Industrial-Automation

System *HIMatrix*

Safety Manual

HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation

HI 800 023 IEA

Important Notes

All HIMA products mentioned in this manual are protected under the HIMA trademark. Unless not explicitly noted, this may apply for other referenced manufacturers and their respective products.

All technical statements and data in this manual have been written with great care and effective quality measures have been taken to ensure their validity; however this manual may contain flaws or typesetting errors.
For this reason, HIMA does not offer any warranties nor assume legal responsibility nor any liability for possible consequences of any errors in this manual. HIMA appreciates any correspondence noting potential errors.

Technical modifications reserved.

For more information see the documentation on CD-ROM and on our web site www.hima.com .

More information can be requested from:

HIMA Paul Hildebrandt GmbH + Co KG
Postfach 1261
68777 Brühl

Tel: +49(6202)709 0
Fax: +49(6202)709 107

e-mail: info@hima.com

About this Manual

This manual contains Information for proper application of the safety-related HIMatrix Automation Devices.

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 HIMatrix 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 HIMA cannot take liability.

HIMatrix 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.

For reasons of clarity this manual does not contain all the details of the HIMatrix Automation Devices.

Intended Readership

This manual address 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.

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

Additional System Documentation

The following documentation is also available for configuring HIMatrix systems:

Name	Contents	Document no. D = german E = english	Part no.
HIMatrix Engineering Manual	Engineering and construction of HIMatrix systems	HI 800 100 (D) HI 800 101 (E)	pdf file
HIMatrix System Manual Compact Systems	Hardware descriptions of compact systems with specifications	HI 800 140 (D) HI 800 141 (E)	pdf file
HIMatrix System Manual Modular System F60	Hardware description of the modular system F60 with specifications	HI 800 190 (D) HI 800 191 (E)	pdf file
Test report for the certificate *	Test basics, safety requirements, results	(D) (E)	96 9000104 96 9000105
HIMatrix Manual First Steps	Introduction to ***ELOP II Factory***	HI 800 005 (D) HI 800 006 (E)	96 9000013 96 9000014 pdf file

* only supplied with a HIMatrix system

Terminology

Term	Definition
AI	Analog Input
AIO	Analog Input/Output
AO	Analog Output
COM	Communication Module
CPU	Central Processing Unit
DI	Digital Input
DIO	Digital Input/Output
DO	Digital Output
EMC	Electromagnetic Compatibility
FB	Field bus
FBD	Function Block Diagram
FTZ	Fault Tolerance Time
IEC	International Electrotechnical Commission
LC	Line Control
MEZ	Multiple fault occurrence time
NSP	Non-Safety-related Protocol
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PADT (PC)	Programming and Debugging Tool (according IEC 61131-3)
PES	Programmable Electronic System
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
R/W	Read/Write
RC	Requirement Class
SFC	Sequential Function Chart
SIL	Safety Integrity Level (according to IEC 61508)
SNTP	Simple Network Time Protocol (RFC 1769)
TMO	Timeout
W	Write
WD	Watchdog
WDZ	Watchdog time

Contents

1 Introduction

1.1 Certification

The safety-related HIMA HIMatrix programmable controllers (Programmable Electronic Systems, PES) are tested and certified by TÜV for functional safety in accordance to CE and the standards listed below:

TÜV Anlagentechnik GmbH
Automation, software and information technology
Am Grauen Stein
51105 Köln

Certificate and test report No. 968/EZ 128.04/03
Safety-related automation devices
HIMatrix F20, F30, F31, F35,
F1 DI 16 01, F2 DO 4 01, F2 DO 8 01, F2 DO 16 01,
F3 AIO 8/4 01, F3 DIO 20/8 01, F3 DIO 20/8 02
HIMatrix F60

International standards:

IEC 61508, parts 1-7: 2000	up to SIL 3
EN 954-1: 1996	up to category 4
EN 298: 1994	
NFPA 8501: 1997	
NFPA 8502: 1999	
EN 61131-2: 1994 and A11: 1996, A12: 2000	
EN 61000-6-2: 2000, EN 50082-2: 1996, EN 50081-2: 1993	
F 60 and F35: EN 54-2: 1997, NFPA 72: 1999	

National standards:

DIN V VDE 0801: 1990 and A1: 1994	
DIN V 19250: 1994	up to RC 6
DIN VDE 0116: 1989, prEN 50156-1: CDV 2000	

Chapter **9 Operating Conditions** contains a detailed listing of all applied environment and EMC tests.

All devices are labeled with the CE sign.

To program of the HIMatrix devices, a PADT (programmer unit, PC) running the programming tool

ELOP II Factory

and the program languages Function Block Diagram (FBD) and Sequential Function Chart (SFC) in accordance to IEC 61131-3 is used. This software assists the user in creating safety-related programs and operation of the PES.

1.2 Safety

The programmable controllers are designed on the deenergize to trip mode, i.e. the peripherals and the function of the controller interpret a de-energized state as a safe state.

In the event of a fault, the input and output signals revert to a voltage-free or current-free state to ensure a safe operation.

PFD and PFH calculations have been carried out for the HIMatrix systems in accordance to IEC 61508.

IEC 61508-1 sets a PFD of 10^{-4} to 10^{-3} and a PFH of 10^{-8} to 10^{-7} per hour for SIL 3.

For the controller (PES), 15 % of the limit value is assumed from the standard for PFD and PFH. This results in limit values of $1.5 * 10^{-4}$ per hour (for the PFD section of the controller) and $1.5 * 10^{-8}$ per hour (for the PFH section).

The interval for the repeat test for HIMatrix systems is set to 10 years, 3 years for relay output modules (Off-line Proof Test, see IEC 61508-4, paragraph 3.8.5).

The safety functions, consisting of a safety-related loop (input, processing module, output and communication between HIMatrix systems), fulfil the above requirements whichever way they are combined. The remote I/O modules also fulfil these requirements.

Further information is available on request.

1.2.1 Deenergize to Trip Mode / Energize to Trip Mode

The programmable controllers are designed for the deenergize to trip mode.

The HIMatrix systems are certificated for process controllers, safety systems, burner systems and machine controllers.

A system operating according to the deenergize to trip mode does not need energy to perform its safety function.

In the event of a fault, the input and output signals revert to voltage-free or current-free states to ensure safe operation.

The HIMatrix controllers can also be used in energize to trip mode applications.

A system operating according to the energize to trip mode needs energy, for example electrical or pneumatic energy, to perform its safety function.

Therefore the HIMatrix F60, F35 and F3 AIO 8/4 01 were tested and certificated according to EN54 and NFPA72 for use in fire alarm systems and fire extinguish systems. In these systems it is necessary that on demand the active state is used for controlling the danger (further details see chapter 8).

1.3 Notes for Danger and Use

This manual contains specially highlighted advices that indicate safety requirements:

1.3.1 Notes for Danger

Important information regarding situations or operations. Failure to observe these instructions could cause personal injury and/or damage to property.

These notes

- indicate danger,
- help you avoid danger,
- make you aware of the consequences.

1.3.2 Notes for Use

Note	Special instructions to aid understanding and correct use.

These instructions will help you to operate the controller correctly and will provide you with better understanding of the system.

1.4 Safety Requirements

The following safety requirements must be followed when using the safety-related PES of the HIMatrix system:

1.4.1 Hardware Configuration

Product independent requirements

- To ensure the safety-related operation, only the permitted, fail-safe hardware modules and software components should be used. The permitted hardware modules and software components are listed in the *Liste zur Verfolgung der Versionsfreigaben der Baugruppen und der Firmware der HIMatrix-Systeme der Firma HIMA Paul Hildebrandt GmbH + Co KG, Zertifikatsnummer 968/EZ 128.00/02*. The valid versions are contained in the version list, which is maintained together with the approval authority.
- The specified operating conditions (see section 9) regarding EMC, mechanical, chemical and climatic influences must be followed.
- Hardware modules and software components that are not fail-safe (but which do not cause any reactions) can be used to process non-safe signals. They cannot, however, be used to carry out safety-related tasks.
- The deenergize to trip mode should be used in all external safety circuits connected to the system.

Product dependent requirements

- Only equipment that can be safely isolated from the mains should be connected to the system.
- The safe electrical isolation of the power supply must take place in the 24 V supply. Only PELV or SELV power supplies may be used.

1.4.2 Programming

Product independent requirements

- In the case of safety-relevant applications, ensure that the safety-relevant system variables are correctly configured. The Safety Manual describes the configurations available.
- Particular attention should be paid to the system configuration, the maximum cycle time and the safety time.

Product dependent requirements

Requirements for using the programming system

- The ELOP II Factory tool must be used for programming purposes.
- After the application has been created, check that the compilation was successfully carried out by manually compiling and comparing the CRCs.
- The correct conversion of the specification of the application should be validated and verified. A comprehensive test of the logic must be carried out.
- This procedure must be repeated each time a modification is made to the application.
- The error response of the system (when a fault occurs in the fail-safe input/output modules) must be determined by the application program according to the plant-specific safety aspects.

1.4.3 Communication

- When safety-related communication is used between different devices, ensure that the total response time of the system does not exceed the fault tolerance time. The basis for calculations listed in section 7.2 should be used.
- At present it is not permitted to transfer safety-related data using public networks (e.g. the internet).
- If the data is to be transferred across company/factory networks, care must be taken (via administrative or technical means) to ensure that sufficient protection is provided against manipulation (e.g. using a firewall to keep the safety-relevant part of the network separate from other networks).
- At this stage, the serial interfaces should only be used for non-safety-related purposes.
- Only devices that have safe electrical isolation should be connected to the communication interfaces.

1.4.4 Special Operating Modes

- When using "Maintenance Override", the most recent version of the "Maintenance Override" document of TÜV Rheinland and TÜV Product Service should be followed (see section 5.5).
- If necessary, the operator must consult the acceptance department responsible for the application to determine the administrative measures required to provide access protection to the systems.

1.5 Safety Times

Individual errors, which can lead to a dangerous operating state, are detected by the self-test devices and, within the safety time, will lead the controller to defined error responses which transfer the faulty components into a safe state.

Fault tolerance time (FTZ, see DIN VDE 0801, appendix A1 2.5.3)

The fault tolerance time is a characteristic of the process and it describes the period of time in which the process can receive faulty signals without a dangerous situation arising. A dangerous situation can arise if a fault is present for longer time than the FTZ.

Safety time (of PES)

The safety time is the time in which the PES (in RUN state) must react after an internal error has occurred.

In terms of the actual process, the safety time is the maximum amount of time within which the safety system must respond to the outputs when the input signals change (response time).

In case of the controllers, times in the region of 20 ms to 50,000 ms can be achieved.

Multi-fault occurrence time (MEZ)

The occurrence time for multiple faults is the period of time within which the probability of multiple faults occurring (which, when combined, are critical with regard to safety) is sufficiently small.

The multi-fault occurrence time is defined as 24 hours in the operating system.

Response time

The maximum response time of cyclic HIMatrix controllers is twice the cycle time of these systems, but only if there is no delay caused by parameterization or logic of the application program.

The cycle time of a controller involves the following important operations:

- Reading the inputs
- Processing the application program
- Writing the outputs
- Process data communication
- Carrying out test routines

In addition, in the worst case scenario for the whole system, the switching times of the inputs/outputs should be taken into account.

Watchdog time of the CPU (in PES)

The watchdog time is specified as the time in the menu for setting the PES attributes. It is the maximum permitted duration of a RUN cycle (cycle time). If the cycle time exceeds the specified watchdog time, the CPU goes into ERROR STOP.

The CPU watchdog time must be set between

2 ms and ½ ∗ safety time of the PES.

The maximum value permitted is 5,000 ms.

Default settings:	controllers (F20, F30, F31, F35, F60)	50 ms,
	remote I/O modules	10 ms.

1.6 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.

1.6.1 Execution of the Offline Proof Test

The execution of the offline proof test depends 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.

1.6.2 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 Central Functions

The device types F1.., F2.., F3.. are compact systems, which cannot be modified.

Type F60 controllers are modular systems; up to six I/O modules can be inserted inside a controller with a power supply module and a central processing module.

2.1 Power Supplies

A power supply module is only available with F60. In the case of compact devices, this function is integrated into the system and cannot be viewed in a modular way.

The power supply module PS 01 (for F60) or the integrated function converts the 24 V system supply voltage to 3.3 V and 5 V (use for internal I/O bus).

2.2 Functional Description of the Central Section

The central module (example) consists of the following function blocks:

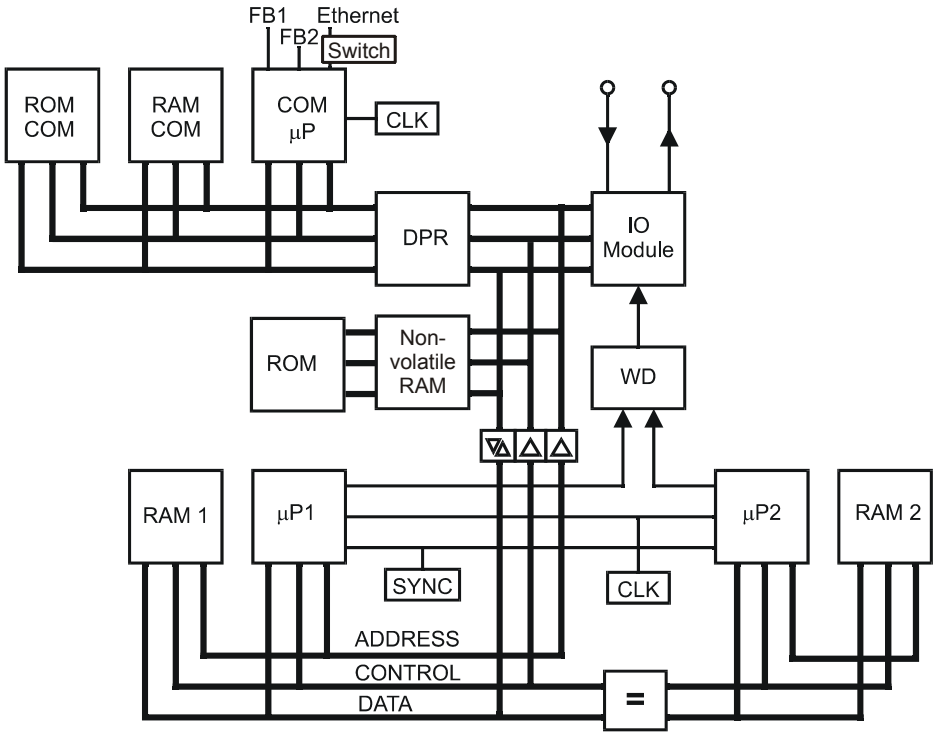


Figure 1: Function blocks, using CPU 01 of F60 as an example

Attributes of the central module CPU 01 of F60

- Two synchronous microprocessors (µP 1 and µP 2)
- Each microprocessor has its own RAM memory
- Testable hardware comparators for all external accesses of both microprocessors
- In the event of an error the watchdog is set to a safe state
- Flash EPROMs of program memories for operating systems and application programs, suitable for at least 100,000 storage cycles
- Data memory in NVRAM
- Multiplexer for connecting I/O bus, Dual Port RAM (DPR)
- Backup supply (goldcap) for date/time
- Communication processor for field bus and Ethernet connections
- Interface for data transfer between F3../F60 devices and the PADT, based on Ethernet
- Optional interface(s) for data exchange via field bus
- Signaling of system status via LEDs
- I/O bus logic for connection to I/O modules
- Safe watchdog (WD)
- Power supply monitoring, testable (3.3 V / 5 V system voltages)

2.3 Self Tests

The most important self-test routines of the safety-related central modules of the controllers and the coupling to the I/O tier are listed below:

Microprocessor test

The following are tested:

- all commands and addressing modes used,
- the writability of the flags and the commands generated by them,
- the writability and crosstalk of the registers.

Test of the memory areas

The operating system, application program, constants and parameters as well as the variable data are saved in both processor areas in each central module and are tested by a hardware comparator.

Fixed memory areas

The operating system, application program and parameter area are each stored in a memory. They are protected by write protection and a CRC test.

RAM test

The modifiable RAM areas, in particular stuck-at and crosstalk, are tested with a write and read test.

Watchdog test

The watchdog signal switches off if it is not triggered from both CPUs within a defined time window and also if the test of the hardware comparator fails. A separate test determines whether the watchdog signal is able to switch off.

Test of the I/O bus inside the controller

The connection between the CPU and the associated inputs and outputs (I/O modules) is tested.

Reactions to faults in the CPU

A central hardware comparator permanently checks whether the data in microprocessor system 1 is identical to the data in microprocessor system 2. If it is not identical or if the central test routines return a negative result, the controller automatically goes into ERROR STOP and the watchdog signal is switched off. This means that input signals are no longer processed and the outputs switch to the de-energized, switched off state.

2.4 Error Diagnosis

All F60 modules have an LED to indicate errors in the event of faults in the module or the external wiring. This facilitates a quick fault diagnosis of a module that has been signaled as faulty.

Due to the fact that F1.., F2.., F3.. systems are compact systems, these fault displays are grouped together as a group fault signal.

In addition, an evaluation of various system signals can take place in the application program with status displays of the inputs/outputs or of the CPU.

Fault signaling only takes place if the fault does not prevent communication with the CPU, i.e. the CPU is still able to evaluate the signals.

The error codes of all input and output signals and those for the system signals can be evaluated via the logic of the application program.

An extensive diagnostic record of system performance and the faults detected is stored in the diagnostic memory of the CPU and the COM. The record can be read out via the PADT, even after a system fault.

Details about the analysis of diagnosis messages see **System Manual Compact Systems or System Manual Modular System F60,** chapter "Diagnosis".

3 Inputs

3.1 Overview

F20 controller				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	8	•	•	–

F30 controller				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	20	•	•	–

F31 controller				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	20	•	•	–

F35 controller				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	24	•	•	–
24 bit counter	2	•	•	–
Analog inputs	8	•	•	–

Remote I/O module F1 DI 16 01				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	16	•	•	–

Remote I/O module F3 DIO 8/8 01				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	8	•	•	–

Remote I/O module F3 DIO 16/8 01				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	16	•	•	–

Remote I/O module F3 AIO 8/4 01				
System section	Quantity	safety-related	non-interacting	electrically isolated
Analog inputs	8	•	•	–

Remote I/O module F3 DIO 20/8 01 and 20/8 02				
System section	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs	20	•	•	–

Modular F60 controller				
Module	Quantity	safety-related	non-interacting	electrically isolated
Digital inputs: DIO 24/16 01 DI 32 01 (configurable with Line Control) DI 24 01 (110 V)	 24 32 24	 • • •	 • • •	 • • •
24 bit counter: CIO 2/4 01	 2	 •	 •	 •
Analog inputs: AI 8 01	 8	 •	 •	 •
Analog or digital inputs MI 24 01	 24	 •	 •	 •

3.2 General

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

Apart from the diagnostic LEDs of the modules, the controllers also send status signals to the application program, which can be evaluated. I/O errors stored in the diagnostic memory can be read using ***ELOP II Factory***.

Safety-related input modules are automatically subject to stringent cyclic self-tests during operation. These test routines are TÜV tested and monitor the safe functioning of the relevant module.

In the event of a fault, a 0-signal is sent to the application program. Detailed fault information will be also generated in any case. This fault information can be evaluated in the application program by reading the error codes.

For a few component failures, which do not impinge on safety, no diagnostic information is generated.

3.3 Safety of Sensors, Encoders and Transmitters

In a safety-related application, both the PES and the sensors connected to it must meet the safety requirements (SIL).

The safety-related sensors, encoders and transmitters with the required SIL can be connected to the PES inputs. If there are no sensors, encoders and transmitters with the specific SIL, they can also be connected. However, the application program must then handle the logic and monitoring of the signals.

Information on how to achieve the required SIL is contained, for example, in IEC 61511-1, Paragraph 11.4.

3.4 Safety-related Digital Inputs

The points listed below apply to both digital input channels of F60 modules and digital input channels of all compact systems (unless stated otherwise).

3.4.1 General

The digital inputs are read once per cycle and saved internally; cyclic tests are carried out to assure their function safety.

Input signals, which are present for shorter time than the time between two samplings (i.e. shorter than a cycle time), are possibly not recorded.

3.4.2 Test Routines

The online test routines check whether the input channels, regardless of the pending input signals, are able to connect both signal levels (L and H signals). This test is carried out each time the input signals are read.

3.4.3 Reaction in the Event of a Fault

If the test routines detect a fault in the digital inputs, a 0-signal is processed in the application program for the defective channel according to the deenergize to trip mode. The "FAULT" LED is then activated (at F60 the "ERR" LED on the module).

In addition to the signal value of the channel, the relevant error code must be taken into account in the application program. The error code gives the user the ability to provide fault handling in the application program and to diagnose the external wiring.

3.4.4 Diagram of the Digital Inputs

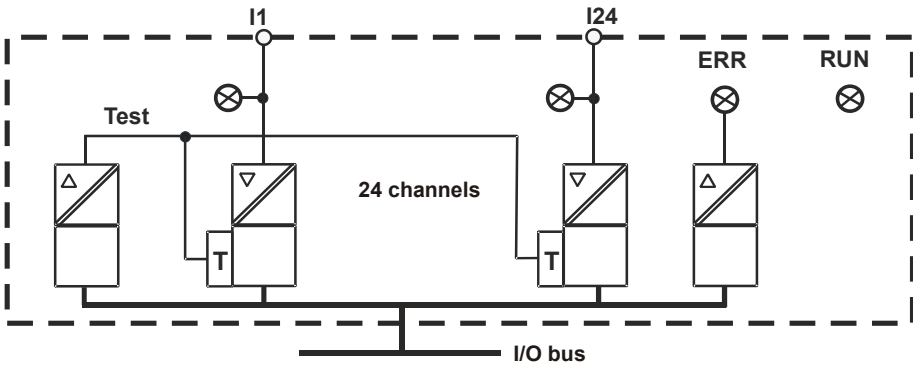


Figure 2: View of the functions, using the DIO 24/16 01 module as an example

3.4.5 Surge on Digital Inputs

In the case of digital inputs, an EN 61000-4-5 surge impulse can be read as a short-time H signal (caused by the short cycle time of the HIMatrix system).

Note

To avoid errors of this type, one of the following measures must be taken in respect to the applications:

- Installation of shielded input lines to prevent the effects of surges in the system,
- Fault masking in the application program: A signal must be present for at least two cycles before it is evaluated.

Attention: This extends the reaction time of the system!

The mentioned measures can be neglected if surges in the system can be excluded by the construction of the plant. The construction includes especially protection measures concerning overvoltage, lightning strike, earthing and wiring on base of manufacturers instructions and relevant standards.

3.4.6 Parameterizable Digital Inputs

The digital inputs of the F35 control and the MI 24 01 module operate according to the principle of analog inputs, but set to digital values by parameterization of operating points.

For parameterizable digital inputs the test routines and safety functions for analog inputs apply as mentioned in chapter 3.5.2.

3.4.7 Line Control

Line Control is a short-circuit and line break monitoring system, for example, of EMERGENCY STOP devices (cat. 4 according to EN 954-1), which can be configured on HIMatrix systems with digital inputs (not with parameterizable digital inputs).

In addition, digital outputs DO are connected to the digital inputs DI of the same system, as shown below (example):

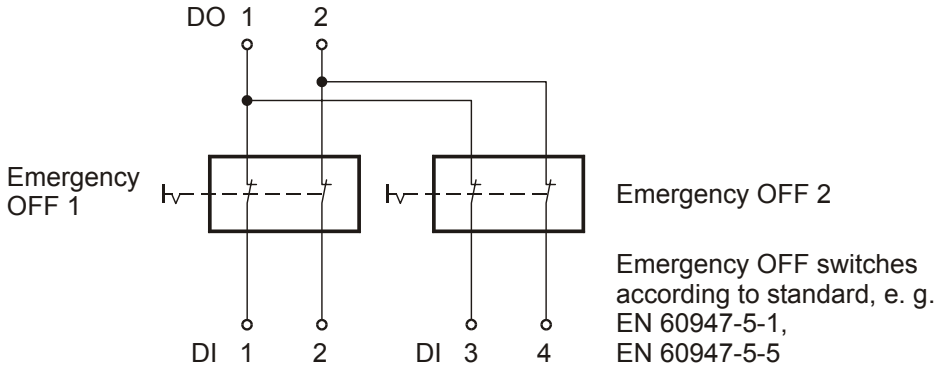


Figure 3: Line Control

The digital outputs DO 1, DO 2 are pulsed (T1, T2) and in this way the lines to the digital inputs are monitored. The signals for the pulsed outputs must begin at DO[01].Value and must be directly sequential (see system signals in corresponding data sheets):

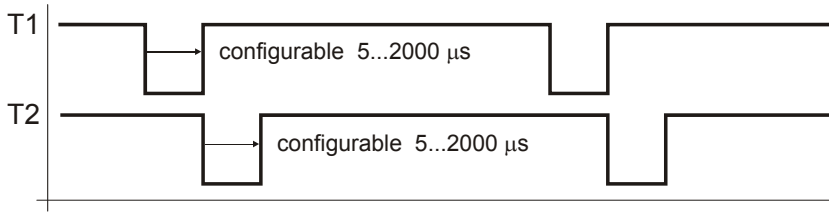


Figure 4: Pulsed outputs

The "FAULT" LED on the front plate of the controller/module flashes, the inputs are set to 0 and an error code (which can be evaluated) is generated when the following faults occur:

- Short-circuit between two parallel lines,
- Change of two lines (e.g. DO 2 to DI 3),
- Earth fault on one of the lines (only with earthed reference pole),
- Line break or opening of the contacts, i.e. when one of the Emergency OFF switches (displayed above) is pressed, the LED flashes and the fault code is generated.

3.5 Safety-related Analog Inputs (F35, F3 AIO 8/4 01 and F60)

3.5.1 General

The input signals in the analog input channels are converted to an INTEGER value. The application program can then use this value.

The safety-related accuracy is the guaranteed accuracy of the analog input without error reaction of the module. This value should be taken into account when the safety functions are configured.

The following input values are available:

F35 controller

Input channels	Measuring method	Current, voltage	Range of values in the application		Safety accuracy
			FS1000[1)]	FS2000[1)]	
8	unipolar	0...+10 V	0...1000	0...2000	2 %
8	unipolar	0...20 mA	0...500[2)] 0...1000[3)]	0...1000[2)] 0...2000[3)]	2 %

[1)] settable via type selection in ***ELOP II Factory Hardware Management***
[2)] with external shunt adapter 250 Ω, HIMA no.: 98 2220059
[3)] with external shunt adapter 500 Ω, HIMA no.: 98 2220067

Remote I/O module F3 AIO 8/4 01

Input channels	Measuring method	Current, voltage	Range of values in the application	Safety accuracy
8	unipolar	0...+10 V	0...2000	2%
8	unipolar	0/4...20 mA	0...1000[2)] 0…2000[3)]	2%

[2)] with external shunt adapter 250 Ω, HIMA no.: 98 2220059
[3)] with external shunt adapter 500 Ω, HIMA no.: 98 2220067

F60 controller

Input channels AI 8 01	Measuring method	Current, voltage	Range of values in the application		Safety accuracy
			FS1000[1)]	FS2000[1)]	
8	unipolar	-10 V...+10 V	-1000...1000	-2000...2000	1 %
8	unipolar	0...20 mA	0...1000[3)]	0...2000[3)]	1 %
8	unipolar	0...20 mA	0...500[2)]	0...1000[2)]	4 %
4	bipolar	-10 V...+10 V	-1000...1000	-2000...2000	1 %
MI 24 01					
24	unipolar	0...20 mA	0...2000[4)]		1 %

[1)] specified via device type selection (F60)
[2)] with external shunt 250 Ω, HIMA no.: 00 0710251
[3)] with external shunt 500 Ω, HIMA no.: 00 0603501 (accurancy 0.05%, P 1W)
[4)] internal shunts

The module AI 8 01 of the F60 can be configured in the application program for eight unipolar or four bipolar functions. However, the mixing of functions on a module is not permitted.

The analog inputs of the controller F35, the remote I/O module F3 AIO 8/4 01 and the F60 module AI 8 01 operate with *voltage* measurement. With the analog inputs of the HIMatrix F35 and F3 AIO 8/4 01 digital outputs of the own device (F35) or of other HIMatrix controllers can be monitored on line break. Further informations are available in the data sheets of the corresponding HIMatrix controllers.

In the case of an open-circuit fault (there is no line monitoring in the system), any input signals will be received on the high-resistance inputs. The value resulting from this fluctuating input voltage is not reliable; with voltage inputs, the channels must be terminated with a 10 kΩ resistor. The internal resistance of the source should be taken into account.

To measure a *current*, the shunt is connected in parallel to an input; the 10 kΩ is then not required.

The inputs of the MI 24 01 module are only current inputs, because of the internal shunts, and cannot be used as voltage inputs.

If input channels are not used, the measurement input must be connected to the reference potential. Negative influences (fluctuating input voltages) on other channels in case of a line break are avoided.

For the unused input channel the corresponding signal ***AI[0x].Used*** has to be set to the default value "FALSE" or "0" in ***ELOP II Hardware Management***. By this the channel is decommissioned in the application program, i.e. no signals of this channel are available within the logic.

3.5.2 Test Routines

The analog values are processed in parallel via two multiplexers and two analog/digital converters with 12-bit resolution and the results are compared. In addition, test values are connected to digital/analog converters and converted back to digital values, which are then compared with the specified value.

When an error is detected, the input is set to "0" for further processing by the application program, and the error state is set.

3.5.3 Reaction in the Event of a Fault

If there are channel faults in the analog inputs, the error code of the corresponding channel is set to a value > 0. If the entire module is faulty the error code for the module is set to a value > 0. The "FAULT" LED is activated in both cases (at F60 the "ERR" LED on the module).

The analog input value must be interlocked with this status information (error code of analog inputs) within the application program. In case of a value > 0 a safety-related reaction must be programmed.

3.5.4 Diagram of the Analog Inputs

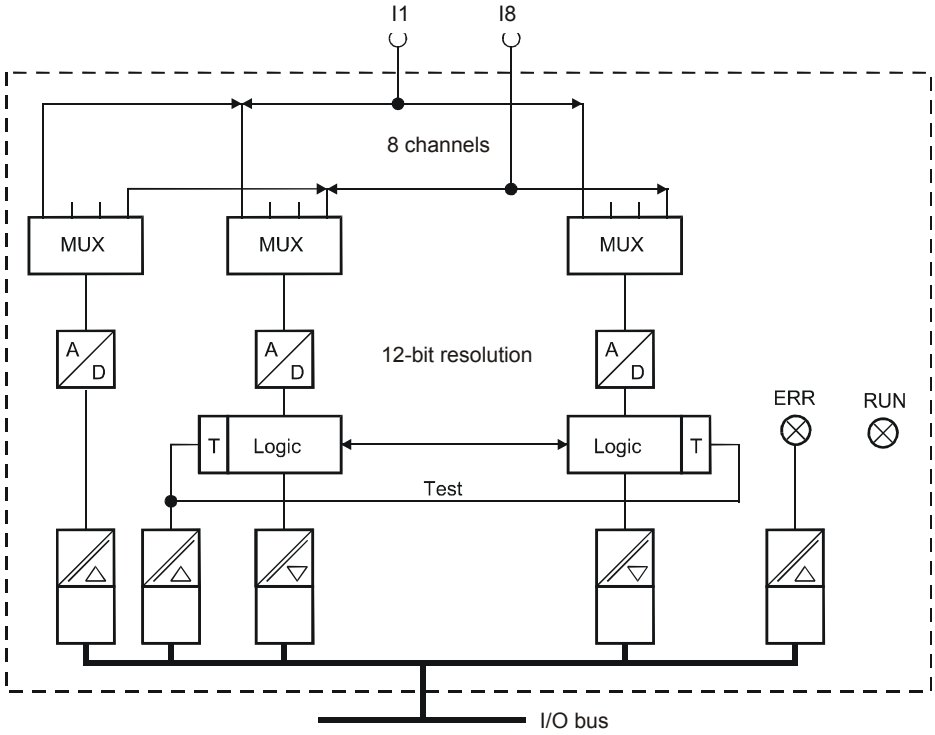


Figure 5: View of the functions, using input module AI 8 01 as an example

3.6 Safety-related Counters (F35 and F60)

The points listed below apply to both F60 counter modules and F35 counters (unless stated otherwise).

3.6.1 General

Depending on the configuration, the counter module can be operated in the application program as a high-speed up or down counter with 24-bit resolution or as a decoder in Gray code.

If used as high-speed up or down counters, the pulse input and count direction input signals are required in the application. A reset only takes place in the application program.

The F60 counter module has 4- or 8-bit encoder resolution, whereas the F35 has a resolution of 3- or 6-bit. A reset is possible.

The interconnection of two independent 4-bit inputs to an 8-bit input (example of F60) can only be carried out via the application program. A switching option for this purpose is not planned.

The encoder function monitors the change of the bit pattern on the input channels. The bit patterns on the inputs are transferred directly to the application program. The display on the PADT is in the form of a decimal number (*Counter[0x].Value*) that corresponds to the bit pattern.

Depending on the application, this number (which corresponds to the Gray Code bit pattern) can be converted into, for example, the corresponding decimal value.

3.6.2 Reaction in the Event of a Fault

If a fault is detected in the counter section of the module, a status bit is set for evaluation in the application program. Additionally the relevant error code can be taken there into consideration. The "FAULT" LED is activated (at F60 the "ERR" LED on the module).

The error code enables the user to provide additional fault handling in the application program.

3.6.3 Diagram of Counters

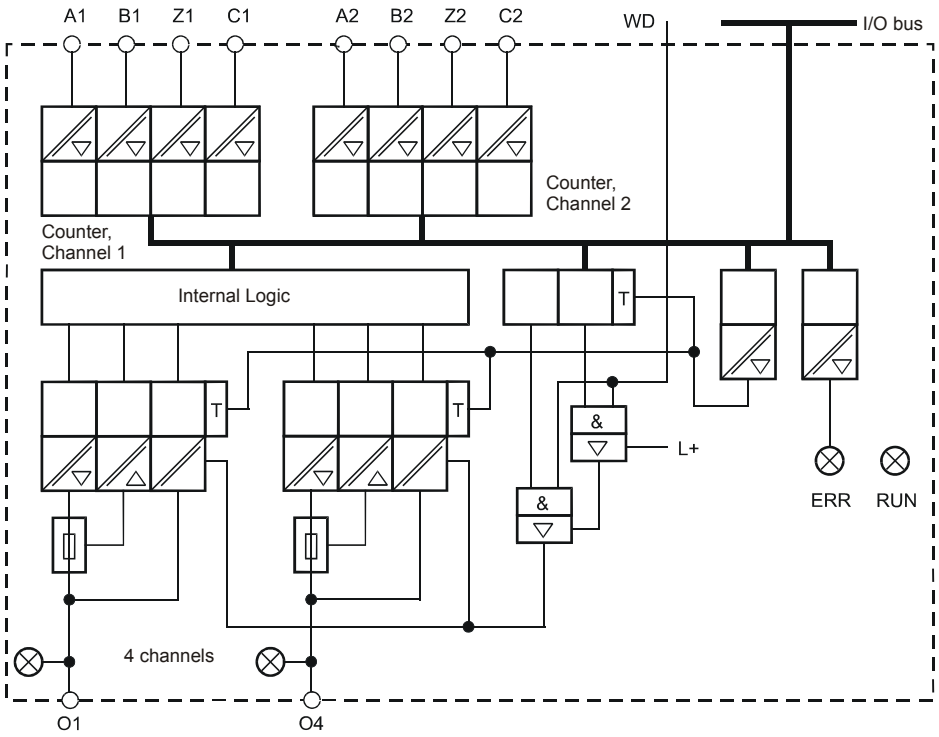


Figure 6: View of the functions, counter module CIO 2/4 01 as an example

3.7 Check List for safety-related Inputs

We recommend that the checklist below is used during the configuration, programming and commissioning of safety-related inputs. It can be used as a planning document, and at the same time proves that the planning has been carefully carried out.

As part of the configuring or commissioning phases, a separate requirements checklist can also be compiled for each of the safety-related input channels installed in the system. This ensures that all the requirements are noted in a clear, comprehensive manner. It also enables documentation regarding the connection of external wiring to the application program to be produced.

HIMatrix Safety Manual Check list for configuring, programming and commissioning				
Company				
Location				
Loop				
Safety-related inputs for		☐ **HIMatrix compact system F..** ☐ **HIMatrix modular system F60**		
No.	**Requirement**	**Yes**	**No**	**Remarks**
1	Is this a safety-related input?	☐	☐	
2	Is the fault display processed in the application program? [VALUE=0] and [ERRORCODE≠0]	☐	☐	
3	Is this a digital input?	☐	☐	
4	HIMatrix F35 / MI 24 01: Is the hysteresis for the digital inputs configured correctly?	☐	☐	
5	Is this an analog input?	☐	☐	
6	unipolar 0 to +10 VDC unipolar 0 to ±10 VDC (F60 only)	☐	☐	
7	unipolar 0 to 20 mA	☐	☐	
8	bipolar ±10 VDC (F60 only)	☐	☐	
9	Voltage input terminated or failure caused by line break can be excluded?	☐	☐	
10	Do the sensor areas match the channel configuration?	☐	☐	
11	Are the unused analog inputs short-circuited?	☐	☐	
12	Are the releases (AI[0x].Used) for the concerning inputs parameterized?	☐	☐	
13	Is this input a counter input?	☐	☐	
14	Function: Pulse counter?	☐	☐	
15	Function: Decoder (Gray code)?	☐	☐	
16	Is a safety-related encoder/sensor provided for this input?	☐	☐	

4 Outputs

4.1 Overview

F20 controller			
System section	Quantity	safety-related	electrically isolated
Digital outputs	8	•	–
Pulsed outputs	4	–	–

F30 controller			
System section	Quantity	safety-related	electrically isolated
Digital outputs (configurable for Line Control)	8	•	–

F31 controller			
System section	Quantity	safety-related	electrically isolated
Digital outputs (configurable for Line Control)	8	•	–

F35 controller			
System section	Quantity	safety-related	electrically isolated
Digital outputs	8	•	–

Remote I/O module F1 DI 16 01			
System section	Quantity	safety-related	electrically isolated
Pulsed outputs	4	–	–

Remote output module F2 DO 4 01			
System section	Quantity	safety-related	electrically isolated
Digital outputs	4	•	–

Remote output module F2 DO 8 01			
System section	Quantity	safety-related	electrically isolated
Relay outputs	8	•	•

Remote output module F2 DO 16 01			
System section	Quantity	safety-related	electrically isolated
Digital outputs	16	•	–

Remote output module F2 DO 16 02			
System section	Quantity	safety-related	electrically isolated
Relay outputs	16	•	•

Remote I/O module F3 DIO 8/8 01			
System section	Quantity	safety-related	electrically isolated
Digital outputs	8 1-pole 2 2-pole	•	–

Remote I/O module F3 DIO 16/8 01			
System section	Quantity	safety-related	electrically isolated
Digital outputs	16 1-pole 8 2-pole	•	–

Remote I/O module F3 AIO 8/4 01			
System section	Quantity	safety-related	electrically isolated
Analog outputs	4	– *	–

*** but with common safety-related shutdown**

Remote I/O module F3 DIO 20/8 01 and 20/8 02			
System section	Quantity	safety-related	electrically isolated
Analog outputs (configurable for Line Control)	8	•	–

Modular F60 controller			
Module	Quantity	safety-related	electrically isolated
Digital outputs: CIO 2/4 01 DIO 24/16 01 (configurable for Line Control)	 4 16	 • •	 • •
DO 8 01 (with relay contacts)	8	•	•
Analog outputs: AO 8 01	8	•	•

4.2 General

The safety-related output modules are written once every cycle, the output signals are read back and compared with the specified output data.

The safe state of the outputs is the "0" value or an open relay contact.

Three testable switches are integrated in series into the safety-related output channels. This enables the independent second disconnection path (required for safety reasons) to be integrated into the output module.

This integrated safety shutdown mechanism safely disconnects all the channels of the defective output channel (de-energized state).

Besides that the WD signal of the CPU is the second possibility of the safety shutdown: With loss of the WD signal the system is immediately transferred into the safe state.

This function is only effective for all digital outputs and relay outputs of the controller.

The relevant error code enables the user to provide additional fault reactions in the application program.

4.3 Safety-related Digital Outputs

The points listed below apply to both digital output channels of F60 modules and digital output channels of the compact devices. The relay modules are excluded in both cases, unless specified otherwise.

4.3.1 Test Routines for Digital Outputs

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

- Read back of the output signal of the switching amplifier. The switching threshold for a read-back 0-signal is 2 V. The diodes used prevent a feed back of signals,
- Checking the integrated redundant safety shutdown,
- A shutdown test of the outputs is carried out within the MEZ for a max. of 200 µs. The minimum time between two tests is ≥ 20 seconds.

The operating voltage of the entire system is monitored, de-energizing all outputs at an undervoltage of < 13 V.

4.3.2 Reaction in the Event of a Fault

If a faulty 1-signal is detected, the concerning output of the module is set to a safe, de-energized "0" state via the safety switches. In case of a module fault all outputs are switched off. Both faults are also indicated via the "FAULT" LED (at the F60 the "ERR" LED on the module).

4.3.3 External Short-Circuit or Overload Performance

If the output is short-circuited to L- or an overload, it is still possible to carry out tests on the module. A safety shutdown is not required.

The total current consumption of the module is monitored. If the threshold is exceeded, all the channels of the output module are set to the safe "0" state.

In this state the outputs are cyclically checked (in periods of several seconds) if the overload is still present. At a normal state the outputs are connected again to the load.

4.3.4 Diagram of the Digital Outputs

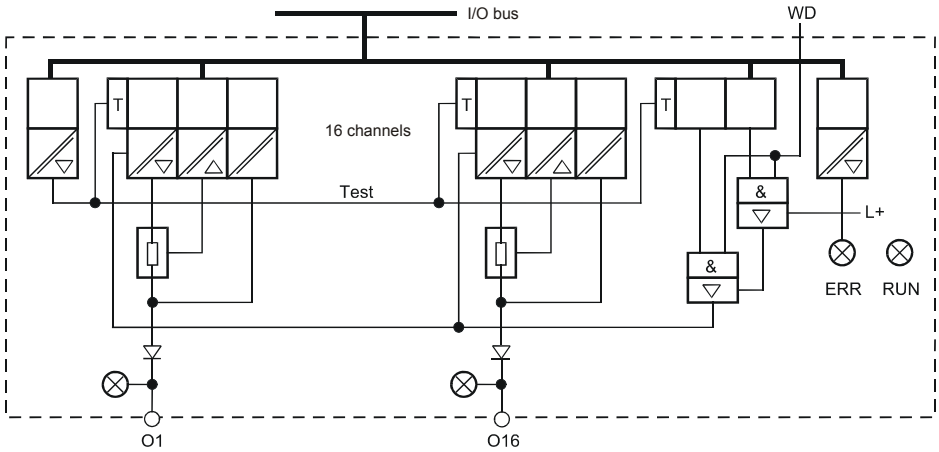


Figure 7: View of the functions, using the DIO 24/16 01 module as an example

4.3.5 Line Control

Safety-related digital outputs can be cycled with the safety-related digital inputs of the same system (but not with parameterizable digital inputs). This enables short-circuit or line break monitoring to be carried out, for example, with EMERGENCY STOP devices according to Cat. 4 as specified in EN 954-1 (see section 3.4.7 Line Control).

Pulsed outputs must not be used as safety-related outputs, e.g. for control of safety-related actuators!

Relay outputs cannot be used as pulsed outputs.

4.4 Safety-related 2-Pole Digital Outputs

The points listed below apply to 2-pole digital outputs of the compact devices.

4.4.1 Test Routines for 2-Pole Digital Outputs

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

- Read back of the output signal of the switching amplifier. The switching threshold for a read-back signal is 2 V. The diodes are used to prevent a feed back of signals.
- Checking the integrated (redundant) safety shutdown
- A shutdown test of the outputs is performed within the MEZ for a max. of 200 µs. The minimum time between two tests is ≥ 20 seconds.
- Line monitoring at 2-pole connection
  F3 DIO 16/8 01:
  - short-circuit to L+, L-
  - short-circuit between 2-pole connections
  - line break in one of the 2-pole lines

  F3 DIO 8/8 01:
  - short-circuit to L+, L-
- Test of L- switch capability at 2-pole connection with line monitoring (F3 DIO 16/8 01)
- Monitoring of the output current of the device

The operating voltage of the entire system is monitored, de-energizing all outputs at an undervoltage of < 13 V.

4.4.2 1-Pole / 2-Pole Connection (F3 DIO 8/8 01, F3 DIO 16/8 01)

The digital outputs can be configured as follows:

- Digital output with 2-pole connection with line monitoring
- Digital output with 2-pole connection without line monitoring
- Digital output with 1-pole positive-switching DO+
- Digital output with 1-pole negative-switching DO-

4.4.2.1 2-Pole Connection

At applications according to EN 954-1 Cat. 4 the status signal of the line monitoring has to be used to switch off the outputs (DO+, DO-) in case of a fault.

Note If the requirements mentioned above cannot be fulfilled the following case has to be regarded:

At short-circuit from DO- to L- a relay can switch on or an other actuator can be switched in another operating state.

Reason: During monitoring time of line monitoring a 24 V voltage (DO+ output) is impressed at the load (relay, actuator), so that the amount of electric energy could be great enough to switch the load in another operating state.

At 2-pole parameterization no DI input may be connected to a DO output. This would prevent a detection of a line break.

Inductive loads must be connected with a protection diode on the load.

4.4.3 Reaction in the Event of an Internal Fault

DO- outputs

If a faulty 1-signal is detected, the concerning output of the module is set to a safe, de-energized "0" state via the safety switches. In case of a module fault all outputs are switched off. Both faults are also indicated via the "FAULT" LED.

DO+ outputs

If a faulty 1-signal is detected, the concerning output of the module is set to a safe, de-energized "0" state via the safety switches. In case of a module fault all outputs are switched off. Both faults are also indicated via the "FAULT" LED.

4.4.4 External Short-Circuit or Overload Performance

If the output is short-circuited to L-, L+ or an overload, it is still possible to carry out tests on the module. A safety shutdown is not required.

The total current consumption of the module is monitored. If the threshold is exceeded, all the channels of the output module are set to the safe "0" state.

In this state the outputs are cyclically checked (in periods of several seconds) if the overload is still present. At a normal state the outputs are connected again to the load.

4.4.5 Diagram of the 2-Pole Digital Outputs

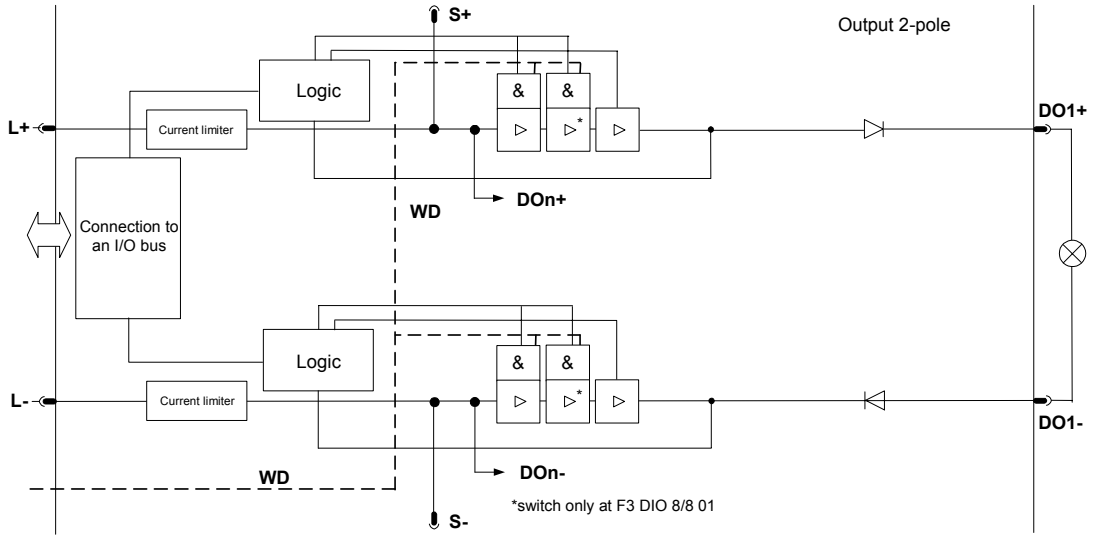


Figure 8: View of the functions, using the F3 DIO 8/8 01, F3 DIO 16/8 01 module as an example

4.5 Relay Outputs

4.5.1 Test Routines for Relay Outputs

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

- Read back of the output signals of the switching amplifiers before the relays,
- Testing the switching of the relays with positively guided contacts,
- Testing the integrated redundant safety shutdown.

The operating voltage of the entire system is monitored, de-energizing all outputs at an undervoltage of < 13 V.

At the module DO 8 01 and the remote I/O module F2 DO 8 01, F2 DO 16 02 the outputs are equipped with three safety relays: two relays with positively guided contacts and one standard type relay. So the outputs can be used for safety shutdowns.

4.5.2 Reaction in the Event of a Fault

If a faulty 1-signal is detected, the concerning output of the module is set to a safe, de-energized "0" state via the safety switches. In case of a module fault all outputs are switched off. Both faults are also indicated via the "FAULT" LED (at the F60 the "ERR" LED on the module).

4.5.3 Diagram of the Relay Outputs

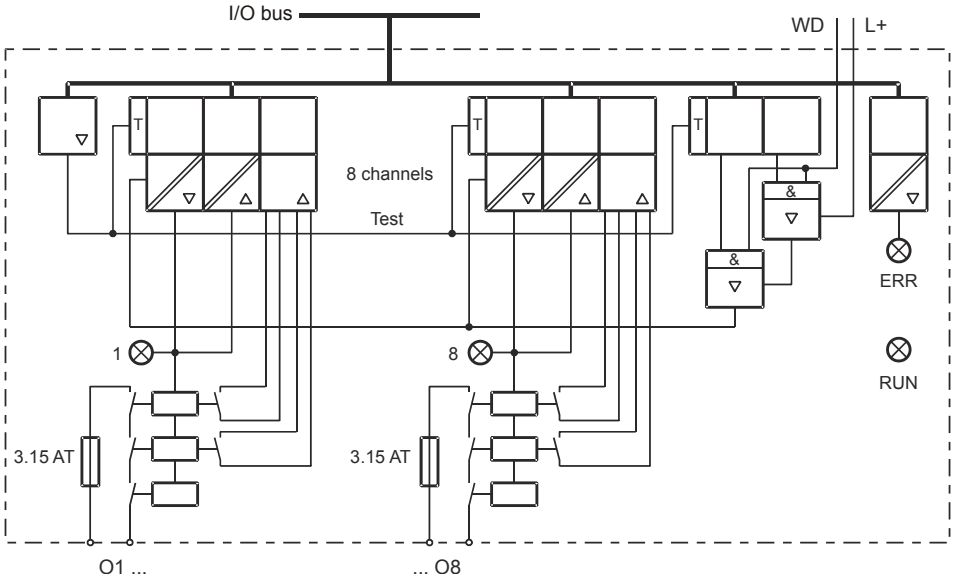


Figure 9: View of the functions, using the DO 8 01 module as an example

4.6 Safety-related Analog Outputs (F60)

4.6.1 General

The intelligent module AO 8 01 has an own safety-related 1oo2 A/D microprocessor system with safe communication. The analog outputs are written once every cycle and the values saved internally. The module itself tests the function.

The safety-related analog output modules can be set to voltage or current outputs using the DIP switches on the module. Ensure that the settings correspond to how they are applied in the system and configured in the application program. Failure to do so leads to unpredictable module reaction.

Before installing the module in the system: Check the DIP switch settings on the module and their configuration in the application program!

Depending on the selection of the device type (…FS1000, …FS2000) via the resource of the F60 you have to consider different values for the signal ***AO[0x].Value*** in the logic to get equal output values (see data sheet AO 8 01, chapter "Signals and Error Codes of the Outputs", analog outputs AO 8 01).

Respectively two analog outputs are DC coupled to each other (output 1 and 2, output 3 and 4, output 5 and 6, output 7 and 8).

The analog output circuits have current or voltage monitoring, readback and test channels (even for parallel output circuits), as well as two additional safety switches for the safe disconnection of the output circuits in the event of a fault. This ensures that the safe state is achieved (current output: 0 mA, voltage output: 0 V).

4.6.2 Test Routines

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

- duplicated readback of the output signal,
- crosstalk test between the outputs,
- checking the integrated safety shutdown.

4.6.3 Reaction in the Event of a Fault

The output signals are read back once every cycle and compared with the internally saved output signals of the intelligent module. If there is a discrepancy, the defective output channel is switched off via both safety switches, and the module error is signaled via the "ERR" LED on the module.

The error code signal enables the user to provide additional fault handling in the application program.

To obtain the worst case response time of the analog outputs, add twice the watchdog time ($2 * WDZ_{CPU}$) to twice the watchdog time of the AO-CPU ($2 * WDZ_{AO\text{-}\mu C}$).

The worst case response time is shown in the data sheet.

4.6.4 Diagram of the Analog Outputs

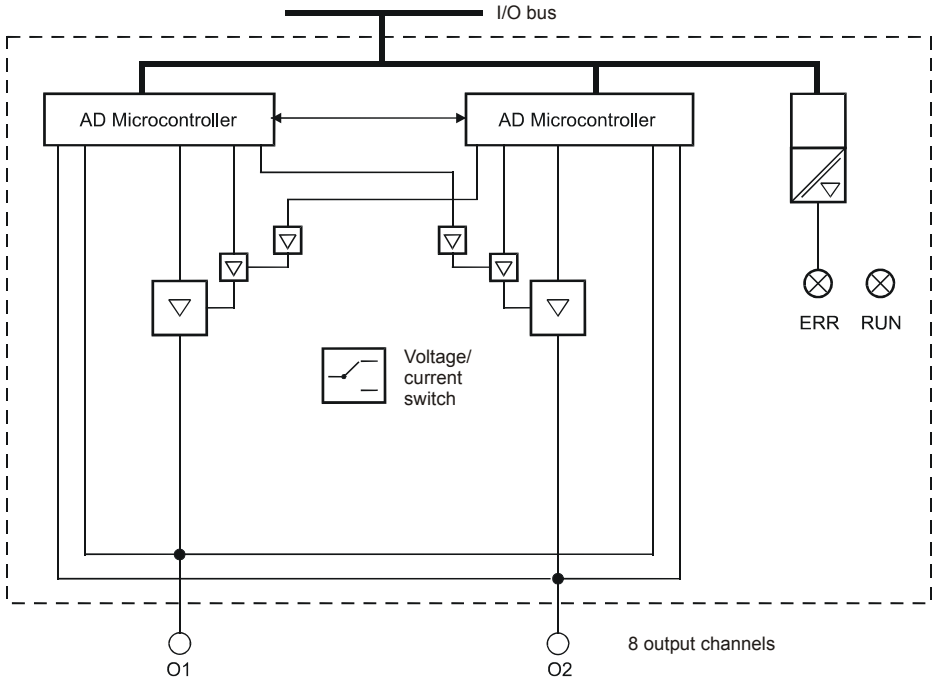


Figure 10: View of the functions, using module AO 8 01 as an example

4.7 Analog Outputs with safety-related Shutdown (F3 AIO 8/4 01)

4.7.1 General

The analog outputs are written once every cycle and the values saved internally.

All the outputs are non-safety-related, but all together they can be shut down safely.

To reach SIL 3 the output values must be read back via safety-related analog inputs and evaluated in the application program. There also reactions to incorrect output values must be specified.

4.7.2 Test Routines

Both the safety switches for the shutdown of all four outputs of the module are automatically tested during operation.

4.7.3 Reaction in the Event of a Fault

In case of an internal error all four output channels are shut down via both safety switches at the same time, and the module error is signaled via the "FAULT" LED on the front plate.

The error code signal enables the user to provide additional fault handling in the application program.

4.8 Check List for safety-related Outputs

We recommend that the checklist below is used during the configuring, programming and commissioning of safety-related outputs. It can be used as a planning document, and at the same time proves that the planning has been carefully carried out.

A separate requirements checklist for the configuration or commissioning can also be compiled for each of the safety-related output channels installed in the system. This ensures that all the requirements are noted in a clear, comprehensive manner. Documentation regarding the connection of external wiring to the application program could also be produced.

HIMatrix Safety Manual Check list for configuring, programming and commissioning				
Company				
Location				
Loop				
Safety-related outputs for		☐ **HIMatrix compact system F..** ☐ **HIMatrix modular system F60**		
No.	**Requirement**	**Yes**	**No**	**Remarks**
1	Is this a safety-related output?	☐	☐	
2	Is the fault signal processed in the application program?	☐	☐	
3	Is this a digital output?	☐	☐	
4	Does the channel load correspond to the maximum permitted value?	☐	☐	
5	Does the module load correspond to the maximum permitted value?	☐	☐	
6	Are there RC circuits (free-running circuits) fitted to the actuators?	☐	☐	
7	Has the actuator been connected according to the data sheet? (two-pole connection)	☐	☐	
8	Is this an analog output?	☐	☐	
9	Application of voltage output: DIP switch positions according to configuration in application program?	☐	☐	
10	Application of current output: DIP switch positions according to configuration in application program?	☐	☐	
11	Are unused analog current outputs short-circuited?	☐	☐	
12	Are the releases (AO[0x].Used) for the concerning outputs parameterized?	☐	☐	
13	Is a safety-related actuator provided for this output?	☐	☐	

5 Software for HIMatrix Systems

The software for the safety-related programmable controllers of HIMatrix systems can be divided into the following blocks:

- Operating system,
- Application program,
- ***ELOP II Factory*** programming tool (conforms to IEC 61131-3).

The *operating system* is loaded into the CPU of the controller and should be used in the valid, TÜV-certified form required for safety-related applications.

The *application program* is created with the ***ELOP II Factory*** programming software and contains the system-specific functions that the programmable controller needs to carry out. The ***ELOP II Factory*** system software is also used to configure and control operating system functions.

The application program is translated into machine code using the code generator. This machine code is transferred into the Flash EPROMs of the programmable controller via an Ethernet interface.

5.1 Safety Aspects of the Operating System

Each approved operating system is marked accordingly. To be able to better distinguish between operating systems, the revision and CRC signature are given. The valid versions of the operating system (approved by the TÜV for safety-related programmable controllers) and the relevant signatures (CRCs) are subject to revision control and are documented in a list, which is drawn up in conjunction with the TÜV.

The running operating system version can only be read using the ***ELOP II Factory*** programming tool. The user must carry out a check (see 5.7 Checklist for creating an application program).

5.2 Mode of Operation and Functions of the Operating System

The operating system executes the application program cyclically. The following functions are carried out in a very simplified form:

- Reading the input data,
- Processing the logic functions that have been programmed according to IEC 61131-3,
- Writing the output data.

The following important functions are also performed:

- Extensive self tests,
- I/O module tests during operation,
- Data transfer,
- Diagnosis.

5.3 Safety Aspects of the Programming

5.3.1 *ELOP II Factory* Safety Concept

The ***ELOP II Factory*** safety concept ensures that,

- the programming system (PADT) functions correctly:
- errors in the programming system can be detected,
- the user operates the (PADT) correctly:
- errors on the part of the user are detected.

When a safety-related controller is commissioned for the first time or when the application program is modified, a comprehensive functional test has to be carried out to check the safety of the whole system. The following three steps must be carried out to guarantee the safety of the system:

1. the application program should be compiled twice and the code versions (CRC) compared by the user,
2. check correct implementation of the application using the data and signal flows,
3. comprehensive test of the logic by trial (see 5.3.2).

5.3.2 Checking the Configuration and the Application Program

To check that the application program is performing the specific safety functions, the user must generate suitable test cases to cover the requirements in the specification.

An independent test of each loop (consisting of input, (from an application point of view important) interlockings and output) is normally sufficient. ***ELOP II Factory*** and the measures described in this safety manual make it sufficiently unlikely that a semantically and syntactically correct code is produced that still contains unrecognized systematic errors from the code generation process.

Suitable test cases should also be generated for the numerical evaluation of formulas. Equivalent class tests are the most appropriate, i.e. tests within defined ranges of values, on the limits or that use invalid values. The test cases must be chosen in a way that demonstrates the calculation is correct. The required number of test cases depends on the formula used and must include critical value pairs.

An active simulation with sources must be used, only so the correct wiring of the system sensors and actuators (also connected via communication with remote I/O modules) can be proven. This is also the only way of checking the system configuration.

This procedure should be used when first creating an application program and when carrying out any modifications to it.

5.3.3 Creating a Project Archive

When creating a project archive the following steps should be carried out in the specified order:

1. Print the application program to compare the logic with the requirements,
2. Compile the application program to generate the configuration CRC of the CPU,
3. Note the version of the configuration CRC of the CPU by checking the CRCs. This is done by selecting the controller in Hardware Management. The versions are displayed in the **"About Configuration"** context menu item. The following is relevant when specifying a version:
   - *rootcpu.config* shows the safety-related configuration of the CPU, the configuration CRC of the CPU,
   - *rootcom.config* shows the non-safety-related configuration of the COM,
   - *root.config* shows the entire configuration including the remote I/O modules (CPU + COM).
4. Create an archive of the project on a data medium and make a note of the names of the application programs, the configuration CRCs of the CPUs and the date (this does not replace the internal documentation requirements of the user).

5.3.4 Possibility for Program and Configuration Identification

The application programs can be uniquely identified by the configuration CRCs of the *root.config*. The relevant archive can then be easily identified. The name given to an archive should contain the configuration CRCs of the *root.config*.

To ensure that the archive is not modified, compile the resource after recovery and then compare the configuration CRC of the *root.config* with the CRCs of the loaded configurations, which can be displayed using ***ELOP II Factory***.

For monitoring you can check the menu **Resource → Check Consistency** in the Control Panel.

5.4 Parameters of the programmable Controller

The parameters listed below are defined by ***ELOP II Factory*** as permitted measures in the safe operation of the programmable controller, and designated as safety-related parameters.

The settings possible during safety-related operation are not linked to one specific requirement class; they must be agreed in conjunction with the approval authority for each application in which the programmable logic controller is used.

Safety-related parameters	Safe setting
Safety time in ms	process-dependent
Watchdog time in ms	max. 50 % of safety time
Start/Restart *	Reset/Off (in RUN only)
Force enable	Reset/Off
Force (single switch) *	Reset/Off
Main enable switch (modifying the safety parameters) *	Reset/Off (in RUN only)
Test mode *	Reset/Off

*** not changeable on remote I/O modules (except F3 DIO 20/8 01)**

Table 1: Parameters of the programmable controller

5.5 Forcing

Forcing is only permitted after consulting the approval authority responsible for the plant acceptance.

When forcing is being carried out, the person responsible must ensure that sufficient safety monitoring of the process is being performed through other technical and organizational measures.

The following options are available with forcing:

- Forcing can be prohibited on a configuration by configuration basis. The PES then accepts no more force values that are defined as user-specific. In this case, new force values can only be set after the controller has been enabled for forcing again.
- All the signals can be displayed using the Force Editor of the ***ELOP II Factory*** programming tool.
- In the Force Editor it can be checked which signals are actually forced.
- All forced signals can be deactivated again via the Stop command in the Force Editor of the ***ELOP II Factory*** programming tool. The individual force values and switches remain in the same state; this means that they become active again if the Start command is activated again.

Refer to the HIMatrix manuals for further information regarding forcing.

Note	Force switches and Force parameters are explained in chapter 6.2.3.6 in this manual.

Basic information on forcing can be found in the TÜV "Maintenance Override" document.

The document can be accessed on the following TÜV homepages:

http://tuvasi.com (TÜV Rheinland)

http://www.tuv-fs.com (TÜV Süddeutschland)

5.6 Protection from Manipulation

Together with the relevant approval authority, the user must define, which measures are to be taken to provide protection from manipulation.

Protection mechanisms built into the PES and the ***ELOP II Factory*** programming system prevent unintentional or unapproved modifications to the safety system.

- A modification to the application program or the configuration generates a new CRC. These modifications can only be transferred to the PES via a download (during which the PES is in STOP).
- The operating options require that the user is logged into the PES.
- The ***ELOP II Factory*** programming tool requires a password to connect to the PES when the user logs on.
- The connection between the PADT and the PES is not required when in RUN mode.

The safety and application requirements regarding protection from manipulation should be observed. It is the responsibility of the operator to authorize staff and to take the necessary protective measures.

The password must be protected from unauthorized access. The default login and password settings must both be changed.

PES data can only be accessed if the PADT in use has access to the ***ELOP II Factory*** programming tool and the currently running version of the application project (archive maintenance!).

The connection between the PADT and the PES is only required for downloading the application program or for reading the variables/signals. During normal operation the PADT is not required; disconnecting the PADT from the PES in normal operation provides protection from unauthorized access.

5.7 Check List for the Creation of an Application Program

We recommend that the checklist below is used in order to ensure safety aspects are observed during programming and before and after loading a new or modified program.

HIMatrix Safety Manual Check list for creation of an application program			
Company			
Location			
Project			
File/archive			
Checks	**Yes**	**No**	**Remarks**
With program creating / Before a modification			
Have the PES configuration and application program been created with safety in mind?	☐	☐	
Were programming guidelines used when creating the application program?	☐	☐	
Are functionally independent sections of the program encapsulated in functions and function blocks?	☐	☐	
Were only safe signals used for all safety functions?	☐	☐	
Does each safety-related signal source correctly (also via communication) reach the application program?	☐	☐	
Is each safety-related signal drain correctly (also via communication) written?	☐	☐	
	☐	☐	
After a modification – *before* loading			
Has a person not involved in the program creation carried out a check of the application program with regard to the mandatory system specifications?	☐	☐	
Has the result of the test been documented and released (date/signature)?	☐	☐	
Has the application program been compiled twice with a subsequent comparison of both the configuration CRCs produced?	☐	☐	
Has an archive of the entire project been made before loading the program into the PES?	☐	☐	
After a modification – *after* loading			
Have an adequate number of tests been carried out for all safety-relevant logical operations (including I/O) and for all mathematical operations?	☐	☐	
Has all the force information been reset before safety mode?	☐	☐	
Do the Enable switches correspond to the settings for the maximum/specified protection?	☐	☐	
Are the CPU operating system and the CRC official TÜV-approved versions?	☐	☐	

6 Safety Aspects of the Application Program

6.1 General Sequence

General sequence in the programming of HIMatrix programmable controllers for safety-related applications:

- Specification of the controller functions,
- Writing the application program,
- Compiling the application program with the C-Code generator,
- Second compilation of the application program (both results (CRC) should be compared),
- The program is generated with no errors and is executable,
- Verification and validation.

The program can then be tested by the user and the PES can assume safe operation.

6.2 Framework for safety-related Operation

(Conditions and rules, explanations to the safety requirements see chapter 1.4)

The application program is loaded with the ***ELOP II Factory*** programming software for PCs with the operating system Windows 2000® service pack 4 and Windows XP® service pack 1.

The main features of the ***ELOP II Factory*** programming system are:

- Input (function block editor), monitoring and documentation
- Variables with symbolic names and data types (BOOL, UINT, etc.)
- Assignment of the HIMatrix system controllers
- Code generator (conversion of the application program into machine code)
- Hardware configuration
- Communication configuration

6.2.1 Programming Basics

The task that the controller will perform should already exist in the form of a specification. The specification should be used to check whether its requirements have been correctly implemented in the program. The way in which the specification is presented depends on the task in hand. This can be:

Combinatorial logic

- Cause/effect diagram
- Logic operation with functions and function blocks
- Function blocks with specified characteristics

Sequential controllers (sequence control)

- Verbal description of the enabling step conditions and of the actuators to be controlled
- Flowcharts
- Matrix or table showing the step enabling conditions and the actuators to be controlled
- Definition of the ancillary constraints, e.g. operating states, EMERGENCY STOP, etc.

The I/O concept for the system must contain an analysis of the field circuits, i.e. the types of sensors and actuators:

Sensors (digital or analog)

- Signal in normal operation (deenergize to trip mode with digital sensors, live-zero with analog sensors)
- Signals in the event of a fault
- Determining the required safety redundancies (1oo2, 2oo3) (see section 3.3)
- Discrepancy monitoring and reaction

Actuators

- Position and activation during normal operation
- Safe reaction/position in event of shutdown or power failure

Targets when writing the application program

- easy to understand
- easy to implement
- easy to modify
- easy to test

6.2.2 Signal and Variable Declaration

A **variable** is a substitution for a value within the program logic. The memory space with the stored value is symbolically addressed by the variable name. These symbolic names can have up to 256 characters. A variable is generated in the variable declaration of the program or the function block.

A **signal** is used as an allocation between the different areas of the entire control. The signal is generated in the signal editor and corresponds to the global layer of a VAR_EXTERNAL if the relation was set up.

The use of symbolic names as opposed to physical addresses has two distinct advantages for the user:

- The system designations of inputs and outputs can be used in the application program,
- Changes to how signals are assigned to input and output channels have no effect on the application program.

6.2.2.1 Assignment to the I/O Level

When the value of a variable shall be allocated to an I/O channel, an identically named signal must be generated in the signal editor of the Hardware management. Then the signal is dragged (per drag&drop) to the variable list of the program and to the channel list of the I/O module.

The required test routines for safety-related I/O modules or I/O channels are carried out automatically by the operating system.

6.2.2.2 Types of Variables

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

Variable Type	Program	Function Block	Function	Use
VAR	• (CONST)	• (CONST)	• (CONST)	Local variable
VAR_INPUT		•	•	Input variable
VAR_OUTPUT		•	•	Output variable
VAR_EXTERNAL	• (CONST, RETAIN *)	• (CONST, RETAIN *)		External to / from other POU or higher global level
VAR_GLOBAL	• (CONST)			Global to / from other POU

CONST Constants that cannot be modified by the application program (e. g. switching point)

RETAIN buffered value at warm start, initial value at cold start (* only if signal)

Table 2: Types of variables

The main feature is the inclusion of functions in function blocks that you create yourself and functions derived from standard functions. This enables a program to be clearly structured into modules (functions, function blocks). Each module can be seen as a separate entity, and a large, complex function can also be created by connecting modules together to form a larger module or program.

6.2.3 Functions of the Application Program

The programming is not subject to any hardware restrictions. The application program functions can be programmed as required.

When programming, the deenergize to trip mode must be borne in mind with physical inputs and outputs. Only components complying with IEC 61131-3 and their relevant functional requirements are used within the logic.

- The physical inputs and outputs generally operate according to the deenergize to trip mode, i.e. their safe state is "0".
- The application program contains appropriate logical and/or arithmetic functions irrespective of the deenergize to trip mode of the physical inputs and outputs.
- The logic should be designed and documented in a clear manner so that errors can easily be located. This includes the use of function charts.
- Negation can be used as required.
- Fault signals from inputs/outputs or from logic modules must be evaluated by the programmer.

6.2.3.1 System Parameters of the CPU

(not Remote I/O Modules except F3 DIO 20/8 01)

The parameters listed below determine the performance of the controller during operation and are specified in the resource attributes.

The permitted operations for the safe operation of the controller are set here using the programming tool (PADT) and the safety-related parameters are specified.

Switch	Function	Default value	Setting for safe operation
Main Enable	Following switches/parameters can be modified during operation (= RUN) with the PADT	ON	OFF*
Autostart	Automatic start after power ON of the CPU	OFF	ON/OFF**
Start/Restart allowed	Cold start, warm start or hot start by PADT in RUN or STOP mode	ON	OFF*
Loading allowed	Load release for an application program	ON	ON
Test Mode allowed	Test Mode allowed or forbidden. At Test Mode the program execution will be frozen or stopped. The outputs remain actuated and the program execution can be done in single cycle steps.	OFF	OFF
Online Test allowed	Values of signals/variables can be displayed and changed in the online test (OLT) fields	ON	OFF
Forcing allowed	Input or activation of values for PES inputs/outputs are permitted, regardless of the current value of the process/logic signal	OFF	Determined by approval authority
Stop on Force timeout	STOP of CPU after force time is exceeded	ON	Determined by approval authority

Table 3: System parameters of the CPU

* In RUN mode only setting to the value OFF is possible

** The application will determine whether it is set to ON or OFF

Additional switches and parameters can be specified for forcing (also see section 6.2.3.6 Forcing of Inputs and Outputs)

6.2.3.2 Locking the PES (not Remote I/O Modules except F3 DIO 20/8 01)

"Locking" the PES means that system functions and user access are blocked during operation. This means that the application program cannot be manipulated. The extent to which everything is blocked depends on the safety requirements regarding the use of the PES. However, it can also be determined in consultation with the approval authority responsible for the plant acceptance.

The following procedure should be followed when locking a PES:

1. The following values should be set on the controller and before compilation (see also chapter "Code Generation):

Main Enable	to	TRUE
Forcing allowed	to	FALSE (depend. on application)
Test Mode allowed	to	FALSE
Start/Restart allowed	to	TRUE
Loading allowed	to	TRUE
Autostart	to	TRUE/FALSE
Stop on Force Timeout	to	TRUE (depend. on application)

2. After loading and starting up, the following switches should be changed in the controller online in the order shown:

Start/Restart allowed	to	FALSE
Loading allowed	to	FALSE
Main Enable	to	FALSE

The following switches can only be set to different values after consulting the approval authority:

Forcing allowed	to	TRUE
Stop on Force Timeout	to	TRUE/FALSE
Start/Restart allowed	to	TRUE
Autostart	to	TRUE

To ensure safe operation, never set the "Test mode" switch to TRUE.

6.2.3.3 Unlocking the PES

"Unlocking the PES" means the removal of the active blocks, i.e. so that work can be carried out on the controller.

To unlock the PES (Main Enable to ON), the controller must be in STOP mode. Main Enable cannot be activated when the controller is running (in RUN). It can, however, be deactivated in RUN mode.

To carry out another start after the CPU is initialised (following a power failure), the procedure below should be followed to unlock the PES:

1. Main Enable to TRUE
2. Start/Restart allowed to TRUE
3. Start the application program
4. Then "lock" the PES again
   (see section 6.2.3.2 Locking the PES)

6.2.3.4 Code Generation

The code is generated after the application program has been fully entered and the inputs/outputs of the controller have been assigned. The configuration CRC of the *root.config* is also created at this time. It must be compiled twice and the configuration CRC must be identical in both compile cycles.

This is the signature of the entire CPU and remote I/O modules configuration and is displayed as a hex code in 32-bit format. All components that can be configured or modified, i.e. logic, variables, switch settings, are included in it.

6.2.3.5 Loading and Starting the Application Program

The loading process of a HIMatrix system PES can only take place when the PES has already been set to STOP.

Online loading is not possible at present.

Only *one* application program can be loaded into the relevant PES. The entire loading of the application program is monitored. The application program can then be started, i.e. the cyclic execution of routines begins.

6.2.3.6 Forcing of Inputs and Outputs

(not Remote I/O Modules except F3 DIO 20/8 01)

Forcing is the application of values to the signals (e.g. of inputs, outputs, communication) irrespective of the current value of a signal from the connected process or the result of a logic operation.

The following table shows force switches and parameters:

Switch	**Function**	**Default value**	**Setting for safe operation**	
Forcing allowed	Enable the forcing function	OFF	OFF/ON*	
Stop on Force Timeout	CPU stop after force time is exceeded	ON	ON*	
Parameter	**Function**	**Default value**	**Display**	
Forcing activated	Forcing active	OFF	OFF	ON
Remaining Force Time	Time limitation applied to the force value, time (in seconds)	0	0	Remaining Force Time or -1*

Table 4: Force switches and parameters

* Refer to the Warnings below:
The switches "Forcing allowed" and "Stop on Force Timeout" cannot be changed during operation with a "locked PES", i.e. this setting should already have been defined before locking the PES.

The switch "Forcing allowed" must only be set after consulting the approval authority.

For Forcing without time limit the value -1 for the force time must be set.

Forcing without time limit is only admissible after consulting the approval authority for the plant.

The *Forcing allowed* switch enables forcing centrally via the CPU to be either permitted or forbidden.

CPU-Switch *Forcing allowed*

- ***Not set:***

  Forcing is not possible (default setting).
  Entered force values remain in the system, but have no effect.

- ***Set:***

  Forcing is allowed.

  The entered force values only become effective if the relevant force switch is set for the data source.

After the force time has elapsed or by stopping the forcing, forcing is finished and the process value is activated again.

If "Stop on Force Timeout" is set in the properties of the controller (see information field), the controller goes into STOP state after the force time and the process values are activated again.

If "Stop on Force Timeout" is not set the controller is not stopped after the force time. Forcing is deactivated and the forced values (R-Force values) are exchanged by their process values.

This can result in **unintentional reactions of the whole system**.

With the **Stop** button in the force editor forcing will be stopped manually. In this case the controller remains in the state RUN, because the timeout time was not reached and the reaction "Stop on Force Timeout" was not set.

Forcing is only permitted after consulting the approval authority responsible for the plant acceptance.

When forcing is being carried out, the person responsible must ensure that sufficient safety monitoring of the process is being carried through other technical and organizational measures.

The period during which forcing is applied can be limited. If the forcing time is exceeded, it can be specified whether the CPU will go into STOP or if the forcing value is no longer applicable and normal operation can be resumed. Exceeding the forcing time therefore always has an impact on the application program and so on the process.

The force value is saved in the CPU. If the CPU is switched from RUN to STOP mode, forcing is deactivated to prevent the controller from being unintentionally started with active force signals.

6.2.3.7 Online Test

With the function *Online Test* OLT (Online Test) fields could be used within the logic for displaying and for forcing of signals/variables during operation of the controller.

CPU-Switch *Online Test allowed*

- ***Not set:***

  Online Test is not possible.

  If the switch *Online Test allowed* is switched off then values of signals/variables could only be displayed in OLT fields but not changed.

- ***Set:***

  Online Test is possible (default setting)

  If the switch *Online Test allowed* is switched on then values of signals/variables could be displayed and forced in the OLT fields. The forced value is only valid until a function in the logic overwrites the value.

Further informations about using OLT fields you could find under the index "OLT field" in the online help of ***ELOP II Factory Project Management***.

6.2.4 Program Documentation for safety-related Applications

The ***ELOP II Factory*** programming system enables project documentation to be automatically printed. The main types of documentation are:

- Interface declaration
- List of signals
- Logic
- Description of data types
- Configurations for system, modules and system parameters
- Network configuration
- Signal cross-reference list
- Code generator information

The documentation is part of the functional acceptance of a system requiring approval from an authority (e. g. TÜV). The functional acceptance only relates to the user functions, not to the safety-related modules and programmable controllers of the HIMatrix system that have already been type tested.

6.2.5 Approval by Approval Authorities

When configuring a system requiring approval, we recommend to involve the approval authorities as early as possible.

7 Communication Configuration

7.1 Non-safety-related Communication

Besides with the physical input/output signals, signals can also be exchanged with another system via a data link. The variables required for this purpose are declared in the protocol area using the ***ELOP II Factory*** programming system.

Data can be exchanged in both read and write forms.

All data imported from non-safe sources must not be used for the safety functions of the application program.

Depending on the device, Modbus, OPC, TCP-SR, SNTP, Profibus-DP and Interbus are available for non-safety-related communication.

7.2 Safety-related Communication (Peer-to-Peer)

Monitoring of a safety-related communication has to be configured in the Peer-to-Peer editor.

The "ReceiveTMO" monitoring time must also be specified. If no further imported signals are received within the specified time, the signals are set to their initial values (specified by the user) in the PES.

»ReceiveTMO« is a safety-related parameter!

The value of a signal must be present longer than "Receive TMO" or be monitored via Loop-Back, if each value has to be transferred.

7.2.1 ReceiveTMO

ReceiveTMO is the monitoring time on PES_1 during which a correct response must be received from PES_2.

Note	ReceiveTMO also applies in the reverse direction, i.e. from PES_2 to PES_1.

The ReceiveTMO (safety-related) is part of the Worst Case Reaction Time T_R (see maximum response time, chapter 7.2.2). The ReceiveTMO must be calculated and entered via the Peer-to-Peer Editor.

If the communication partner does not receive a correct answer within the ReceiveTMO the safety-related communication is closed and all signals imported over this communication channel will be set to the initial values defined by the user.

The following requirement must be met for a network in which potential lost of data packages could occur:

ReceiveTMO ≥ 2 * Response Time (minimum)

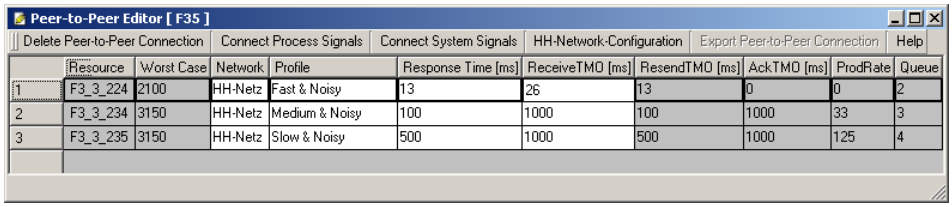
(valid for profile "Fast & Noisy")

If this requirement is met, the loss of at least one data packet can be tolerated without the Peer-to-Peer connection being dropped.

If this requirement is not met, the availability of a Peer-to-Peer connection can only be guaranteed in a network that is free of collisions and faults. However, this does not affect the safety of the CPU.

Note	The maximum permitted value for ReceiveTMO depends on the application process and is set in the Peer-to-Peer Editor together with the maximum expected Response Time and the profile.

Example values for parameters of a Peer-to-Peer connection:

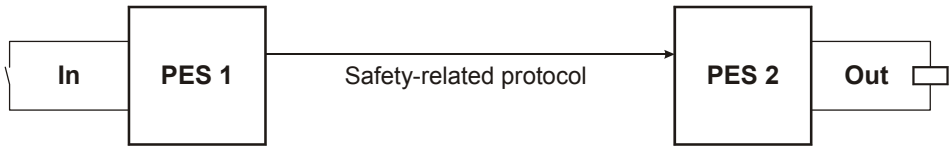


	Resource	Worst Case	Network	Profile	Response Time [ms]	ReceiveTMO [ms]	ResendTMO [ms]	AckTMO [ms]	ProdRate	Queue
1	F3_3_224	2100	HH-Netz	Fast & Noisy	13	26	13	0	0	2
2	F3_3_234	3150	HH-Netz	Medium & Noisy	100	1000	100	1000	33	3
3	F3_3_235	3150	HH-Netz	Slow & Noisy	500	1000	500	1000	125	4

Figure 11: Peer-to-Peer connection parameters

7.2.2 Calculating the maximum Response Time

The maximum response time T_R ("Worst Case") between changing a transmitter of PES 1 (In) and the response of the output (Out) of PES 2 can be calculated as follows:



$$T_R = t_1 + t_2 + t_3 + t_4$$

T_R worst case

t_1 2 ∗ watchdog time of PES 1

t_2 0 ms, if "Production Rate" = 0 (normal case),

otherwise "ReceiveTMO" + watchdog time of PES 1

t_3 ReceiveTMO

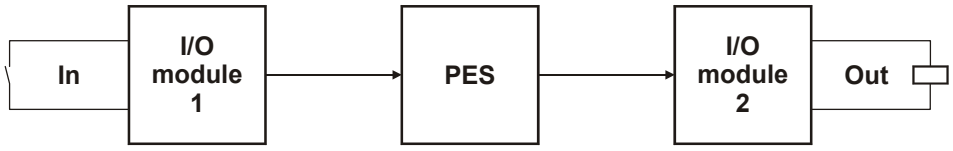
t_4 2 ∗ watchdog time of PES 2

The time T_R can be found in the Peer-to-Peer editor in the "Worst Case" column.

The maximum response time depends on the process and must be determined in conjunction with the acceptance authorities/department.

7.2.3 Calculation of the max. Response Time with Remote I/O Modules

The maximum response time T_R between changing a transmitter (In) of the first remote I/O module (i.e. F3 DIO 20/8 01) and the response of the output of the second remote I/O module (Out) can be calculated as follows:



$$T_R = t_1 + t_2 + t_3 + t_4 + \quad \text{(input path)}$$

$$+ t_5 + t_6 + t_7 \quad \text{(output path)}$$

T_R worst case

t_1 2 ∗ watchdog time of remote I/O module 1

t_2 0 ms, if "Production Rate" = 0 (normal case),

otherwise "ReceiveTMO$_1$" + watchdog time of remote I/O module 1

t_3 ReceiveTMO$_1$

t_4 2 ∗ watchdog time of PES

t_5 ReceiveTMO$_2$

t_6 0 ms, if "Production Rate" = 0 (normal case),

otherwise "ReceiveTMO$_2$" + watchdog time of PES

t_7 2 ∗ watchdog time of remote I/O module 2

Note: Both remote I/O modules 1 and 2 can be identical. The times also apply if a PES is used in place of a remote I/O module.

Terms

ReceiveTMO	Monitoring time in PES 1 during which a valid reply must be received from PES 2. After the time has expired, the safety-related communication is closed.
ReceiveTMO$_1$	remote I/O module 1 → PES
ReceiveTMO$_2$	PES → remote I/O module 2
Production Rate	Minimum time between two data transmissions
Watchdog Time	Maximum permitted duration of the RUN cycle of a PES
Worst Case	Maximum response time between the transfer of the signal change of a physical input (In) of a PES 1 and the change of the physical output (Out) of a PES 2.

The data are transferred using a safety-related protocol.

The operator must ensure that the Ethernet used for Peer-to-Peer communication is adequately protected from unauthorized access (i.e. by hackers).
The nature and extent of the measures to be taken must be determined in conjunction with the approval authorities.

8 Use in Central Fire Alarm Systems

All HIMatrix systems with analog inputs can be used for central fire alarm systems in accordance with DIN EN 54-2 and NFPA 72.

The application program must fulfil the functions laid down for central fire alarm systems according to the cited standards.

The required maximum cycle time of 10 seconds (DIN EN 54-2) for central fire alarm systems can easily be achieved with the systems as the cycle times of these systems can be measured in milliseconds. Similarly, the required 1 second safety time (if necessary) can also be easily achieved (error response time).

According to EN 54-2 the fire alarm system has to be in the fault report state within 100 seconds after the HIMatrix system has received the fault report.

The fire alarms are connected using the energize to trip mode with line monitoring for the detection of short-circuits and breaks. The digital and analog inputs can be used with F35, the analog inputs with F3 AIO 8/4 01 and the AI 8 01 analog input module with F60.

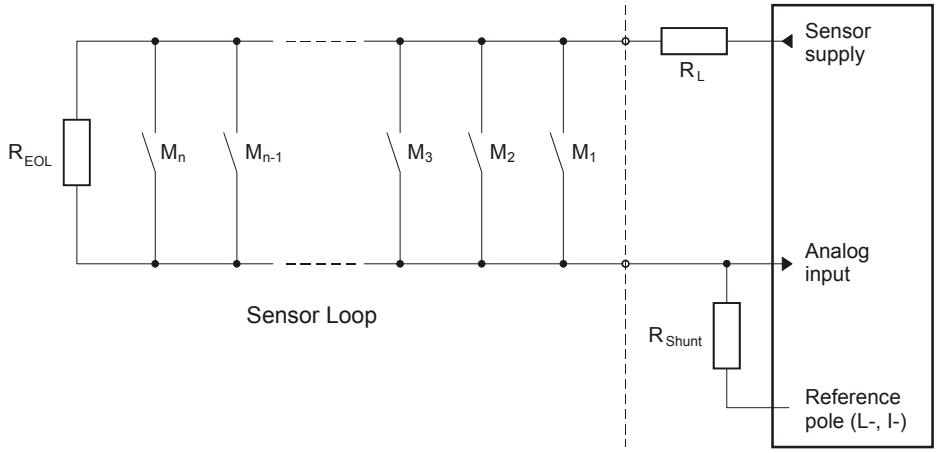


Figure 12: Wiring of fire alarms

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

For the application, the resistance of R_{EOL}, R_L and R_{Shunt} should be calculated depending on the sensors being used and the number of sensors per alarm loop. The required data is contained in the relevant data sheet from the sensor manufacturer.

The alarm outputs, used for activating lamps, sirens, horns, etc, are operated using the energize to trip mode. These outputs must be monitored for line breaks and short-circuits. This can be done by feeding back the output signals directly from the actuator to the inputs.

The current in the actuator circuit should preferably be monitored via an analog input with an appropriate shunt. A series connection of zener diode and series protects the input against over-voltage in case of short-circuit.

For an explicit line break monitoring (at de-energized outputs DO) a transmitter supply additionally to the analog inputs is necessary (see scheme below):

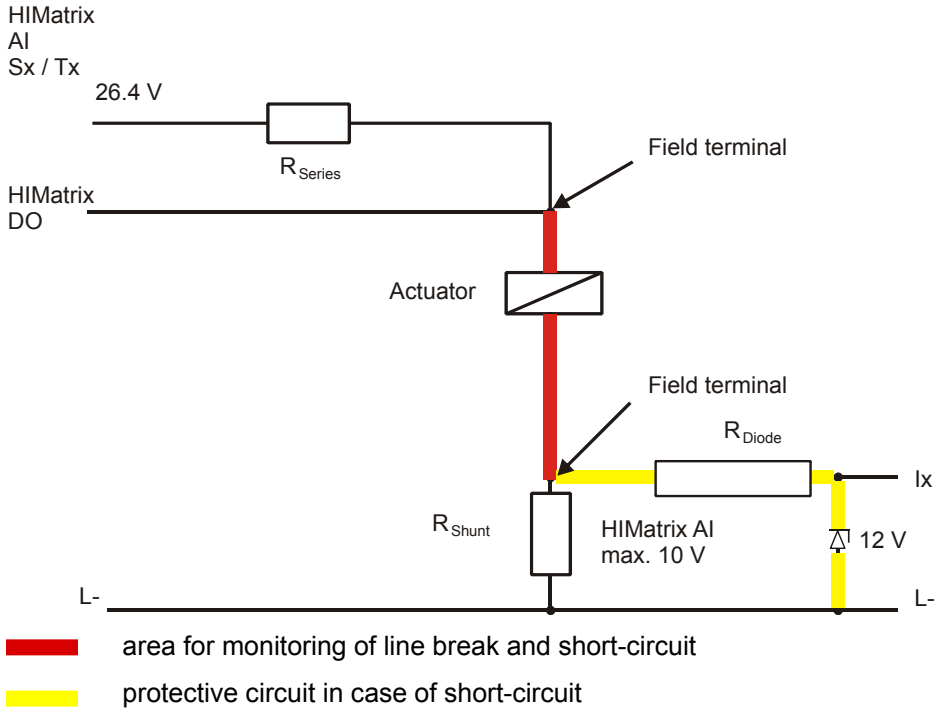


Figure 13: Example for line break and short-circuit monitoring of digital outputs (actuator circuit)

In chapter "Line Monitoring" at HIMatrix F35 you will find an example for monitoring short-circuit and line break of actors via analog inputs.

Visual display systems, indicator light panels, LED displays, alphanumeric displays, audible alarms, etc. can all be controlled using an appropriate application program.

The routing of fault signals via input and output modules or to routing equipment must be carried out using the deenergize to trip mode.

Fire alarms can be transmitted from one HIMatrix system to another using the Ethernet communications (OPC) standard available. Any breakdown in communications must be signaled.

HIMatrix systems that are used as central fire alarm systems must have a redundant power supply. Precautions must also be taken against the power supply failing, i.e. using a battery-powered horn. There must be no interruption in operation when switching between the mains supply and the back-up supply. Voltage dips of up to 10 ms are permitted.

When there is a fault in the system, the system signals specified in the application program are written by the operating system. This enables error signaling to be programmed to signal errors detected by the system. In the event of an error, safety-related inputs and outputs are switched off, i.e. 0-signals are applied to all the channels of faulty inputs and all the channels of faulty outputs are switched off.

9 Operating Conditions

The devices were developed in compliance with the requirements of the following standards for EMC, climate and environment:

IEC/EN 61131-2	Programmable Controllers, Part 2 Equipment Requirement and Tests
IEC/EN 61000-6-2	EMC Generic Standards, Part 6-2 Immunity for Industrial Environments
IEC/EN 61000-6-4	EMC Generic Emission Standard Industrial Environment

For the use of the safety-related HIMatrix controller systems the following common conditions have to be met:

Protection class	Protection class II according to IEC/EN 61131-2
Pollution	Pollution degree II
Altitude	< 2000 m
Enclosure	Standard: IP 20 If requested by the relevant application standards (e. g. EN 60204, EN 954-1), the device must be installed in a required enclosure (e. g. IP 54).

9.1 Climatic Conditions

The most important tests and limit values for climatic conditions are listed in the following table:

IEC/EN 61131-2 Chapter 6.3.4	**Climatic Tests**
	Temperature, operating: 0...60 °C (Test limits -10...+70 °C)
	Storage Temperature: -40...85 °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

9.2 Mechanical Conditions

The most important tests and limit values for mechanical conditions are listed in the following table:

IEC/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

9.3 EMC Conditions

The most important tests and limit values for EMC conditions are listed in the following tables:

IEC/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
6.3.6.2.2 IEC/EN 61000-4-3	RFI test (10 V/m): 26 MHz...1 GHz, 80 % AM
6.3.6.2.3 IEC/EN 61000-4-4	Burst test: 2 kV power supply / 1 kV signal lines
6.3.6.2.4 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

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

9.4 Voltage Supply

The most important tests and limit values for the voltage supply of the equipment are listed in the following table:

IEC/EN 61131-2 Chapter 6.3.7	Verification of DC Power Supply Characteristics
	The power supply must meet alternatively the following standards: IEC/EN 61131-2 or SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage)
	The fusing of the HIMatrix devices must be in accordance to the statements of this manual
6.3.7.1.1	Voltage range test: 24 VDC, -20 %...+25 % (19.2 V...30.0 V)
6.3.7.2.1	Momentary interruption immunity test: DC, PS 2: 10 ms
6.3.7.4.1	Reversal of DC power supply polarity test: application note in the concerning 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

HIMA
...the safe decision.

HIMA Paul Hildebrandt GmbH + Co KG
Industrial Automation
Postfach 1261 • D - 68777 Bruehl
Phone: (+49) 6202 709-0 • Fax: (+49) 6202 709-107
E-mail: info@hima.com • Internet: www.hima.com

(0610)