HIMatrix® M45

Safety Manual

SAFETY
NONSTOP

HIMA

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

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

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

Contact

HIMA contact details:

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Revision index	Changes	Type of change	
		technical	editorial
1.00	First issue	X	X
1.01	Reviewed, deleted: fault tolerance time, energize-to-trip principle Section: Reaction in the event of a fault	X	X
1.02	Modified: Chapters concernin the safety manual, proof test		X
2.00	Adjusted to SILworX V7, operating system V11/16, Added: Reaction in the event of a fault Changed: Response time	X	X

Table of Contents

1 Safety Manual

This manual contains information on how to operate the HIMatrix safety-related automation devices in the intended manner.

The following conditions must be met to safely install and start up the HIMatrix M45 automation devices, and to ensure safety during their operation and maintenance:

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

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

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

HIMA develops, manufactures and tests the HIMatrix M45 automation systems in compliance with the pertinent safety standards and regulations. The use of the devices is only allowed if the following conditions are met:

- They are only used for the intended applications.
- They are only operated under the specified environmental conditions.
- They are only operated in connection with the approved external devices.

To provide a clearer exposition, this manual does not specify all details of all versions of the HIMatrix M45 automation devices. Refer to the corresponding manuals for further details.

This safety manual represents the "Original instructions" as of Directive on Machinery (Directive 2006/42/EC).

The "Original documentation" for the HIMA system is written in German language. The statements made in the German documentation shall apply.

1.1 Structure and Use of the Document

This safety manual examines the following topics:

- Intended use
- Safety concept
- Central functions
- Inputs
- Outputs
- Software
- Safety-related aspects of the user program
- Communication configuration
- Use in fire alarm systems
- Appendix:
  - Increasing the SIL of sensors and actuators
  - Glossary
  - Indexes

1.2 Target Audience

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

1.3 Writing Conventions

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

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

Safety notices and operating tips are particularly marked.

1.3.1 Safety Notices

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

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

⚠ SIGNAL WORD

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

The signal words have the following meanings:

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

NOTE

Type and source of damage!
Damage prevention

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

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

Useful tips and tricks appear as follows:

TIP	The tip text is located here.

2 Usage Notes

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

2.1 Intended Use

This chapter describes the conditions for using HIMatrix M45 systems.

2.1.1 Scope

The safety-related HIMatrix controllers can be used in applications up to SIL 3 in accordance with IEC 61508.

The HIMatrix systems are certified for use in process controllers, protective systems, burner controllers, and machine controllers.

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

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

If a fault occurs, a system operating in accordance with the de-energize-to-trip principle enters the de-energized state to perform its safety function.

2.1.1.2 Use in Fire Alarm Systems

HIMatrix systems are suitable for use in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72. For these fire alarm systems, the following requirements must be met:

- To contain the risks, the active must be adopted state on demand.
- Open-circuit and short-circuit detection must be provided.

The environmental requirements must be observed.

For details, refer to the safety manual of the HIMatrix F systems (HI 800 023 E).

2.2 Environmental Conditions

Condition type	
Protection class	Protection class III in accordance with IEC/EN 61131-2
Ambient temperature	0...+60 °C
Storage temperature	-40...+85 °C
Pollution	Pollution degree II in accordance with IEC/EN 61131-2
Altitude	< 2000 m
Enclosure	Standard: IP20
Requirements of the application	If required by the relevant application standards (e.g., EN 60204, EN 13849), the HIMatrix system must be installed in an enclosure of the specified protection class (e.g., IP54).
Supply voltage	24 VDC

Table 1: Environmental Conditions

All the environmental requirements specified in this manual must be observed when operating the HIMatrix system.

2.3 Tasks of Operators and Machine and System Manufacturers

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

Machine and system manufacturers must sufficiently validate that the HIMatrix systems were properly programmed.

2.3.1 Connection of Communication Partners

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

2.3.2 Use of Safety-Related Communication

When implementing safety-related communications between various devices, ensure that the overall response time does not exceed the fault tolerance time. All calculations must be performed in accordance with the rules given in this chapter.

2.4 ESD Protective Measures

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

NOTE

Electrostatic discharge can damage the electronic components within the HIMatrix systems!

- **When performing the work, make sure that the workspace is free of static, and wear an ESD wrist strap.**
- **If not used, ensure that the module is protected from electrostatic discharge, e.g., by storing it in its packaging.**

2.5 Residual Risk

No imminent risk results from a HIMatrix M45 system itself.

Residual risk may result from:

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

2.6 Safety Precautions

Observe all local safety requirements and use the protective equipment required on site.

2.7 Emergency Information

A HIMatrix M45 system is a part of the safety equipment of a plant. If a device or a module fails, the system enters the safe state.

In case of emergency, no action that may prevent the HIMatrix M45 systems from operating safely is permitted.

2.8 Additional System Documentation

In addition to this manual, the following documents for configuring HIMatrix M45 systems are also available:

Name	Content	Document no.	Format
HIMatrix M45 system manual	Description of the M45 system with the corresponding specifications	HI 800 651 E	PDF file
Certificate	Test result		PDF file
Version list	Versions tested by the TÜV		PDF file
HIMatrix M45 module manuals			PDF files
Communication manual	Description of the communication protocols, ComUserTask and their configuration in SILworX	HI 801 101 E	PDF file
SILworX online help	Instructions on how to use SILworX	-	CHM file
SILworX first steps manual	Introduction to SILworX	HI 801 103 E	PDF file

Table 2 HIMatrix M45 System Documentation

For more details on the modules, refer to the corresponding manuals.

3 Safety Concept for Using the PES

This chapter contains important general information on the functional safety of HIMatrix M45 systems.

- Safety and availability
- Time parameters important for safety
- Proof test
- Safety requirements
- Certification

3.1 Safety and Availability

The HIMatrix M45 systems are certified for use in process controllers, protective systems, burner controllers, and machine controllers.

No imminent risk results from the HIMatrix M45 systems.

⚠ WARNING

Possible physical injury caused by safety-related automation systems improperly connected or programmed.

Check all connections and test the entire system for compliance with the specified safety requirements before start-up!

3.1.1 Calculating the PFD, PFH and SFF Values

The PFD, PFH and SFF values have been calculated for the HIMatrix M45 systems in accordance with IEC 61508.

The PFD, PFH and SFF values are provided by HIMA upon request.

3.1.2 Self-Test and Fault Diagnosis

The operating system of the controllers executes comprehensive self-tests at start-up and during operation. The following components are tested:

- Processors
- Memory areas (RAM, NVRAM)
- Watchdog
- The individual I/O channels

If faults are detected during the tests, the operating system switches off the defective module or faulty I/O channel.

In non-redundant systems, this means that sub-functions or even the entire PES may shut down.

All HIMatrix M45 modules are equipped with LEDs to indicate that faults have been detected. This allows the user to quickly diagnose faults detected in a device or the external wiring.

Additionally, the user program can evaluate various system variables displaying the module status.

Extensive diagnostics of the system performance and detected faults are stored in the diagnostic memory of the controllers. The diagnostics can also be read after a system fault using the PADT.

For more information on evaluating diagnostic messages, refer to the system manual (HI 800 651 E).

For a very few number of component failures that do not affect safety, the HIMatrix M45 system does not provide any diagnostic information.

3.1.3 PADT

Using the PADT, the user creates the program and configures the controller. The safety concept of the PADT supports the user in the proper implementation of the control task. The PADT implements numerous measures to check the entered information.

The PADT is a personal computer installed with the SILworX programming tool.

3.2 Time Parameters Important for Safety

These are:

- Safety time
- Watchdog time
- Worst case reaction time

3.2.1 Safety Time (of PES)

The safety time is the time period after an internal fault occurred, during which the PES is in the RUN state and must provide a response.

From the process view point, the safety time is the maximum time within which the safety system must provide a response on the output after a change of the input signals (response time).

The safety time setting does not affect the HIMatrix M45 PES.

3.2.2 User Program Safety Time

The safety time for the user program cannot be set directly. To calculate the safety time for a user program, HIMatrix M45 uses the parameters *Max. Safety Time* of the resource and *Maximum Number of Cycles*. Refer to Chapter 8.2.9 for more details.

3.2.3 Worst Case Reaction Time

The worst case reaction time applies to an undisturbed system. It is the maximum time that a HIMatrix M45 system may require to respond to a change of an input signal with an output signal. In HIMatrix M45 controllers running in cycles, the worst case reaction time is twice the maximum cycle time, i.e., twice the watchdog time. The requisites are:

- The logic of the user program does not include any delaying elements.
- A user program cycle takes a processor system cycle.

The cycle time of the controller includes processing of the following tasks:

- Reading the inputs
- Processing the user program/s
- Writing to the outputs
- Process data communication
- Performing test routines

Further, the switching times of the inputs and outputs must be taken into account when determining the worst case for the overall system.

In general, the response time is composed of:

- Switching time of the input
- Twice the value of the user program's watchdog time
- Switching time of the output

To calculate the response time during communication, refer to Chapter 9 or the communication manual (HI 801 101 E).

3.2.4 Processor System Watchdog Time

The watchdog time is preset in the menu for configuring the PES properties. This time is the maximum permissible duration of a RUN cycle (cycle time). If the cycle time exceeds the preset watchdog time, the system is shut down. Afterwards, if Autostart was configured, the system restarts. If Autostart was not configured, the system enters the STOP/VALID CONFIGURATION state.

The processor system watchdog time may be set to ≤ ½ * PES safety time.

Range of values for the watchdog time	Default value
4...5 000 ms	200 ms

Table 3: Range of Values for the Watchdog Time

The value set for the processor system's watchdog time must be sufficiently high to ensure that load peaks occurring during faulty-free operation cannot cause the watchdog time to be exceeded.

To estimate a suitable value, HIMA recommends testing a system that is as complete as possible:

- The HIMatrix M45 hardware is completely mounted.
- Communication partners exist, potentially as simulations.
- Sensors and actuators potentially exist as simulations.
- The project exists as complete as possible.

To determine the minimum value for the watchdog time

1. Operate the system under full load. Communication should also run under full load.
2. Specify input data to allow that the longest program paths are preferably passed through. To this end, input value sequences may be necessary.
3. Perform the reload.
4. In the Control Panel, observe the maximum cycle time values. Note down the largest cycle time values.

► The minimum watchdog time value is the largest cycle time among the ones noted down.

The value set for the watchdog time should be the minimum value just determined increased by a safety margin.

3.2.5 Watchdog Time of the User Program

Each user program has its own watchdog time.

The watchdog time for the user program cannot be set directly. To calculate the watchdog time for a user program, HIMatrix M45 systems use the parameters *Watchdog Time* of the resource and *Maximum Number of Cycles*.

Make sure that the calculated watchdog time is half the response time value required for the process portion processed by the user program.

3.3 Proof Test (in Accordance with IEC 61508)

A proof test is a periodic test performed to detect any hidden faults in a safety-related system so that, if necessary, the system can be restored to a state where it can perform its intended function.

HIMA safety systems must be subject to a proof test **in intervals of 10 years**.

This interval can often be extended by calculating and analyzing the implemented safety loops.

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

3.3.1 Proof Test Execution

The execution of the proof test depends on how the system (EUC = equipment under control) is configured, its intrinsic risk potential and the standards applicable to the equipment operation and required for approval by the responsible test authority.

According to IEC 61508 1-7, IEC 61511 1-3, IEC 62061 and VDI/VDE 2180 sheets 1 to 4, the operator of the safety-related systems is responsible for performing the proof tests.

3.3.2 Frequency of Proof Tests

The HIMatrix M45 controller can be proof tested by testing the entire safety loop.

In practice, shorter proof test intervals are required for the input and output field devices (e.g., every 6 or 12 months) than for the HIMatrix M45 controller. Testing the entire safety loop together with a field device automatically includes the test of the HIMatrix M45 controller. There is therefore no need to perform additional proof tests of the HIMatrix M45 controller.

If the proof test of the field devices does not include the HIMatrix M45 controller, the HIMatrix M45 controller must be tested for SIL 3 at least once every 10 years. This can be achieved by restarting the HIMatrix M45 controller.

If additional proof test requirements apply for special modules, the manual of the corresponding module must be observed.

3.4 Safety Requirements

The following safety requirements must be met when using the safety-related PES of the HIMatrix M45 system:

3.4.1 Hardware Configuration

Personnel configuring the HIMatrix M45 hardware must observe the following safety requirements.

3.4.1.1 Product-Independent Requirements

- To ensure safety-related operation, only approved safety-related hardware and software may be used. The approved hardware and software are listed in the *Version List of Devices and Firmware of HIMatrix M45 Systems of HIMA Paul Hildebrandt GmbH*, *Certificate-No. 01/205/5355/00/13*. The latest versions can be found in the version list maintained together with the test authority. The latest version list can be downloaded from the HIMA website at `www.hima.com`.
- All environmental conditions specified in this safety manual (see Chapter 2.2) about EMC, mechanical, chemical, and climatic influences must be observed.

3.4.1.2 Product-Dependent Requirements

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

  Even if faults occur, the power supply units must ensure a supply voltage not exceeding 35 V!

3.4.2 Programming

Personnel developing user programs must observe the safety requirements specified below.

3.4.2.1 Product-Independent Requirements

- In safety-related applications, ensure that the safety-relevant system parameters are properly configured.
- In particular, this applies to the system configuration, maximum cycle time and safety time.

3.4.2.2 Product-Dependent Requirements

Requirements for using the programming tool

- **SILworX** must be used for programming.
- **The proper implementation of the application specification must be validated and verified. A complete test of the logic must be performed by trial.**
- The system response to faults in the fail-safe input and output modules must be defined in the user program in accordance with the system-specific safety-related conditions.

3.4.3 Communication

- When implementing safety-related communications between the various devices, ensure that the system's overall response time does not exceed the allowed response time. All calculations must be performed in accordance with the rules given in 9.2.
- During the transfer of (safety-related) data, cyber security (IT security) rules must be observed.

  The transfer of safety-relevant data through public networks like the Internet is only permitted if additional security measures such as VPN tunnel and firewall have been implemented.
- If data is transferred through company-internal networks, administrative or technical measures must be implemented to ensure sufficient protection against manipulation, e.g., using a firewall to separate the safety-relevant components of the network from other networks.
- Never use the standard protocols to transfer safety-related data.
- Only devices with safe electrical separation may be connected to the communication interfaces.

3.4.4 Maintenance Work

Operators are responsible for ensuring proper maintenance work. They must take the required measures to guarantee safe operation during maintenance.

Whenever necessary, the operator must consult with the test authority responsible for the factory acceptance test (FAT) and define administrative measures appropriate for regulating access to the systems.

3.4.5 Cyber Security for HIMatrix M45 Systems

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

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

A HIMatrix M45 installation consists of the following parts to be protected:

- HIMatrix M45 PES
- PADT
- OPC server: X-OPC DA, X-OPC AE (optional)
- Communication connections to external systems (optional)

HIMatrix M45 with basic settings is already a system fulfilling the requirements for cyber security.

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

- Each change to the user program or configuration results in a new configuration CRC.
- The operating options depend on the rights of the user logged into the PES.
- The programming tool prompts the user to enter a password in order to log in to the PES.

- PES data can only be accessed if the PADT is operating with the current version of the user project (archive maintenance!).
- Connection between the PADT and PES is not required in RUN and can be interrupted.
  The PADT can be shortly connected for maintenance work or diagnostic tasks.

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

⚠ WARNING

Physical injury possible due to unauthorized manipulation of the controller!

The controller must be protected against unauthorized access!

For instance:

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

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

- Meaningful allocation of user groups.
- Maintained network maps help ensuring that secure networks are permanently separated from public networks, and if required, only a well-defined connection exists (e.g., via a firewall or a DMZ).
- Use of appropriate passwords which cannot be guessed easily.

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

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

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

3.5 Certification

HIMA safety-related automation devices (programmable electronic systems, PES) of the HIMatrix M45 system have been tested and certified by TÜV for functional safety in accordance with CE and the standards listed below:

In addition to the specified standards, the individual devices can be certified for further application areas. Refer to the device-specific manuals for further details.

3.5.1 TÜV Certificate/EU Type Approval Test

TÜV Rheinland Industrie Service GmbH
Automation, Software and Information Technology
Am Grauen Stein
51105 Köln

Certificate/EC Type Test Certificate n. 01/205/5355/13
Safety PES System Family
HIMatrix M45

3.5.2 Current Standards

International standards:

EN / IEC 61508, Parts 1-7: 2010	SIL 3
EN / IEC 61511, Parts 1-3: 2004	SIL 3
EN ISO 13849-1: 2008 + AC:2009	Performance level e
EN 62061: 2005 + AC:2010 + A1:2013	SIL CL 3
EN 50156-1: 2004	SIL 3
EN 12067-2: 2004	
EN 298: 2012	
NFPA 85: 2011	
NFPA 86: 2011	
EN 61131-2: 2007	
EN 61326-3-1:2008	
EN 54-2: 1997 + AC:1999 + A1:2006	
EN 50130-4: 2011	Test standard for EN 54-2
NFPA 72: 2013	
EU Directives	See the corresponding declarations of conformity

The following chapter contains a detailed list of all environmental and EMC tests performed.

All devices have received the CE mark of conformity.

3.5.3 Test Conditions

The devices have been tested to ensure compliance with the following standards for EMC, climatic and environmental requirements:

Standard	Content
IEC/EN 61131-2: 2007	Programmable controllers, Part 2 Equipment requirements and tests
IEC/EN 61131-6: 2012	Programmable controllers, Part 6 Functional Safety
IEC/EN 61000-6-2: 2005	Electromagnetic Compatibility (EMC) Part 6-2: Generic standards. Immunity for industrial environments
IEC/EN 61000-6-4: 2007 + A1:2011	Electromagnetic Compatibility (EMC) Part 6-4: Generic standards. Emission standard for industrial environments.

Table 4: Standards for EMC, Climatic and Environmental Requirements

3.5.3.1 Climatic Conditions

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

Standard	Climatic tests
IEC/EN 61131-2	Ambient temperature: 0...+60 °C (test limits: -10...+70 °C)
	Storage temperature: -40...+85 °C
	Dry heat and cold resistance tests: +70 °C / -40 °C, 16 h, +85 °C, 1 h Power supply not connected
	Temperature changes, withstand test: Fast temperature changes: -40 °C / +70 °C, power supply not connected
	Immunity test Slow temperature changes: -10 °C / +70 °C, power supply not connected
	Cyclic damp-heat withstand tests: +25 °C / +55 °C, 95 % relative humidity, power supply not connected
EN 54-2	Damp-heat 93 % relative humidity, 40 °C, 4 days in operation 93 % relative humidity, 40 °C, 21 days, power supply not connected

Table 5: Climatic Conditions

Operating requirements other than those specified in this document are described in the manuals of the compact controllers, remote I/Os or modules.

3.5.3.2 Mechanical Conditions

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

IEC/EN 61131-2	Mechanical tests
	Vibration immunity test: 5...8,4 Hz, 3,5 mm 8.4...150 Hz, 1 g, EUT in operation, 10 cycles per axis
	Shock immunity test: 15 g, 11 ms, EUT in operation, shocks per axis and direction (18 shocks)

Table 6: Mechanical Tests

3.5.3.3 EMC Conditions

In accordance with IEC 61131-2, the interference levels specified in table Table 7 are required for programmable controllers. HIMatrix systems meet these requirements.

Test standards	Interference immunity tests	Criterion
IEC/EN 61000-4-2	ESD test: 4 kV contact discharge, 8 kV air discharge	B
IEC/EN 61000-4-3	RFI test (10 V/m): 80 MHz...1 GHz, 80 % AM RFI test (3 V/m): 1.4 GHz...2 GHz, 80 % AM RFI test (1 V/m): 2.0 GHz...2.7 GHz, 80 % AM	A
IEC/EN 61000-4-4	Burst test Supply voltage: 2 kV Signal lines: 2 kV Shielded communication lines: 1 kV	B
IEC/EN 61000-4-5	Surge: Supply voltage: 2 kV CM, 1 kV DM Signal lines (AC): 2 kV CM, 1 kV DM Shielded lines: 2 kV CM Other: 1 kV CM	B
IEC/EN 61000-4-6	High frequency, asymmetrical 10 V, 150 kHz...80 MHz, 80 % AM 20 V, ISM frequencies, 80 % AM (in accordance with EN 298)	A
IEC/EN 61000-4-18	Damped oscillatory wave test 2,5 kV L-, L+ / PE 1 kV L+ / L- Signal lines (AC): 2.5 kV CM, 1 kV DM Shielded lines: 0.5 kV CM Other: 1 kV CM, 0.5 kV DM	B

Table 7: Interference Immunity Tests in accordance with IEC 61131-2, Zone C

Higher interference levels are required for safety-related systems. HIMatrix systems meet these requirements in accordance with IEC 62061 and IEC 61326-3-1.

Test standards	Interference immunity tests	Criterion
IEC/EN 61000-4-2	ESD test: 6 kV contact discharge, 8 kV air discharge	FS
IEC/EN 61000-4-3	RFI test (20 V/m): 80 MHz...1 GHz, 80 % AM RFI test (10 V/m): 1.4 GHz...2 GHz, 80 % AM RFI test (3 V/m): 2.0 GHz...2.7 GHz, 80 % AM	FS FS FS
IEC/EN 61000-4-4	Burst test Supply voltage: 3 kV Signal lines: 2 kV	 FS FS
IEC/EN 61000-4-5	Surge: DC supply voltage: 2 kV CM, 1 kV DM Signal lines: 2 kV CM	 FS FS
IEC/EN 61000-4-6	High frequency, asymmetrical 10 V, 150 kHz...80 MHz, 80 % AM	 FS
IEC/EN 61000-4-16	Supply and signal lines: 1…10 V, 20 dB/decade (1.5…15 kHz) 10 V (15…150 kHz) 10 V constant (with DC, $16^2/_3$ Hz, 50/60 Hz, 150/180 Hz) 100 V temporary (1 s, with DC, $16^2/3$ Hz, 50/60 Hz)	 FS FS FS FS

Table 8: Interference Immunity Tests in accordance with IEC 61326-3-1

Higher interference levels are required for safety-related systems. HIMatrix systems meet these requirements in accordance with IEC 61326-3-2.

Test standards	Interference immunity tests	Criterion
IEC/EN 61000-4-2	ESD test: 6 kV contact discharge, 8 kV air discharge	A
IEC/EN 61000-4-3	RFI test (10 V/m): 80 MHz...1 GHz, 80 % AM RFI test (10 V/m): 1.4 GHz...2 GHz, 80 % AM RFI test (3 V/m): 2.0 GHz...2.7 GHz, 80 % AM	A
IEC/EN 61000-4-4	Burst test Supply voltage: 2 kV Signal lines: 1 kV	A
IEC/EN 61000-4-5	Surge: Supply voltage: 1 kV CM, 0.5 kV DM Signal lines: 1 kV CM	 A FS
IEC/EN 61000-4-6	High frequency, asymmetrical 10 V, 10 kHz...80 MHz, 80 % AM 20 V, ISM frequencies, 80 % AM	A

Table 9: Interference Immunity Tests in accordance with IEC 61326-3-2

IEC/EN 61000-6-4	Noise emission tests
EN 55011 Class A, Group 1	Emission test: radiated, conducted

Table 10: Noise Emission Tests

3.5.3.4 Supply Voltage

The following table lists the most important tests and limits for the supply voltage of the HIMatrix systems:

IEC/EN 61131-2	Supply voltage failures immunity test
	Voltage range test: 24 VDC, -20...+25 % (19.2...30.0 V)
	Momentary external current interruption immunity test: DC, PS 2: 2 ms
	Reversal of DC power supply polarity test, tested for 10 s

Table 11: Supply Voltage Failures Immunity Test

4 Central Functions

In a controller of the HIMatrix M45 family, this is a modular system. In addition to the processor module and power supply modules, up to 62 I/O modules can be used in one controller. These I/O modules may include up to three communication modules.

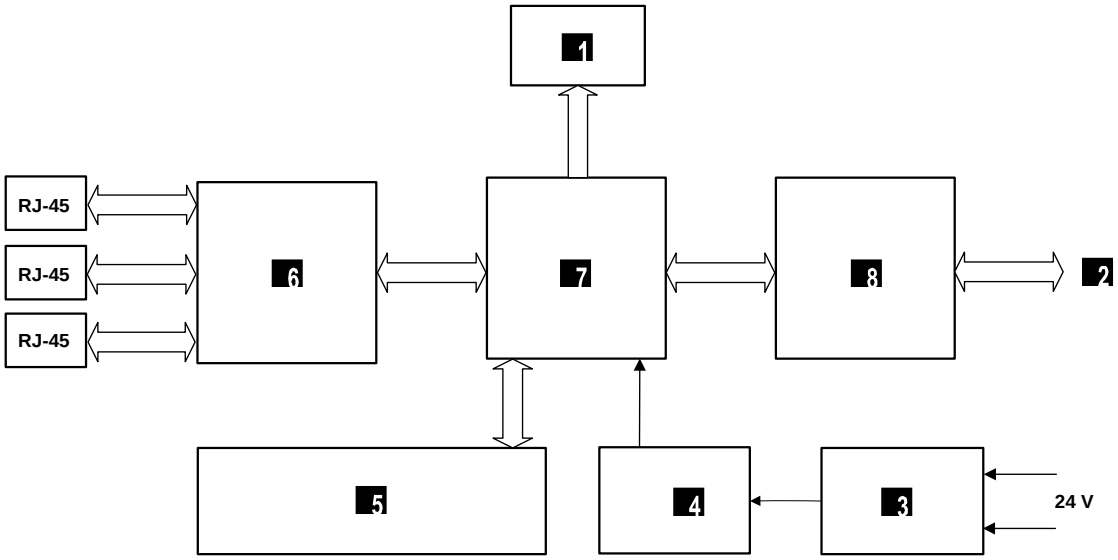
4.1 Power Supply

One power supply module M-PWR 01 must be inserted in the socket of the processor module M-CPU 01. If the current input exceeds 10 A, additional power supply modules must be inserted between the I/O modules. For more details, see the power supply module-specific manual (HI 800 659 E).

4.2 Functional Description of the Processor System

In the modular system M45, the processor system is included in a separate module.

The processor system is composed of the following function blocks:



1 Watchdog
2 System Bus
3 Power Supply
4 Voltage Monitoring
5 Non-Volatile Random Access Memory (NVRAM)
6 Ethernet Switch
7 1oo2 Processor System
8 Ethernet Switch System Bus

Figure 1: Function Blocks of the M-CPU 01

Properties of the M45 M-CPU 01 processor module

- Two synchronous microprocessors.
- 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 no longer triggered and is set to the safe state.
- Flash EPROM for operating system and user program, suitable for at least 100 000 memory cycles.
- Data memory for retain variables in NVRAM.
- Hardware clock buffered with Goldcap.
- Communication processor for fieldbus and Ethernet connections.
- safe**ethernet** interfaces to exchange data between HIMatrix M45 controllers, remote I/Os, and the PADT.

- LEDs for indicating the system states.
- I/O bus logic for connection to I/O modules.
- Safe watchdog (WD).
- Monitoring of all system voltages.

4.3 Self-Tests

The self-test facilities detect individual faults that may lead to a dangerous operating state and trigger, within the safety time of the controller, predefined fault reactions which bring the faulty components into a safe state.

The following section specifies the most important self-test routines of controllers' safety-related processor modules.

4.3.1 Microprocessor Test

The following is tested:

- All commands and addressing modes used.
- The writability of the flags and the commands affected by the flags.
- The writability and crosstalk of the registers.

4.3.2 Memory Areas Test

The operating system, user program, constants and parameters as well as the variable data are stored in memory areas of both processors and are tested by a hardware comparator.

4.3.3 Protected Memory Areas

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

4.3.4 RAM Test

A write and read test is performed to check the modifiable RAM areas, in particular for stuck-at issues and crosstalk.

4.3.5 Watchdog Test

The watchdog signal is switched off if it is not triggered by both CPUs within a defined time window or if the hardware comparator test fails. The watchdog itself is tested.

4.3.6 Reactions to Faults in the Processor System

If the self-test routines detect a fault, the watchdog signal is switched off automatically, and the controller enters the error stop state. This means that the input signals are no longer processed by the controller and the outputs switch to the de-energized state.

If such a fault occurs for the first time, the controller is restarted (reboot). If a further internal fault occurs within the first minute after start-up, the controller enters the STOP/INVALID CONFIGURATION state and will remain in this state.

If an automatic restart is not desired, set the resource parameter *Autostart* to OFF.

4.4 Fault Diagnosis

Each M45 module has an own LED for reporting module malfunctions or faults in the external wiring. This allows the user to quickly diagnose faults detected in a module.

Additionally, the user program can evaluate various system variables associated with the inputs, outputs or the controller.

Faults are only signaled if they do not hinder communication with the processor system, i.e., the processor system must be still able to evaluate the faults.

The user program logic can evaluate the error codes of the system signals and of all input and output signals and of the system variables.

Extensive diagnostics of the system performance and detected faults are stored in the diagnostic memory of the processor module. The diagnostics can also be read after a system fault using the PADT.

For more information on how to evaluate the individual diagnostic messages, see the M45 system manual (HI 800 651 E).

5 Inputs

Overview of the HIMatrix M45 system inputs:

Module	Type	Number of inputs	Safety-related	Interference-free	Galvanically separated
M-DI 8 01 (configurable for line control)	Digital	8	•	•	-
M-CI 8 01	Counter	8	•	•	-

Table 12: Overview of the HIMatrix M45 System Inputs

5.1 General

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

The controllers provide status and fault information as follows:

- Through diagnostic LEDs on the modules.
- Using system variables that the user program is able to evaluate.
- Storing messages in the diagnostic memory which can be read by the PADT.

Safety-related input modules automatically perform high-quality, cyclic self-tests during operation.

5.2 Safety of Sensors, Encoders and Transmitters

In safety-related applications, the controller and connected sensors, encoders and transmitters must all meet the safety requirements and achieve the specified SIL. For information on how to achieve the required SIL for sensors, see IEC 61511-1, Section 11.4.

5.3 Reaction in the Event of a Fault

If the test routines detect a fault, an M45 module activates the *Err* LED.

With respect to inputs, the user program processes the initial value of the global variables.

The error code and other system variables can be used to program application-specific fault reactions. Refer to the module-specific manual for more details.

5.4 Safety-Related Digital Inputs

The described properties are valid for the digital input channels of the M45 modules.

5.4.1 General

The digital inputs are read once per cycle and their value is stored internally. The safe functionality of the inputs is tested cyclically.

Input signals that are present for shorter than the time between two samplings, i.e., shorter than a cycle time, may not be detected.

5.4.2 Test Routines

The online test routines check whether the input channels are able to forward both signal levels (LOW and HIGH), irrespective of the signals actually present on the input. This functional test is performed whenever the input signals are read.

5.4.3 Surges on Digital Inputs

Due to the short cycle time of the HIMatrix systems, a surge pulse as described in EN 61000-4-5 can be read in to the digital inputs as a short-term high level.

The following measures ensure proper operation in environments where surges may occur:

1. Install shielded input wires.
2. Program noise blanking in the user program. A signal must be present for at least two cycles before it is evaluated. The fault reaction is triggered with a corresponding delay.

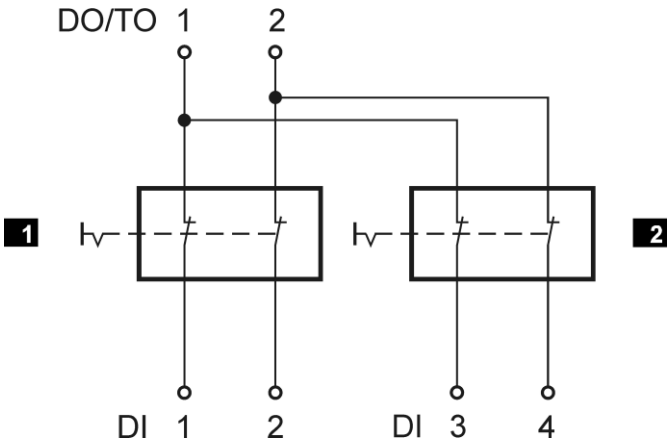
i The measures specified above are not necessary if the plant design precludes surges from occurring within the system.

In particular, the design must include protective measures with respect to overvoltage, lightning, earth grounding and plant wiring in accordance with the relevant standards and the instructions specified in the system manual (HI 800 651 E).

5.4.4 Line Control

Line control is used to detect short-circuits, open-circuits, or cross-circuits, e.g., on EMERGENCY STOP devices, and can be configured for the HIMatrix systems with digital inputs.

To this end, connect the digital outputs of the system to the digital inputs (DI) of the same system as follows (example):

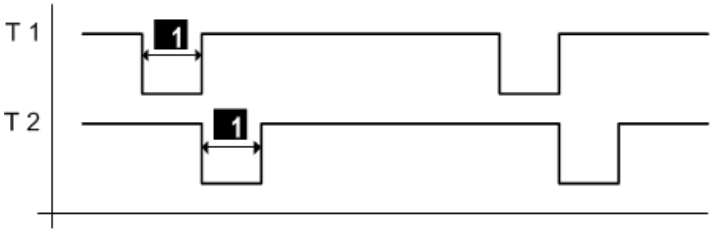


1 EMERGENCY STOP 1
2 EMERGENCY STOP 2

EMERGENCY STOP devices in accordance with EN 60947-5-1 and EN 60947-5-5

Figure 2: Line Control

The controller pulses the digital outputs to detect short-circuits and open-circuits on the lines connected to the digital inputs. To do so, configure the *Value [BOOL] ->* system variable in SILworX. The variables for the pulsed outputs must begin with channel 1 and reside in direct sequence, one after the other, see the section about system variables in the corresponding manuals.



1 Configurable 5...2 000 µs

Figure 3: Pulsed Signal T1, T2

Line control detects the following faults:

- Cross-circuit between two parallel wires.

- Invalid connections of two lines (e.g., TO 2 to DI 3).
- Earth fault of a line (with earthed ground only).
- Open-circuit or open contacts.

If such a fault occurs, the following reactions are triggered:

- The *Err* LED on the module's front plate blinks. The LED does not blink if open-circuits or open contacts occur.
- The inputs are set to low level.
- An evaluable error code is created.

To detect short-circuits and open-circuits, the module can pulse the pulsed outputs and use them with the safety-related digital inputs of the same module.

Pulsed outputs must not be used as safety-related outputs (e.g., for activating safety-related actuators)!

5.5 Safety-Related Counter Module

The counter module is in accordance with SIL 1.

Redundant sensors must be used for SIL 3 applications, and must be wired as specified in the M-CI 8 01 manual (HI 800 667 E).

A counter channel can be configured for operation as up counter with 24-bit resolution.

A channel pair is necessary for quadrature counter operation.

5.6 Checklist for Safety-Related Inputs

HIMA recommends using the following checklist for engineering, programming and starting up safety-related inputs. It can be used for helping with planning as well as to demonstrate later on that the planning phase was carefully completed.

When engineering or starting up the system, a checklist must be filled out for each of the safety-related input channels used in the system to verify the requirements to be met. This is the only way to ensure that all requirements were considered and clearly recorded. The checklist also documents the relationship between the external wiring and the user program.

The checklist *HIMatrix_M45_Checklist_Inputs.docx* is available as Microsoft© Word© document. The ZIP file *HIMatrix_M45_Checklists.zip* contains all the checklists and can be downloaded from the HIMA website at www.hima.com.

6 Outputs

Overview of the HIMatrix M45 system outputs:

Module	Type	Number of outputs	Safety-related	Galvanically separated
M-DO 2 01	Relay	2	•	•
M-DO 8 01	Digital	8	•	-
M-DI 8 01	Digital	2	-	-

Table 13: Overview of the HIMatrix M45 System Outputs

6.1 General

The controller writes to the safety-related outputs once per cycle, reads back the output signals and compares them with the specified output data.

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

Two testable switches are integrated in series in the safety-related output channels. The required second independent switch-off function is thus integrated in the output channel. If a fault occurs, this integrated safety switch-off function safely de-energizes the individual channels of the defective output module (de-energized state).

Additionally, the watchdog signal of the CPU is the second safety switch-off function: If the watchdog signal is lost, the CPU immediately enters the safe state.

In the user program, the state of the module's system variables can be evaluated.

6.2 Safety of Actuators

In safety-related applications, the controller and connected actuators must all meet the safety requirements and achieve the specified SIL. For information on how to achieve the required SIL for actuators, see IEC 61511-1, Section 11.4.

6.3 Reaction in the Event of a Fault

If the test routines detect a fault, an M45 module activates the *Err* LED.

The output affected by a fault is switched off, e.g., set to the safe state by the controller.

The error code and other system variables can be used to program application-specific fault reactions. Refer to the module-specific manual for more details.

6.4 Safety-Related Digital Outputs

The named items are valid for the digital output channels of the M45 modules except for the relay outputs.

6.4.1 Test Routines for Digital Outputs

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

- Read back of the output signal.
- Checking the integrated redundant safety shutdown.
- Shutdown test of the outputs.
- Monitoring the supply voltage

6.4.2 Behavior in the Event of External Short-Circuit or Overload

If the output is short-circuited to L- or overloaded, the module is still safe.

The controller monitors the module's total current input and sets all output channels to the safe state if the threshold is exceeded.

In this state, the outputs are checked every few seconds to determine whether the overload is still present. In a normal state, the outputs are switched on again.

6.5 Relay Outputs

The relay outputs make use of relays with forcibly guided contacts.

6.5.1 Test Routines for Relay Outputs

The module automatically tests its outputs during operation. The main test functions are:

- Reading of the output signals back from the switching amplifiers located before the relays.
- Checking the integrated redundant safety shutdown.
- Monitoring the supply voltage

6.6 Checklist for Safety-Related Outputs

HIMA recommends using this checklist for engineering, programming and starting up safety-related outputs. It can be used for helping with planning as well as to demonstrate later on that the planning phase was carefully completed.

When engineering or starting up the system, a checklist must be filled out for each of the safety-related output channels used in the system to verify the requirements to be met. This is the only way to ensure that all requirements were considered and clearly recorded. The checklist also documents the relationship between the external wiring and the user program.

The checklist *HIMatrix_M45_Checklist_Outputs.docx* is available as Microsoft© Word© document. The ZIP file *HIMatrix_Checklists.zip* contains all the checklists and can be downloaded from the HIMA website at www.hima.com.

7 Software for HIMatrix M45 Systems

The software for the safety-related automation devices of the HIMatrix M45 systems consist of the following components:

- Operating system.
- User program.
- Programming tool in accordance with IEC 61131-3.

The operating system is loaded into the controller's central unit (CPU) and must be used in the current version certified by TÜV for safety-related applications.

The programming tool serves for creating the user program with the application-specific functions that should be performed by the automation device. The programming tool is also used to configure and operate the operating system functions.

The code generator integrated in the programming tool translates the user program into a machine code. The programming tool uses the Ethernet interface to transfer this machine code to the flash EPROM of the automation device.

7.1 Safety-Related Aspects of the Operating System

Each approved operating system is identified by a unique name. The version number and the CRC signature are given to help distinguish the systems from one another. The valid versions of the operating system and corresponding signatures (CRCs) - approved by the TÜV for use in safety-related automation devices - are subject to a revision control and are documented in a list maintained by HIMA in co-operation with the TÜV.

The current version of the operating system can be read using the programming tool. The user must check the version of the operating system to make sure that during safety-related operation the version authorized for the plant is used. (see 7.5 Checklist for Creating a User Program)

7.2 Operation and Functions of the Operating System

The operating system executes the user program cyclically. It performs the following functions:

- Reading the input data of physical inputs and communication partners.
- Processing of the logic functions, programmed in accordance with IEC 61131-3.
- Writing the output data to physical outputs and communication partners.

The following basic functions are also executed:

- Comprehensive self-tests.
- Test of inputs and outputs during operation.
- Data transfer.
- Diagnosis.

7.3 Safety-Related Aspects of Programming

7.3.1 Safety Concept for the Programming Tool

Safety concept for the SILworX programming tool:

- When the programming tool is installed, a CRC checksum helps ensure the program package's integrity on the way from the manufacturer to the user.
- The programming tool performs validity checks to reduce the likelihood of faults while entering data.
- The programming tool and the application of the measures defined in this safety manual make it sufficiently improbable that a code generated properly from a semantic and syntactic view point can still contain undetected systematic faults resulting from the code generation process.

i Whenever the safety-related controller is started up, the verification and validation requirements specified in the application standards must be observed!

When starting up a safety-related controller for the first time, a comprehensive functional test must be performed to verify the safety of the entire system.

- Verify that the tasks to be performed by the controller were properly implemented using the data and signal flows.
- Perform a thorough functional test of the logic by trial (see Chapter 7.3.2).

The safe revision comparator in SILworX can be used to determine and display all changes relative to the previous version.

If a user program is modified, only the program components affected by the change must be tested.

7.3.2 Verifying the Configuration and the User Program

To verify that the user program created performs the required safety function, suitable test cases must be created for the required system specification.

An independent test of each loop (consisting of input, the key interconnections in the application and output) is usually sufficient.

Suitable test cases must also be created for the numerical evaluation of formulas. Equivalence class tests are convenient, which are tests within defined ranges of values, at the limits of or within invalid ranges of values. The test cases must be selected such that the program logic can be proven to be correct. The required number of test cases depends on the program logic used and must include critical value pairs.

An active simulation with data sources is the only way to prove that the sensors and actuators in the system (also those connected to the system via communication with remote I/Os) are properly wired. This is also the only way to verify the system configuration.

SILworX can be used as testing aid for:

- checking inputs
- forcing outputs

This procedure must be followed both when initially creating and when modifying the user program.

7.3.3 Archiving a Project

HIMA recommends archiving the project whenever the program is loaded into the controller. This applies in particular to download and reload processes.

SILworX creates a project in a project file. This must be suitably stored, e.g., on an external storage medium.

7.3.4 Options for Identifying the Program and the Configuration

The user programs are unambiguously identified with the configuration CRC of the project. This configuration CRC can be compared to the configuration CRC of the loaded projects.

To ensure that the saved project file remained unchanged, compile the corresponding resource and compare the configuration CRC with the CRC of the loaded configuration. This CRC can be displayed with SILworX.

7.4 Resource Parameters

⚠ WARNING

Physical injury possible due to defective configuration!

Neither the programming system nor the controller can verify project-specific parameters. For this reason, enter these parameters correctly and verify the whole entry.

These parameters are the Rack ID, see system manual (HI 800 651 E), and the parameters marked in Table 14.

The following parameters are defined in the programming tool for actions permitted during the automation device's safety-related operation and are referred to as safety-related parameters.

Parameters that may be defined for safety-related operation are not firmly bound to any specific requirement classes. Instead, each of these must be agreed upon together with the competent test authority for each separate implementation of the controller.

7.4.1 System Parameters

The distinction is made between system parameters of the resource and system parameters of the hardware.

7.4.1.1 System Parameters of the Resource

The system parameters of the resource determine the controller behavior during operation and can be set in SILworX, in the *Properties* dialog box of the resource.

System Parameters	S[1)]	Description	Setting for safe operation
Name		Name of the resource	Arbitrary
System ID [SRS]	X	System ID of the resource 1...65 535, default value: 60 000 The value assigned to the system ID must differ from the default value, otherwise the project is not able to run!	Unique value within the controller network. This network includes all controllers that can potentially be interconnected.
Safety Time [ms]		Safety time in milliseconds (20...22 500 ms, default value: 600 ms) **Not applicable for HIMatrix M45 controllers!**	-
Watchdog Time [ms]	X	Watchdog time in milliseconds: 4...5000 ms, default value: 200 ms (changeable online)	Application-specific

Target Cycle Time [ms]		Targeted or maximum cycle time, see *Target Cycle Time Mode*, 0...7500 ms, default value: 0 ms. The maximum target cycle time value may not exceed the *Watchdog Time [ms]* - minimum value that can be configured for *Watchdog Time [ms]* (4 ms, see above); otherwise it is rejected by the PES. If the default value 0 ms is set, the target cycle time is not taken into account. See Chapter 7.4.1.2. (changeable online)	Application-specific
Target Cycle Time Mode		Use of *Target Cycle Time [ms]* (changeable online), see Chapter7.4.1.2 Default value: Fixed-tolerant	Application-specific
Multitasking Mode		Mode 1: The duration of a CPU cycle is based on the required execution time of all user programs. Mode 2: The processor makes execution time, which lower priority user programs do not require, available to higher priority user programs. Operation mode for high availability. Mode 3: The processor waits until the execution time not needed by the user programs has expired, thus increasing the cycle. Default value: Mode 1	Application-specific
Max. Com. Time Slice ASYNC [ms]		Highest value in ms for the time slice used for communication during a resource cycle, see the communication manual (HI 801 101 E), 2...5000 ms, default value 60 ms. See Chapter 7.4.1.3.	Application-specific
Max. Duration of Configuration Connections [ms]		It defines how much time within a CPU cycle is available for configuration connections, 2...3500 ms, default value: 12 ms	Application-specific
Maximum System Bus Latency [µs]		Not applicable for HIMatrix M45 controllers! (Default value: 0 µs)	-
Allow Online Settings	X	ON: **All** the switches/parameters listed below OFF can be changed online using the PADT. This is only valid if the system variable *Read-only in RUN* has the value OFF. OFF: These parameters may **not** be changed online ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* These parameters may be changed online if *Reload Allowed* is set to ON. ▪ *Watchdog Time* (for the resource) ▪ *Safety time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* If *Reload Allowed* is set to OFF, they are not changeable online. i *Allow Online Settings* can only be set to ON via reload or if the PES is stopped. Default value: ON	OFF is recommended
Autostart	X	ON: If the processor module is connected to the supply voltage, the user program/programs start automatically OFF: The user program does not start automatically after connecting the supply voltage. Default value: OFF	Application-specific
Start Allowed	X	ON: A cold start or warm start permitted with the PADT in RUN or STOP OFF: Start not allowed Default value: ON	Application-specific
Load Allowed	X	ON: Configuration download is allowed. OFF: Configuration download is not allowed Default value: ON	Application-specific

System Parameters	S[1)]	Description	Setting for safe operation
Reload Allowed	X	ON: Configuration reload is allowed	Application-specific
		OFF: Configuration reload is not allowed. A running reload process is not aborted when switching to OFF	
		Default value: ON	
Global Forcing Allowed	X	ON: Global forcing is permitted for this resource	Application-specific
		OFF: Global forcing is not permitted for this resource	
		Default value: ON	
Global Force Timeout Reaction		Specifies how the resource should behave when the global force timeout has expired: ▪ Stop Forcing ▪ Stop Resource Default value: Stop Forcing	Application-specific
Minimum Configuration Version		With this setting, code compatible with previous or newer CPU operating system versions in accordance with the project requirements may be generated. See Chapter 7.4.1.4. Default value: SILworX V7	SILworX V7
		SILworX V2 Not applicable for HIMatrix M45 controllers! SILworX V3 SILworX V4 SILworX V5	
		SILworX V6 Setting for HIMatrix M45. Generates code suitable for CPU operating system V10.	
		SILworX V6b Setting for HIMatrix M45. Generates code suitable for CPU operating system V10.	
		SILworX V7 Setting for HIMatrix M45. Generates code suitable for CPU operating system V11.	
Fast Start-Up		After connecting the supply voltage, the resource starts up faster. See Chapter 7.4.1.5. Default value: OFF	Application-specific

Table 14: Resource System Parameters

7.4.1.2 Use of the Parameters *Target Cycle Time* and *Target Cycle Time Mode*

These parameters can be used to constantly maintain the cycle time as close to the *Target Cycle Time [ms]* value as possible. To do this, this parameter must be set to a value > 0. HIMatrix M45 then limits tasks such as reload to ensure that the target cycle time is maintained.

The following table describes the effect of *Target Cycle Time Mode*.

Target Cycle Time Mode	Effect on user programs	Effect on reload of processor modules
Fixed	The PES maintains the target cycle time and extends the cycle if necessary. If the processing time of the user programs exceeds the target cycle time, the cycle duration is increased.	Reload is not processed if the target cycle time is not sufficient.
Fixed-tolerant		At most, the duration of every five cycle is increased to allow reload.
Dynamic-tolerant	HIMatrix executes the cycle as quickly as possible.	At most, the duration of every five cycle is increased to allow reload.
Dynamic		Reload is not processed if the target cycle time is not sufficient.

Table 15: Effect of Target Cycle Time Mode

7.4.1.3 Calculating the *Maximum Duration of Configuration Connections [µs]*

If communication is not completely processed within a CPU cycle, it is resumed in the next following CPU cycle at the interruption point.

This slows down communication, but it also ensures that all connections to external partners are processed equally and completely.

Suitable value: Select the value such that the cyclic processor tasks can be executed within the time resulting from *Watchdog Time - Max. Duration of Configuration Connections*.

The volume of the configuration data to be communicated depends on the number of configured remote I/Os, the existing connections to PADTs and the system modules with an Ethernet interface.

A first setting can be calculated as follows:

$T_{Config} = (n_{Com} + n_{RIO} + n_{PADT}) * 0.25$ ms + 2 ms, where

T_{Config}	System parameter *Max. Duration of Configuration Connections [ms]*
n_{Com}	Number of modules with Ethernet interfaces {CPU, COM}
n_{RIO}	Number of configured remote I/Os
n_{PADT}	Maximum number of PADT connections = 5

The calculated time can either be modified in the properties of the resource or directly online based on the figure gathered in the online statistics.

When generating the code or converting the project, a warning message is displayed in the PADT if the value defined for *Max. Duration of Configuration Connections* is less than the value resulting from the previous formula.

i If *Max. Duration of Configuration Connections* is set too low, communication between PADT and PES runs very slow and may even fail!

7.4.1.4 Notices Concerning the *Minimum Configuration Version* Parameter:

- In a new project, the latest *Minimum Configuration Version* is selected. Verify that this setting is in accordance with the hardware in use. In HIMatrix M45 devices, the *Minimum Configuration Version* must be set to *SILworX V6* or higher.
- In a project converted from a previous SILworX version, the value for *Minimum Configuration Version* remains the value set in the previous version. This ensures that the configuration CRC resulting from the code generation is the same as in the previous version and the generated configuration is still compatible with the operating systems in the hardware.

  For this reason, the value of *Minimum Configuration Version* should only be changed in connection with other changes performed to the affected resource.
- If features only available in higher configuration versions are used in the project, SILworX automatically generates a higher configuration version than the preset *Minimum Configuration Version*. This is indicated by SILworX at the end of the code generation. The hardware denies loading a higher configuration version than that matching its operating system.

  To remove such incompatibilities, it can be helpful to compare the information provided by the version comparator with the overview of the module data.

7.4.1.5 Notice Concerning the *Fast Start-Up* Parameter

This parameter exists for SILworX V7 and higher and requires an M45 resource with CPU operating system V11 or higher. Additionally, the resource must be equipped with a boot loader V11.2 and higher or V16.8 and higher. The bootloader and the OS loader (emergency loader) is not the same and cannot be replaced by the user.

Fast start-up is only effective when the PES supply voltage is connected. Operation at SIL 3 level is still ensured.

Fast start-up is achieved through:

- Reduced self-test
- No detection of duplicate IP addresses

  If detection of duplicate IP addresses is deactivated and the network configuration is faulty, duplicate IP addresses may be in use in the network!

  The parameter settings must ensure that no duplicate IP addresses exist in the network!

If an LED test is required during start-up, the parameter *Fast Start-Up* must be set to OFF!

7.4.1.6 Hardware System Variables

These variables are used to change the behavior of the controller while it is operating in specific states. These variables can be set in the hardware detail view of the SILworX Hardware Editor.

Parameter	Function	Default setting	Setting for safe operation
Force Deactivation	Prevents the start of forcing and immediately stops any force activity.	FALSE	Application-specific
Spare 0 ... Spare 16	No function	-	-
Emergency Stop 1... Emergency Stop 4	Emergency stop switch to shut down the controller if faults are detected by the user program	FALSE	Application-specific
Relay Contact 1... Relay Contact 4	Not applicable for M45!	FALSE	Application-specific
Read-only in RUN	After starting the controller, no operating action such as stop or online change is permitted in SILworX, except for forcing and reload.	FALSE	Application-specific
Reload Deactivation	Prevents the controller from being by performing a reload.	FALSE	Application-specific
Power Save Mode	Switches the outputs to power save mode, i.e., to OFF	FALSE	Application-specific
User LED 1...User LED 2	Controls the corresponding LED on the front plate.	FALSE	-

Table 16: Hardware System Variables

Global variables can be connected to these system variables; the value of the global variables is modified using a physical input or the user program logic.

Example: A key switch is connected to a digital input. The digital input is assigned to a global variable associated with the system variable *Read-Only in Run*. The key owner can thus activate or deactivate the operating actions 'stop', 'start' and 'download'.

7.5 Checklist for Creating a User Program

To comply with all safety-related aspects during the programming phase, HIMA recommends using the checklist prior to and after loading a new or modified program.

The checklist *HIMatrix_M45_Checklist_Program.docx* is available as Microsoft© Word© document. The ZIP file *HIMatrix_M45_Checklists.zip* contains all the checklists and can be downloaded from the HIMA website at www.hima.com.

8 Safety-Related Aspects of the User Program

General sequence for programming HIMatrix M45 automation system for safety-related applications:

- Specify the controller functionality.
- Write the user program.
- Compile the user program using the C-code generator.
- The program generated is error-free and able to run.
- Verify and validate the user program.

Finally, the PES can start the safety-related operation.

8.1 Scope for Safety-Related Use

(Refer to Chapter 3.4 for more details about specifications, rules and explications to safety requirements)

Enter the user program with the allowed programming tool SILworX.

Which operating systems for personal computer have been released, is specified in the release notes of the programming tool.

The programming tool includes the following functions:

- Input (Function Block Editor, Structured Text Editor), monitoring and documentation.
- Variables with symbolic names and data types (BOOL, UINT, etc.).
- Assignment of HIMatrix M45 controllers.
- Code generator (for translating the user program into a machine code).
- Hardware configuration.
- Communication configuration.

8.1.1 Programming Basics

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

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

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

- Sensors (digital or analog).
  - Signals during normal operation (de-energize-to-trip principle with digital sensors, 'life-zero' with analog sensors).
  - Signals if a fault occurs.
  - Definition of safety-related redundancies required for safety (1oo2, 2oo3)

  - Monitoring of discrepancy and reaction.
- Actuators.
  - Positioning and activation during normal operation.
  - Safe reaction/positioning at shutdown or after power loss.

Programming goals for user program:

- Easy to understand.
- Easy to trace and follow.
- Easy to modify.
- Easy to test.

8.1.2 Functions of the User Program

Programming is not subject to hardware restrictions. The user program functions can be freely programmed.

- Only elements complying with IEC 61131-3 together with their functional requirements are permitted within the logic.
- The physical inputs and outputs usually operate in accordance with the de-energize-to-trip principle, i.e., their safe state is *0*. This must be observed during programming.
- The user program may be built of logic and/or arithmetic functions irrespective of the de-energize-to-trip principle of the physical inputs and outputs.
- The program logic should be clear and easy to understand and well documented to assist in debugging. This includes the use of functional diagrams.
- Negations are permitted at all points within the logic.
- Fault signals from the inputs or outputs, or from logic blocks must be evaluated.

It is important to encapsulate functions to user-specific function blocks and functions based on standard functions. This ensures that a program can be clearly structured in modules (functions, function blocks). Each module can be considered individually; the user can create a comprehensive, complex function by grouping the individual modules to form a single larger module or a single program.

8.1.3 Variable Declaration

A variable is a placeholder for a value within the program logic. The variable name is used to symbolically address the storage space containing the stored value. A variable is defined in a variable declaration within the project. The name of a variable may consist of up to 120 characters.

After a cold start, variables with no user-defined initial value are set to the default value 0 or FALSE.

Variables with invalid source, e.g., due to a hardware fault in a physical input, adopt the configured initial value.

8.1.4 Documentation of the User LEDs

The M-CPU 01 processor module is equipped with LEDs, *User 1* and *User 2*, that can be used in accordance with the application requirements. A project-specific description of these LEDs must be provided for the operator and shall supplement the HIMA documentation.

8.2 Procedures

This chapter describes the procedures typically used for developing the user programs for safety-related HIMatrix M45 controllers.

8.2.1 Assigning Variables to Inputs or Outputs

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

To assign a variable to an I/O channel

1. Define a global variable of a suitable type.
2. Enter an appropriate initial value, when defining the global variable.
3. Assign the global variable the channel value of the I/O channel.
4. In the user program, evaluate the error code -> *Error Code [Byte]* and program a safety-related reaction.

► The global variables is associated with an input/output channel.

8.2.2 Locking and Unlocking the Controller

Locking the controller locks all functions and prevents users from accessing them during operation. This also protects against manipulations to the user program. The locking extent should be considered in connection with the safety requirements for the PES application, and can also be agreed upon with the test authority responsible for the factory acceptance test (FAT).

Unlocking the controller deactivates any locks previously set (e.g., to perform work on the controller).

Three system variables serve for locking:

Variable	Function
Read-only in Run	ON: Starting, stopping, and downloading the controller are locked. OFF: Starting, stopping, and downloading the controller are possible.
Reload Deactivation	ON: Reload is locked. OFF: Reload is possible.
Force Deactivation	ON: Forcing is deactivated. OFF: Forcing is possible.

Table 17: System Variables for Locking and Unlocking the PES

If all three system variables are ON: no access to the controller is possible.

Simple example for using these system variables:

To make a controller lockable

1. Define a global variable of type BOOL and set its initial value to OFF.
2. Assign global variables to the three system variables *Read-only in Run*, *Reload Deactivation*, and *Force Deactivation*.
3. Assign the global variable to the channel value of a digital input.
4. Connect a key switch to the digital input.
5. Compile the program, load it on the controller, and start it.

► The owner of a corresponding key is able to lock and unlock the controller. If the corresponding digital input module or input channel fails, the controller is unlocked.

The example describes a simple case, in which a single key is used to block or permit all interventions on the PES.

The simple example can be modified using multiple global variables, digital inputs and key switches so that the permissions for forcing, reload, stop, start and download can be distributed on different keys and persons.

8.2.3 Code Generation

After entering the complete user program and the I/O assignments of the controller, generate the code. The code generator creates the configuration CRC. This is a signature for the entire configuration of CPU, inputs, outputs and communication, and is issued as a 32-bit, hexadecimal code. The signature includes all of the configurable or modifiable elements such as the logic, variable or switch parameter settings.

If used with the default setting, SILworX generates the code twice and compares the generated configuration CRCs to exclude influences of the non-safe PC. The two resulting configuration CRCs must be identical.

► If the two configuration CRCs are equal, the generated code may be used for safety-related operation and for the system's certification performed by the test authority.

8.2.4 Loading and Starting the User Program

The configuration can only be loaded into the a HIMatrix M45 PES by performing a download, if it has been set to the STOP state beforehand.

The system monitors that the user program is loaded completely. Afterwards, the user program can be started, i.e., the routine begins to be processed in cycles.

i The PADT is only able to operate the resource, e.g., by performing a reload and forcing, if the project loaded in the resource is opened in SILworX. Without the project in SILworX, only a STOP of the resource is possible!

HIMA recommends performing a project data backup, e.g., on a removable medium, after loading a user program into the controller.

This is done to ensure that the project data corresponding to the configuration loaded into the controller remains available even if the PADT fails.

HIMA recommends performing a data backup on a regular basis also independently from the program load.

8.2.5 Reload

If user programs were modified, the changes can be transferred to the PES during operation. The operating system checks and activates the modified user program which then assumes the control task.

The use of reload must be agreed upon with the responsible test authority on an individual basis!

i **Observe the following points when reloading step sequence:**

The reload information for step sequences does not take the current sequence status into account. The step sequence can be accordingly changed and set to an undefined state by performing a reload. The user is responsible for this action.

Examples:

- Deleting the active step. As a result, no sequence step has the *active* state.
- Renaming the initial step while another step is active.
  As a result, a sequence has two active steps!

Observe the following points when reloading actions:

During the reload, actions are loaded with their corresponding data. All potential consequences must be carefully analyzed prior to performing a reload.

Examples:

- If a timer action qualifier is deleted due to the reload, the timer expires immediately. Depending on the remaining settings, the *Q* outputs can therefore be set to TRUE.
- If the status action qualifier (e.g., the *S* action qualifier) is deleted for a set element, the element remains set.
- Deleting a *P0* action qualifier set to TRUE actuates the trigger function.

8.2.6 Forcing

Forcing is the procedure by which a variable's current value is replaced with a force value. The variable receives its current value from a physical input, communication or a logic operation. If the variable is forced, its value does no longer depend on the process, but is defined by the user.

⚠ WARNING

Failure of safety-related operation possible due to forced values possible!

- **Forced value may lead to incorrect output values.**
- **Forcing prolongates the cycle time. This can cause the watchdog time to be exceeded.**

Forcing is only permitted after receiving consent from the test authority responsible for the factory acceptance test (FAT).

When forcing values, the person in charge must take further technical and organizational measures to ensure that the process is sufficiently monitored in terms of safety. HIMA recommends setting a time limit for the forcing procedure.

Refer to the M45 system manual (HI 800 651 E) for further details on forcing.

8.2.6.1 Forcing of data sources

Changing the assignment of a forced global variable to one of the following data sources can lead to unexpected results:

- Physical inputs
- Communication protocols.
- System variable

The following sequence of actions causes a variable to be unintentionally forced:

1. A global variable A is assigned a forced data source and is thus forced itself
2. The assignment is removed.
3. Another global variable B is assigned the forced data source previously used.
4. A reload is performed to load the project change into the PES.

The **newly assigned** variable B results to be forced, even if this was not intended!

Workaround: First stop forcing variable A.

Which channels have been forced is displayed in the channel view of the Force Editor.

Global variables having the user program as data source retain the *forced* setting whenever an assignment is changed.

8.2.7 Changing the System Parameters during Operation

The system parameters specified in Table 18 may be changed during operation (online).
A typical application case is the temporary increase of the watchdog time to be able to perform a reload.

Prior to using an online command to set parameters, make sure that this change will not result in a dangerous state of the plant. If required, organizational and/or technical measures must be taken to preclude any damage. The application standards must be observed!

The safety time and watchdog time values must be checked and compared to the safety time required by the application and to the actual cycle time. These values cannot be verified by the PES!

The controller ensures that the watchdog time is not set to a value less than the watchdog time value of the configuration loaded in the PES.

Parameter	Changeable in this PES state
System ID	STOP
Watchdog Time (for the resource)	RUN, STOP_VALID_CONFIGURATION
Safety Time	RUN, STOP_VALID_CONFIGURATION
Target Cycle Time	RUN, STOP_VALID_CONFIGURATION
Target Cycle Time Mode	RUN, STOP_VALID_CONFIGURATION
Allow Online Settings	ON->OFF: All OFF->ON: STOP
Autostart	All
Start Allowed	All
Load Allowed	All
Reload Allowed	All
Global Forcing Allowed	All
Global Force Timeout Reaction	All

Table 18: Online Changeable Parameters

System parameters may also be changed during operation by performing a reload.

8.2.8 Project Documentation for Safety-Related Applications

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

- Interface declaration
- List of variables
- Logic
- Description of data types
- Configurations for system, modules and system parameters
- Network configuration
- Variable Cross-Reference List
- Code generator details

This documentation is required for the factory acceptance test (FAT) of a system subject to approval by a test authority (e.g., TÜV). The factory acceptance test (FAT) only applies to the user functionality, but not to the safety-related modules and automation devices of the HIMatrix M45 system that have already been approved.

8.2.9 Multitasking

Multitasking refers to the capability of the HIMatrix M45 systems to process up to 32 user programs within the processor module.

The individual user programs can be started and stopped independently from one another.

A user program cycle can take multiple processor cycles. This can be controlled with the resource and user program parameters. SILworX uses these parameters to calculate the user program watchdog time:
Watchdog time$_{\text{user program}}$ = *watchdog time*$_{\text{processor module}}$ ** maximum number of cycles*

Operation of the individual user programs is usually interference-free and independent of one another. However, reciprocal influence can be caused by:

- Use of the same global variables in several user programs.
- Unpredictably long runtimes can occur in individual user programs if a limit is not configured with *Max. Duration for Each Cycle [µs]*.
- The distribution of user program cycle over processor module cycles strongly affects the user program response time and the response time of the variables written by the user program!
- A user program evaluates global variables written by another user program after at least one processor module cycle. Depending on the value set in the programs for *Program's Maximum Number of CPU Cycles*, the reading process may be prolonged by many processor module cycles. The reaction to changes performed to such global variables is thus delayed!

Refer to the system manual (HI 800 651 E) for details on multitasking.

8.2.10 Factory Acceptance Test and Test Authority

HIMA recommends involving the test authority as soon as possible when designing a system that is subject to approval.

The factory acceptance test (FAT) only applies to the user functionality, but not to the safety-related modules and automation devices of the HIMatrix M45 system that have already been approved.

9 Communication

HIMatrix M45 supports safe protocols and standard protocols.

9.1 Standard Protocols

Many communication protocols only ensure a non-safety-related data transmission. These protocols can be used for the non-safety-related aspects of an automation task.

⚠ WARNING

Physical injury possible due to usage of unsafe import data!

Do not use data imported from unsafe sources for the user program's safety functions.

Depending on the controller variant, the following standard protocols are available:

Protocol	Interface	Option of the communication module.
SNTP	RJ-45	All
Send/Receive TCP	RJ-45	All
Modbus (master/slave)	RJ-45, D-Sub	M-COM 010 2
PROFIBUS DP Master	D-Sub	M-COM 010 2
PROFIBUS DP slave	D-Sub	M-COM 010 3
SSI	D-Sub	M-COM 010 7
CAN	D-Sub	M-COM 010 8
RS422/RS485	D-Sub	All

Table 19: Standard Protocols

9.2 Safety-Related Protocol: safe**ethernet**

Safety-related communication via safe**ethernet** is certified up to SIL 3.

Use the safe**ethernet** Editor to configure how safety-related communication is monitored.

For determining the *Receive Timeout* and *Response Time* safe**ethernet** parameters, the following condition applies:
The communication time slice must be sufficiently high to allow all the safe**ethernet** connections to be processed within one CPU cycle.

The **Use Initial Data** setting may only be used for safety-related functions implemented via safe*ethernet*.

NOTE

Unintentional transition to the safe state possible!

***Receive Timeout* is a safety-related parameter!**

If all values must be transferred, the value of a signal must either be present for longer than *Receive Timeout* or it must be monitored using a loop back.

9.2.1 Receive Timeout

Receive Timeout is the monitoring time in milliseconds (ms) within which a correct response from the communication partner must be received.

If a correct response is not received from the communication partner within *Receive Timeout*, safety-related communication is terminated. The input variables of this safe**ethernet** connection react in accordance with the preset parameter *Freeze Data on Lost Connection [ms]*.

The **Use Initial Data** setting may only be used for safety-related functions implemented via safe**ethernet**.

Since *Receive Timeout* is a safety-relevant component of the worst case reaction time T_R (see Chapter 9.2.3 et seqq.), its value must be determined as described below and entered in the safe**ethernet** Editor.

Receive Timeout ≥ 4*delay + 5*max. cycle time

Condition: The communication time slice must be sufficiently high to allow all the safe**ethernet** connections to be processed within one CPU cycle.

Delay:	Delay on the transmission path, e.g., due to switch or other transport media as satellite.
Max. Cycle Time	Maximum cycle time of both controllers.

i A wanted fault tolerance of communication can be achieved by increasing the value of *Receive Timeout*, provided that this is permissible in terms of time for the application process (worst case reaction time).

i **The maximum value permitted for *Receive Timeout* depends on the application process and is configured in the** safe**ethernet Editor, along with the expected maximum response time and the profile.**

9.2.2 Response Time

Response Time is the time period expressed in milliseconds (ms) until the sender of the message receives acknowledgement from the recipient.

When configuring the safe**ethernet** protocol, the **Response Time** expected to result from the physical conditions of the transmission path must be set and a suitable safe**ethernet** profile must be selected.

The *Response Time* set affects the configuration of all the safe**ethernet** connection parameters. The *Response Time* is determined as follows:

Response Time ≤ Receive Timeout / n

n = 2, 3, 4, 5, 6, 7, 8.....

The ratio between *Receive Timeout* and *Response Time* influences the capability of tolerating faults, e.g., when packets are lost (resending lost data packets) or delays occur on the transmission path.

In networks where packets can be lost, the following condition must be given:

min. Response Time ≤ Receive Timeout / 2 ≥ 2*Delay + 2.5*max. Cycle Time

If this condition is met, the loss of at least one data packet can be intercepted without interrupting the safe**ethernet** connection.

i If this condition is not met, the availability of a safe**ethernet** connection can only be ensured in a collision and fault-free network. However, this is not a safety problem for the processor module!

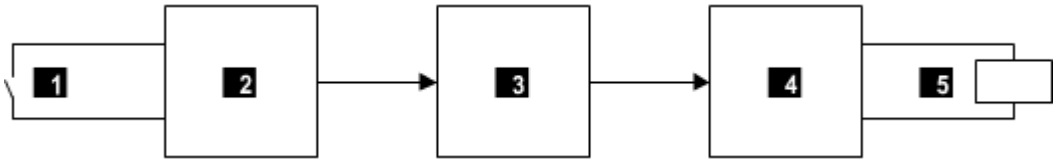
i The user must ensure that the transmission path complies with the configured response time!

If this conditions cannot always be ensured, a corresponding connection system variable for monitoring the response time is available. If more than on occasion the measured response time exceeds the receive timeout by more than a half, the configured response time must be increased.

The receive timeout must be adjusted according to the new value configured for response time.

9.2.3 Calculating the Worst Case Reaction Time with 2 Remote I/Os

The worst case reaction time T_R is the time between a change on the input of the first HIMatrix M45 PES or remote I/O (e.g., F3 DIO 20/8 01) and a reaction on the corresponding output of the second HIMatrix M45 PES or remote I/O. It is calculated as follows:



1 Input
2 Remote I/O 1
3 HIMatrix M45 Controller
4 Remote I/O 2
5 Output

Figure 4: Response Time with Remote I/Os

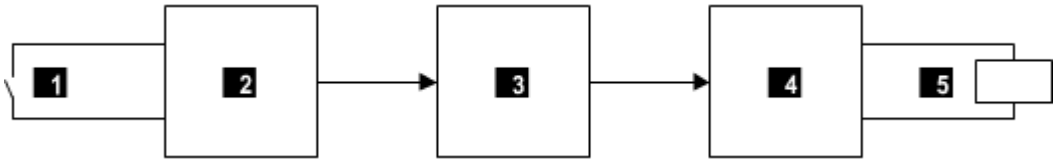
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

T_R Worst Case Reaction Time
t_1 2 * watchdog time of remote I/O 1
t_2 Receive Timeout$_1$
t_3 2 * watchdog time of the HIMatrix M45 controller
t_4 Receive Timeout$_2$
t_5 2 * watchdog time of remote I/O 2

Note: Remote I/O 1 and remote I/O 2 can also be identical. The time values still apply if a HIMatrix M45 controller is used instead of a remote I/O.

9.2.4 Calculating the Worst Case Reaction Time with 2 HIMatrix M45 and 1 HIMatrix Controller

The worst case reaction time T_R is the time between a change on the input of the first HIMatrix M45 PES and a reaction on the corresponding output of the second HIMatrix M45 PES. It is calculated as follows:



1 Input
2 HIMatrix M45 Controller 1
3 HIMax Controller
4 HIMatrix M45 Controller 2
5 Output

Figure 5: Response Time with 2 HIMatrix M45 Controllers and 1 HIMax Controller

$T_R = t_1 + t_2 + t_3 + t_4 + t_5$

T_R	Worst case reaction time
t_1	2 * watchdog time of the HIMatrix M45 controller 1
t_2	Receive Timeout$_1$
t_3	2 * watchdog time of the HIMax controller.
t_4	Receive Timeout$_2$
t_5	2 * watchdog time of the HIMatrix M45 controller 2

Remark: HIMatrix M45 controller 1 and HIMatrix M45 controller 3 can also be identical.

9.2.5 Terms

Receive Timeout	Monitoring time of controller 1 within which a correct response from controller 2 must be received. Once the time has expired, safety-related communication is terminated.
Production Rate	Minimum interval between two data transmissions.
Watchdog time	Maximum permissible duration of a controller's RUN cycle (cycle time).
Worst Case Reaction Time	The worst case reaction time is the time between a change in a physical input signal of controller 1 and a reaction on the corresponding output of controller 2.

9.2.6 Assigning safe**ethernet** Addresses

Take the following points into account when assigning network addresses (IP addresses) for safe**ethernet**:

- The addresses must be unique within the network used.
- When connecting safe**ethernet** to another network (company-internal LAN, etc.), make sure that no disturbances may occur. Potential sources of disturbances include:
  - Data traffic.
  - Coupling with other networks (e.g., Internet).

In these cases, implement suitable measures to counteract against such disturbances using Ethernet switches, firewall and similar.

Appendix

Glossary

Term	Description
AI	Analog input
AO	Analog output
ARP	Address resolution protocol: Network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CRC	Cyclic redundancy check
DI	Digital input
DO	Digital output
EMC	Electromagnetic compatibility
EN	European norm
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
ICMP	Internet control message protocol: Network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Supposing that two input circuits are connected to the same source (e.g., a transmitter). An input circuit is termed *interference-free* if it does not distort the signals of the other input circuit.
MAC Address	Media access control address: Hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX
PE	Protective earth
PELV	Protective extra low voltage
PES	Programmable electronic system
R	Read: The system variable provides value, e.g., to the user program
R/W	Read/Write (column title for system variable type)
r_P	Peak value of a total AC component
SB	System Bus
SELV	Safety extra low voltage
SFF	Safe failure fraction, portion of faults that can be safely controlled
SIL	Safety integrity level (in accordance with IEC 61508)
SILworX	Programming tool for HIMatrix systems
SNTP	Simple network time protocol (RFC 1769)
SRS	System.Rack.Slot addressing of a module
SW	Software
TMO	Timeout
W	Write: System variable is provided with value, e.g., from the user program
Watchdog (WD)	Time monitoring for modules or programs. If the watchdog time is exceeded, the module or program enters the error stop state.
WDT	Watchdog time

Index of Figures

Index of Tables

Index

HI 800 653 E

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

SAFETY
NONSTOP

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