from others with a fire-wall).
- To the communication interfaces may only be connected equipment providing a save electrical isolation.

2.6 Special Operating Modes; Product Independent Conditions

- Online modifications in safety applications are only permitted after consultation with the test authority responsible for plant acceptance and with the aid of certified tools approved for this purpose (ELOP II version 3.5).
- During the entire online modification, the person responsible for the online modification must ensure that there is sufficient safety monitoring of the process through other technical and organizational measures.
- Prior to each online modification the version changes against the application software currently running are to be determined with the aid of a certified tool approved for this purpose. With ELOP II (version 3.5) this tool is to be the C-code comparator.
- In the case of mono online modifications, the duration of the entire modification plus twice the cycle time may not exceed the failure tolerance time of the process.
- For the use of „Maintenance Override“, the relevant current version of the document „Maintenance Override“ written by TÜV Rheinland and TÜV Product Service is to be observed.
- With ELOP II (version 3.5) a static offline test of the logic is possible. The offline simulation was not subject to a safety-relevant testing. Therefore the simulation cannot replace a functional test of the plant.
- If required the operator must determine administrative measures for access protection to the PES in accordance with the test authority responsible for the application.

-
1. Due to the proprietary protocols and interfaces of the operating system only HIMA products can be used.

Chapter 2 Central Modules

1 Overview of the Modules in the Central Area of the H41q, H41qc and H51q Systems

1.1 Central Area of HIMA Automation Devices of the H41q, H41qc and H51q Systems

The components required for the central area of the different types of HIMA automation devices are assembled in a kit. The kit of an operative central module consists of the following components:

- Central module rack
- Central modules
- Power supply modules
- Accessories

The exact scope of supply as well as the cabling of the of the supply voltage and the connection of the IO level are described in the data sheets of the catalogue „Programmable Systems, System Families H41q/H51q“.

1.2 Overview of the Central Modules for the H41q, H41qc and H51q Systems

Module/ Kit		Safety- related	Non-interact- ing
The H41q and H41qc System Families			
F 8652 F 8652A F 8652E	Central module, double processor 1oo2	•	
F 8653 F 8653E	Central module		•
B 4231	Central device kit H41q-MS	•	
B 4233-1	Central device kit H41q-HS	•	
B 4233-2	Central device kit H41q-HRS	•	
B 4235	Central device kit H41qc-MS	•	
B 4237-1	Central device kit H41qc-HS	•	
B 4237-2	Central device kit H41qc-HRS	•	
The H51q System Family			
F 8650 F 8650A F 8650E	Central module, double processor 1oo2	•	
F 8651 F 8651E	Central module		•
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	IO subrack	•	

1.2.1 Other Modules for the H41q, H41qc and H51q Systems in the Central Device Area

Module/ Kit		Safety- related	Non-interact- ing
Power distribution modules			
F 7132	4fold power distribution module		•
F 7133	4fold power distribution module 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	Coprocessor module for H51q		•
F 8625	Communication module for Ethernet		•
F 8626	Communication module for Profibus DP (Slave)		•
F 8627	Communication module for Ethernet		•
Bus connections			
F 7553	IO bus connection module for H51q		•
Bus connection modules for the configuration of HIPRO			
F 7505	Interface converter RS 485, V.24/20mA/2-wire/4-wire (HIPRO)		•
F 7506	Bus connection terminal for the configuration of 2-wire buses		•

2 General Notes on the Safety and Availability of safety-related Central Modules

For the system allocation of the central modules and power supply module components as well as bus components of the H41q, H41qc, and H51q system families, the following requirements apply:

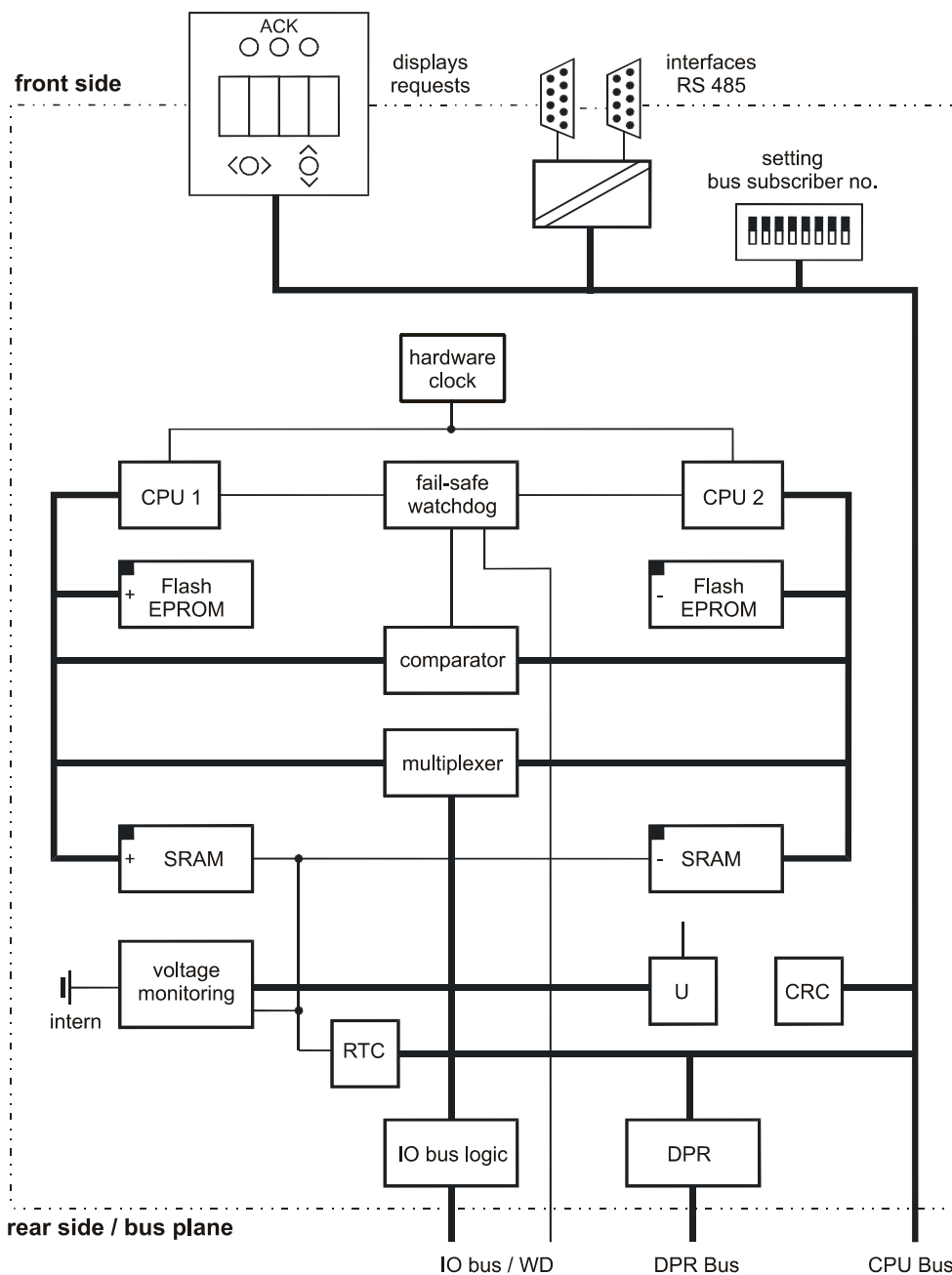
Systems H41q, H41qc	System H51q
<p>On the H41q system subrack</p> <ul style="list-style-type: none"> • two central modules • 12 IO modules • two power supply modules • three fuse modules <p>can be used.</p> <p>On the H41qc system subrack,</p> <ul style="list-style-type: none"> • two central modules • two communication modules • 13 IO modules • two power supply modules <p>can be used.</p> <p>Fusing of the inputs/outputs by automatic circuit-breakers</p>	<p>On the central module subrack</p> <ul style="list-style-type: none"> • two central modules • three F 8621/A coprocessor modules or five F 8625, F 8626, F 8627, F 8628 communication modules per central module <p>can be plugged in.</p> <p>The basic components for IO subracks are assembled in kits.</p>

2.1 Power Supply Modules

In safety-related applications, one more 24 V DC / 5 V DC power supply module than is required due to power consumption is to be used. This applies to the central module subrack and for the additional power supply. The power supply modules are decoupled via diodes and are monitored by the central devices.

2.2 Functional Description of the Safety-related F 8652 (A, E) / F 8650 (A, E) Central Modules for the H41q, H41qc and H51q Systems

The F 8652 (A, E) or F 8650 (A, E) central module for safety-related applications includes the function blocks shown below.



Each central module of type F 8652 (A, E) or F 8650 (A, E) consists of the following function blocks:

- Two microprocessors with synchronized clock
- 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 comparator for external access by both microprocessors;
- in the event of a fault the watchdog is put into the safe state and the processor status is signalled.
- Flash EPROMs of the program memories for the operating system and the user program are suitable for at least 100,000 memory cycles
- Data storage in the SRAM (static RAM)
- Multiplexer for the connection of the IO bus, the Dual Port RAM (DPR) and the redundant central module
- Back-up of the SRAMs effected by batteries on the central module with monitoring of the bus PCB
- Two RS 485 interfaces with electrical isolation, baud rate: 57600 bps; can be set to 9600 bps and 57600 bps via switch or via the software (other baud rates are also possible); the software values have priority
- Diagnosis display and 2 LEDs for information from the system, the IO area and the user program
- DPR for fast, two-way alternate access to the second central module
- Hardware clock with battery back-up
- IO bus logic for connection with the IO modules
- Fail-safe watchdog
- Power supply module monitoring, testable (5 V system voltage)
- Battery monitoring.

3 The Principles of Function of Safety-related Central Modules

3.1 Self Test Routines

The following explanations describe in brief the self-test routines of the safety-related F 8650 (A, E) and F 8652 (A, E) central modules and the coupling to the IO level:

- **CPU test:** The types of command and addressing, writing property of flags and the commands triggered by flags, the writing property and the crosstalk of the registers and the ALU are tested.
- **Test of the memory areas:** The operating system, the user program, the constants and parameters as well as the variable data are stored in the central module in a direct and an inverted version. By a hardware comparator they are checked for antivalence.
- **Permanent memory areas:** The operating system, the user program and parameter area are each stored in a Flash EPROM and they are assured by a CRC test.
- **RAM test:** The RAM areas are tested by a read/write test especially for crosstalk.
- **Watchdog test:** The watchdog signal is switched off unless it is triggered within a determined period of time by both CPUs with antivalent bit patterns or if the hardware comparator between the two memories (direct and inverted) detects a difference. A further test checks the switch-off capability of the watchdog signal.
- **Test of the connection to the IO level within the central module:**
With redundant central modules in the systems H41q-HS / H41qc-HS / H51q-HS and a single-channel IO bus the interlock of the IO access of the central module is protected via an arbiter circuit. The arbiter circuit is checked by self tests.

With a two-channel IO level - HRS system - the right to IO access is read back and checked.

With a single-channel IO level - MS system (single-channel IO modules and single-channel CPU) - the right to IO access is read back and checked.

- **Test of the connection module on the IO subracks:**
The addressing is tested in cycles each time a safety-related IO module has been processed.
The addresses of all agreed IO module positions are read back and tested. The safety switches of the F 7553 module are tested.

3.2 Response on Errors Detected in Central Modules

The test routines ensure that errors are detected and that the defective central module is switched off. At the same time the diagnostic display indicates the errors and enters them into the system diagnosis. For a central module - MS system - this means a complete shut-down of the automation device. In case of redundant central modules - HS and HRS systems - the defective central module is switched off and the second one continues operation.

If in redundant systems the defective central module is replaced by a new one having the same user program, the new central module receives the current data from the running central module and the system returns to redundant operation.

3.3 Diagnostic Display

The diagnostic display is part of the central module. It consists of a 4-digit alphanumeric display for the representation of texts and values, of an LED for the general display of central module faults and an LED for the general display of faults in safety-related IO modules. An acknowledgement push button (ACK) and two push buttons for calling further system information are also provided.

If errors occur in the central modules, STOP is displayed and, additionally, the error code can be called. If errors occur in safety-related modules in the IO level, the position of the module is displayed and, if possible, the disturbed channel.

In addition to this, all error codes are provided in the diagnostic system for the visual display on a process control system.

An error history supports the detection of problems in the system.



The diagnostic display is not fail-safe! Therefore no safety-related action must be taken based on the information on the diagnostic display.

4 Response on Errors Detected in the IO Bus Area

If errors occur in the IO area between the central module and the connection modules, all IO subbracks affected by this fault are switched off.

If an error in the IO bus area occurs within the IO subbrack only, the connection module switches off the output modules on the IO subbrack affected.

5 Instructions for the Replacement of Central Modules

Defective modules of both the central and the IO areas can be replaced during operation. The automation device does not have to be switched off.



We urgently recommend replacing defective central modules.

In the event of a fault or for maintenance purposes, the module should be replaced obeying the following instructions:

- Central modules for single-channel automation devices with integrated back-up battery must be stored without the user program, if this program contains non-volatile variables (retain variables). These variables are not set to their initial value while the system is booting.
- Central modules for redundant automation devices with integrated back-up battery can be stored containing the user program, even if this program includes non-volatile variables (retain variables). During system booting, these variables are taken over by the central device already in operation.

The diagnostic display of the central module signalizes BATI in case the battery of the central module is discharged.

A recommendation for replacing the batteries on the modules can be found in the datasheet.



When there is both a battery and a power failure, the RETAIN variables are newly initialized during system booting and thus lose the stored values.

Chapter 3 Input Modules

1 Overview of the Input Modules for the H41q, H41qc and H51q Systems

Module		Safety-related	Non-interacting	(Ex)i	Related SW function block
Digital input modules					
F 3221	16-channel input module		•		
F 3222	8-channel input module		•		
F 3223	4-channel input module		•	•	
F 3224A	4-channel input module		•	•	
F 3236	16-channel input module	•	•		
F 3237	8-channel input module	•	•		HB-RTE-3
F 3238	8-channel input module	•	•	•	HB-RTE-3
F 3240	8-channel input module	•	•		
F 3248	16-channel input module	•	•		
F 5203	14 bit ring counter		•		
F 5220	2-channel counter module	•	•		HF-CNT-3, -4
Analog input modules					
F 6208	Signal converter		•	•	
F 6213	4-channel analogue input module	•	•		HA-RTE-3
F 6214	4-channel analogue input module	•	•		HA-RTE-3
F 6215	8-channel analogue input module		•		
F 6216A	8-channel analogue input module with transmitter power source		•		
F 6217	8-channel analogue input module	•	•		
F 6220	8-channel thermocouple input module	•	•		HF-TMP-3
F 6221	8-channel analogue input module	•	•	•	HF-AIX-3

2 Safety and Availability of Safety-related Input Modules

2.1 General notes on safety-related input modules



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

Due to their increased complexity, some types of the analogue and digital inputs modules have their own 1002 microprocessor system which automatically performs safety-related online tests and provides the verified data for the safety-related processing module.

The safety-related input modules allow the use of a diagnostic display and thus improved error detection and localization.



In safety-related systems, safety-related and non-interacting input modules can be mixed.

We recommend equipping the system with the highest possible degree of safety-related input modules.

Safety-related input modules in the H41q, H41qc and H51q system are automatically subjected to a high-quality cyclical self test during operation. The input modules contain circuit parts which allow the online test of the input module function via special test routines integrated into the operating system. These test routines are TÜV tested and ensure the correct function of the corresponding modules. Whenever an error is detected, an error message is generated. These error messages automatically trigger the safety-related function of the system and display diagnostic information for the system operator. This allows the design of a flexible diagnosis system in the planning and realization stage of the plant.



Due to the safety concept of the H41q, H41qc and H51q systems, a single-channel solution for safety-related input modules is possible up to SIL 3 in the input area.

To increase availability or for other system-related reasons, the safety-related input modules can also be used in parallel (redundantly).



The safety of the system will not be affected in any way by redundant input modules.

The following rules have to be obeyed concerning the permissible slots for input modules on the system subracks and the IO subracks for the H41q, H41qc and H51q systems:



Systems H41q, H41qc	System H51q
The input modules are plugged into the system subrack. Kits with 12 slots (H41q) or 13 slots (H41qc) for IO modules are available.	The input modules are plugged into IO subracks (IOSR) having 16 IO module slots each. The required basic components for IOSRs are assembled in kits.



If a plant operates in "deenergized to trip" mode, the reaction to a failure of an input module has to be - if no redundancy exists:

- Transition into safe state (if necessary, shutdown)
- Annunciation of the failure.

If a plant operates in "energized to trip" mode (e.g. fire alarm systems, see Chapter 6 Operating Conditions) then - if no redundancy exists - the PES has to do:

- Annunciation of the failure of the input module
- No further reaction necessary.

2.1.1 Safety of Sensors, Detectors, Transmitters

Safety-related signals are only given if the external sensors, detectors or transmitters have a related proof of safety. Safety-related operation of external sensors, detectors or transmitters can also be ensured by special wiring (see below).

If the transmitters have no proof of safety, the detectors have to be wired in a 1oo2-, 2oo3- or NooM circuit
(Remark: 1oo2 means "1 out of 2").

The safety and availability of the sensor technology can be increased by a 1oo2-, 2oo3- or NooM circuit of the sensors. Methods of implementing various ways of sensor wiring under the aspect of safety and availability are described in detail in Chapter 5, Software. The user program has to be designed accordingly.

Based on the IEC 61508 standard, according safety proof is possible by the determination of offline prove test intervals. Detailed determinations are to be made for the specific application.

2.2 The F 3236, F 3237, F 3238, F 3240 and F 3248 Safety-related Digital Input Modules

2.2.1 Test Routines

The online test routines check whether the input channels are able to switch through both signal levels (L and H signals) irrespective of the applied input signals. This function test is performed each time the input signals are read. Each time an error occurs in the input module, the user program processes the 0 signal (safe state).

The modules for initiators and for contact makers with line monitoring additionally test the line up to the contact maker. A safety-related initiator can be connected to these modules. Due to the self tests, all requirements concerning the detection of the thresholds of the safety-related initiators are fulfilled.

The monitoring of the power supply of a sensor contact requires the connection of two resistors according to the data sheet.

2.2.2 Response of the System on Failures Detected at Safety-related Digital Input Modules

Kind of failure	Response of system	Comment
Defective module (input module)	Storage of the FALSE signal for all channels in logic processing	This ensures the safe function of the system depending on the selected system configuration.
Wire break in the sensor circuit	Reading of the FALSE signal in the corresponding channel	With modules having line monitoring, a line fault is signalled. For safety-related inputs, this signal must be evaluated by the HB-RTE-3 function block (see chapter 5) to ensure a safe response of the system.
Short circuit in the sensor circuit	Reading of the TRUE signal in the corresponding channel	With modules having line monitoring, a line fault is signalled. For safety-related inputs, this signal must be evaluated by the HB-RTE-3 function block (see chapter 5) to ensure a safe response of the system.
General	The position of the defective module is shown on the diagnostic display. If input modules with line break and short-circuit monitoring of the sensor circuit are used, the diagnostic display also shows the faulty channel of the defective module.	

2.3 The F 5220 Safety-related Counter Module

This 2-channel counter module has its own dual-processor system with one safety-related output per channel. It can be used for pulse counting or - with its adjustable gate interval - for frequency measurements or rotational speed measurements. It can also be used for monitoring the sense of rotation.



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

2.3.1 Test Routines

The module has its own 1002 microprocessor system which automatically performs safety-related online tests. The safe data for the safe signal processing are available through the HF-CNT-3 function block.

2.3.2 Response of the System on Failures Detected at Safety-related F 5220 Counter Modules

Type of failure	Response of system	Comment
Module failure	Switching off of the safety-related outputs.	In the event of an error the only possible response is switching to the safe state.
Channel failure	Switching off of the assigned safety-related output.	In the event of an error the only possible response is switching to the safe state.
Line break or short circuit in the initiator circuit or other failures	Switching off of the assigned safety-related output.	After fault recovery, reset signal at the input of the HF-CNT-3 function block required.

2.4 The F 6213, F 6214 and F 6217 Safety-related Analogue Input Modules

In parallel operation of safety-related analogue input modules, the average value (for F 6213, F 6214 generated by the appertaining function block, for F 6217 by the user program) of operative modules is processed (only within the range of permissible deviations!) In the event of an error, only the value from the operative module is processed.

2.4.1 Test Routines

Via the test DA converter, the test values are applied and tested via the AD converter which also digitizes the input signal.

2.4.2 Response of the System on Failures Detected at Safety-related F 6213, F 6214 Analogue Input Modules

Type of failure	Response of system	Comment
Module or channel failure with single-channel analogue inputs	The configured value is processed by the HA-RTE-3 function block (see appendix).	In the event of an error the only possible response is switching to the safe state.
Module or channel failure with redundant analogue input modules and redundant transmitters	If an input module fails, the value coming from the redundant module or the configured error value is processed.	Either min., max or mean value generation via the HA-RTE-3 function block (see appendix).
Short circuit in the transmitter circuit	Display of the module position and the faulty channel on the diagnostic display.	only when using 4...20 mA.

2.4.3 Response of the System on Failures Detected at Safety-related F 6217 Analogue Input Modules

Type of failure	Response of system	Comment
Channel failure	Analog value = 0000 Channel error bit = TRUE	Channel error bit must be processed in a safety-related way in the user program.
Module failure	All analogue values = 0000 All channel error bits = TRUE	See channel error, applies to all channel error bits
Measuring range exceeded	Analog value = 0000 or 4095 Channel error bit = TRUE	Max. admissible value must be defined in the user program.

This module has its own 1oo2 microprocessor system which automatically performs safety-related online tests and provides the saved data for the safety-related processing module. An analogue value and a related channel error bit exist for each channel. Depending on the requirements, the necessary function block can be created in the user program.



When the channel error bit has been set, a safety-related response in relation to the corresponding analogue input must be programmed.

2.5 The F 6220 Safety-related and Intrinsically Safe Thermocouple Input Module

The thermocouple input module has eight channels for the connection of various types of thermocouples (according to the parameters of the HF-TMP-3 function block) and one input for the connection of a Pt100 resistance temperature detector as a reference temperature input. It has its own dual-processor system. The parameterization of the module is performed via the HF-TMP-3 for each channel used.

2.5.1 Test Routines

The module has its own 1002 microprocessor system which automatically performs safety-related online tests. The safe data for the safe signal processing are available through the HF-TMP-3 function block. Each of the 8+1 input channels supplies safe input values and a safe error status.

2.5.2 Response of the System on Failures Detected at Safety-related F 6220 Thermocouple Input Modules

Type of failure	Response of system	Comment
Module failure	The „Value“ output (INT) at the HF-TMP-3 function block is 0. The „Channel error“ output at the HF-TMP-3 function block switches to TRUE.	The error indication value must be set in the user program by using the „Channel error“ output signal.
Channel failure	The „Channel error“ output at the HF-TMP-3 function block switches to TRUE.	The failure indicating value must be set in the user program.
Underflow	The „Underflow“ output at the HF-TMP-3 function block switches to TRUE.	The failure indicating value must be set in the user program.
Overflow	The „Overflow“ output at the HF-TMP-3 function block switches to TRUE.	The failure indicating value must be set in the user program.

The limits for underflow or overflow are to be set at the inputs „Underflow level“ or „Overflow level“, depending on the HF-TMP-3 function block.

Additional notes on project planning

Not used inputs have to be short-circuited.

When using the module in SIL 3 the reference temperature from the user program is to be used or the reference temperature is to be determined via comparison of the reference temperatures of two modules. All possible deviations have to be considered and have to be regarded in the evaluation of the measuring values.

For use in SIL 3, the input temperature is to be determined via comparison of the temperatures of two different thermocouples.

2.6 The F 6221 Safety-related Analogue and Intrinsically Safe Input Module

The analogue input module has eight channels for the direct connection of analogue transmitters from the (Ex) area. The transmitter supply voltage can be delivered from the output module F 3325 (or other generators according the data sheet standards). This transmitter supply voltage is to connect via the module F 6221 for monitoring.

Each used channel is parameterized via a separate function block HF-AIX-3.

2.6.1 Test Routines

The module has its own 1002 microprocessor system which automatically performs safety-related online tests. The safe data for the safe signal processing are available through the HF-AIX-3 function block. Each of the eight channels supplies safe input values and a safe error status.

2.6.2 Response of the System on Failures Detected at Safety-related F 6221 Analogue Input Modules

Type of failure	Response of system	Comment
Module failure	The „Value“ output (INT) at the HF-AIX-3 function block is 0. The „Channel error“ output at the HF-AIX-3 function block switches to TRUE.	The failure indicating value must be set in the user program by using the „Error Value“ input signal of the function block.
Channel failure	The „Channel error“ output at the HF-AIX-3 function block switches to TRUE.	
Underflow	The „Underflow“ output at the HF-AIX-3 function block switches to TRUE.	
Overflow	The „Overflow“ output at the HF-AIX-3 function block switches to TRUE.	

The limits for underflow or overflow are to be set at the inputs „Underflow level“ or „Overflow level“, depending on the HF-AIX-3 function block.

Additional notes on project planning

Voltage inputs (0...1 V) not used are to be short-circuited on the terminal strip.
Current inputs not used are terminated by a shunt in the cable connector.

Only uses mentioned in the data sheet of the F 6221 module are admissible.

The (Ex) protection regulations and the (Ex) connection conditions must be met.

3 Instructions for the Replacement of Input Modules



We urgently recommend replacing defective input modules.

In the event of a module failure or for maintenance purposes, please follow the instructions described below:

- Unscrew the cable connector or pull out the input module with its cable connector plugged in.
- Insert new input module without its cable connector and fasten by screwing.
- Plug in the cable connector and fasten by screwing.
- Operate the acknowledgement button (push button marked ACK on the central module).


4 Check Lists for Project Planning, Programming and Commissioning safety-related Input Modules

For each safety-related input module used in a system a check list must be completed to ensure that all relevant requirements are met. This is to be done during project planning or commissioning. It is the only way to make sure that the requirements are recorded clearly and completely. At the same time the check lists serve as evidence that project planning has been carried out carefully.


The check lists of this Safety Manual are available as MS Word files (*.doc) on a data medium.

- "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
- "SANAE-F5220" for safety-related analogue modules
- "SANAE-F6213 / 6214" for safety-related analogue modules
- "SANAE-F6217" for safety-related analogue modules
- "SANAE-F6220" for safety-related analogue modules
- "SANAE-F6221" for safety-related analogue modules


4.1 F 3236 Safety-related Digital Input Module (16-channel)

				
F 3236 Safety-related digital input module (16-channel)		Check list No. SDIGE-F3236-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	If yes, is the redundant module of the same type?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		


4.2 F 3237 Safety-related Digital Input Module (8-channel)

				
F 3237 Safety-related digital input module (8-channel)		Check list No. SDIGE-F3237-E Version 2.0/32.05		
Project data				
Project designation		File name of the check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is each safety-related input evaluated by the HB-RTE-3 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Does an HB-RTE building block exist in the user programme for each module or for two redundant modules, respectively?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are safety-related proximity switches connected to the module?	<input type="checkbox"/>	<input type="checkbox"/>	
6	Are the contacts equipped with resistors (1 k / 10 k) according to the data sheet?	<input type="checkbox"/>	<input type="checkbox"/>	
7	Is the line monitoring of the sensor channels evaluated?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Has the building block HB-RTE-3 building block been parameterised according to the requirements stated in the manual?	<input type="checkbox"/>	<input type="checkbox"/>	See Safety Manual, appendix
9	Are the unused inputs of the module wired accordingly?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

4.3 F 3238 (Ex)i Safety-related Digital Input Module (8-channel)


				
F 3238 Safety-related digital input module (8-channel)		Check list No. SDIGE-F3238-E Version 2.0/32.05		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is each safety-related input evaluated by the HB-RTE-3 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Does an HB-RTE-3 building block exist in the user program for each module or for two parallel redundant modules?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are safety-related proximity switches connected to the module?	<input type="checkbox"/>	<input type="checkbox"/>	
6	Are the contactors equipped with resistors (1 k / 10 k)?	<input type="checkbox"/>	<input type="checkbox"/>	
7	Is the line monitoring of the sensor channels evaluated?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Has the HB-RTE-3 building block been parameterized according to the requirements stated in this manual?	<input type="checkbox"/>	<input type="checkbox"/>	See Safety Manual, appendix
9	Are the unused inputs of the module wired accordingly?	<input type="checkbox"/>	<input type="checkbox"/>	
10	Have the special requirements for the application of the (Ex)i module as stated in the data sheet and the appendix to the EC-type-examination certificate been met?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

4.4 F 3240 Safety-related Digital Input Module (16-channel)

				
F 3240 safety-related digital input module (16-channel)		Check list No. SDIGE-F3240 Version 2.0/32.05		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	If yes, is the redundant module of the same type?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Are the input leads correctly connected and laid considering safe electric insulation?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are cables with double or reinforced insulation used for the connection wiring? *	<input type="checkbox"/>	<input type="checkbox"/>	
6	Can it be made sure that the input signals lead up to 127 V AC ?	<input type="checkbox"/>	<input type="checkbox"/>	
7	Can it be made sure that the input signals lead up to 110 V DC ?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		


* according to IEC 61131-2 Ed 2:2003 no longer required if the use of the module meets SELV or PELV conditions

4.5 F 3248 Safety-related Digital Input Module (16-channel)


				
F 3248 Safety-related digital input module (16-channel)		Check list No. SDIGE-F3248 Version 2.0/32.05		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	If yes, is the redundant module of the same type?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Are the input leads correctly connected and laid considering safe electric isolation?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is the connection wiring done by using cables with safety isolation? *	<input type="checkbox"/>	<input type="checkbox"/>	
6	Do the input signals have up to 48 V AC?	<input type="checkbox"/>	<input type="checkbox"/>	
7	Do the input signals have up to 48 V DC?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

* according to IEC 61131-2 Ed 2:2003 no longer required if the use of the module meets SELV or PELV conditions


4.6 F 5220 Safety-related Counter Module (2-channel)

				
F 5220 Safety-related counter module (2-channel)		Check list No. SDIGE-F5220-E Version 2.0/32.05		
Project data				
Project designation		File name of the check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is each safety-related module evaluated by the HF-CNT-3 /-4 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are the pulse inputs for proximity switches correctly connected?	<input type="checkbox"/>	<input type="checkbox"/>	See data sheet
4	Are the pulse inputs for mechanical contacts correctly connected?	<input type="checkbox"/>	<input type="checkbox"/>	See data sheet
5	Has the HF-CNT-3 /-4 building block been parameterized according to the requirements stated in the Safety Manual?	<input type="checkbox"/>	<input type="checkbox"/>	See Safety Manual, appendix for building blocks
Date		Created by		


4.7 F 6213 / F 6214 Safety-related Analogue Input Module (4-channel)

				
F 6213 / F 6214 safety-related analogue input module (4-channel)		Check list No. SANAE-F6213-14-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is each safety-related input evaluated by the HA-RTE-3 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Does an HA-RTE-3 building block exist in the user program for each module or for two redundant modules, respectively?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Has the HA-RTE-3 building block been parameterized according to the requirements stated in the manual?	<input type="checkbox"/>	<input type="checkbox"/>	See safety manual, appendix
6	Are the unused inputs of the module wired accordingly?	<input type="checkbox"/>	<input type="checkbox"/>	See data sheet
Date		Created by		


4.8 F 6217 Safety-related Analog Input Module (8-channel)

				
F 6217 safety-related analogue input module (8-channel)		Check list No. SANAE-F6217-E Version 2.0/32.05		
Project data				
Project description		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is the channel error bit (digital input) processed in a safety-related way at each analogue input?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Does a function building block exist in the user program for each channel or for two redundant channels, respectively?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are the unused inputs of the module wired accordingly?	<input type="checkbox"/>	<input type="checkbox"/>	See data sheet
Date		Created by		

4.9 F 6220 (Ex)i Safety-related Analog Thermocouple Input Module (8-channel)

				
F 6220 (Ex)i Safety-related analog thermocouple input module (8-channel)		Check list No. SANAE-F6220 Version 2.0/32.05		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Is each safety-related input evaluated by the HF-TMP-3 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are the errors of the module and channel, overflow and underflow evaluated in the user program by an error value?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Are the unused input circuits short-circuited?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are the special requirements met for the application of the (Ex)i module as stated in the data sheet and the appendix to the EC-type-examination certificate?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
6	Is the max. resistance in the measuring circuits less than 500 Ω?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
7	Does a redundant measuring input exist when used in a higher SIL?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Where does the value of the comparison temperature come from? - external - from the module - from redundant measuring?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

4.10 F 6221 (Ex)i Safety-related analogue input module (8-channel)

				
F 6221 (Ex)i Safety-related analog input module (8-channel)		Check list No. SANAE-F6221 Version 2.0/32.02		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the inputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a parallel, redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	If YES, is the redundant module of the same type?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Is the transmitter feeding coming from module F 3325?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
5	Are all recommendations for engineering taken into consideration according the permitted variants?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet F6221, see data sheets of other device
6	Is there forced ventilation by means of a fan right above / below the module?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet H51q: above, H41q: below
7	Have the special requirements been met for the application of the (Ex)i module as stated in the data sheet?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
8	Is a supervision of the transmitter voltage supply be implemented	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
9	Is the building block HF-AIX-3 been used in the program	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
Date		Created by		

Chapter 4 Output Modules

1 Overview of Output Modules for the H41q/H41qc and H51q Systems

Module		safety-related	non-inter-acting	loadability	related SW function block
Digital output modules					
F 3322	16-channel digital output module		•	≤ 0.5 A	
F 3325	6-channel supply module (Ex)		•	22 V ≤ 0.02 A	
F 3330	8-channel digital output module	•	•	≤ 0.5 A	
F 3331	8-channel digital output module	•	•	≤ 0.5 A	HB-BLD-3, HB-BLD-4 ¹
F 3332	4-channel digital output module		•	≤ 2 A	
F 3333	4-channel digital output module	•	•	≤ 2 A	
F 3334	4-channel digital output module	•	•	≤ 2 A	HB-BLD-3, HB-BLD-4 ¹
F 3335	4-channel digital output module (Ex)	•	•	22 V ≤ 0.053 A	
F 3348	8-channel digital output module	•	•	≤ 0,5 A	
F 3349	8-channel digital output module	•	•	≤ 0,5 A ≤ 48 V	HB-BLD-3, HB-BLD-4 ¹
F 3422	8-channel relay module		•	≤ 2 A, ≤ 60 V	
F 3430	4-channel relay module	•	•	≤ 4 A, ≤ 250 V	
Analog output modules					
F 6705	2-channel D/A converter	•	•	0...20 mA	HZ-FAN-3 ²
F 6706	2-channel D/A converter		•	0...20 mA	

1. For error display and parameterization of other modes of operation (excluding closed-circuit current).
2. Required for error evaluation in current sink mode.

2 General Notes on the Safety and Availability of Safety-related Output Modules

The safety-related output modules are written in every cycle; the output signals are read back and compared with the output data evaluated by the user logic.

Additionally, a walking bit test over all outputs is performed within the multiple fault occurrence time. The test signal is applied for max. 200 µs. Thus the ability of the outputs to switch is tested without affecting the function of the connected actuators. Due to this, the freezing of each output is detected even if the output signal is a static one.

Safety-related output modules with line monitoring can detect errors in the lead wires going to the load. The line monitoring meets the safety requirements up to SIL 1. The output signal can be used in all applications for safety requirements up to SIL 3.

System H41q/H41qc	System H51q
The output modules are plugged into the system subrack. Kits with 12 slots (H41q) or 13 slots (H41qc) for IO modules are available.	The output modules are plugged into specially designed IO subracks (IOSRs), each having a maximum of 16 slots for IO modules. The required basic components for IOSRs are comprised in kits (see Chapter 2).



If a plant operates in "deenergized to trip" mode, the reaction to a failure of an output module has to be - if no redundancy exists:

- Transition into safe state (if necessary, shutdown)
- Annunciation of the failure.

If a plant operates in "energized to trip" mode (e.g. fire alarm systems, see Chapter 6 Operating Conditions) then - if no redundancy exists - the PES has to do:

- Annunciation of the failure of the output module
- No further reaction possible.

Therefore, a plant-specific solution must exist to enable the transition into the safe state, e.g. by providing a redundant output module, or by monitored operation.

2.1 Safety-related Digital Output Modules

The test routines detect an error by comparing the back-read output signals with the internal output data. The module in the module position detected as defective is put to the safe state by the operating system and indicated on the diagnostic display.

With modules having output circuit monitoring, a detected line break is signaled by the indication of the faulty channel of the module on the diagnostic display. By the integrated safety shutdown the defective module is safely switched off.

In addition to this, one or more shutdown groups can be defined via the H8-STA-3 function block. If one output module in an output group fails, all other output modules belonging to this group are switched off.

Depending on the safety requirements of the system, a complete shutdown of the control can be configured via the IO parameters in the resource properties.

2.2 Safety-related Analog Output Modules

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

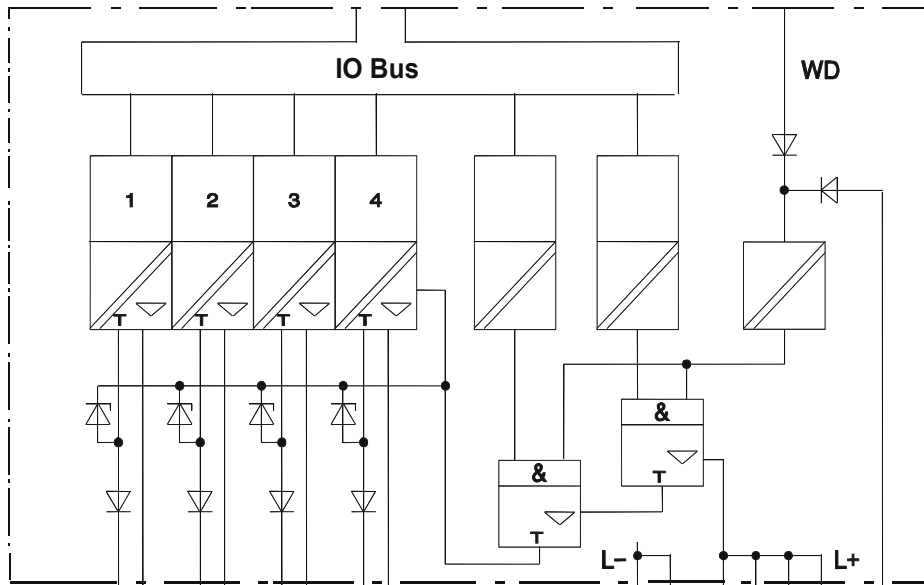
In current source mode, the safe state (output voltage 0 mA) is achieved by the integrated safety shutdown in the event of a failure.

In current sink mode, the safe state can only be achieved by additional measures. The supply voltage for the current loop must be safely shut down by the user program. For the evaluation of errors, the HZ-FAN-3 function block is to be used.

In parallel operation (redundancy) of safety-related analogue output modules, the operational modules process the mean value. In the event of a failure only the value of the operational module is processed.

3 The Principles of Function of Safety-related Output Modules

In safety-related output modules, three testable semiconductor switches are connected in series. Due to this, the required independent second way of shutdown is integrated in the output module. This so-called integrated safety shutdown switches all channels of the defective output module safely off if an error occurs (de-energized state).



Circuit principle of output modules with integrated safety shutdown

3.1 The F 3330, F 3331, F 3333, F 3334, F3335, F 3348, F3349 Safety-related, Digital Output Modules

3.1.1 Test routines

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

1. Reading back of the output signal. The operating point for a 0 signal read back is £ 6.5V. In the event of an error, the value of the 0 signal may rise up to this value and this may not be detected.
2. Reading of the line diagnosis of the switched-on channels (F 3331, F 3334, and F 3349 only).
3. Application of test patterns and testing for crosstalk (walking bit test) within the multiple fault occurrence time.
4. Reading of the line diagnosis of all channels (F 3331, F 3334, and F 3349 only).
5. Test of the integrated safety shutdown.

3.1.2 Response of the System on Failures Detected at Safety-related Digital Output Modules

- If errors are detected on the module, it is put to the safe, de-energized state, i.e. the module is switched off.
- In the event of external short circuits which cannot be distinguished from internal failures, the module is also switched off.
- Line failures are only signalled. They do not result in the module being switched off.

3.2 The F 3430 Safety-related Digital Relay Output Module

3.2.1 Test Routines

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

1. Reading back the output signal of the switching amplifier for the relay switch in 3-channel diversity.
2. Application of test patterns and testing for crosstalk (walking bit test) within the multiple fault occurrence time.
3. Test of the integrated safety shutdown.

3.2.2 Response of the System on Failures Detected at Safety-related Digital Relay Output Modules

- If errors are detected on the module, it is put to the safe, de-energized state, i.e. the module is switched off.
- In the event of external short circuits the fuse for the relevant channel blows. An error message is not generated.

3.2.3 Notes for Projecting with F 3430

Relays are electromechanical elements, and due to their construction they have a limited life. The life of relays depends on the switching capacity of the contacts (voltage/current) and the quantity of switching cycles.

The life at nominal operating conditions is approx 300,000 cycles at 30 V DC and 4 A.

To meet the requirements according to IEC 61508 (PFD/PFH, cf. chapter 1.2) for the modules applies an offline proof-test interval of 3 years for use in SIL 3 and 6 years for use in SIL 2.

The necessary tests are made by the manufacturer.

3.3 The F 6705 Safety-related Analog Output Module

3.3.1 Test Routines

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

1. Reading back of the output signal.
2. Checking the DA converter for linearity.
3. Testing for crosstalk between the outputs.
4. Test of the integrated safety shutdown.

3.3.2 Response of the System on Failures Detected at Safety-related Analogue Output Modules

In current source mode, the module is put to the safe, de-energized state in case an error is detected, i.e. the modules switches off due to its integrated safety shutdown.

An external line break cannot be distinguished from internal failures and results in the module being switched off.

In current sink mode, the safe, de-energized state can only be achieved by external switch-off. The voltage supply for the current loop must be safely switched off by the user program. This is why the HZ-FAN-3 function block must be used for error evaluation.

4 Instructions for the Replacement of Output Modules



We urgently recommend replacing defective output modules.

In the event of a module failure or for maintenance purposes, please follow the steps described below:

- Unscrew the cable connector or pull out the output module with its cable connector plugged in.
- Insert the new output module without its cable connector and fasten by screwing.
- Plug in the cable connector and fasten by screwing.
- Operate the acknowledgement button (push button marked ACK on the central module).


5 Check Lists for Project Planning, Programming and Commissioning Safety-related Output Modules

For each safety-related output module used in a system, a check list must be completed to ensure that all relevant requirements are met. This is to be done during project planning or commissioning. This is the only way to make sure that the requirements are recorded clearly and completely. At the same time, the check lists serve as evidence that project planning has been carried out carefully.


The check lists of this Safety Manual are available as MS Word files (*.doc) on a data medium.

- "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 analogue modules


5.1 F 3330 Safety-related Digital Output Module

				
F 3330 safety-related digital output module (8-channel)		Check list No. SDIGA-F3330-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Has a supplementary circuit with a 4.7 Ω series resistor been implemented for lamp wattages from 4 W to 10 W?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		


5.2 F 3331 Safety-related Digital Output Module

				
F 3331 safety-related digital output module (8-channel)		Check list No. SDIGA-F3331-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in the subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	In case of line monitoring: Does an HB-BLD-3 building block exist for each module in the user program in case of non-redundant operation?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist?	<input type="checkbox"/>	<input type="checkbox"/>	
4	In case of line monitoring: Does one HB-BLD-4 building block exist in the user program for two redundant modules?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is each safety-related output evaluated by the HB-BLD-3 or HB-BLD-4 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
6	Has the HB-BLD-3 or HB-BLD-4 building block been parameterized according to the specific values?	<input type="checkbox"/>	<input type="checkbox"/>	See safety manual, appendix
7	Are at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Has it been ensured that the minimum load for line break monitoring is 10 mA?	<input type="checkbox"/>	<input type="checkbox"/>	
9	Has it been made sure that the signal "line break" must only be evaluated up to SIL 1 in the user program?	<input type="checkbox"/>	<input type="checkbox"/>	
10	Are free-wheeling circuits connected to the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		


5.3 F 3333 Safety-related Digital Output Module

				
F 3333 safety-related digital output module (4-channel)		Check list No. SDIGA-F3333-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are there at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Has it been made sure that at maximum load (2 A) only two channels have the maximal current?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		


5.4 F 3334 Safety-related Digital Output Module

				
F 3334 safety-related digital output module (4-channel)		Check list No. SDIGA-F3334-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in the subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	In case of line monitoring: Does an HB-BLD-3 building block exist for each module in the user program in case of non-redundant operation?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	In case of line monitoring: Does <i>one</i> HB-BLD-4 building block exist in the user program for two redundant modules?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is each safety-related output evaluated by the HB-BLD-3 or HB-BLD-4 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
6	Has the HB-BLD-3 or HB-BLD-4 building block been parameterized according to the specified values?	<input type="checkbox"/>	<input type="checkbox"/>	See safety manual, appendix
7	Are there at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Has it been made sure that at maximum load (2 A) only two channels have the max. current?	<input type="checkbox"/>	<input type="checkbox"/>	
9	Has it been ensured that the minimum load for line break monitoring is 10 mA?	<input type="checkbox"/>	<input type="checkbox"/>	
10	Has it been made sure that the signal "line break" must only be evaluated up to SIL 1 in the user program?	<input type="checkbox"/>	<input type="checkbox"/>	
11	Has a time between 1 ms and 50 ms been set at the input "MAKING CURRENT IN ms" of the HB-BLD-3 or HB-BLD-4 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
12	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

5.5 F 3335 Safety-related Digital Output Module


				
F 3335 (Ex)i Safety-related digital output module (4-channel)		Check list No. SDIGA-F3335 Version 2.0/32.05		
Project data				
Project designation	File name of check list/ archiving number			
	Position in subrack / IOSR			
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Is there a forced convection for the module with a fan just below?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
4	Are the electrical data of the connected valves below the output characteristic of the module F 3335?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
5	Are the special requirements met for the application of the (Ex)i module as stated in the data sheet?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
6	Are the special (Ex)-requirements met for use of parallel connections in redundancy?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
7	Is the engineering made exclusively according to the approved modifications?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
Date		Created by		

5.6 F 3348 Safety-related Digital Output Module


				
F 3348 safety-related digital output module	Check list No. SDIGA-F3348 Version 2.0/32.05			
Project data				
Project designation	File name of check list/ archiving number			
	Position in subrack / IOSR			
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are there at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Are the output leads correctly connected and laid considering safe electric insulation? *	<input type="checkbox"/>	<input type="checkbox"/>	
6	Are cables with double or reinforced insulation used for the connection wiring? *	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

* according to IEC 61131-2 Ed 2:2003 no longer required if the use of the module meets SELV or PELV conditions

5.7 F 3349 Safety-related Digital Output Module


				
F 3349 safety-related digital output module (8-channel)		Check list No. SDIGA-F3349-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in the subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	In case of line monitoring: Does an HB-BLD-3 building block exist for each module in the user program in case of non-redundant operation?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Does a redundant module exist for this module?	<input type="checkbox"/>	<input type="checkbox"/>	
4	In case of line monitoring: Does one HB-BLD-4 building block exist in the user program for two redundant modules?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is each safety-related output evaluated by the HB-BLD-3 or HB-BLD-4 building block?	<input type="checkbox"/>	<input type="checkbox"/>	
6	Has the HB-BLD-3 or HB-BLD-4 building block been parameterized according to the specific values?	<input type="checkbox"/>	<input type="checkbox"/>	See safety manual, appendix
7	Are there at most 10 output modules energized with rated load assembled within one IOSR?	<input type="checkbox"/>	<input type="checkbox"/>	
8	Has it been ensured that the minimum load for line break monitoring is 10 mA?	<input type="checkbox"/>	<input type="checkbox"/>	
9	Has it been made sure that the signal "line break" must only be evaluated up to SIL 1 in the user program?	<input type="checkbox"/>	<input type="checkbox"/>	
10	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

5.8 F 3430 Safety-related Digital Output Module

				
F 3430 Safety-related digital output module		Check list No. SDIGA-F3430 Version 2.0/32.05		
Project data				
Project designation		File name of check list/ archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do the relay circuits have fuses with max. current of 4 A?	<input type="checkbox"/>	<input type="checkbox"/>	
3	Are free-wheeling circuits provided at the actuators?	<input type="checkbox"/>	<input type="checkbox"/>	
4	Are the output leads correctly connected and laid considering safe galvanic isolation?	<input type="checkbox"/>	<input type="checkbox"/>	
5	Is intended to replace the module after end of the relay life?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet (regard switching cycles)
6	Is the required test by the manufacturer intended (for SIL 3 use every 3 years, for SIL 2 use every 6 years)?	<input type="checkbox"/>	<input type="checkbox"/>	see data sheet
7	Are cables with double or reinforced insulation used for the connection wiring? *	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

* according to IEC 61131-2 Ed 2:2003 no longer required if the use of the module meets SELV or PELV conditions

5.9 F 6705 Safety-related Analogue Output Module

				
F 6705 safety-related digital output module		Check list No. SANAA-F6705-E Version 2.0/32.05		
Project data				
Project designation		File name of check list / archiving number		
		Position in subrack / IOSR		
Requirements for the project planning of the module and the user program				
No.	Requirement	fulfilled		Comment
		yes	no	
1	Are the outputs of this module named which perform a safety-related function?	<input type="checkbox"/>	<input type="checkbox"/>	
2	Are unused channels bridged to avoid error messages from modules? Channel 1: Bridge b6 - b8 Channel 2: Bridge b22 - b24	<input type="checkbox"/>	<input type="checkbox"/>	
Redundant current connection				
3	Are the channels switched in parallel used in the same mode of operation (current source mode or current sink mode)?	<input type="checkbox"/>	<input type="checkbox"/>	
4	In case of redundant connection: Are the connected actuators capable of tolerating a current burst to the half or the double value for 2 to 3 cycles?	<input type="checkbox"/>	<input type="checkbox"/>	
Date		Created by		

For Your Notes

Chapter 5 Software

1 Software for Safety-related HIMA H41q/H41qc and H51q Automation Devices

The software for the safety-related HIMA automation devices of the H41q/H41qc and H51q system families is subdivided into three blocks: operating system, user program and programming tool according to IEC 61131-3 (ELOP II system software package with integrated safety tool).

The operating system is to be used in its latest applicable version which is TÜV certified for safety-related applications. This version can be found in the common document „List for tracing the version releases pertaining to the modules and Firmware of the Company HIMA Paul Hildebrandt GmbH + Co KG“. This document is created by the common modification service of TÜV Product Service GmbH - IQSE and HIMA.

The user program is created with the help of the ELOP II system software package and contains the plant specific functions which the automation device is to perform. The ELOP II system software is the parameterizing platform for operating system functions. The user program is compiled into the machine code by a code generator. This machine code is transmitted to the Flash-EPROMs of the central module of the automation device via a serial interface.

The main functions of the operating system and the specifications for the user program derived from them are listed in the table below:

Functions of the operating system	Specification in user program
Cyclical processing of the user program	Function blocks, functions, variables
HIMA standard function blocks (included in the operating system)	Standard function blocks, variables
Configuration of the automation device 1 or 2 IO buses, number of power supply modules, etc.	Determination by the resource type
Reload of the user program	possible adherence to restrictions (see ELOP II Resource Type H41q/H51q Manual)
Tests in the central area and in the IO bus	- - -
Tests of IO modules (depending on the type)	Type of IO module
Response in the event of a failure	in parts specified, in other parts configurable
Diagnostic display	- - -
Diagnosis mode for testable IO modules	HZ-DOS-3 function block diagnosis, not safety-related
Communication via serial interfaces with personal computer permissible actions during operation	ELOP II Determination in the resource type
External coupling to master system	Variable declaration, Variable names, BUSCOM
External coupling to slave systems	Variable declaration, HK-MMT-3 function block
Event transmission	Variable names, event controlled
PES master, not safety-related	Variable declaration, HIPRO-N communication
PES master Ethernet communication, safety-related	Variable declaration, safety-related HIPRO-S communication
Master systems with 3964R protocol	Variable declaration, 3964R
Logic plan controlled logging	Variable declaration, event controlled, protocol texts

2 Safety Aspects concerning the Operating System

2.1 Designation, Current Approved Version for Safety-related Applications (CRC Signature)

Each new operating system is identified by its designation. The signature of the operating system serves to further identify the operating system. This signature can be retrieved on the diagnostic display during operation of the automation device. The current applicable versions of the operating system, TÜV approved for safety-related automation devices, and their corresponding signatures (CRCs) can be found in the report enclosed in the certificate for the HIMA H41q/H51q automation system.

2.2 Signatures of the User Program

Code version number

The code version number is generated via the functions of the programmed logic. The function of the control can be viewed on a PC only if the code version of the program in the control and in the programming device are the same.

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. of forced information
- Shifting of lines or modules, respectively (but only if the sequence of operation is not influenced)
- 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 (but do not necessarily have to) result in a change of the code version number. With all other changes, the code version number changes as well.

Run version number

The run version number is generated during operation by the control itself. By comparing it with a currently valid and documented run version number, you can see whether the program in the control has been influenced in the meantime (see by calling it on the diagnostic display).

The run version number will be changed if:

- there is a different code version number (not at all types of modifications)
- modules are inserted or deleted
- system parameters change
- VAR_CONST is inserted or deleted
- VAR_CONST values are changed
- the resource type is changed
- settings are changed online
- force values of IO variables in the online test field are changed
- the position of the force mains switch is changed.

Data version number

The data version number refers to the definition of non-safety-related imported or exported variables. It will change if:

- the name of a variable with attributes for HIPRO (not safety-related) changes
- these variables are compressed at the generation of a non-reloadable code (if memory gaps exist).

Area version number

The area version number records all variables defined in a project. It will change if:

- modules are deleted or new modules are set
- if more variables are allocated to the attributes of the following types than are deleted: HIPRO-N, HIPRO-S, BUSCOM, event, 3964R
- the memory has to be reorganized. This may occur when the capacity limit of the memory is reached and if gaps have formed in memory allocation due to prior repeated generation of codes.

Changes of the basic addresses for external/MODBUS coupling may (but do not necessarily have to) result in a change of the area version number.

2.3 Procedures and Functions of the Operating System

The operating system processes the user program in cycles. The following shows this sequence in simplified form:

- Reading of input data
- Processing of the logic functions according to IEC 61131-3 Section 4.1.3
- Writing of output data.

The cycle also comprises the following essential functions:

- Extensive self tests
- Tests of the IO modules during operation
- Data transfer and data comparison.

A cycle is processed in seven stages. These stages are shown in detail in the operating system manual HI 800 105.

3 Safety Aspects Concerning Programming with ELOP II

For implementing the application program, the programming tool *ELOP II* is used. It can be used on standard PCs running the operating system Windows. The current version of the tool is applicable on Windows 2000® and Windows XP®.

3.1 The ELOP II Safety Concept

The ELOP II safety concept ensures that

- the programming system (PS) works correctly, i.e. programming system errors are detected,
- the user uses the PS correctly, i.e. user errors are detected.

When a safety-related control is commissioned, the safety of the complete system is checked by an overall function test. The two above points will be verified. Until now, after a modification of a user program, another complete function test had to be performed to ensure the safety-related function of the system.

The safety tool of ELOP II according to IEC 61131-3 is now designed to check only the modifications in the user program. This safety tool detects user errors and programming system errors.

The safety tool of ELOP II consists of three sections which are important for safety:

- C code comparator
- target code comparator
- proven GNU-C compiler.

With the C code comparator modifications made to the user program are identified. The target code comparator compares two target codes subsequently generated by the GNU-C compiler (GNU-CC). This method prevents errors caused by a non-safety-related PC.

Non-safety-related tools are:

- The revision management in ELOP II. This can only be used for the identification of the relevant project versions
- The offline-simulation shown in the flow chart in chapter 3.1.2. The offline-simulation verifies the user program against the specification but without influence to the process.

3.1.1 Application of the Safety Tool of ELOP II for the Creation of the Program

1. The user program is generated according to a binding specification (e. g. according to IEC 61508, DIN V VDE 0801 or a corresponding user standard); in the flow chart the points (1) to (4).
2. The modified user program is compiled into the C code by the C code generator and additionally a comparison file is generated; point (5).
- 3.



For the user program, a cross-reference list has to be generated and checked for correct use of the variables. It has to be verified that all variables are used only in those places provided by the specification.

4. The C code and the comparison file are compiled by the proven compiler (GNU-CC), points (6) and (13). The target code and the comparison code are generated.
- 5.



The target code comparator must be activated; point (14). It compares the target code and the comparison code. Errors caused by a non-safety-related PC are detected and signaled.

6. The program generated in this way is now ready to run and it is loaded into the H41q/H51q system (point 7). There the program must be tested completely by the user and accepted (point 8).
7. A backup of the target code is generated and the PES starts safety-related operation.

3.1.2 Application of the Safety Tool of ELOP II for Program Modifications

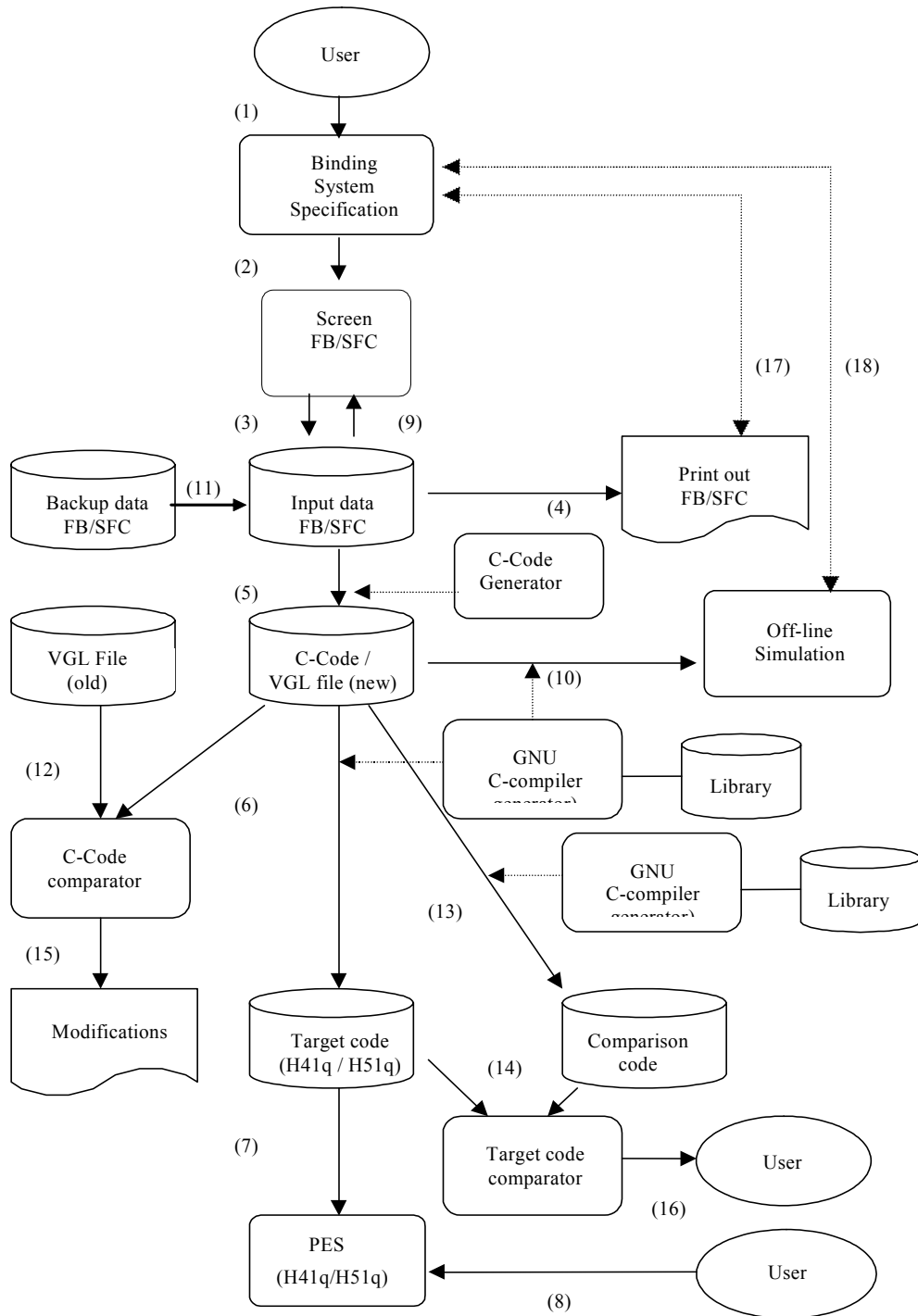
1. The user program is modified according to a mandatory specification (e. g. according to IEC 61508, DIN V VDE 0801 or corresponding user standard); in the flow chart this refers to points (1) to (4).
2. For the modification the backup of the running user program is used. This backup contains
 - the VGL file
 - the target code
 - input data.
3. The modifications of the user program are entered.
- 4.



The modified user program is (newly) compiled into the C code by the C code generator; point (5).

5. The C code comparator must be activated; point (12). It compares the new C code with the old C code of the previous program version; point (11). The backup must be indicated as the comparison file (old C code).

6. The result of the comparison, point (15), is documented.
7. The user checks whether the C code comparator indicates all the changes made to the user program. Only code relevant changes are indicated.
8. If the C code comparator
 - a) indicates changes which the user does not recognize, this may have the following reasons:
 - the modification made by the user results in further modifications which were not planned
 - there is an internal error.
 - b) does not indicate modifications made by the user, this may be due to the following:
 - there are changes which the C code comparator does not recognize, e. g. graphical modifications or modifications of initial values
 - changes have been incorrectly adopted.
9. The new C code (new) and the comparison file (new) are compiled by the proven C compiler (GNU-CC); points (6) and (13). The target code and the comparison code are generated.
10. The target code comparator must be activated; point (14). It compares the target code with the comparison code. Errors caused by a non-safety-related PC are detected and signalized.
11. This so generated program free of errors is now ready to run and it is loaded into the H41q/H51q system. All modified parts of the program must now be tested by the user. By testing the changes the user can verify whether the target code is correct.
12. If there is no malfunction, a backup of the new, current program must be generated. The PES can start safety-related operation.



Flow chart, function of the safety tool

3.1.3 Program Identification Possibilities



The user program can be clearly identified by its code version number. This way the associated backup can be clearly determined.

If the user is not sure which backup is the correct one, the backup in question has to be compiled (with download option), and then the target code is to be compared with the code version

of the loaded program.

But for reloadable code, this is only possible, if the code had been generated in the following way:

1. Do the last change
2. Generate reloadable code (compile), results in code version A
3. Load control device with code version A
4. Generate reloadable code, results in code version B, may be identical to code version A
5. Load Control device with code version B
6. Each additional code generation without change results in code version B.

Modification management

With the help of modification management, the user can administrate his program versions. With the help of document administration and the version check, the user can document the modifications indicated by the C code comparator.

Using document administration, you can collect various ELOP II objects in one document object in order to

- commonly print out these documents and to
- have a common revision maintenance.

The supplementary product - Version Management - of ELOP II is used to store and manage ELOP II objects in an archive. These data may be copied from the archive any time for further processing.

For the time being, the data of the following objects can be stored and administrated in an archive:

- POU (program type, function, type of function block)
- data type
- global variable
- program/type instance
- task
- document object.

The following possibilities are provided

- Saving of the working version of the object as a version in the archive
- Copying an object version from the archive.

Note: In project management you can further process the current object version after archiving one. As all versions of the object are stored in the archive, you can copy a version from the archive other than that most recently saved.



If an object version is copied from the archive, it will replace the working version in project management.

For further explanations, see the online help of the ELOP II program.

3.1.4 Check of the User Program to Meet the Specified Safety-related Function

The user has to perform a number of suitable test cases covering the specification. It is not necessary to perform 220 test cases for a 20-channel AND gate. Normally the independent test of each input and the most important logic circuits should be sufficient. This extent of test case is sufficient since the measures implemented in the software program ELOP II since version 2.1 and the measures described in the safety manual ensure a sufficient correct semantic and syntactic code containing no undetected errors of the process of the code generation.

Also for the numeric evaluation of forms a suitable number of tests have to be performed. It makes sense to create equivalence class tests. That means tests in the defined range of values, at the limits and in not permitted ranges of values. The tests have to be selected in that way that the correctness of the calculation has to be established. The necessary number of tests depends on the used formula and has to consider critical pairs of values.

The online test facility can be used to support the tests, e. g. to enter values or to check intermediate values. However, an active simulation with sensors and actuators has to be performed to establish the correct wiring and function of sensors and actuators. In addition only this is the way to establish the correctness of the system configuration.

3.2 Guidelines for the ELOP II User

Definitions

New load

This term means that a program is loaded either as download or reload mode into the PES (formerly expression: PLC).

Download

If a program is loaded into the PES in download mode, all outputs of the PES will be reset and the PES will be stopped.

Reload

If a user program is loaded into a redundant PES in reload mode, the modified user program for the central modules will be loaded one after the other. One central module will always be in operation (MONO) and the system will not be stopped.

The outputs of a PES having only one central module will be held during the reload process.

The reload mode requires the prior generation of a reloadable code.

3.3 Parameterization of the Automation Device

The parameters listed below determine the reaction of the automation device during operation. They are set in the menu for resource properties.

3.3.1 Safety

Here the permissible actions of the automation device in safety-related operation are determined and the safety-related parameters are given.

Safety-related parameter	
Safety time in s	Depending on process
Watchdog in ms	Maximum half the safety time
Test operation	reset
Start/Restart	reset
Change of constants	reset
Change of variables (forcing of variables in the OLT)	reset
Forcing (main switch and individual switches)	reset
Reload	reset
Change of configuration (change of safety parameters)	reset



The safety time must **not** be set to the value **255 s!** Only the value range **1 to 254** is permitted!



The allocations possible during safety-related operation are not rigidly bound to one SIL. They have to be coordinated with the test authority in charge for each application of the automation system.

3.3.2 Failures in Safety-related Output Amplifiers

Parameter “Display only“

Switch off by means of the integrated safety shutdown inside the output amplifier. If not possible then shutdown of the watchdog signal in the IO rack by means of the coupling module (only in systems H51q). No shutdown of the watchdog signal of the appertaining central unit. This parameter is permissible only up to SIL 1.



Parameter “Emergency off“


Switch off of the watchdog signal of the appertaining central unit and thus shutdown of the output amplifiers.



Parameter “Normal operation“

Reaction as with parameter “Display only“, additionally switch off of the watchdog signal of the appertaining central unit if necessary. Parameterization required from SIL 2. Normal and recommended parameter.

3.4 Check list: Measures Required for the Creation of a User Program

			
Measures required for the creation of a user programme		Checklist No. MEAP-0001-E Version 2.1 / 02.07	
Project data			
Project designation		File name of checklist / archiving number	
Notes, verifications	yes	no	Comments
Prior to change			
Is the configuration and the user program based on a safety assessment?			
Are programming guidelines used to create a user program?			
Are only tested and approved programming organization units (functions, function blocks, program) used to create the user program?			
Are functionally independent parts of the PES encapsulated by the use of function and function building blocks?			
Is it taken into consideration that after a change of variable names and subsequent reload a re-initialization of the variables is performed?			
Is it taken into consideration that after a reload, set outputs will remain set although these set outputs are not assigned a value after the deletion of parts of the user logic?			
If the online change of a constant is to be retained after reload: Has this constant been adapted accordingly in the program prior to the generation of the code?			

After modification			
Notes, verifications	yes	no	Comments
Prior to loading			
Have all force markers been removed from the application program?			
Has a review of the user program against the binding specification been performed by a person not involved in the implementation of the program?			
Has the result of the review been documented and released (date/signature)?			
Has an off-line test been performed?			
After loading			
Is the RUN version of the program which can be changed online identical to the RUN version of the program adapted after an on-line change of constants?			
Check at the diagnostic display: Has the desired program been loaded?			
Check at the diagnostic display: Does the error display show non-existing modules or other error messages?			
Has a backup of the complete program been made after the program has been loaded into the PES?			
Has an online test been performed?			
Has a sufficient number of tests been performed for all safety-related logical circuits (including inputs and outputs) and for all mathematical calculations (intermediate results, limits etc.)?			
After the rejection of a modification of an online constant: Has the program been reloaded or has the constant been reset online to its original value?			
Has the correct data transmission to other systems been tested?			
Has forced information been reset prior to safety-related operation?			
Date	Created by		

3.5 Reload (Reloadable Code)

The formerly used term „online changes“ has been replaced by “reload”.



Reload is only possible after consultation with the test authority in charge of plant acceptance. For the duration of the reload, the person in charge has to ensure appropriate safety-related monitoring of the process by other technical and organizational measures.



Prior to each reload, the changes in the user program as compared to the user program still running have to be determined using the C code comparator contained in the safety-tool ELOP II.



Before they are transmitted to the PES, the reloads have to be tested carefully using simulators.



If a function is deleted in a reload, e. g. a function controlling a physical output, the process image remains unchanged. Therefore all the outputs affected by a reload must be deleted. That means the outputs to be deleted by a reload have to be reset before the reload.



If an input variable (VAR_INPUT) of a function block is no longer written after a reload (e.g. because the variable or assignment left of the function block has been deleted), the input variable keeps its former value and is not reset automatically to FALSE / 0!

This behaviour concerns all function blocks, but not the functions. The cause of this behaviour is the fact that during reload all values of all variables are stored to make possible a continuous operation. Inputs of standard and user-defined function blocks are processed internally as variables.

Remedy: such an input must be connected to a new variable set to the desired value.



All variables with the attribute „const“ are set to their initial value again during a reload even if they were assigned other values online.



All system parameters are set to their configured value again during a reload even if they were assigned other values online. This may have influence on watchdog, safety time, baud rate of the interfaces, and many other things.

If a reload of the user program of the central module(s) is possible, this is indicated by the mes-

sage „Code reloadable“ during the compilation run of the code generators.

Reloadability is lost if

- modules are inserted or deleted in the cabinet,
- more variables are allocated to the attributes of the following types than are deleted: HIPRO-N, HIPRO-S, BUSCOM, event, 3964R
- the basic addresses for BUSCOM are changed,
- system variables are inserted or their allocations are changed,
- names of HIPRO-S variables are modified.

3.5.1 Systems with one Central Module



If a reload is performed in systems having only one central module, this change must be performed within in the fault tolerance time of the process.

While the user program is being loaded, there is no access to the IO level, i.e. IO modules are not read / written or tested.

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

3.5.2 Systems with Redundant Central Modules

Reload of automation devices having redundant central modules are possible without adhering to the restrictions relating to the single-channel systems mentioned above.

After the start of the reload, the second central module continues processing the user program in mono mode while the first central module is being loaded. Then the newly loaded central module receives the current data from the central module in operation and takes over mono operation with the new user program. When the second central module has been loaded, it receives the current data and both central modules go to redundant operation.

3.6 Offline Test

Changes in the user program can be simulated with the offline test in ELOP II. This simulation is an excellent means of assessing the effects of a change. It is, however, not sufficient for the validation of the changes made in safety-related controls. This requires a test in the actual control or in a simulator.

3.7 Forcing



Forcing is only possible after consultation with the test authority in charge of plant acceptance. For the duration of the forcing process, the person in charge has to ensure appropriate safety-related monitoring of the process by other technical and organizational measures.



When forcing is to be done in safety-related controls, the latest applicable version of the document „Maintenance Override“ issued by TÜV Rheinland and TÜV Product Service must be obeyed.

Forcing possibilities provided to the user:

- Forcing can be forbidden by the configuration. In this case, the PES does no longer accept forced values with user-specific definition. New forced values can only be set after the system has been switched off.
- When the user exits the control panel, he will be shown if any and how many forced values are still set.
- Inputs and outputs may be reset by two separate force main switches.

For further details on the forcing procedure are stated in the User Manual.



Before starting the safety-related operation, all force markers must be removed from the application program.

Details of force markers are described in the online help of ELOP II.

3.8 Protection against Manipulations



The user must determine the measures for the protection of the system against manipulation in co-operating with the test authority in charge.

Protective mechanisms are integrated in the PES and in the programming system ELOP II which prevent unintentional or unauthorized changes to the safety system.

1. In the PES the system parameters can be set in way that a change of the program is not possible without reloading.
 2. The ELOP II programming system has a hardlock and can additionally be protected against unauthorized access by the password mechanisms provided in Windows®.
-



The requirements for the safety and application standards concerning protection against manipulation have to be obeyed. The operator is responsible for the authorization of employees and the necessary protective measures.

4 Safety Aspects Concerning the User Program

4.1 General Programming Procedure for Automation Systems of the H41q/H51q Families for Safety-related Applications

- Specification of the control function
- Writing of the user program
- Verification of the user program by an offline simulation
- Compilation of the user program with the C code generator
- The C code is compiled twice by the proven C compiler (GNU-CC); the target code and the comparison code are generated.
- The target code comparator compares the target code with the comparison code. Errors caused by a non-safety-related PC are detected and signaled.
- The program thus generated is error free and ready to run. It is loaded into the H41q/H51q system. There the program can be tested by the user and the PES can start safety-related operation.

4.2 Use of Standard Function Blocks for Safety-related Applications

The following list shows the HIMA standard function blocks for safety-related applications. The description of the function of these function blocks can be found on the internet site www.hima.com and on the CDROM.

4.2.1 Standard Function Blocks Independent of the IO Level

Type	Function	TÜV test	
		safety-related	non-interacting
H8-UHR-3	Date and time		•
HK-AGM-3	PES master monitoring		•
HK-COM-3	Monitoring of communication module		•
HK-LGP-3	LGP evaluation and configuration		•
HK-MMT-3	MODBUS master		•
HA-LIN-3	Temperature linearization	•	
HA-PID-3	PID controller	•	
HA-PMU-3	Measuring transducer, capable of being parameterized	•	

4.2.2 Standard Function Blocks Depending on the IO Level

Type	Function	TÜV test	
		safety-related	non-interacting
H8-STA-3	Group formation of safety-related testable outputs	•	
HA-RTE-3	Monitoring of analogue testable input modules F 6213 / F 6214	•	
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 analogue testable input modules F 6221	•	
HF-CNT-3	Counter function block for F5220 module	•	
HF-CNT-4	Counter function block for F5220 module	•	
HF-TMP-3	Configuration function block for F6220 module	•	
HZ-FAN-3	Error display for testable IO modules		•
HZ-DOS-3	Non-safety-related diagnosis		•

In the „TÜV test“ column „•“ indicates that a TÜV safety certificate exists for the corresponding function block. For the safety-related application of the function blocks, please refer to the documentation of these function blocks.

The following function blocks can be used in safety-related applications but not for safety-related functions:

H8-UHR-3, HK-AGM-3, HK-LGP-3, HK-MMT-3, HZ-FAN-3, HZ-DOS-3.

For further notes see the internet site www.hima.com or the CDROM.

4.3 Prerequisites and Rules for the Use in Safety Applications (Requirements from Prototype Certificates etc.)

The user program is entered into the PC via ELOP II programming system. This program is suitable for computers with the Windows® operating system. In addition to this, the PC must be equipped with a HIMA hardlock module.

The essential parts of the ELOP II programming system are the following:

- Entry (function block editor), monitoring and documentation
- Variables with symbolical names and type of variable (BOOLEAN, UINT etc.)
- Allocation of the resource type (HIMA automation systems H41q/H51q)
- Code generator (compilation of the user program into the machine code with C code generator and GNU-C compiler).

4.3.1 Basic Programming

The task to be performed by the control is to be laid down in the form of a specification. This documentation is the basis of correct implementation into the program. How this task is actually specified depends on the kind of task. This may be:

Combinatorial logic

- Cause / effect scheme
- Logic of the combination with functions and function blocks
- Function blocks with specified characteristics.

Sequential controls (sequence control systems)

- Verbal description of the steps with step enabling conditions and actuators to be controlled
- Sequence diagrams according to DIN EN 60848
- Matrix or chart form of the step enabling conditions and the actuators to be controlled
- Definition of the marginal conditions, such as operation modes, EMERGENCY OFF etc.

The Process I&C technology concept of the plant must contain the analysis of the field circuits, i.e. the kind of sensors and actuators:

Sensors (digital or analogue)

- Signal in normal operation (closed-circuit current principle for digital sensors, life-zero for analogue sensors)
- Signal in the event of an error or failure
- Determination of redundancies required for safety-related operation (1oo2, 2oo3)
- Monitoring of discrepancies and response.

Actuators

- Position and activation during normal operation
- Safe response/position in the event of a shutdown or power failure.

The created user program should be

- easy to understand
- easy to trace
- easy to change.

4.3.2 Variable Declaration and Entering of Process I&C Names

With the help of the variable declaration editor, the variables and their data types are defined. Symbolical names are allocated to all variables of the user program. These symbolical names may have up to 256 characters.

For physical inputs and outputs symbolical Process I&C names are used which also may have up to 256 characters.

For the user the use of symbolical names instead of the physical address has two essential advantages:

- In the user program the plant names of inputs and outputs are used.
- Changes of the allocation of the signals in the input and output channels do not affect the user program.

4.3.2.1 Allocation of Process I&C Names with Variable Names

The measuring point list or a list of the sensors and actuators should serve as the basis of the allocation of Process I&C names with variable names.

Variable names are allocated to the hardware used in the notebook for the resources under „Process cabinet“. The desired subrack position (1-1 to 1-8 or 2-1 to 2-8, respectively) and type, the slot and type of the required module as well as the Process I&C names to be allocated to the variable names are entered into the notebook.



For practical reasons the variable name and the Process I&C name should be the same.

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

We recommend assembling the input and output modules used in the IO subracks into functional groups.

Groups may be formed under the following aspects:

- a) Grouping according to plant parts
 - the same way of arranging the modules in the groups, e.g.
 - 1) digital / analogue plant parts
 - 2) safety-related / non-safety-related IO modules
 - redundant grouping in the various IO subracks in the same order

- b) Spare modules or spare channels for later reloads (reloadable code)

variable declaration of the program instance.

It is possible to provide Boolean variables with the 'event' attribute. Events are signal changes of Boolean variables with additional information about the point of time (date and time). The time stamp of an event corresponds to the time of the automation device with millisecond precision.

4.3.3 Functions of the User Program

Programming is not restricted in any way by the hardware. The functions of the user program are freely programmable. When programming make sure that the closed-circuit current principle at the inputs and outputs is obeyed. A line break will e. g. result in the shutdown of the corresponding actuator.

- Unlike in the case of hard-wired safety-related controls, „line breaks“ do not have to be considered in the logic functions (user program) in programmable logic controls.
- Any negations are permissible.
- 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 analogue input module, a defined value will be processed. For further information, see the description of the function blocks in the Manual „ELOP II Resource Type“.

If an error occurs in a safety-related digital input/output module, an input will be set to safe „0“, and the digital output module will be switched off by the integrated safety shutdown. For further information, see the description of the function blocks in the Manual „ELOP II Resource Type“.

Unlike hard-wired controls, programmable logic controls are provided with a more extensive range of functions, especially with byte and word processing.

4.3.3.1 Group Shutdown

The safety-related modules used for a certain plant area (e.g. a burner) can be assembled in a group. For this purpose, the H8-STA-3 function block is entered in the user program for each group. In this function block all the positions of the output amplifiers belonging to one group are set. If one output module fails, all the output amplifiers belonging to this group are shut down. For the safety of the system, the integrated safety shutdown of the output modules alone is sufficient.

4.3.3.2 Function Blocks for Individual Safety-related IO Modules

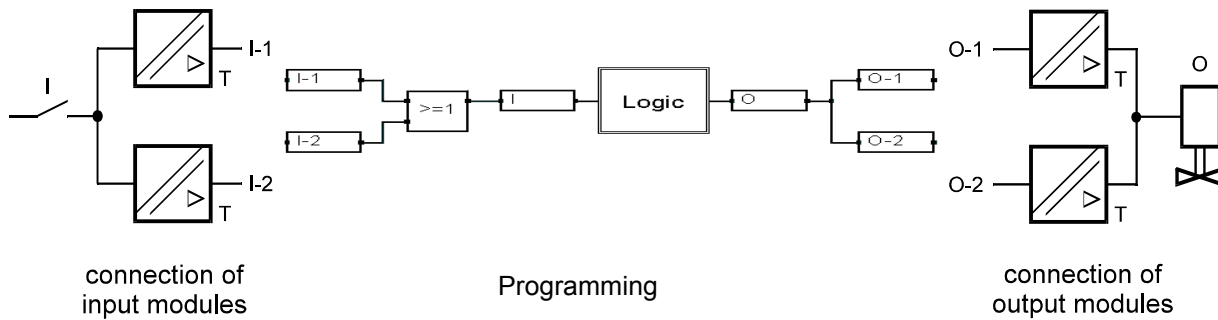
Input module		Output module	
digital		digital	
	Function Block		Function Block
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
analogue		analogue	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		

Input module		Output module	
F 6221	HF-AIX-3		

For the safety-related IO modules the associated function blocks must be entered into the user program. For further information see Appendix, check list and description of the function blocks in the Manual „ELOP II Resource Type“.

4.3.3.3 Redundant IO Modules

To increase availability without affecting safety, safety-related input or output modules can be switched in parallel as shown in the sketch below. Maximum availability is achieved, if in this case also automation devices with 2 IO buses are used and if the redundant IO signals are input into separate IO modules.



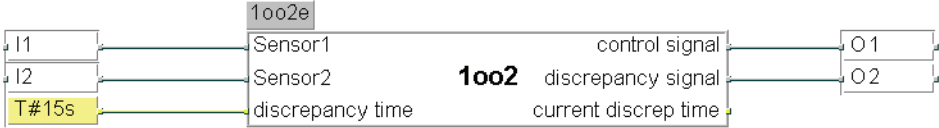
Parallel IO modules for increasing the availability

4.3.3.4 Redundant, Non-safety-related Sensors

Hardware

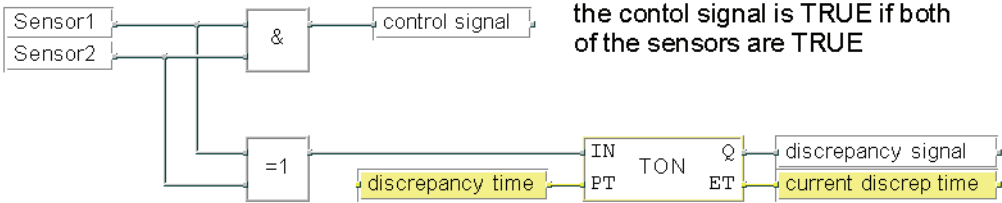
Depending on the type of the control signal (mechanical contact, proximity switch, intrinsically safe / not intrinsically safe) input modules type F 3236, F 3237 or F 3238 are used. The two sensors operate in a 1oo2 configuration, e. g. after the response of one of the sensors the safety-related circuit is switched off at once. A discrepancy is indicated after a preset time. This function can be included in a function for the input module F 3236. For input modules type F 3237 or F 3238 the block HB-RTE-3 is available

User program, input module F 3236.



input signals

signals to logic / annunciation



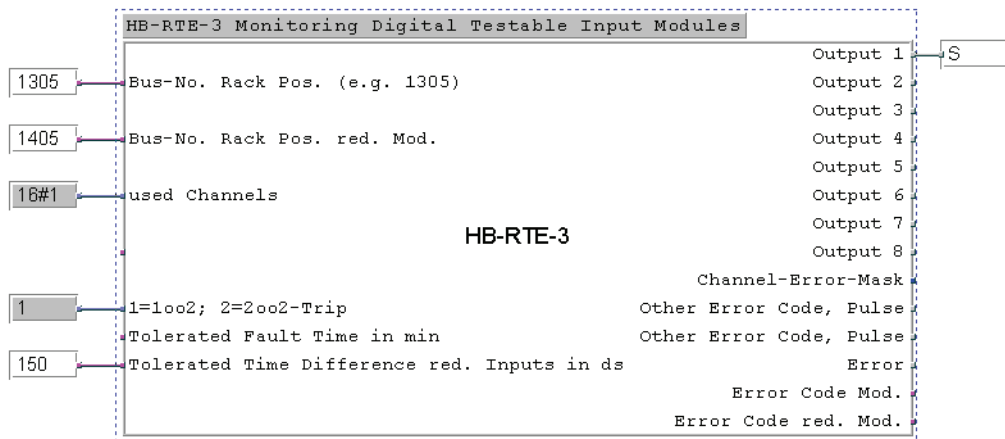
the contol signal is TRUE if both of the sensors are TRUE

discrepancy signal is TRUE if the sensor signals differ after the discrepancy time has elapsed

Function block 1002 and logic of the function block

User program, F 3237 or F 3238 input module

Use of the HB-RTE-3 function block



The signals S-1 and S-2 are directly connected to the first channels of the module F 3237 or F 3238. No other hardware allocation.

Safety aspects

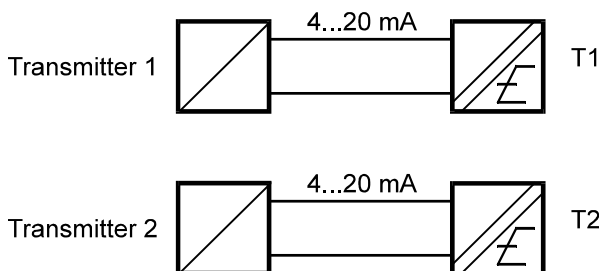
If one of the sensors responds or if a component inside the system fails, the system is switched off. As 'normal' sensors are used, we recommend checking the sensor circuits at regular intervals (e. g. after a couple of months), if the signals are not switched through the process within shorter periods of time. In addition to this, we recommend monitoring to verify whether the signals are equal (logic with F3236 input module) or parameterization of the HB-RTE-3 function block (F 3237, F 3238 input modules).

Availability aspects

No availability, as each component failure results in a shutdown.

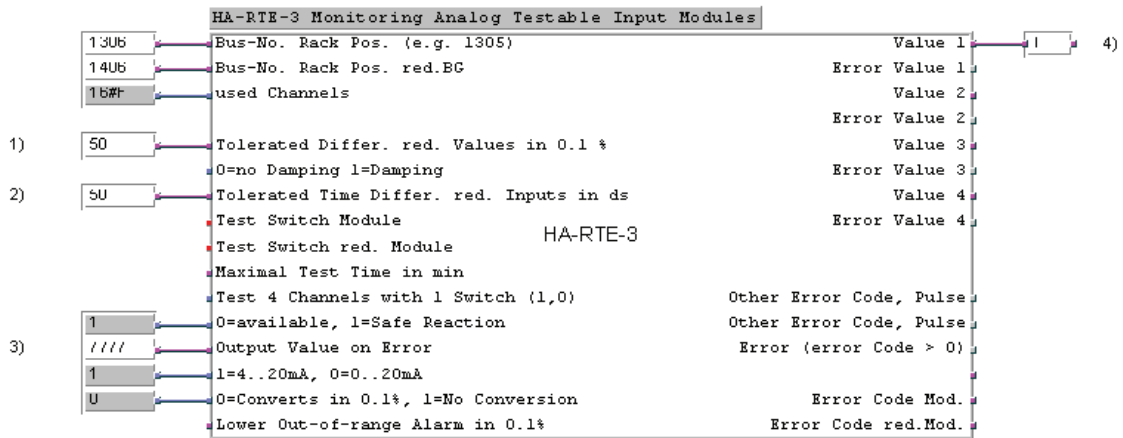
4.3.3.5 Analog Redundant Transmitters

Hardware wiring



User program, F 6213 or F 6214 input module

Use of HA-RTE-3 function block

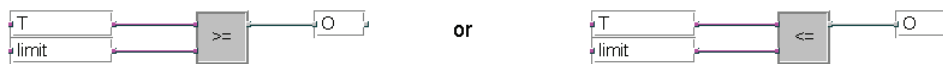


The signals T1 and T2 are directly connected to the first channels of the module F 6213 and F 6214. No other hardware allocation.

- 1) e. g. 50
- 2) e. g. 50
- 3) 7777, if physical value becomes larger in case of danger (all four channels of the module),
0000, if physical value becomes smaller in case of danger (all four channels of the module)
- 4) Values 0...1066

Note: numerical values are parameter values at the function block, not absolute quantities

Comparing element for alarm or shutdown if the permissible limit value is achieved



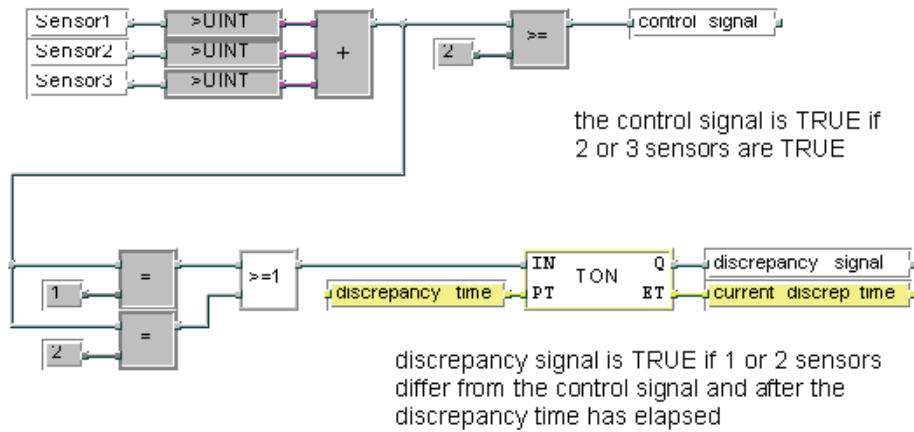
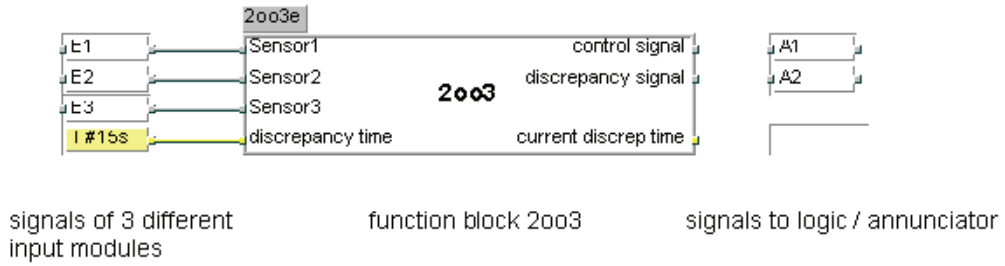
Safety aspects

If one of the transmitters responds or if a component inside the system fails, output A has L signal. As 'normal' transmitters are used, we recommend checking the sensor circuits at regular intervals (e.g. after a couple of months), if the signals are not switched through the process within shorter periods of time. In addition to this, we recommend monitoring to verify whether the signals are equal (parameterization of the HA-RTE-3 function block).

Availability aspects

No availability, as each component failure or the response of a sensor results in a shutdown.

4.3.3.6 Input Modules with 2oo3 Circuit



Function block 2oo3 and logic of the function block



For practical reasons the circuits shown above are combined to form the function block “2003”.

In a PES with two IO buses the sensor signal of the second sensor is connected to two input channels, one at a channel of the 1st IO bus and one at a channel of the 2nd IO bus. In the user program these 2 signals are OR-gated. It is also possible to connect in parallel all the 3 sensor signals to each IO bus and then three times OR-gated in the user program. Then the function block like shown above is used.

Notes concerning sensors



The user should not only consider the availability of the electronic modules but also the safety of the sensors. If no safety-related sensors exist, two sensors can be installed in the same measuring point and combined with a 1oo2 circuit. If safety and availability are required, three sensors are installed in one measuring point and combined with a 2oo3 circuit. In both cases discrepancy monitoring of the two or, respectively, three sensor signals is required.

4.4 Program Documentation for Safety-related Applications

The ELOP II programming system allows the automatic printout of the documentation of a project. The most important kinds of documentation are the following:

- Interface declaration
- List of variables
- Logic
- Description of data types
- Configurations of the cabinet, subracks, modules and system parameters
- Process I&C/variables cross-reference
- Code generator information

The layout of the various kinds of documentation is freely adjustable.

The documentation is part of the function acceptance of a plant subject to approval by an inspection authority (TÜV). The function acceptance only applies to the user function but not to the safety-related HIMA automation devices H41q-MS, H51q-MS, H41q-HS, H51q-HS, H41q-HRS, H51q-HRS. These devices have a prototype certificate.



For plants subject to approval, we recommend for the project planning to engage the authority in charge as soon as possible.

5 Safety Aspects for Communication (Safety-related Data Transmission)

The communication protocol HIPRO-S is certified for SIL 3.

5.1 Safety-related Communication

In the notebook 'Resource properties' the data exchange with safety-related allocated resources can be monitored via the PES master. For this purpose a monitoring time can be set as 'Time Interval' parameter, and the command 'delete imported variables' can be activated as soon as the monitoring time is exceeded.

The monitoring time to be set depends on the process and must be agreed with the acceptance authority.

The safety-related communication can also be effected via the F 8625, F 8626, F 8627(X), and F 8628(X) Ethernet communication modules. They use the protocol "safeethernet" certified by TÜV.

5.2 Time Requirements

In order to achieve a constant transmission time, we recommend providing a separate PES master and a separate bus for safety-related data transmission with a baud rate of 57.6 kbit/s.

The data transmission time T_T taken from the point of time a sensor at a PES changes up to the point of time an output responds at another PES is the following:

$$T_T = 2 \cdot ZZ_1 + 2 \cdot T_D + 2 \cdot ZZ_2$$

ZZ_1 cycle time of PES 1

ZZ_2 cycle time of PES 2

T_D data transmission time between two PES, depending on the type of data connection used:

Serial data connection: use the value of the bus cycle time. To determine the bus cycle time, refer to the operating system manual, section "Safety-related data transmission via HIPRO-S".

Ethernet connection: assume the maximum transmission time, refer to the datasheet of the F 8627 (X), section "Calculating the Monitoring Time for HIPRO-S / HIPRO-S DIRECT Connections".

As the import variables are updated at regular intervals, a monitoring time can be set via the SIO parameters in the dialog for resource properties. The relevant factor is the applicable safety-delay time of the plant PESs. If no imported safety-related variables are written within the defined period of time, this fact is annunciated by setting a system variable. Moreover, the user can parameterize that all those variables in the automation device are set to 0 in this case.

5.3 Instructions for the Creation of the User Program

The Ethernet network in ELOP II for HIPRO-S is configured automatically. However, the following items have to be obeyed when the user program is created:



The resource name in ELOP II must have eight characters of which the last two must be numbers. Numbers between 0 and 64 can be used. The numbers must be unique so that they can be used without the risk of collision to determine the IP address in the communication module.



Safety-related communication with HIPRO-S in NORMAL mode is to be designed in a way that each automation device is configured for safety-related data exchange with every other automation device (i.e. exchange of dummy data, if no user data are exchanged).
If using HIPRO-S-DIRECT mode, this is not necessary (no dummy data have to be exchanged).



To check the HIPRO-S configuration the PES master program is to be compiled. If errors have occurred, they are to be corrected afterwards.



For the safety-related communication the transmission data "Zero" must be the safe state.



Remove all force markers before starting the safety-related operation and before certification by an authority.

6 Use for Central Fire Alarm Systems according to DIN EN 54-2 and NFPA 72

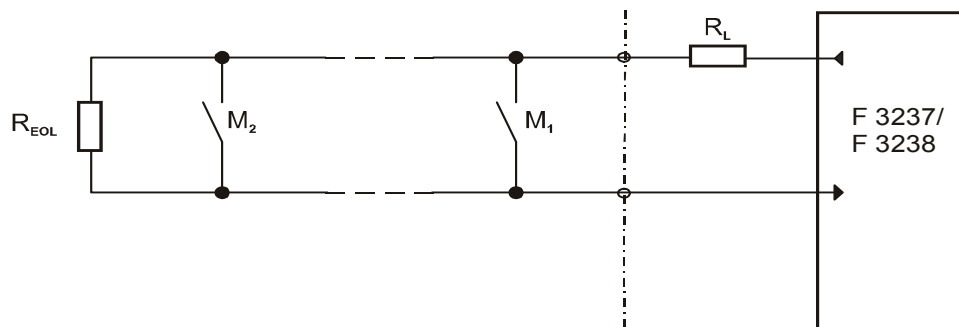
The H41q/H41qc and H51 systems can be used for central fire alarm systems according to DIN EN 54-2 and NFPA 72.

For this purpose the user program must comply with the functions of central fire alarm systems according to the mentioned standards.

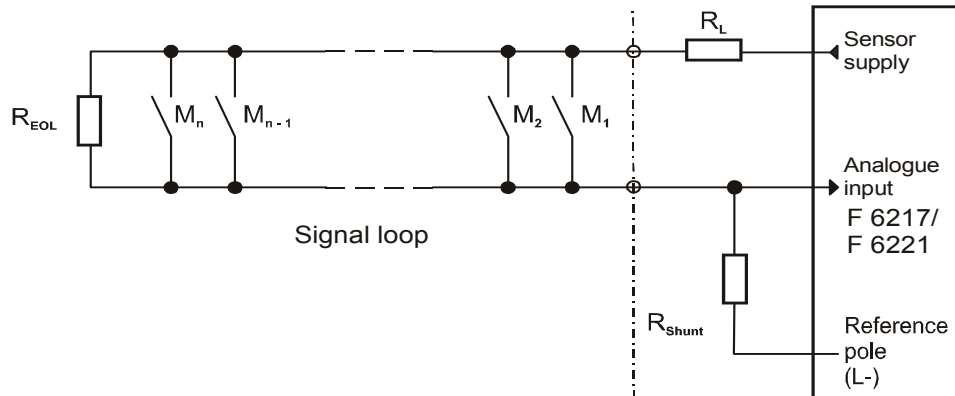
The maximum cycle time for central fire alarm systems of 10 seconds, as it is required in DIN EN 54-2, can easily be fulfilled by the H41q, H41qc and H51q systems, as the cycle times of these systems are in a range < 0.5 seconds, also the possibly requested safety time of 1 second (fault response time).

The connection of the fire alarm boxes (call points) is carried out in the open-circuit principle with monitoring for line break and short circuit. Here the F 3237 / F 3238 input modules can be used for boolean connections or the F 6217 / F 6221 for analogue connections with the following external wiring:

boolean connections



analogue connections



Wiring of fire alarm boxes:

- M Fire alarm box (call point)
- R_{EOL} Termination resistor at the last sensor of the loop
- R_L Limitation of the maximum admissible current of the loop
- R_{shunt} Measuring shunt

For the application the resistors R_{EOL} , R_L and R_{Shunt} must be dimensioned depending on the sensors and their quantity in a loop. Therefore also the data sheets of the sensor manufacturers must be regarded.

Additionally the specified current values of the F 3237 and F 3238 modules (cf. data sheets) must be considered. This is especially true for fire detectors without mechanical contacts, but electronic outputs.

The alarm output circuits for controlling lamps and audible alarms etc. are also carried out in the open-circuit principle. Therefore output modules with monitoring for line break and short circuit must be used, for instance the F 3331 or F 3334 output modules.

The control of visualization systems, indicator light panels, LED displays, alphanumeric displays, audible alarms etc. can be realized with an according user program. For this purpose other products can be used.

The transmission of fault signals via input/output modules or to transmission modules for fault signals must be made in the closed-circuit principle.

The transmission of fire alarms between HIMA systems can be realized by using the communication standards available such as MODBUS, HIPRO-S, or OPC (Ethernet). Monitoring of the communication is part of the user program. It is recommended using redundant communication to ensure transmission even if a transmission component (line, hardware fault, etc.) fails. The failure of a component must be indicated and it should be possible to replace or repair the faulty component during operation.

The H41q/H41qc or H51q systems used as control and indicating equipment must have redundant power supplies. Precautions must be taken in case the electricity supply system fails, for example battery operated alarm horns. The switch-over between mains supply and stand-by supply is to be carried out fast enough to ensure uninterrupted duty. Voltage drops up to 10 ms are admissible.

During malfunctions of the system, the system variables defined in the user program are written by the operating system. So an error signalling for the failures detected by the system can be programmed. Safety-related inputs and outputs are switched off in the case of an error, i. e. processing of Low-signals in all channels of the faulty input module and switch-off of all channels of the faulty output module.

For Your Notes

Chapter 6 Operating Conditions

The safety-related controls H41q, H41qc and H51q are developed to observe the requirements of the following standards for EMC, climate and environmental conditions.

IEC 61131-2	Programmable Controllers, Part 2 Equipment Requirement and Tests
IEC 61000-6-2	EMC Generic Standard, Part 6-2 Immunity for Industrial Environments
IEC 6100-6-4	Electromagnetic compatibility (EMC) Generic Emission Standard, Industrial Environment

1 Climatic Conditions

The most important tests and limits for climatic conditions are listed in the table below:

EN 61131-2 Chapter 6.3.4	Climatic Tests
	Temperature, operating: 0...+60 °C (Test limits: -10...+70 °C)
	Storage temperature: -40...+80 °C (with battery: only -30 °C)
6.3.4.2	Dry heat and cold, withstand test: +70 °C / -25 °C, 96 h EUT power supply unconnected
6.3.4.3	Change of temperature, withstand and immunity test: -25 °C / +70 °C and 0 °C / +55 °C EUT power supply unconnected
6.3.4.4	Cyclic damp heat, withstand test: +25 °C / +55°C, 95% relative humidity EUT power supply unconnected

2 Mechanical Conditions

The most important tests and limits for mechanical conditions are listed in the table below:

EN 61131-2 Chapter 6.3.5	Mechanical Tests
	Vibration test, operating: 5...9 Hz / 3.5 mm 9...150 Hz / 1 g
6.3.5.1	Immunity vibration test: 10...150 Hz, 1 g, EUT operating, 10 cycles per axis
6.3.5.2	Immunity shock test: 15 g, 11 ms, EUT operating, 2 cycles per axis

3 EMC Conditions

The most important tests and limits for EMC conditions are listed in the table below:

EN 61131-2 Chapter 6.3.6.2	Noise Immunity Tests
6.3.6.2.1 IEC/EN 61000-4-2	ESD test: 4 kV contact / 8 kV air discharge
6.3.6.2.1 IEC/EN 61000-4-3	RFI test (10 V/m): 26 MHz...1 GHz, 80% AM
6.3.6.2.1 IEC/EN 61000-4-4	Burst test: 2 kV power supply / 1 kV signal lines
6.3.6.2.1 IEC/EN 61000-4-12	Damped oscillatory wave immunity test: 1 kV

IEC/EN 61000-6-2	Noise Immunity Tests
IEC/EN 61000-4-6	Radio frequency common mode: 10 V, 150 kHz...80 MHz, AM
IEC/EN 61000-4-3	900 MHz pulses
IEC/EN 61000-4-5	Surge: 1 kV, 0,5 kV

	Noise Emission Tests
EN 61000-6-4 EN 50011 Class A	Emission test: radiated, conducted

4 Power Supply Conditions

The most important tests and limits for the power supply conditions are listed in the table below:

EN 61131-2 Chapter 6.3.7	Verification of DC Power Supply Characteristics
	The power supply must meet alternatively the following standards: IEC 61131-2 or SELV (Safety Extra Low Voltage, EN 60950) or PELV (Protective Extra Low Voltage, EN 60742)
	The fusing of the systems H41q, H41qc and H51q must be in accordance to the statements of the data sheets
6.3.7.1.1	Voltage range test: 24 V DC, -20 %...+25 % (19.2...30.0 V DC)
6.3.7.1.2	Momentary interruption immunity test of the external power supply: DC, PS 2: 10 ms
6.3.7.4.1	Reversal of DC power supply polarity test: see application note in the concerning chapter of the system manual or in the data sheet of the power supply module
6.3.7.5.1	Backup duration withstand test: Test B, 1000 h, Lithium battery is used for backup

For Your Notes

Appendix

1 Standard Function Blocks for the Central Area

For functions of the central modules, standard function blocks can be called and allocated. You can find a detailed description of these function blocks in the Manual „ELOP II Resource Type“.

1.1 Function Block HK-AGM-3

With this function block the function of an H51q automation device serving as HIPRO master is monitored.

This function block has no safety relevance. Its outputs are for information purposes only and no safety-related action in the user program must be derived from it.

1.2 Function Block HK-COM-3

With this function block the function of the communication modules in a system H41qc or H51q is monitored.

This function block has no safety relevance. Its outputs are for information purposes only and no safety-related action in the user program must be derived from it.

1.3 Function Block HK-MMT-3

With this function block an H41q, H41qc or H51q automation device can be used as MODBUS master.

This function block has no safety relevance. Its outputs are for information purposes only and no safety-related action in the user program must be derived from it.

1.4 Function Block H8-UHR-3

This function block allows external setting or changing of the date and time of the automation device.

The outputs of this function block are for information purposes only, and no safety-related action in the user program must be derived from them.

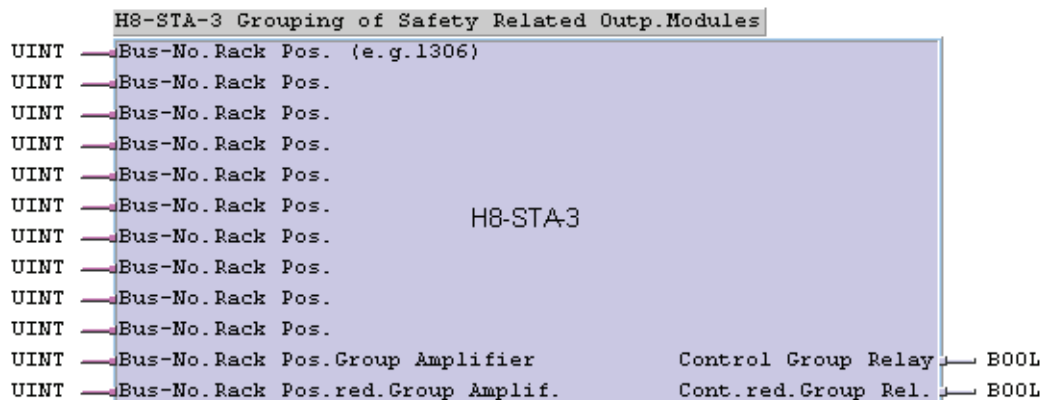
2 Allocation of Standard Function Blocks for the IO Area

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

The special programming instructions described in this section must be adhered to. For more detailed information on the functions of these function blocks and the allocation of the inputs and outputs, please refer to the Manual „ELOP II Resource Type“.

2.1 Function Block H8-STA-3

This function block is used to configure group shutdown. It is used once in the user program for each shutdown group.



Function block inputs:

The positions of the modules belonging to a shutdown group are designated by a four-digit decimal number according to the determination in the selected resource.

Example: „1306“ means:

Cabinet 1, subrack 3, module position 06

For one of the inputs 'Bus No. Rack Pos. Group Amplif.' or 'Bus No. Rack Pos. red. Group Amplif.', a possible but non-existent slot has to be entered.

Module outputs:

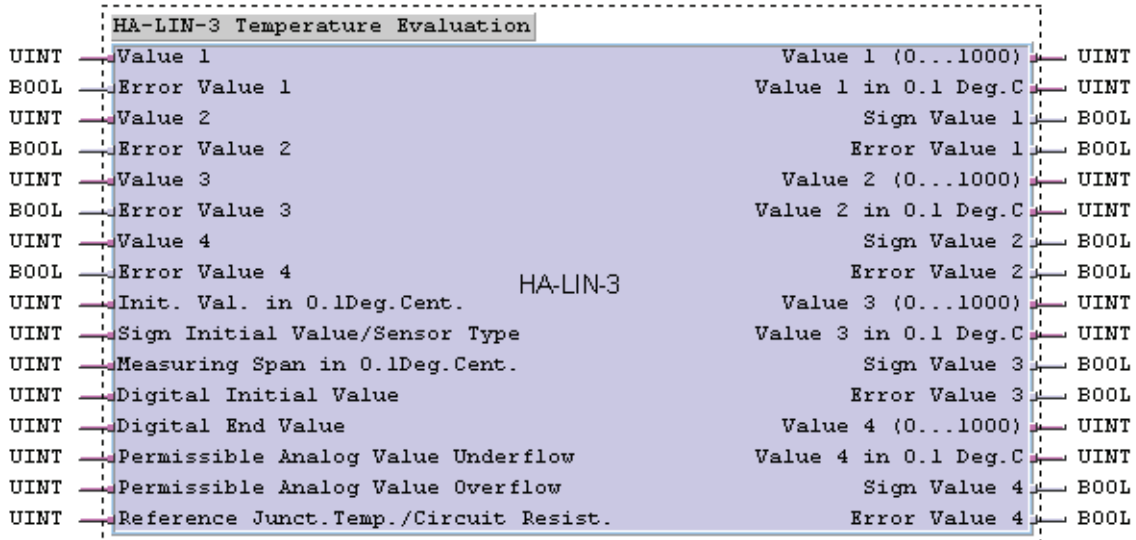
Names of the group amplifier channels. Further programming in the logic of the user program is not necessary.



Output modules having integrated safety shutdown do not need group shutdown. However, group shutdown may be configured for these modules. In this case all modules belonging to a group are switched off if one output module fails (according to the settings in function block H8-STA-3).

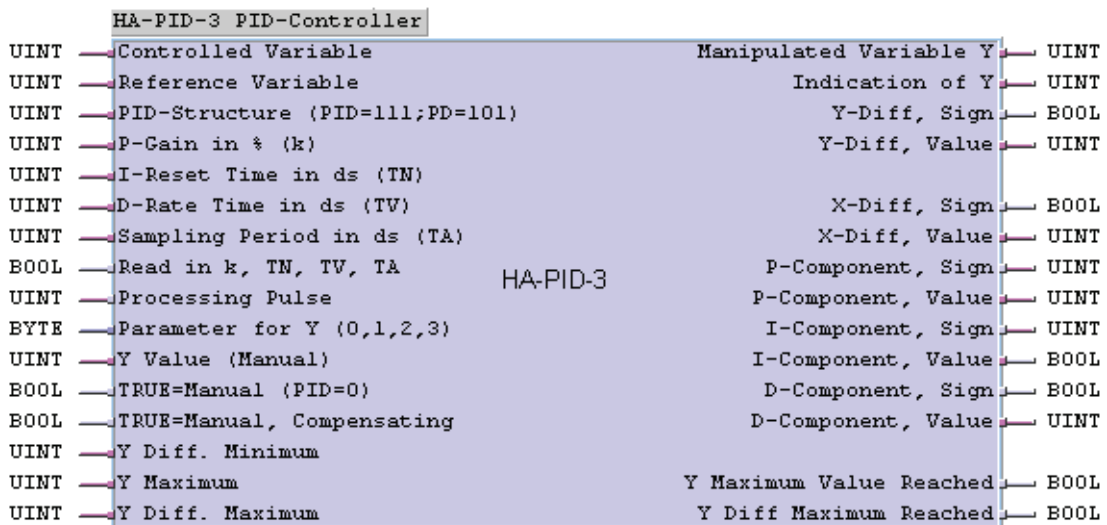
2.2 Function Block HA-LIN-3

This function block is used to linearize temperature measurements with thermocouples and Pt 100 resistance thermometers. Correct parameterization must be verified if the values are to be used for circuits relevant to safety (see Manual „ELOP II Resource Type“).



2.3 Function Block HA-PID-3

This function block contains a digital control which can be operated in the following modes: P, I, D, PI, PD and PID. The mode must be determined by parameterisation.



Function block inputs:

„H signal = manual (PID = 0)“ and „H signal = manual, Compensating“

If this control function block is used in safety-related operation, these inputs may not be allocated. Any deviations from this must be approved by the authority in charge of acceptance.

Online changes of parameters and constants are only permissible upon permission of the responsible acceptance authority and in monitored operation.

The allocation of the function block inputs with non-safety-related imported variables is not allowed.

Function block outputs:

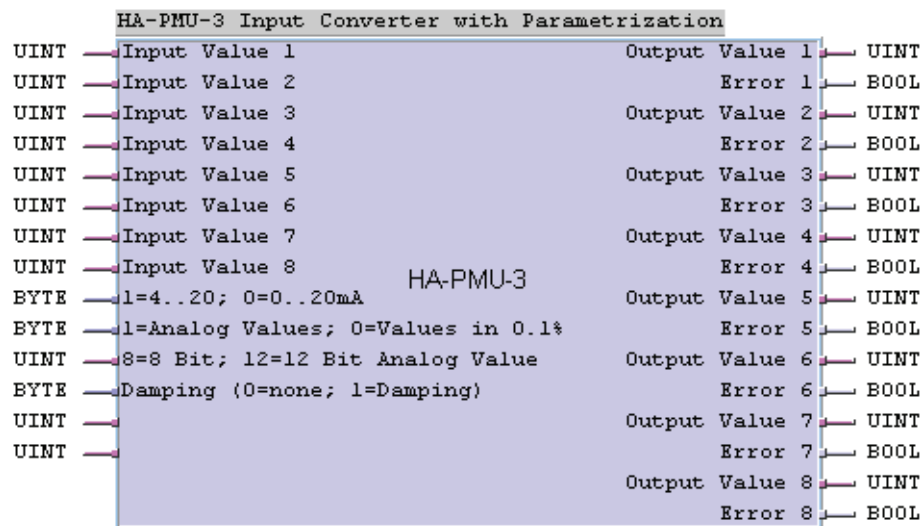
A safety shutdown is only permissible via:
 "Y Maximum Value Reached" and „Y Diff Maximum Reached"
 Any deviations from this must be approved by the responsible acceptance authority.



The safe state of a plant cannot be achieved in every case by the control algorithm of the function block alone. In the specific case, additional measures may become necessary.

2.4 Function Block HA-PMU-3

This building is used for both the conversion of digitized measuring values into %o values and the conversion of %o values into digitized analogue values. Correct parameterization has to be verified if these values are used for the shutdown of safety-relevant circuits (see Manual „ELOP II Resource Type“).



2.5 Function Block HA-RTE-3

This function block is used to process values and to indicate errors of safety-related analogue input modules in single-channel or redundant operation. It must be used once in the user program for each safety-related analogue input module (F 6213/F 6214). If two parallel, redundant IO modules are used, the function block must exist only once in the user program.

HA-RTE-3 Monitoring Analog Testable Input Modules			
UINT	Bus-No. Rack Pos. (e.g. 1305)	Value 1	1
UINT	Bus-No. Rack Pos. red.BG	Error Value 1	1
BYTE	used Channels	Value 2	1
		Error Value 2	1
UINT	Tolerated Differ. red. Values in 0.1 %	Value 3	1
BYTE	0=no Damping 1=Damping	Error Value 3	1
UINT	Tolerated Time Differ. red. Inputs in ds	Value 4	1
MOS A	Test Switch Module	Error Value 4	1
MOS A	Test Switch red. Module		
UINT	Maximal Test Time in min		
BYTE	Test 4 Channels with 1 Switch (1,0)	Other Error Code, Pulse	1
BYTE	0=available, 1=Safe Reaction	Other Error Code, Pulse	1
UINT	Output Value on Error	Error (error Code > 0)	1
BYTE	1=4..20mA, 0=0..20mA		1
BYTE	0=Converts in 0.1%, 1=No Conversion	Error Code Mod.	1
UINT	Lower Out-of-range Alarm in 0.1%	Error Code red.Mod.	1

Inputs:

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

"Bus No. Rack Pos. red. Mod"

Position of the safety-related analogue input module and, if existing, the redundant module designated by a four-digit decimal number.

Example: "1305" means:

Cabinet 1, subrack 3, module position 05 (for redundant operation, the redundant module must be given a different position)

"0=no Damping, 1=Damping"

1 only for redundant operation. The difference taken from the current value and the value of the previous cycle is added to the permissible difference in 0.1 % („Tolerated Differ. red. Values in 0,1 %“).

"Maximal Test Time in min"

Limitation of the testing time given in minutes. After the testing time elapses, the actual value is processed in the user logic. See also the "Maintenance Override" information issued by TÜV Bavaria and TÜV Rhineland. This information is part of the HIMA USD service.

Outputs:

"Value1...4"

The use of the values must be checked if these values are used for the shutdown of safety-related circuits.

"Error value 1...4"

The outputs must be allocated to be able to trigger a shutdown in the case of an error by their Boolean signal.

The other outputs are for information purposes only, and no safety-related action in the user program must be derived from them.

2.6 Function Block HB-BLD-3

This function block is used for error evaluation and display related to the channels of the safety-related digital output modules types F 3331, F 3334, and F 3349. It must be used only once for each module.

HB-BLD-3 Testb.Baugr, Leit.-Diagnose, Monobetrieb			
UINT	Bus-No. Rack Pos. (e.g. 1305)	Channel Fault Mask	UINT
UINT	Mode Channel 1 (0,1,2)	Error Channel 1	BOOL
UINT	Mode Channel 2 (0,1,2)	Error Channel 2	BOOL
UINT	Mode Channel 3 (0,1,2)	Error Channel 3	BOOL
UINT	Mode Channel 4 (0,1,2)	Error Channel 4	BOOL
UINT	Mode Channel 5 (0,1,2)	Error Channel 5	BOOL
UINT	Mode Channel 6 (0,1,2)	Error Channel 6	BOOL
UINT	Mode Channel 7 (0/1/2)	Error Channel 7	BOOL
UINT	Mode Channel 8 (0/1/2)	Error Channel 8	BOOL
UINT	Max. Time Inrush Current in ms	Pulse on Error	BOOL
		Pulse on Error	BOOL
		Error	BOOL
		Error Code	UINT

Inputs:

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

Position of the safety-related digital output module designated by a four-digit decimal number.

Example: „1305“ means:

Cabinet 1, subrack 3, module position 05

„Mode Channel n (0/1/2)“

Allocation by 1:

Normal operation. Detected error is signaled by H-signal at corresponding output „Error channel n“. The output circuit of the module is closed.

Allocation by 0:

Error evaluation, error messages are suppressed

Allocation by 2:

Only applicable if permitted by the plant specifications. Inverted operation, i.e. the output circuit is to be open.

In safety-related control circuits the closed-circuit principle must always be applied.

„Max. Time Inrush Current in ms“

Determination of the delay time for the detection of a line break or time allowed for the tolerating of the current limit. During this time, the error display is suppressed. An increase of the delay time results in an increase of the cycle time.

The outputs „Pulse on Error“ (2x), „Error“ and „Error code“ are for information purposes only, and no safety-related action in the user program must be derived from them.

2.7 Function Block HB-BLD-4

This function block is used for channel-related error evaluation and display for safety-related digital output modules types F 3331, F 3334, and F 3349 in redundant operation. It must be used only once for a pair of redundant modules.

HB-BLD-4 Testable red.Outp.Modules with Line Diagnostic			
UINT	Bus-No. Rack Pos. (e.g. 1305)	Channel Fault Mask Mod. 1	UINT
UINT	Bus-No. Rack Pos. red. Mod.	Channel Fault Mask Mod. 2	UINT
UINT	Mode Channel 1 (0,1,2)	Error Channel 1	BOOL
UINT	Mode Channel 2 (0,1,2)	Error Channel 2	BOOL
UINT	Mode Channel 3 (0,1,2)	Error Channel 3	BOOL
UINT	Mode Channel 4 (0,1,2)	Error Channel 4	BOOL
UINT	Mode Channel 5 (0,1,2)	Error Channel 5	BOOL
UINT	Mode Channel 6 (0,1,2)	Error Channel 6	BOOL
UINT	Mode Channel 7 (0,1,2)	Error Channel 7	BOOL
UINT	Mode Channel 8 (0,1,2)	Error Channel 8	BOOL
UINT	Max. Time Inrush Current in ms, Mod.	Pulse on Error	BOOL
UINT	Max. Time Inrush Current in ms, red.Mod.	Pulse on Error	BOOL
		Error	BOOL
		Error Code Mod.	UINT
		Error Code red. Mod.	UINT

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, the redundant module designated by a four-digit decimal number.

Example: „1305“ means:

Cabinet 1, subrack 3, module position 05

„Mode Channel n (0/1/2)“

Allocation by 1:

Normal operation. Detected error is signaled by H signal at corresponding output „Error Channel n“. The output circuit of the module is closed.

Allocation by 0:

Error evaluation, error messages are suppressed

Allocation by 2:

Only applicable if permitted by the plant specifications.

Inverted operation, i.e. the output circuit is to be open.

In safety-related control circuits the closed-circuit principle must always be applied.

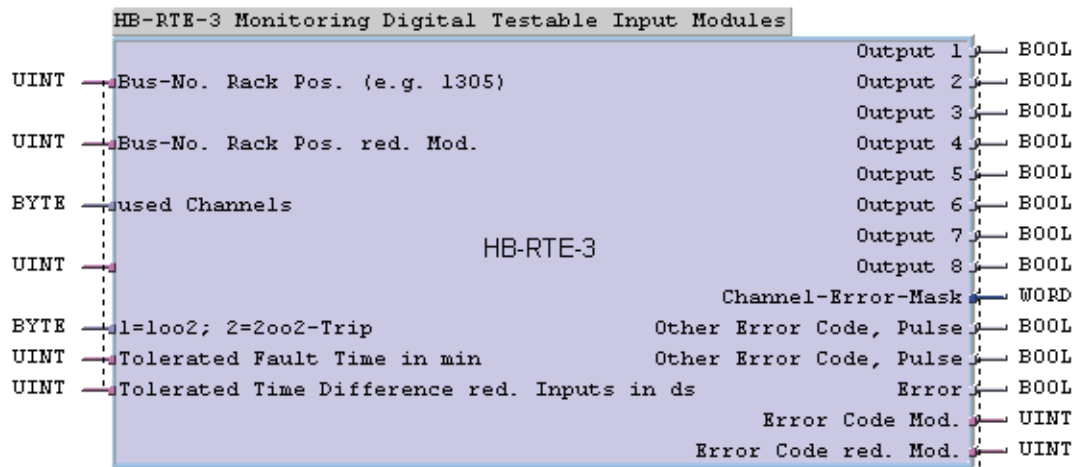
„Max. Time Inrush Current in ms, Mod.“ and „Max. Time Inrush Current in ms, red. Mod.“

Determination of the delay time for the detection of a line break or time allowed for the tolerating of the current limit. During this time, the error display is suppressed. An increase of the delay time results in an increase of the cycle time.

The outputs „Pulse on Error“ (2x), „Error“, „Error Code Mod.“ and „Error Code red. Mod.“ are for information purposes only, and no safety-related action in the user program must be derived from them.

2.8 Function Block HB-RTE-3

This function block is used for evaluating and displaying errors of safety-related digital input modules in single-channel or redundant operation. It must be used once in the user program for each input module type F 3237 or F 3238, or respectively, for two input modules type F 3237 or F 3238 working in parallel.



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, the redundant module given as a four-digit decimal number.

Example: 1305 means:

Cabinet 1, subrack 3, module position 05

„1 = 1oo2; 2 = 2oo2-Trip“

Allocated by „1“

„Tolerated Fault Time in min“

No effect on the shutdown within the indicated time after a sensor test, component failure or line error. Must be approved by the acceptance authority in charge.

„Tolerated Time Difference red, Inputs in ds“

Time difference of the switching points between two redundant sensors. The time depends on the sensors. Must be approved by the acceptance authority in charge.

The outputs „Channel Error Mask“, „Other Error Code, Pulse“ (2x), „Error“, „Error Code Mod.“ and „Error Code red. Mod.“ are for information purposes only and no safety-related action in the user program must be derived from them.

2.9 Function Block HF-AIX-3

The function block HF-AIX-3 is used for parameterization and evaluation of one channel of the safety-related analogue (Ex)i input module F 6221. with a resolution of 0...10,000.

For each channel of the F 6221 module one HF-AIX-3 function block is required in the user program.

HF-AIX-3 Voltage or Current measurement for F6221	
Bus-No. Rack Pos (e.g.1305)	Value
Channel-No. (1..8)	
HF-AIX-3	
Enable configuration	Active
Mode (1=0.01%, 2=digits, 3=scaling/physical)	
Live Zero	
Scaling minimum value for 0/4 mA	
Scaling maximum value for 20 mA	
Monitor transmitter voltage	
Underflow level in 0.1 mA (32=3.2 mA)	Underflow
Overflow level in 0.1 mA (210=21 mA)	Overflow
Recalibration	
MOS (TRUE=test operation)	
Maximum time for test operation in min	Remaining time
	Error
Value on Error	Error code

The analogue input module has one safety-related output per channel, controlled independently from the cycle of the central unit. The status of this output is indicated at the output of the HF-AIX-3 function block and can be processed by the user program.

Via parameter settings the value of the analogue input module can additionally be converted and spread.

By entry of a value at the function block input "Value on error" this value is switched to the output "Value" in case of channel or module errors as well as in case of measurement range overflow or underflow, and in the user program it can be processed instead of the actual value.

2.10 Function Block HF-CNT-3

The HF-CNT-3 function block is used to configure the two channels of the F 5220 safety-related, 24-bit resolution counter module and to evaluate the signals. The counter module can be used for pulse counting, measuring of frequencies or rotational speeds and for detection of the sense of rotation.

For each F 5220 counter module one HF-CNT-3 function block is required in the user program.

```

HF-CNT-3 Counterblock for F5220
Bus-No. Rack Pos. (e.g. 1305)

Counter channel 1

Enable Configuration
Signal type (1=5V; 2= 24V; 3= initiator)          Counter (24 bit)
Preset value                                       Output state
Gate in 50ms                                       Rotation direction
Maximum deviation of frequency                    (TRUE = right; FALSE = left)
Counting mode (1=right,left;2=right;3=left)      Line break/Short circuit
                                                    Active

Reset counter
Stop counter
MOS (TRUE = testoperation)
Maximum time for testoperation in min             Remaining time
Forcevalue for testoperation

Counter channel 2                                HF-CNT-3

Enable Configuration
Signal type (1=5V; 2=24V; 3= initiator)          Counter (24 bit)
Preset value                                       Output state
Gate in 50ms                                       Rotation direction
Maximum deviation of frequency                    (TRUE = right; FALSE = left)
Counting mode (1=right,left;2=right;3=left)      Line break/Short circuit
                                                    Active

Reset counter
Stop counter
MOS (TRUE = testoperation)
Maximum time for testoperation in min             Remaining time
Forcevalue for testoperation

Module error code

```

The counter module has one safety-related output per channel, which is controlled independent from the cycle time of the central module. The "Output state" is indicated at the output of the HF-CNT-3 counter function block and can be processed by the user program.

With a TRUE signal at the „MOS“ input (Maintenance Override Switch) the output of the counter function block may directly be controlled within the time interval for test operation, i.e. the output indicates the value given at the "Forcevalue for maintenance" input. See also document "Maintenance Override" by TÜV Bayern and TÜV Rheinland.



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

2.11 Function Block HF-CNT-4

This function block has the same functionality as HF-CNT-3, but additionally has an output „Error“ for channel error.

HF-CNT-4 Counterblock for F5220	
Bus-No. Rack Pos. (e.g. 1305)	
Counter channel 1	
Enable Configuration	
Signal type (1=5V; 2= 24V; 3= initiator)	Counter (24 bit)
Preset value	Output state
Gate in 50ms	Rotation direction
Maximum deviation at frequency	(TRUE = right; FALSE = left)
Counting mode (1=right,left;2=right;3=left)	Line break/Short circuit
Reset counter	Active
Stop counter	Error
MOS (TRUE = testoperation)	
Maximum time for testoperation in min	Remaining time
Forcevalue for testoperation	
HF-CNT-4	
Counter channel 2	
Enable Configuration	
Signal type (1=5V; 2=24V; 3= initiator)	Counter (24 bit)
Preset value	Output state
Gate in 50ms	Rotation direction
Maximum deviation at frequency	(TRUE = right; FALSE =
Counting mode (1=right,left;2=right;3=left)	Line break/Short circuit
Reset counter	Active
Stop counter	Error
MOS (TRUE = testoperation)	
Maximum time for testoperation in min	Remaining time
Forcevalue for testoperation	
Module error code	

2.12 Function Block HF-TMP-3

One HF-TMP-3 function block is used for each channel of the F 6220 thermocouple module. A channel without proper configuration via HF-TMP-3 doesn't work, i.e. the output values are 0 or FALSE, respectively. There is no default functionality or setting. A type 1 sensor may only be assigned to channel 9.

```

HF-TMP-3 Temperature measurement for F6220
┌Bus-No. Rack Pos. (e.g. 1305) Value
┌Channel-No. (1 .. 9)
HF-TMP-3
┌Enable Configuration Active
┌Sensor type (1=PT100,2=R,3=S,4=B,5=J,6=T,7=E,8=K,9=no thermoelem.)
┌Scaling of range in 0.1%
┌Minimum value of range
┌Maximum value of range
┌Enable external reference temperature
┌External reference temperature in 0.1°C
┌Underflow level Underflow
┌Overflow level Overflow
┌Recalibration
┌MOS (TRUE = testoperation)
┌Maximum time for testoperation in min Remaining time
Channel error
Error code

```

The signal „Enable external comparison temperature“ will only be evaluated, if the mode is set to temperature measurement (values 2..8 at the „Sensor type“ input). If the above mentioned input „Enable external comparison temperature“ is TRUE, the value given at the „External reference temperature“ input is taken as reference value. If the input is FALSE, the value of the resistance temperature detector located on the module will be processed as reference temperature.

The „Value“ output of the function block indicates 0 in case of a channel or module failure. Therefore the „Channel error“ output must be evaluated by the user program, and a special fault value must be defined in the user program, which is used in case of a failure.

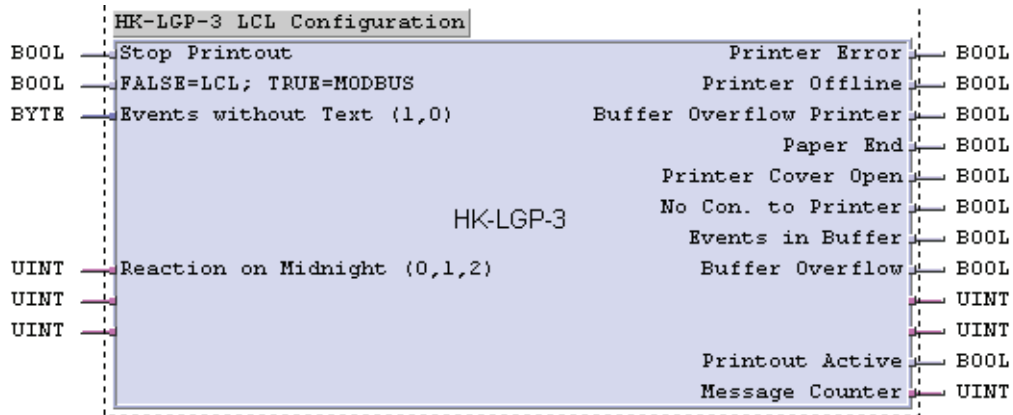
In safety-related applications according to SIL 3, the value for the reference temperature is to be taken from two different modules, this is also true for the thermocouples.

For the detection of the environmental conditions of the module (such as temperature), an automatic recalibration is performed in intervals of 5 minutes. During this procedure also the internal failure messages of the module are reset. This function can also be started by applying a TRUE signal to the „Recalibration“ input via the user program. This TRUE signal may only be applied for one cycle.

With a TRUE signal at the „MOS“ input (Maintenance Override Switch) the „Value“ and „Channel error“ outputs of function block are held for the duration of the test operation. See also document „Maintenance Override“ by TÜV Bayern and TÜV Rheinland.

2.13 Function Block HK-LGP-3

This function block is used for the evaluation and configuration of event recording and the switch-over between BUSCOM and LCL (logic-plan controlled logging). If more than one automation device is connected to one printer, the function block also enables printing.

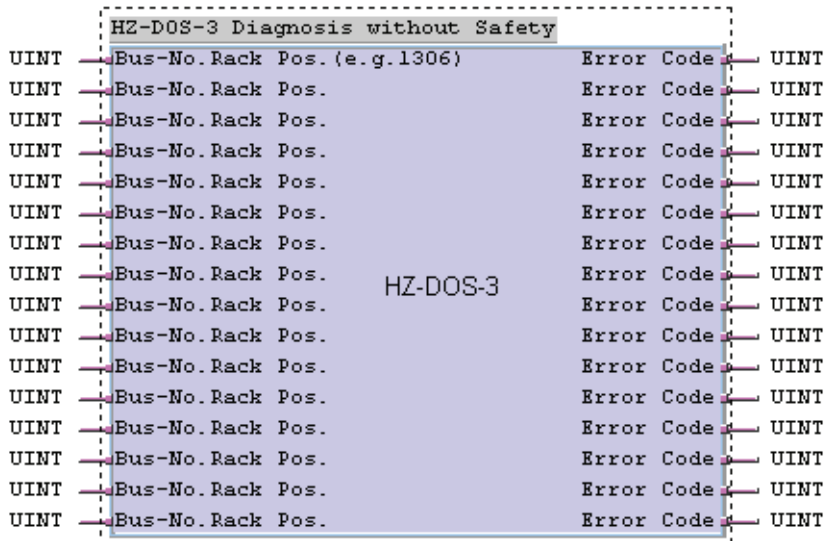


This function block is not relevant to safety. Its outputs are for information purposes only and no safety-related action in the user program must be derived from them.

2.14 Function Block HZ-DOS-3

This function block is used to determine which safety-related IO modules are to be operated in the diagnostic mode only. Up to sixteen modules can be monitored by one function block. The function block can be used several times in the user program.

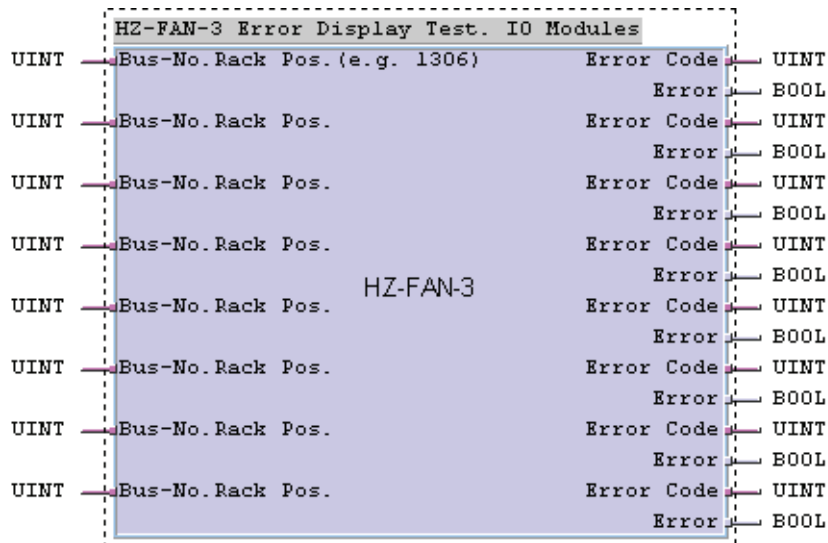
This function block is not relevant to safety. Its outputs are for information purposes only and no safety-related action in the user program must be derived from them.



All safety-related IO modules listed at the HZ-DOS-3 function block may not be used for safety-related functions.

2.15 Function Block HZ-FAN-3

This function block is used for the evaluation and display of errors in safety-related IO modules. One function block can monitor up to eight modules. This function block can be used several times in the user program.



Inputs:

„Bus No. Rack Pos. (e.g. 1306)“

The positions of the safety-related IO modules are indicated by a four-digit decimal number.

Example: „1306“ means:

Cabinet 1, subrack 3, module position 06

All inputs of the function block are for information purposes only and no safety-related action in the user program must be derived from them.



HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation
P.O. Box 1261 • D-68777 Brühl • Germany
Telephone: (+49 6202) 709-0 • Telefax: (+49 6202) 709-107
E-mail: info@hima.com • Internet: www.hima.com

(0702)