

Manual

# HIMatrix<sup>®</sup>F

Safety Manual



All of the HIMA products mentioned in this manual are trademark protected. Unless noted otherwise, this also applies to other manufacturers and their respective products referred to herein.

HIQuad®, HIQuad®X, HIMax®, HIMatrix®, SILworX®, XMR®, HICore® and FlexSILon® are registered trademarks of HIMA Paul Hildebrandt GmbH.

All of the technical specifications and information in this manual were prepared with great care and effective control measures were employed for their compilation. 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.

All the current manuals can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com).

© Copyright 2020, HIMA Paul Hildebrandt GmbH

All rights reserved.

## Contact

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](mailto:info@hima.com)

Document designation	Description
HI 800 022 D, Rev. 6.00 (2022)	German original document
HI 800 023 E, Rev. 6.00.00 (2025)	English translation of the German original document

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>7</b>
1.1	Validity and Current Version	7
1.2	Target Audience	7
1.3	Writing Conventions	8
1.3.1	Safety Notices	8
1.3.2	Operating Tips	9
1.4	Safety Lifecycle Services	10
<b>2</b>	<b>Use of the HIMatrix System</b>	<b>11</b>
2.1	Intended Use	11
2.1.1	Application in Accordance with the De-Energize to Trip Principle	11
2.1.2	Application in Accordance with the Energize to Trip Principle	11
2.1.3	Use in Fire Alarm Systems	11
2.1.4	Explosion Protection	11
2.2	Tasks of Operators and Machine and System Manufacturers	12
2.2.1	Connecting to Communication Partners	12
2.2.2	Implementing Safety-Related Communications	12
2.3	ESD Protective Measures	12
2.4	Additional System Documentation	13
<b>3</b>	<b>Safety Concept</b>	<b>14</b>
3.1	Safety and Availability	14
3.1.1	Calculating the PFD and the PFH Values	14
3.1.2	Self-Test and Fault Diagnostics	15
3.1.3	PADT	15
3.1.4	Structuring Safety Systems in Accordance with the Energize to Trip Principle	16
3.1.4.1	Detection of Failed System Components	16
3.1.4.2	Safety Function in Accordance with the Energize to Trip Principle	16
3.2	Safety-Relevant Time Parameters	17
3.2.1	Process Safety Time	17
3.2.2	Safety Time [ms] Parameter of the Resource	17
3.2.3	Watchdog Time (of the Resource)	18
3.2.4	Estimating the Watchdog Time	18
3.2.5	Determining the Watchdog Time through Testing	19
3.2.6	Response Time	20
3.3	Proof Test (in Accordance with IEC 61508)	21
3.4	Safety Requirements	22
3.4.1	Product-Independent Hardware Requirements	22
3.4.2	Product-Dependent Hardware Requirements	22
3.4.3	Product-Independent Programming Requirements	22
3.4.4	Product-Dependent Programming Requirements	23
3.4.5	Communication	23
3.4.6	Maintenance	23
3.4.7	Temperature Monitoring	23
3.4.8	Environmental Requirements	24
3.5	Automation Security	25
3.5.1	Product Properties	25
3.5.2	Risk Analysis and Planning	26

<b>3.6</b>	<b>Certification</b>	<b>27</b>
3.6.1	CE Declaration of Conformity	27
3.6.2	EC Type Test Certificate	27
3.6.3	Current Standards	28
3.6.4	Test Requirements	29
3.6.4.1	Climatic Tests	30
3.6.4.2	Mechanical Tests	30
3.6.4.3	EMC Tests	30
3.6.4.4	Supply Voltage	31
<b>4</b>	<b>Central Functions</b>	<b>32</b>
4.1	Power Supply	32
4.2	Functional Description of the Processor System	32
4.3	Self-Tests	33
4.4	Responses to Faults in the Processor System	33
4.5	Fault Diagnostics	33
<b>5</b>	<b>Inputs</b>	<b>34</b>
5.1	General Information	34
5.2	Response in the Event of a Fault	35
5.3	Safety of Sensors, Encoders and Transmitters	35
5.4	Safety-Related Digital Inputs	35
5.4.1	General Information	35
5.4.2	Test Routines	35
5.4.3	Surges on Digital Inputs	35
5.4.4	Configurable Digital Inputs	36
5.4.5	Line Control	36
5.5	Safety-Related Analog Inputs (F35 03, F3 AIO 8/4 01 and F60)	37
5.5.1	Test Routines	38
5.6	Safety-Related Counters (F35 03 and F60)	38
5.6.1	General Information	38
5.7	Checklists for Inputs	39
<b>6</b>	<b>Outputs</b>	<b>40</b>
6.1	General Information	40
6.2	Response in the Event of a Fault	41
6.3	Safety of Actuators	41
6.4	Safety-Related Digital Outputs	41
6.4.1	Test Routines for Digital Outputs	41
6.4.2	Behavior in the Event of External Short-Circuit or Overload	41
6.4.3	Line Control	41
6.5	Safety-Related 2-Pole Digital Outputs	42
6.5.1	Behavior in the Event of External Short-Circuit or Overload	42
6.6	Relay Outputs	43
6.6.1	Test Routines for Relay Outputs	43
6.7	Safety-Related Analog Outputs (F60)	43
6.7.1	Test Routines	44
6.8	Analog Outputs with Safety-Related Shutdown (F3 AIO 8/4 01)	44

6.8.1	Test Routines	44
<b>6.9</b>	<b>Checklists for Outputs</b>	<b>44</b>
<b>7</b>	<b>Software</b>	<b>45</b>
<b>7.1</b>	<b>Safety-Related Aspects of Operating Systems</b>	<b>45</b>
<b>7.2</b>	<b>Operation and Functions of Operating Systems</b>	<b>45</b>
<b>7.3</b>	<b>Safety-Related Aspects of Programming</b>	<b>46</b>
7.3.1	Safety Concept of SILworX	46
7.3.2	Verifying the Configuration and the User Programs	46
7.3.3	Archiving a Project	47
7.3.4	Identifying Configuration and Programs	47
<b>7.4</b>	<b>Resource Parameters</b>	<b>47</b>
7.4.1	Resource System Parameters	48
7.4.1.1	Use of the Parameters <i>Target Cycle Time</i> and <i>Target Cycle Time Mode</i>	51
7.4.1.2	Maximum Communication Time Slice	52
7.4.1.3	Determining the Maximum Duration of the Communication Time Slice	52
7.4.1.4	Calculating the <i>Maximum Duration of Configuration Connections [ms]</i> $T_{\text{Config}}$	53
7.4.1.5	The <i>Minimum Configuration Version</i> Parameter	53
7.4.1.6	The Fast Start-Up Parameter	54
7.4.1.7	Hardware System Variables	55
7.4.2	Locking and Unlocking the Controller	56
<b>7.5</b>	<b>Forcing</b>	<b>56</b>
7.5.1	Use of Forcing	56
7.5.2	Assigning a Data Source Changed through Reload	57
7.5.3	Time Limits	58
7.5.4	Restricting the Use of Forcing	58
7.5.5	MultiForcing	58
7.5.5.1	Objectives of MultiForcing	59
7.5.5.2	Global MultiForcing	59
<b>7.6</b>	<b>Safe Version Comparison</b>	<b>60</b>
<b>7.7</b>	<b>Security Measures for the Application Programming Interface (API)</b>	<b>60</b>
<b>8</b>	<b>Safety-Related Aspects of User Programs</b>	<b>61</b>
<b>8.1</b>	<b>Safety-Related Usage</b>	<b>61</b>
8.1.1	Programming Basics	61
8.1.1.1	I/O Concept	62
8.1.2	Programming Steps	62
8.1.3	User Program Functions	62
8.1.4	User Program System Parameters	63
8.1.5	Notes on the <i>Code Generation Compatibility</i> Parameter	64
8.1.6	Code Generation	65
8.1.7	Loading and Starting the User Program	65
8.1.8	Reload	65
8.1.9	Online Test	66
8.1.10	Test Mode	66
8.1.11	Changing the System Parameters during Operation	67
8.1.12	Project Documentation for Safety-Related Applications	67
8.1.13	Multitasking	68
8.1.14	Factory Acceptance Test and Test Authority	68
<b>8.2</b>	<b>Checklist for Creating a User Program</b>	<b>68</b>

<b>9</b>	<b>Configuring Communication</b>	<b>69</b>
<b>9.1</b>	<b>Standard Protocols</b>	<b>69</b>
<b>9.2</b>	<b>Safety-Related safeethernet Protocol</b>	<b>69</b>
9.2.1	Response Time	70
<b>9.3</b>	<b>Worst Case Response Time for safeethernet</b>	<b>71</b>
9.3.1	Calculating the Worst Case Response Time	72
9.3.2	Calculating the Worst Case Response Time with 2 Remote I/Os	72
9.3.3	Connections to HIMax Controllers	73
<b>9.4</b>	<b>Safety-Related HIPRO-S V2 Protocol</b>	<b>73</b>
<b>9.5</b>	<b>Safety-Related PROFIsafe Protocol</b>	<b>73</b>
<b>9.6</b>	<b>Safety-Related ISOFAST Protocol</b>	<b>73</b>
<b>10</b>	<b>Use in Fire Alarm Systems</b>	<b>74</b>
<b>11</b>	<b>ATEX-Conform Use as Safety, Controlling and Regulating Device</b>	<b>76</b>
<b>12</b>	<b>Use of HIMatrix Devices in Ex Zone 2</b>	<b>77</b>
	<b>Appendix</b>	<b>79</b>
	Glossary	79
	Index of Figures	80
	Index of Tables	81
	Index	82

# 1 Introduction

This manual contains information on how to operate the safety-related programmable electronic system HIMatrix in the intended manner.

The following conditions must be met to safely install and start up the system and to ensure safety during their operation and maintenance:

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

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

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

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

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

To provide a clearer exposition, this manual does not specify all details of all system versions.

This safety manual represents the "Original instructions" as of Machinery Directive (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 Validity and Current Version

This safety manual was created for the following versions:

- HIMatrix operating systems in accordance with revision list.
- SILworX as of V12.

For details on how to use previous HIMatrix and SILworX versions, refer to the corresponding previous versions of this manual.

## 1.2 Target Audience

This document is aimed at the planners, design engineers, programmers and the persons authorized to start up, operate and maintain the automation 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:

<b>Bold</b>	To highlight important parts. Names of buttons, menu functions and tabs that can be clicked and used in the programming tool.
<i>Italics</i>	Parameters and system variables, references.
<code>Courier</code>	Literal user inputs.
<b>RUN</b>	Operating states are designated by capitals.
Chapter 1.2.3	Cross-references are hyperlinks even if they are not specially marked. In the electronic document (PDF): When the mouse pointer hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are specially marked.

### 1.3.1 Safety Notices

Safety notices must be strictly observed to ensure the lowest possible risk.

The safety notices are represented as described below.

- Signal word: warning, caution, notice.
- 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 situation which, if not avoided, could result in minor or moderate injury.
- Notice indicates a hazardous situation which, if not avoided, could result in property damage.

#### **SIGNAL WORD**



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

---

#### **NOTICE**



**Type and source of damage!**  
**Damage prevention.**

---



1.3.2      Operating Tips

Additional information is structured as presented in the following example:

---

**i**      The text giving additional information is located here.

---

Useful tips and tricks appear as follows:

---

**TIP**      The tip text is located here.

---

## 1.4 Safety Lifecycle Services

HIMA provides support throughout all the phases of a plant's safety lifecycle, from planning and engineering through commissioning to maintenance of safety and security.

HIMA's technical support experts are available for providing information and answering questions about our products, functional safety and automation security.

To achieve the qualification required by the safety standards, HIMA offers product or customer-specific seminars at HIMA's training center or on site at the customer's premises. The current seminar program for functional safety, automation security and HIMA products can be found on HIMA's website.

### Safety Lifecycle Services:

<b>Onsite+ / On-Site Engineering</b>	In close cooperation with the customer, HIMA performs changes or extensions on site.
<b>Startup+ / Preventive Maintenance</b>	HIMA is responsible for planning and executing preventive maintenance measures. Maintenance actions are carried out in accordance with the manufacturer's specifications and are documented for the customer.
<b>Lifecycle+ / Lifecycle Management</b>	As part of its lifecycle management processes, HIMA analyzes the current status of all installed systems and develops specific recommendations for maintenance, upgrading and migration.
<b>Hotline+ / 24 h Hotline</b>	HIMA's safety engineers are available by telephone around the clock to help solve problems.
<b>Standby+ / 24 h Call-Out Service</b>	Faults that cannot be resolved over the phone are processed by HIMA's specialists within the time frame specified in the contract.
<b>Logistics+ / 24 h Spare Parts Service</b>	HIMA maintains an inventory of necessary spare parts and guarantees quick, long-term availability.

### Contact details:

<b>Safety Lifecycle Services</b>	<a href="https://www.hima.com/en/about-hima/contacts-worldwide/">https://www.hima.com/en/about-hima/contacts-worldwide/</a>
<b>Technical Support</b>	<a href="https://www.hima.com/en/products-services/support/">https://www.hima.com/en/products-services/support/</a>
<b>Seminar Program</b>	<a href="https://www.hima.com/en/products-services/seminars/">https://www.hima.com/en/products-services/seminars/</a>

## 2 Use of the HIMatrix System

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.

The product is operated with SELV or PELV. No imminent risk results from the product itself. Use in the Ex zone is only permitted if additional measures are taken.

### 2.1 Intended Use

This chapter describes the intended use of the safety-related automation system HIMatrix.

The automation system is designed for the industrial process market to control and regulate processes, protective systems, burner control applications, machine controllers and process plants, as well as for factory automation plants. SILworX, HIMA's programming tool, is used for programming, configuring, monitoring, operating and documenting the HIMatrix system.

#### 2.1.1 Application in Accordance with the De-Energize to Trip Principle

The HIMatrix system is designed in accordance with the de-energize to trip principle.

A system operating in accordance with the de-energize to trip principle switches off, for instance, an actuator to perform its safety function.

#### 2.1.2 Application in Accordance with the Energize to Trip Principle

The HIMatrix system can also be used in applications that operate in accordance with the energize to trip principle.

A system operating in accordance with the energize to trip principle switches on, for instance, an actuator to perform its safety function.

When designing the automation system, the requirements specified in the application standards must be taken into account. For instance, line monitoring (SC/OC) for inputs and outputs or message reporting a triggered safety function may be required.

#### 2.1.3 Use in Fire Alarm Systems

The HIMatrix systems with detection of short-circuits and open-circuits are tested and certified for used in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72. To contain the risks, these systems must be able to adopt an active state on demand.

The conditions of use provided in this manual must be observed, see Chapter 10.

#### 2.1.4 Explosion Protection

The HIMatrix automation system is suitable for mounting in zone 2.



The conditions provided in Chapter 12 must be observed.

## 2.2 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.

### 2.2.1 Connecting to Communication Partners

Only devices with electrically protective separation may be connected to the communication interfaces.

### 2.2.2 Implementing Safety-Related Communications

When implementing safety-related communications between various devices, ensure that the overall response time does not exceed the process safety time.

All calculations must be performed in accordance with the rules given in Chapter 9.3 and in the manuals for the communication protocols.

## 2.3 ESD Protective Measures

Only personnel with knowledge of ESD protective measures may work on the HIMatrix system.

### NOTICE



#### Damage to the HIMatrix system due to electrostatic discharge!

- When performing the work, make sure that the workspace is free of static, and wear a grounding strap.
- If not used, ensure that the modules are protected from electrostatic discharge, e.g., by storing them in their packaging.

## 2.4 Additional System Documentation

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

Name	Content	Document no.
HIMatrix system manual	Hardware description of the system	HI 800 141 E
Certificates	Test results	---
Revision list	Operating system versions certified by the TÜV	---
Component-specific manuals	Description of the individual components	---
Maintenance manual	Description of significant operational and maintenance actions.	HI 800 455 E
Communication manual	Description of safe <b>ethernet</b> communication and of the available protocols.	HI 801 101 E
Automation security manual	Description of automation security aspects related to the HIMA systems.	HI 801 373 E
SILworX first steps manual	Introduction to the use of SILworX for engineering, start-up, testing and operation.	HI 801 103 E
SILworX online help (OLH)	Instructions on how to use SILworX	---

Table 1: Overview of the System Documentation

All the current manuals can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com). Registered customers can download the product documentation from the HIMA Extranet.

## 3 Safety Concept

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

- Safety and availability.
- Safety-relevant time parameters.
- Proof test.
- Safety requirements.
- Automation security.
- Certification.
  - CE declaration of conformity.
  - EC type test certificate.

### 3.1 Safety and Availability

The HIMatrix system is approved for use as an automation safety-system up to safety integrity level 3 (SIL 3) in accordance with IEC 61508.

No imminent risk results from the HIMatrix automation systems.

#### WARNING



**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 and the PFH Values

The PFD (probability of failure on demand) and PFH (probability of failure per hour) values for the HIMatrix system have been calculated in accordance with IEC 61508.

For SIL 3, the IEC 61508-1 standard defines the following values:

- $PFD = 10^{-4} \dots 10^{-3}$ .
- $PFH = 10^{-8} \dots 10^{-7}$  per hour.

The values for PFD, PFH and SFF can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com).

### 3.1.2 Self-Test and Fault Diagnostics

The operating system of the controllers executes comprehensive self-tests at start-up and during operation.

The scope of the testing includes:

- Processors.
- Memory areas (RAM, NVRAM).
- The watchdog.
- Individual I/O channels.
- The power supply.

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

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

All HIMatrix controllers, remote I/Os and 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 device status, e.g., the temperature range.

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

For further details on how to evaluate diagnostic messages, refer to the HIMatrix system manual (HI 801 141 E).

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

### 3.1.3 PADT

The PADT is used to configure the controller and create the user program. The safety concept of the PADT supports the user in the proper implementation of the control task. The PADT implements numerous actions to verify the information entered.

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

### 3.1.4 Structuring Safety Systems in Accordance with the Energize to Trip Principle

Safety systems operating in accordance with the energize to trip principle have the following function:

1. The safe state of a module is the de-energized state. This state is adopted, for instance, if a fault has occurred in the module.
2. The controller can trigger the safety function on demand by switching on an actuator.

#### 3.1.4.1 Detection of Failed System Components

Thanks to the automatic tests, the safety system is able to detect that modules have failed.

#### 3.1.4.2 Safety Function in Accordance with the Energize to Trip Principle

The safety function is performed when the safety system energizes one or several actuators.

The users must plan the following actions:

- Line monitoring (short-circuits and open-circuits) with input and output modules. These functions must be configured accordingly.
- The operation of the actuators can be monitored through a position feedback.



## 3.2 Safety-Relevant Time Parameters

The following time parameters must be taken into account for the controller's safety considerations:

- Process safety time.
- Safety time (of the resource).
- Watchdog time (of the resource).
- Response time.

---

i

Resource refers to the image of the controller (PES) in the SILworX programming tool.

---

### 3.2.1 Process Safety Time

According to IEC 61508-4, the process safety time is the time interval between a failure of the EUC or the EUC control system with the potential to cause a hazardous event and the point in time when the EUC response must be completed to prevent the hazardous event from occurring.

During the process safety time, the process may allow faulty signals to exist without a hazardous state occurring.

A safety-related response of the controller including all delays due to sensors, actuators, I/O modules and process (response of the plant to a tripping) must occur within the process safety time.

### 3.2.2 Safety Time [ms] Parameter of the Resource

The *Safety Time [ms] parameter in the resource properties*  $t_{SR}$  affects the response time of the resource  $t_{RR}$  as follows:

$$t_{RR} \leq t_{SR}$$

$t_{SR}$       The *Safety Time [ms]* parameter

When using an F60 AO 8 01, also observe the following:

To determine the worst case response time of the analog outputs, add the double watchdog time of the AO CPU ( $2 \times t_{WD \text{ AO } \mu P}$ ) to the double watchdog time ( $2 \times t_{WD \text{ CPU}}$ ).

$$t_{RR} \leq t_{SR} + 12 \text{ ms}$$

$t_{SR}$       The *Safety Time [ms]* parameter

The following factors prolong the response time of the resource and must be taken into account during set-up:

- Physical delays, e.g., due to the switching times of external relays.
- Delays configured in the user program, e.g., the timer function blocks TON and TOF.

The *Safety Time [ms]* parameter  $t_{SR}$  in the resource properties can be set in SILworX within 20...22 500 ms.

To ensure that the fault response is triggered within the configured resource safety time, the following requirements must be met:

- The user program must respond within a RUN cycle.
- No delays configured through the user program.

### 3.2.3 Watchdog Time (of the Resource)

The watchdog time  $t_{WD}$  is the maximum permissible duration of a RUN cycle (cycle time). The controller is shut down if the cycle time exceeds the watchdog time.

The user can set the watchdog time in accordance with the safety-related requirements of the application.

**Condition for safety:**

$$t_{WD} \leq \frac{1}{2} \times t_{SR}$$

$t_{WD}$  Watchdog time (of the resource)

$t_{SR}$  *Safety Time [ms]* parameter (of the resource)

The watchdog time (of the resource) must be configured. The *Watchdog Time [ms]* parameter can be set within 4...5000 ms and is configured in the resource properties. The default setting is 200 ms for all the controllers and 100 ms for the remote I/Os.

The PADT checks the parameters *Safety Time [ms]* and *Watchdog Time [ms]* and rejects the configuration while generating it if the watchdog time is set to a value greater than  $\frac{1}{2}$  of the resource safety time.

The watchdog time can only be estimated. For the estimation, the following time requirements must be taken into account.

- Cycle duration of the user programs (RUN cycle of the resource).
  - Time for reading in the data.
  - Data processing.
  - Process data communication.
  - Time for issuing the data.
- Processor module synchronization.
- Special time requirements for reload.

#### NOTICE



**The user must consider and observe the mentioned restrictions when performing online changes to the controller!**  
**Carefully check the settings before any online change!**

### 3.2.4 Estimating the Watchdog Time

HIMA strongly recommends the following setting to ensure sufficient availability:

$$3 \times t_{WD} \leq t_{SR} \text{ (Safety Time [ms] parameter)}$$

### 3.2.5 Determining the Watchdog Time through Testing

The watchdog time  $t_{WD}$  can be determined through testing during commissioning or start-up. To this end, the system must be in RUN and operated under full load. All engineered modules must be inserted and all the configured communication connections (e.g., safe**ethernet** and other standard protocols) must be operating.

#### Test requirements:

- The HIMatrix hardware is completely mounted, e.g., the F60 rack includes all designated modules.
- Communication partners, including remote I/Os, are available and connected.
- The user program logic is completely available.
- *Target Cycle Time [ms]* is set to 0.
- *Program's Maximum Number of CPU Cycles* is set to 1 (program properties).
- *Max. Duration for Each Cycle [μs]* is set to 0 (program properties).
- *Max.Com. Time Slice [ms]* is set to a suitable value.
- *Max. Duration of Configuration Connections [ms]* is set to a suitable value.

#### 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 preferably pass through the longest program paths. To this end, input value sequences may be necessary.
3. Reset the cycle time statistics in the Control Panel.
4. Perform the reload multiple times, if required by the application.
5. In the Control Panel, observe the maximum cycle time values.
  - ☒  $t_{Cycle}$  is identified.
6. Determine the maximum deviation between the user program's total execution time and the average total execution time.
  - ☒  $\Delta t_{Peak}$  is identified.
7. Calculate the minimum watchdog time  $t_{WD}$  using:

$t_{WD} = t_{Cycle} + t_{Res} + t_{Com} + t_{Config} + \Delta t_{Peak}$ , where

$t_{Cycle}$	Observed maximum cycle time (basic load, already includes portions of $t_{Com}$ and $t_{Config}$ )
$t_{Reserve}$	Safety margin 6 ms.
$t_{Com}$	System parameter <i>Max. Com. Time Slice ASYNC [ms]</i> , which is configured in the resource properties.
$t_{Config}$	System parameter <i>Max. Duration of Configuration Connections [ms]</i> , which is configured in the resource properties.
$t_{Peak}$	Maximum load peak of the cycle time ( $t_{Peak}$ ) less observed basic load, see step 6.

- The value set for the watchdog time should be: determined minimum value  $t_{WD}$  + margin for future changes or extensions.

The maximum cycle time values during the reload depend on the configured watchdog time. If the PES should be optimized to the lowest possible watchdog time, the value of the **configured** watchdog time must be gradually reduced in a series of measurements.

In the following cases, contact HIMA technical support:

- If the requisites for the above strategy for determining the watchdog time cannot be complied with.
- If the result is not satisfying.

The HIMatrix system allows settings that ensure an even better performance. In-depth knowledge in several areas is required to identify these settings.

### 3.2.6 Response Time

Assuming that no delay results from the configuration or the user program logic, the response time of HIMatrix controllers running in cycles is twice the cycle time of these systems when they are operating properly.

---

**TIP**

If a conservative method should be used to calculate the response time during proper operation, HIMA recommends using the configured watchdog time instead of the cycle time.

---

### 3.3 Proof Test (in Accordance with IEC 61508)

The objective of the proof test is to detect dangerous hidden failures in a safety-related system so that, if necessary, it can be restored to its designed functionality. After a successful proof test, safe operation including the safety functions are ensured again.

The proof test execution depends on:

- The system characteristics (EUC = equipment under control).
- The system's risk potential.
- The standards used for operating the system.
- The standards applied by the test authority for the system's approval.

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 proof testing. The complete safety functions within the HIMA safety-related system must be checked during the proof test.

HIMA safety systems must be subject to a proof test in regular intervals. The proof test interval for HIMA controllers must be in accordance with the interval required by the application-specific safety integrity level (SIL).

The proof test execution is described in the maintenance manual (HI 800 455 E).

### 3.4 Safety Requirements

For using the safety-related HIMatrix automation system, the following safety requirements must be met:

#### 3.4.1 Product-Independent Hardware Requirements

Personnel configuring the HIMatrix hardware must observe the following product-independent safety requirements.

- To ensure safety-related operation, approved fail-safe hardware and software components must be used. Approved HIMA components are listed in the HIMatrix version list. The latest versions can be found in the version list, which is maintained together with the test authority.
- The conditions of use specified in this safety manual about EMC, mechanical, chemical and climatic influences must be observed.
- Non-fail-safe, interference-free hardware components and software components can be used for processing non-safety-relevant signals, but not for handling safety-related tasks. Non-fail-safe components must not be used for processing safety-related tasks.
- The de-energize to trip principle must be applied to all safety circuits externally connected to the system.

#### 3.4.2 Product-Dependent Hardware Requirements

Personnel configuring the HIMatrix hardware must observe the following product-dependent safety requirements.

- Only devices with electrically protective separation from the power supply may be connected to the system
- Only safety-related modules may be used to process safety-related tasks.
- The conditions of use detailed in the system manual, particularly those concerning supply voltage and climate, must be observed.
- The safe, electrically protective separation of the power supply must be guaranteed within the 24 V system supply. Only power supply units of type PELV or SELV may be used.
- The requirements for power supply provided through the mains supply are the same as those applying to power supply units.

#### 3.4.3 Product-Independent Programming Requirements

Personnel developing user programs must observe the following product-independent safety requirements:

- In safety-relevant 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.

### 3.4.4 Product-Dependent Programming Requirements

The SILworX programming tool must be used for programming the HiMatrix system. The following requirements for using SILworX must be met.

- The application described in the specification must be validated, verified and its proper implementation must be documented. Functional tests must be performed to completely test the logic.
- If the user program is changed, all the logic parts affected by the changes must be tested.
- A system response to faults must be defined for faults in safety-related input and output modules in accordance with the application-specific safety-related requirements. These are for instance fault responses in the user program and the configuration of safe initial values for variables.

### 3.4.5 Communication

The following requirements for communication of data and to systems must be met.

- When implementing safety-related communications between various HIMA systems, ensure that the overall response time of the system does not exceed the worst case response time permitted for **safeethernet** or HIPRO-S V2. All calculations must be performed in accordance with the rules given in Chapter *Worst Case Response Time for safeethernet*.
- During the transfer of (safety-relevant) data, IT security rules must be observed.
- The transfer of safety-relevant data through public or publicly accessible networks (e.g., the Internet, WLAN) is only permitted if additional security measures have been implemented, e.g., a VPN tunnel and firewall.
- If data is transferred through company/plant internal networks, administrative and technical measures must be implemented to ensure sufficient protection against manipulation (e.g., a firewall to separate the safety-relevant components of the network from other networks).
- Never use the standard protocols to transfer safety-related data.
- The communication interfaces must be connected to devices with electrically protective separation.

### 3.4.6 Maintenance

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

Whenever necessary, the operator must consult with the test authority responsible for the application and determine the access to the system by implementing administrative and technical measures.

### 3.4.7 Temperature Monitoring

The temperature is measured by embedded sensors and can be displayed and used in the SILworX programming tool. For further details, refer to the system manual (HI 800 141 E).

---

#### i

The temperature can be used in the user program, e.g., as additional shutdown condition; however, the temperature is not recorded in a safety-related manner.

Temperature State may be used as an additional shutdown condition.

---

### 3.4.8 Environmental Requirements

For using the safety-related HiMatrix automation system, the following general environmental requirements must be met:

General information	
Protection class	Protection class III in accordance with IEC/EN 61131-2
Ambient temperature	0...+60 °C
Transport and storage temperature	-40...+70 °C
Pollution	Pollution degree II in accordance with IEC/EN 60664-1
Installation height	< 2000 m
Enclosure	Standard: IP20 If required by the relevant application standards (e.g., EN 60204), the system must be installed in an enclosure with the specified degree of protection (e.g., IP54).
Power Supply Input Voltage	24 VDC

Table 2: Environmental Requirements

Refer to the relevant manual for potential deviations.



### 3.5 Automation Security

HIMA distinguishes between the terms *safety*, which refers to functional safety, and *security*, which refers to the system protection against manipulation.

Industrial controllers (PES) must be protected against IT-specific problem sources, for instance:

- Inadequate protection of IT equipment (e.g., open WLAN, obsolete operating systems).
- Lack of awareness of proper use of the equipment (e.g., USB sticks).
- Direct access to protected areas.
- Attackers inside the company premises.
- Attackers via communication networks inside and outside the company premises.

HIMA safety systems are composed of the following parts to be protected:

- Safety-related automation system.
- PADT.
- Optional X-OPC Server (on a host PC).
- Optional communication connections to external systems.

#### 3.5.1 Product Properties

The HIMatrix controller with basic settings already fulfils the requirements for automation security.

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

- Each change to the user program or controller configuration results in a new configuration CRC.
- Online changes of the safety parameters can be deactivated in the controller. Therefore, changes to the safety parameters are only possible by performing a download or reload.
- The user can set up a user management scheme to increase security. This scheme is used to specify the user groups, user accounts, access permissions for PADT and controllers (PES) for each project. In the user management scheme, the user can define if an authorization is required to open the project and log in to a controller.
- The data of a controller can only be accessed if the user projects loaded in the PADT and controller are the same. The CRCs must be identical (archive maintenance!).
- A physical connection between PADT and controller (PES) is not required during operation and must be interrupted for security reasons. The PADT can be reconnected to the controller for diagnostic and maintenance purposes.

The requirements of the safety and security standards must be complied with. The operator is responsible for authorizing personnel and implementing the required protective actions.

#### WARNING



**Physical injury possible due to unauthorized manipulation of the controllers!**

**Protect the controllers against unauthorized access!!**

- **Change the default settings for login and password.**
- **Supervise access to controllers and PADTs!**
- **For further protection measures, refer to the automation security manual (HI 801 373 E).**

### 3.5.2 Risk Analysis and Planning

Security is a process, not a product. Maintained network maps, for instance, help to ensure that secure networks are permanently separated from public networks. It is recommended to only have one well-defined connection, e.g., via a firewall or a DMZ (demilitarized zone).

Careful planning should identify the necessary measures. The required measures are to be implemented after the risk analysis is completed, and may include:

- Assignment of access permissions for user groups and user accounts according to the intended tasks.
- Use of passwords in accordance with the security requirements.

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

---

## i

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

---

Refer to the HIMA automation security manual (HI 801 373 E) for more details.

### 3.6 Certification

The HIMatrix programmable electronic system complies with the standards listed in this chapter.

#### 3.6.1 CE Declaration of Conformity

With respect to performance and design, the HIMatrix automation system complies with international and European Directives, and also meets complementary national requirements. Conformity was declared through the CE marking.

The declaration of conformity for the automation system can be found on the website [www.hima.com/en](http://www.hima.com/en) or obtained by sending an e-mail request to: [documentation@hima.com](mailto:documentation@hima.com).

#### 3.6.2 EC Type Test Certificate

The test institute TÜV Rheinland has tested and certified the safety-related HIMatrix automation system for applications in accordance with the functional safety standards. The safety-related HIMatrix automation system is provided with the following mark of conformity:



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

**EC type test certificate**  
**Safety-Related Programmable System**  
**HIMatrix**

### 3.6.3 Current Standards

The HIMatrix safety-related automation system is tested in accordance with the following functional safety standards and is certified by the TÜV:

International standards:	Safety level
IEC 61508, Parts 1-7:2010	SIL 3
IEC 61511-1:2016	SIL 3
EN ISO 13849-1:2015	PL e
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015	SIL CL 3
EN 50156-1:2015	SIL 3
EN 12067-2:2004	---
EN 298:2012	---
EN 60079-0:2012 + A11:2013	---
EN 60079-11:2012	---
EN 60079-15:2010	---
EN 60079-29-1: 2007	---
NFPA 72:2016	---
NFPA 85:2015	---
NFPA 86:2015	---
EN 61131-2:2007	Zone C
EN 61131-6:2012	---
EN 61326-3-1:2017	---
EN IEC 61326-3-2:2018	---
EN 54-2:1997 + AC:1999 + A1:2006	---

Table 3: International Standards and Safety Levels

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

### 3.6.4 Test Requirements

The HIMatrix system has been tested for compliance with the following standards related to EMC, climatic, mechanical and voltage testing:

Standard	Content
IEC/EN 61131-2 Zone C	Programmable controllers Part 2: Equipment requirements and tests
IEC/EN 61000-6-2	Electromagnetic compatibility (EMC) Part 6-2: Generic standards – Immunity for industrial environments
IEC/EN 61000-6-4	Electromagnetic compatibility (EMC) Part 6-4: Generic standard – Emission standard for industrial environments
EN 298	Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
EN 61326-1	Electrical equipment for measurement, control and laboratory use - EMC requirements Part 1: General requirements
EN 61326-3-1	Electrical equipment for measurement, control and laboratory use - EMC requirements Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
EN 50130-4	Alarm systems Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder, hold up, CCTV, access control and social alarm systems.
EN 54-2	Fire alarm systems

Table 4: Standards for EMC, Climatic and Environmental Requirements

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

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

Table 5: Noise Emission Tests

### 3.6.4.1 Climatic Tests

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

Standard	Climatic tests
IEC/EN 61131-2	Dry heat and cold; withstand 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 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 6: Climatic Tests

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

### 3.6.4.2 Mechanical Tests

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

Standard	Mechanical tests
IEC/EN 61131-2	Vibration immunity test: 5...8.4 Hz / 3.5 mm 8.4...150 Hz / 1 g, controller in operation, 10 cycles per axis
	Shock immunity test: 15 g, 11 ms, HiMatrix in operation, 3 shocks per axis and direction (18 shocks)

Table 7: Mechanical Tests

### 3.6.4.3 EMC Tests

The controller meets the requirements of the EMC Directive of the European Union, see the system's EU Declaration of Conformity.

All controller modules meet the requirements of the EMC Directive of the European Union (2014/30/EU) and bear the CE marking.

The controller responds safely to interferences exceeding the specified limits.

#### 3.6.4.4 Supply Voltage

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

Standard	Verification of the DC supply characteristics
IEC/EN 61131-2	The power supply must at least comply with one of the following standards or meet one of the following requirements: <ul style="list-style-type: none"> <li>▪ IEC 61131-2</li> <li>▪ SELV (Safety Extra Low Voltage)</li> <li>▪ PELV (Protective Extra Low Voltage)</li> </ul>
	The HIMatrix system must be fuse-protected as specified in the data sheets.
	Voltage range test: 24 VDC, -20...+25 % (19.2...30.0 VDC).
	Momentary external current interruption immunity test: DC, PS 2: 10 ms.
	Reversal of DC power supply polarity test.

Table 8: Verification of the DC Supply Characteristics

## 4 Central Functions

The controllers and remote I/Os of type F1..., F2..., F3... are compact systems that cannot be modified.

The controllers of type F60 are modular systems. In addition to the processor module and the power supply module, one controller of this type may include up to six I/O modules.

### 4.1 Power Supply

The power supply module is only included within a F60. As to compact systems, the power supply function is integrated in the device and cannot be treated as an individual module.

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

### 4.2 Functional Description of the Processor System

In the modular F60 system, the processor system is mounted on a separate module whereas in compact systems, it is included in the compact controller.

Properties of the F60 CPU 03 processor module

- 1oo2 processor system.
- 2 synchronous microprocessors with 1 SDRAM each.
- Testable hardware comparator.
- NVRAM:
  - Diagnostic data.
  - Retain data.
  - Operating system.
  - User program.
- Hardware clock buffered with Goldcap.
- Communication processor.
- Interface for exchanging data between devices, controllers and the PADT, based on Ethernet.
- Optional interface(s) for data exchange via fieldbus.
- LEDs for indicating the system states.
- I/O bus logic for connection to I/O modules.
- Safe watchdog (WD).
- Monitoring of the system voltages.
- Temperature monitoring.



### 4.3 Self-Tests

The operating system of the processor system executes comprehensive self-tests at start-up and during operation. If the operating system detects single faults that could cause a hazardous operating state to occur, the faulty components are switched off. This is the safe state and is performed within the safety time.

The diagnostic measures mandatory for complying with the safety standards are implemented in the safety-related processor system.

The scope of the testing includes:

- The microprocessors.
- Memory areas (RAM, NVRAM).
- The watchdog.
- The I/O bus within the controller.
- The power supply.
- The temperature range.

### 4.4 Responses to Faults in the Processor System

A hardware comparator within the processor system constantly checks if the data from microprocessor 1 is identical to the data from microprocessor 2. If this is not the case or the test routines detect a fault, the watchdog signal is switched off. This means that the input signals are no longer processed by the controller, and the outputs switch to the de-energized, switched-off state.

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

### 4.5 Fault Diagnostics

Each F60 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.

In the F1..., F2..., F3... compact systems, these fault indications are grouped into one common error message.

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 still be able to evaluate the faults.

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

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

For further details on how to evaluate diagnostic messages, refer to the system manual (HI 801 141 E).

## 5 Inputs

The following table provides an overview of the input modules of the HIMatrix system:

Compact system	Type	Number of inputs	Safety-related	Interference-free	Galvanically separated
F30 03 controller <sup>1)</sup>	Digital	20	•	•	-
F35 03 controller <sup>1)</sup>	Digital	24	•	•	-
	24-bit counter	2	•	•	-
	Analog	8	•	•	-
F1 DI 16 01 remote I/O	Digital	16	•	•	-
F3 DIO 8/8 01 remote I/O <sup>1)</sup>	Digital	8	•	•	-
F3 DIO 16/8 01 remote I/O <sup>1)</sup>	Digital	16	•	•	-
F3 AIO 8/4 01 remote I/O <sup>1)</sup>	Analog	8	•	•	-
F3 DIO 20/8 02 remote I/O <sup>1)</sup>	Digital	20	•	•	-
Modular F60 System	Type	Number of inputs	Safety-related	Interference-free	Galvanically separated
DIO 24/16 01 module <sup>1)</sup>	Digital	24	•	•	•
DI 32 01 module (configurable for line control)	Digital	32	•	•	•
DI 24 01 module (110 V)	Digital	24	•	•	•
CIO 2/4 01 module <sup>1)</sup>	24-bit counter	2	•	•	•
AI 8 01 module	Analog	8	•	•	•
MI 24 01 module	Analog or digital	24	•	•	•
<sup>1)</sup> For additional outputs, see Table 13					

Table 9: Overview of the HIMatrix System Inputs

### 5.1 General Information

Safety-related inputs may be used for safety-related as well as for non-safety-related signals. Non-safety-related signals, however, may not be used for safety functions!

The controllers provide status and fault information as follows:

- Through diagnostic LEDs.
- Using system variables that the user program can evaluate.
- Storing messages in the diagnostic memory that the PADT can read.

Safety-related input modules are automatically tested during operation through high-quality, cyclic self-tests. These test routines are TÜV-tested and monitor the safe functioning of the corresponding module.

For a small number of component failures that do not affect safety, no diagnostic information is generated.

## 5.2 Response in the Event of a Fault

If the test routine detects an error, the user program processes the initial value of the global variable assigned to the input. An error code is created.

The error code and other system variables can be used to program application-specific fault responses. For further details, refer to the manual of the corresponding component.

If a fault occurs, a compact system activates the *ERROR* LED, an F60 module the *ERR* LED.

## 5.3 Safety of Sensors, Encoders and Transmitters

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

## 5.4 Safety-Related Digital Inputs

The described properties apply to both the digital input channels of F60 modules and the digital input channels of all compact systems (unless stated otherwise).

### 5.4.1 General Information

The digital inputs are read once per cycle and saved internally; cyclic tests are performed to ensure their safe functioning.

Under certain circumstances, input signals that are present for shorter than the time between two samplings, are not detected.

### 5.4.2 Test Routines

The 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 before 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.

If shielded cables are used for digital inputs, no additional precautionary measures are required to protect against surges.

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

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

---

### i

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

In particular, the design must include protective measures with respect to overvoltage, lightning, ground grounding and plant wiring in accordance with the relevant standards and the instructions specified in the system manual (HI 800 141 EE).

---

#### 5.4.4 Configurable Digital Inputs

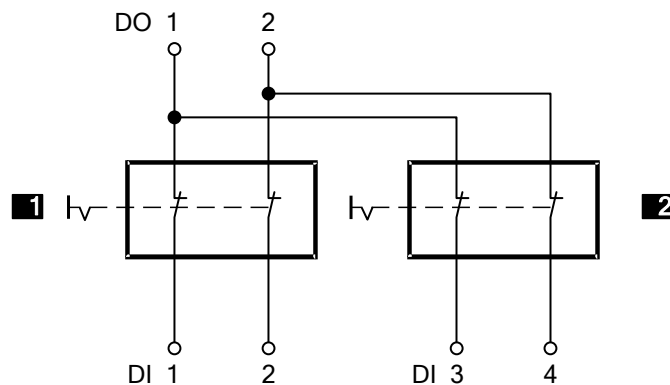
The digital inputs of the F35 03 controller and the MI 24 01 module operate as analog inputs, but return digital values due to the configuration of switching thresholds.

For configurable digital inputs, the same test routines and safety-related functions defined for analog inputs apply as specified in Chapter 5.5.

#### 5.4.5 Line Control

Line control is used to detect short-circuits or open-circuits e.g., on emergency stop devices and can be configured for the HIMatrix systems with digital inputs (not for the F35 03 controller and MI 24 01 module).

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

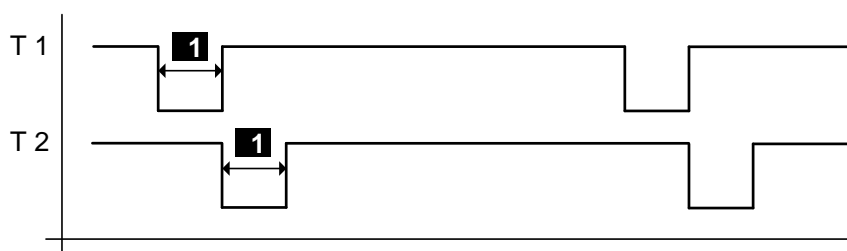


- 1** Emergency stop 1
- 2** Emergency stop 2

Emergency stop switches in accordance with EN 60947-5-1 and EN 60947-5-5

Figure 1: Line Control

The controller pulses the digital outputs to detect short-circuits and open-circuits on the wires connected to the digital inputs. To do so, configure the *Value [BOOL]* -> system variable in SILworX. The pulsed outputs can be assigned to any digital inputs.



- 1** Configurable 5...2000  $\mu$ s

Figure 2: Pulsed Signals T1, T2

An (evaluable) error code is created, if the following errors occur:

- Cross-circuit between two parallel wires.
- Invalid connections of two lines (e.g., DO 2 to DI 3).
- Ground fault on one of the wires (with grounded reference pole only).
- Open-circuit or open contacts.

For a description of line control and further details, refer to the HIMatrix system manual (HI 800 141 E).

## 5.5 Safety-Related Analog Inputs (F35 03, F3 AIO 8/4 01 and F60)

The analog input channels convert the measured input currents into an INTEGER value. The values are available to the user program as variables that are assigned to the system variable -> *Value [INT]*.

The range of values for the inputs depends on the component:

### F35 03 Controller

Input channels	Measurement procedure	Current, voltage	Range of values in the application	
			FS1000 <sup>1)</sup>	FS2000 <sup>1)</sup>
8	Unipolar	0...+10 V	0...1000	0...2000
8	Unipolar	0...20 mA	0...500 <sup>2)</sup> 0...1000 <sup>3)</sup>	0...1000 <sup>2)</sup> 0...2000 <sup>3)</sup>
<sup>1)</sup> Configurable by selecting the type in the PADT. <sup>2)</sup> With external 250 Ω shunt adapter. <sup>3)</sup> With external 500 Ω shunt adapter.				

Table 10: Analog Inputs of the F35 03 Controller

### F3 AIO 8/4 01 Remote I/O

Input channels	Measurement procedure	Current, voltage	Range of values in the application
8	Unipolar	0...+10 V	0...2000
8	Unipolar	0/4...20 mA	0...1000 <sup>1)</sup> 0...2000 <sup>2)</sup>
<sup>1)</sup> With external 250 Ω shunt adapter. <sup>2)</sup> With external 500 Ω shunt adapter.			

Table 11: Analog Inputs of the F3 AIO 8/4 01 Remote I/O

### F60 Modules

Input channels	Measurement procedure	Current, voltage	Range of values in the application	
			FS1000 <sup>1)</sup>	FS2000 <sup>1)</sup>
AI 8 01				
8	Unipolar	-10...+10 V	-1000...1000	-2000...2000
8	Unipolar	0...20 mA	0...1000 <sup>3)</sup>	0...2000 <sup>3)</sup>
8	Unipolar	0...20 mA	0...500 <sup>2)</sup>	0...1000 <sup>2)</sup>
4	Bipolar	-10...+10 V	-1000...1000	-2000...2000
MI 24 01				
24	Unipolar	0...20 mA	0...2000 <sup>4)</sup>	
<sup>1)</sup> Configurable by selecting the type in the PADT (F60).				
<sup>2)</sup> With external 250 Ω shunt.				
<sup>3)</sup> With external 500 Ω shunt (accuracy 0.05 % 1 W). No longer available at HIMA.				
<sup>4)</sup> Internal shunts.				

Table 12: Analog Inputs of the F60 Controller

The F60 module AI 8 01 can be configured in the user program for 8 unipolar or 4 bipolar functions. However, it is not allowed to combine functions on a module.

The analog inputs of the F35 03 controller, the F3 AIO 8/4 01 remote I/O and the AI 8 01 module operate with voltage measurement. With the analog inputs of the F35 03 and F3 AIO 8/4 01, digital outputs of the own system (F35 03) or other HIMatrix controllers can be monitored to detect open-circuits. For further details, refer to the manuals of the corresponding HIMatrix controllers.

If an open-circuit occurs and line monitoring is not active in the system, random input values are processed at the high-resistance inputs. The value resulting from this floating input voltage is not reliable; for voltage inputs, the channels must be terminated with a 10 kΩ resistor. The internal resistance of the source must be taken into account.

To measure currents, the shunt is connected in parallel to an input; in doing so the 10 kΩ resistor is not required.

The inputs of the MI 24 01 module operate as current inputs due to the internal shunts, and cannot be used as voltage inputs.

The measuring input of unused inputs must be connected to the reference potential to prevent negative effects on other input channels in case of open-circuits (floating voltage values). This step is not necessary if no global variables are assigned to the unused inputs.

### 5.5.1 Test Routines

The analog input signal is processed in parallel via two multiplexers and two analog/digital converters with 12-bit resolution. The results are compared to one another. Additionally, analog test values are applied via the D/A converters, converted back and then compared with the default values.

## 5.6 Safety-Related Counters (F35 03 and F60)

Unless otherwise noted, the points previously mentioned apply to the CIO 2/4 01 counter module of the F60 system as well as to the F35 03 counters.

### 5.6.1 General Information

A counter channel can be configured for operation 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 is only carried out in the user program.

The counter encoders have the following resolutions:

- The counters of the F60 module CIO 2/4 01 have 4-bit or 8-bit resolution.
- The F35 03 counters have 3-bit or 6-bit resolution.

A reset is possible.

Two independent 4-bit inputs can only be linked to one 8-bit input (example for F60) via the user program. No switching option is planned for this purpose.

The encoder function monitors the change of the bit pattern on the input channels. The bit patterns on the inputs are directly transferred to the user program. They are represented in the PADT as decimal numbers corresponding to the bit pattern (*Counter[0x].Value*).

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

## 5.7 Checklists for Inputs

HIMA recommends using the available checklist for engineering, programming and starting up safety-related inputs. The checklist can be used as a planning document and also serves as proof of careful planning.

When engineering and 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 provides documentation about the relationship between the external wiring and the user program.

The current checklists can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com). Registered customers can download the product documentation from the HIMA Extranet.

## 6 Outputs

The following table provides an overview of the output modules of the HIMatrix system:

Compact system	Type	Number of outputs	Safety-related	Galvanically separated
F30 03 controller (configurable for line control) <sup>1)</sup>	Digital	8	•	-
F35 03 controller <sup>1)</sup>	Digital	8	•	-
F1 DI 16 01 remote I/O	Pulse	4	-	-
F2 DO 4 01 remote I/O	Digital	4	•	-
F2 DO 8 01 remote I/O	Relay	8	•	•
F2 DO 16 01 remote I/O	Digital	16	•	-
F2 DO 16 02 remote I/O	Relay	16	•	•
F3 DIO 8/8 01 remote I/O <sup>1)</sup>	Digital 1-pole	8 <sup>2)</sup>	•	-
	Digital 2-pole	2 <sup>2)</sup>		
F3 DIO 16/8 01 remote I/O <sup>1)</sup>	Digital 1-pole	16 <sup>2)</sup>	•	-
	Digital 2-pole	8 <sup>2)</sup>		
F3 AIO 8/4 01 remote I/O <sup>1)</sup>	Analog	4	-	-
F3 DIO 20/8 01 and F3 DIO 20/8 02 remote I/Os (configurable for line control) <sup>1)</sup>	Digital	8	•	-
Modular F60 System	Type	Number of outputs	Safety-related	Galvanically separated
DIO 24/16 01 module (configurable for line control) <sup>1)</sup>	Digital	16	•	
DO 8 01 module (250 V)	Relay	8	•	•
CIO 2/4 01 module <sup>1)</sup>	Digital	4	•	
AO 8 01 module	Analog	8	•	Pairwise
<sup>1)</sup> For additional inputs, see Table 9				
<sup>2)</sup> Refer to the corresponding manual for more details.				

Table 13: Overview of the HIMatrix System Outputs

### 6.1 General Information

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.

Three testable switches connected in series are integrated in the safety-related output channels. The required second independent shutdown option is thus integrated in the output module. If a fault occurs, this integrated safety shutdown safely de-energizes all the channels of the defective submodule (de-energized state).

Additionally, the watchdog signal of the CPU is the second safety shutdown option: If the watchdog signal is lost, the CPU immediately enters the safe state of all output channels.

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

The corresponding error code provides additional options for configure fault responses in the user program.



## 6.2 Response in the Event of a Fault

If the test routines detect an error or fault, the controller switches off the affected output is set to the safe state. An error code is created.

The error code and other system variables can be used to program application-specific fault responses. For further details, refer to the manual of the corresponding component.

If a fault occurs, a compact system activates the *ERROR* LED, an F60 module the *ERR* LED.

## 6.3 Safety of Actuators

In safety-related applications, the controller (PES) and connected actuators must all meet the safety requirements and achieve the specified SIL. For details on how to achieve the required SIL for actuators, refer to the IEC 61511-1 standard, Section 11.4.

## 6.4 Safety-Related Digital Outputs

The points listed below apply to both digital output channels of F60 modules and digital output channels of the compact systems. Unless specified otherwise, the relay modules are an exception in both cases.

### 6.4.1 Test Routines for Digital Outputs

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

- Reading the output signals back from the switching amplifier. The switching threshold for a read-back low level is 2 V. The diodes used prevent the signals from being fed back.
- Checking the integrated redundant safety shutdown.
- Shutdown test of the outputs.

The system monitors its operating voltage and de-energizes all outputs at voltages of less than 13 V.

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

If the output is short-circuited to L- or overloaded, the device is still testable. Shutdown via safety shutdown is not required.

The controller monitors the device's total current consumption 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.

### 6.4.3 Line Control

The controller can pulse safety-related digital outputs or special pulsed outputs and use them with the safety-related digital inputs of the same system (not the digital inputs of the F35 03 or F60 MI 24 01) to detect open-circuits and short-circuits (see Chapter 5.4.5).

#### NOTICE



**Malfunctions of the connected actuators are possible!**

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

Relay outputs cannot be used as pulsed outputs.

## 6.5 Safety-Related 2-Pole Digital Outputs

The following points apply to 2-pole digital outputs of the remote I/Os F3 DIO 8/8 01 and F3 DIO 16/8 01.

The remote I/Os are tested automatically during operation. The main test functions are:

- Reading the output signals back from the switching amplifier. The diodes used prevent the signals from being fed back.
- Checking the integrated (redundant) safety shutdown.
- Shutdown test of the outputs.
- Line diagnosis for 2-pole connection.

F3 DIO 16/8 01:

- Short-circuit to L+, L-.
- Short-circuit between 2-pole connections.
- Open-circuit in one of the 2-pole connections.

F3 DIO 8/8 01:

- Short-circuit to L+, L-.

The system monitors its operating voltage and de-energizes all outputs at voltages of less than 13 V.

With a 2-pole connection, observe the following notes:

---

**i**

A relay or actuator connected to the output may accidentally be switched on!

A requirement for applications in machine safety is that the outputs DO+, DO- are switched off if an open-circuit is detected.

---



---

**i**

If the requirements previously described cannot be met, observe the following case:

If a short-circuit occurs between DO- and L-, a relay may be energized or some other actuator may be set to a different switching state.

Reason: During the monitoring time specified for line diagnosis, a 24 V level (DO+ output) is present on the load (relay, switching actuator) allowing it to receive enough electrical power to potentially switch to another state.

The monitoring time must be configured such that an actuator cannot be activated by the line diagnosis test pulse.

---



---

**i**

Detection of open-circuits may be disturbed!

In a 2-pole connection, no DI input may be connected to a DO output. This would inhibit the detection of open-circuits.

---

### 6.5.1 Behavior in the Event of External Short-Circuit or Overload

If the output is short-circuited to L-, L+ or overloaded, the remote I/O is still testable. Shutdown via safety shutdown is not required.

The total current consumption of the remote I/O is monitored. If the threshold is exceeded, the remote I/O sets all channels to the safe state.

In this state, the remote I/O checks the outputs every few seconds to determine whether the overload is still present. In a normal state, the remote I/O switches the outputs on again.

## 6.6 Relay Outputs

The relay outputs correspond to functional digital outputs, but offer galvanic separation and higher electrical strength.

### 6.6.1 Test Routines for Relay Outputs

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

- Reading the output signals back from the switching amplifiers located before the relays.
- Testing the switching of the relay with forcibly guided contacts.
- Checking the integrated redundant safety shutdown.

The system monitors its operating voltage and de-energizes all outputs at voltages of less than 13 V.

The outputs of the DO 8 01 module and those of the remote I/Os F2 DO 8 01 and F2 DO 16 02 are equipped with three safety relays:

- 2 relays with forcibly guided contacts.
- 1 standard relay.

This enables the outputs to be used for safety switch-off functions.

## 6.7 Safety-Related Analog Outputs (F60)

The AO 8 01 module has its own safety-related 1002 A/D microprocessor system with safe communication. It writes to the analog outputs once per cycle and saves the values internally. The module itself tests its functions.

The DIP switches on the safety-related analog output modules can be used to set the outputs to voltage or current outputs. In doing so, ensure that the setting for use in the system comply with the configuration in the user program. If this is neglected, faulty module behavior may result.

### NOTICE



**Module malfunctions are possible!**

**Prior to inserting the module into the system, check the following:**

- **Module's DIP switch settings.**
- **Module configuration in the user program.**

Depending on the device type selected (...FS1000, ...FS2000) during configuration, multiple values must be taken into account in the logic for the output signals to obtain identical output values, see the AO 8 01 manual (HI 800 197 E).

Each group of two analog outputs are galvanically connected:

- Outputs 1 and 2.
- Outputs 3 and 4.
- Outputs 5 and 6.
- Outputs 7 and 8.

The analog output circuits have current or voltage monitoring, read back 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).

### 6.7.1 Test Routines

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

- Reading back the output signal performed twice.
- Crosstalk test between the outputs.
- Checking the integrated safety shutdown.

## 6.8 Analog Outputs with Safety-Related Shutdown (F3 AIO 8/4 01)

The remote I/O writes to the analog outputs once per cycle and saves the values internally.

The outputs are not safety-related, but they can be safely switched off together.

To achieve SIL 3, the output values must be read back via safety-related analog inputs and evaluated in the user program. Responses to faulty output values must be programmed in the user program as well.

### 6.8.1 Test Routines

The remote I/O automatically tests the 2 safety switches used to shut down all 4 module outputs during operation.

## 6.9 Checklists for Outputs

HIMA recommends using the available checklist for engineering, programming and starting up safety-related outputs. The checklist can be used as a planning document and also serves as proof of careful planning.

When engineering and 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 provides documentation about the relationship between the external wiring and the user program.

The current checklists can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com). Registered customers can download the product documentation from the HIMA Extranet.

## 7 Software

The software for the safety-related HIMatrix automation system includes the following parts:

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

The user program, which contains the application-specific functions to be performed by the automation system, is used to create the user program. The programming tool is used to configure and operate the operating system functions of the hardware components.

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 system.

### 7.1 Safety-Related Aspects of Operating Systems

Each approved operating system is clearly identified by the revision number and the CRC signature. 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 version list.

The Revision List of HIMatrix Systems of HIMA Paul Hildebrandt GmbH is created and maintained by HIMA Paul Hildebrandt GmbH in co-operation with the TÜV Rheinland GmbH.

The current version of the operating system can only be read using the SILworX programming tool. Users must ensure that the operating system versions loaded in the modules are valid.

### 7.2 Operation and Functions of Operating Systems

The operating system executes the user program cyclically. In a simplified form, it performs the following functions:

- Reading of the input data.
- Processing of the logic functions, programmed in accordance with IEC 61131-3.
- Writing of the output data.

The following basic functions are also executed:

- Comprehensive self-tests.
- Test of inputs and outputs during operation.
- Data transmission.
- Diagnostics.

### 7.3 Safety-Related Aspects of Programming

When creating or changing a user program, the requirements detailed in this chapter must be observed.

#### 7.3.1 Safety Concept of SILworX

The safety concept for the SILworX programming tool includes the following points:

- When SILworX is installed, a CRC checksum ensures the programming tool's integrity on the way from the manufacturer to the user.
- SILworX performs validity checks to reduce the likelihood of faults while entering data.
- SILworX compiles the program twice and compares the resulting configuration CRCs (checksums) to one another. This ensures that data corruption in the application due to temporary faults in the PC in use is detected.
- SILworX and the measures defined in this safety manual make it sufficiently improbable that a code generated properly from a semantic and syntactic view point can still contain undetected systematic faults resulting from the code generation process.

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

- Verify whether the control tasks were properly implemented based on the data and signal flows.
- Verify the logic of all functions by trial.

If a user program is changed, at least the program components affected by the change must be tested. The safety-related SILworX version comparison can be used to determine and prove changes compared to a previous version.

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

#### 7.3.2 Verifying the Configuration and the User Programs

To check the user programs for compliance with the safety functions, the user must create suitable test cases that validate the specified safety functions.

An independent test of each individual loop (consisting of input, processing including user connections, output) is usually sufficient.

Suitable test cases must be created for the numerical evaluation of formulas. The evaluation can be performed, for instance, using equivalence class tests. The test cases must be selected such that the calculations can be proven to be correct. The required number of test cases depends on the formula used and must include critical value pairs.

HIMA recommend performing an active simulation with data sources. This will prove that the sensors and actuators in the system are properly wired. The same also applies to sensors and actuators that are connected to the system via remote I/Os.

SILworX can be used as test equipment for:

- Checking inputs.
- Forcing outputs.

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

### 7.3.3 Archiving a Project

HIMA recommends archiving the project after each download or reload.

SILworX stores all a project's data to a single file. For reasons of data security, HIMA recommends additionally storing the project on an external medium.

### 7.3.4 Identifying Configuration and Programs

Changes to a program cause the CRC to change and therefore affect the configuration CRC.

To determine the changes to the current configuration, the project is compared to a saved or loaded configuration. The individual changes can be proved using the safe SILworX version comparison.

## 7.4 Resource Parameters

Some parameters are defined in SILworX for actions permitted during the resource's safety-related operation and are referred to as safety parameters.

### WARNING



**Physical injury possible due to invalid configuration!**

**Neither the programming system nor the controller can verify project-specific parameters. For this reason, enter the safety parameters correctly in the programming tool and verify the whole entry upon completion of the PES load from within the controller.**

**These parameters are:**

- **For the rack ID, refer to the system manual (HI 800 141 E).**
- **The parameters marked as safety-related in Table 14.**

Settings 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 Resource System Parameters

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

Parameter	S <sup>1)</sup>	Description	Setting for safe operation
Name	N	Name of the resource.	Any
System ID [SRS]	Y	System ID of the resource. Range of values: 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]	Y	For details on the safety time of the resource (in milliseconds), refer to the safety manual (HI 801 003 E). Range of values: 20...22 500 ms Default value: 600 ms for controllers, 400 ms for remote I/Os (can be changed online)	Application-specific
Watchdog Time [ms]	Y	For details on the watchdog time of the resource (in milliseconds), refer to the safety manual (HI 801 003 E). Range of values: 4...5000 ms Default value: 200 ms for controllers, 100 ms for remote I/Os (can be changed online)	Application-specific
Target Cycle Time [ms]	N	Target or maximum cycle time, see <i>Target Cycle Time Mode</i> . Range of values: 0...5000 ms Default value: 0 ms (can be changed online) The maximum target cycle time value may not exceed the configured <i>Watchdog Time [ms]</i> minus the minimum value that can be set for <i>Watchdog Time [ms]</i> (4 ms, see above); otherwise the entry is rejected. If the default value is set to 0 ms, the target cycle time is not taken into account. For further details, refer to the following chapters.	Application-specific
Target Cycle Time Mode	N	For details on the use of the <i>Target Cycle Time [ms]</i> , see the following chapters. Default value: Fixed-tolerant ( <i>can only be changed online</i> )	Application-specific
Multitasking Mode	N	Mode 1 The duration of a CPU cycle is based on the required execution time for all user programs.	Application-specific
		Mode 2 The processor provides the execution time portion not needed by lower priority user programs to higher priority user programs. Mode of operation 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	
Max. Com.Time Slice [ms]	N	Highest value in ms for the time slice used for communication during a resource cycle, see the communication manual (HI 801 101 E). Range of values: 2...5000 ms Default value: 60 ms	Application-specific



Parameter	S <sup>1)</sup>	Description	Setting for safe operation
Optimized Use of Com. Time Slice	N	<p>The system parameter reduces the response times for communications via processor module(s).</p> <hr/> <p><b>i</b> This can affect the temporal utilization of <i>Max.Com. Time Slice ASYNC [ms]</i> and the system parameter <i>Max. Duration of Configuration Connections [ms]</i> such that these two times can be subject to more demands (e.g., during reload).</p> <hr/>	---
Max. Duration of Configuration Connections [ms]	N	<p>This defines how much time within a CPU cycle is available for configuration connections.  Range of values: 2...3500 ms  Default value: 20 ms  For further details, refer to the following chapters.</p>	Application-specific
Maximum System Bus Latency [μs]	N	<p>Not applicable for HiMatrix controllers!  Default value: System Defaults</p>	---
Allow Online Settings	Y	<p>TRUE: <b>All</b> the switches/parameters listed under FALSE can be changed online using the PADT. This is only valid if the system variable <i>Read-only in RUN</i> has the value FALSE.  Default value: TRUE.</p> <hr/> <p>FALSE: The following parameters <b>cannot</b> be changed online:</p> <ul style="list-style-type: none"> <li>▪ <i>System ID</i></li> <li>▪ <i>Autostart</i></li> <li>▪ <i>Global Forcing Allowed</i></li> <li>▪ <i>Global MultiForcing Allowed</i></li> <li>▪ <i>Global Force Timeout Reaction</i></li> <li>▪ <i>Load Allowed</i></li> <li>▪ <i>Reload Allowed</i></li> <li>▪ <i>Start Allowed</i></li> </ul> <p>The following parameters can be changed online if <i>Reload Allowed</i> is TRUE.</p> <ul style="list-style-type: none"> <li>▪ <i>Watchdog Time (for the resource)</i></li> <li>▪ <i>Safety Time</i></li> <li>▪ <i>Target Cycle Time</i></li> <li>▪ <i>Target Cycle Time Mode</i></li> </ul> <hr/> <p><i>Allow Online Settings</i> can only be TRUE when the controller is stopped or by performing a reload.</p>	HIMA recommends using the FALSE setting.

Parameter	S <sup>1)</sup>	Description		Setting for safe operation
Autostart	Y	TRUE:	If the processor module is connected to the supply voltage, the user programs start automatically. Default value: TRUE.	Application-specific
		FALSE:	The user program does not start automatically after connecting the supply voltage.	
		Observe the settings in the resource program properties!		
Start Allowed	Y	TRUE:	Cold start or warm start permitted with the PADT in RUN or STOP. Default value: TRUE.	Application-specific
		FALSE:	Start not allowed.	
Load Allowed	Y	TRUE:	Configuration download is allowed. Default value: TRUE.	Application-specific
		FALSE:	Start not allowed.	
Reload Allowed	Y	TRUE:	Configuration reload is allowed. Default value: TRUE.	Application-specific
		FALSE:	Configuration reload is not allowed. A running reload process is not aborted when switching to FALSE.	
Global Forcing Allowed	Y	TRUE:	Global forcing is permitted for this resource. Default value: TRUE.	Application-specific
		FALSE:	Global forcing is not permitted for this resource.	
Global Force Timeout Reaction	N	Specifies how the resource should behave when the global force timeout has expired: <ul style="list-style-type: none"><li>▪ <i>Stop Forcing Only.</i></li><li>▪ <i>Stop Forcing and Stop Resource.</i></li></ul> Default value: <i>Stop Forcing Only.</i>		Application-specific
Global MultiForcing Allowed	Y	TRUE:	Users with MultiForcing access can write force data (force values and individual force switches) for global variables in a resource if the required higher-order conditions have been met and the force permissions have been granted.	Application-specific
		FALSE:	Users with MultiForcing access cannot force global variables. Default value: FALSE (can be changed online)	
Minimum Configuration Version	N	With this setting, it is possible to generate code that is compatible with previous or newer HIMatrix operating system versions in accordance with the project requirements. The installed SILworX version is the default setting.		Application-specific
Fast Start-Up	Y	After connecting the supply voltage, the resource starts up faster, <10 s, see Chapter 7.4.1.6. Default value: FALSE.		Application-specific

<sup>1)</sup> The operating system handles the system parameter in a safety-related manner, yes (Y) or no (N).

<sup>1)</sup> The operating system handles the system parameter in a safety-related manner, yes (Y) or no (N).

Table 14: Resource System Parameters

#### 7.4.1.1 Use of the Parameters *Target Cycle Time* and *Target Cycle Time Mode*

Using the settings for the *Target Cycle Time Mode* system parameter, the cycle time can be maintained as constant as possible at the value of *Target Cycle Time [ms]*. To do this, the system parameter must be set to a value > 0.

HIMatrix limits reload to ensure that the target cycle time is maintained.

The following table describes the settings for the *Target Cycle Time Mode* system parameter.

Setting	Description
Fixed	<p>If a CPU cycle is shorter than the defined <i>Target Cycle Time</i>, the CPU cycle is extended to the target cycle time. If the CPU cycle takes longer than the target cycle time, the CPU resumes the cycle without delay.</p> <hr/> <p><b>i</b> A reload process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time).</p> <hr/>
Fixed-tolerant	<p>Similar to <i>Fixed</i>, but with the following difference: To ensure that the reload can be performed successfully, the target cycle time may be violated for 1 to n CPU cycles (where n is the number of changed user programs).</p> <p>Default value: <i>Fixed-tolerant!</i></p> <hr/> <p><b>i</b> After the first reload activation cycle, the values of watchdog time, target cycle time and target cycle time mode apply in accordance with the new configuration. A maximum of every fifth cycle can be extended during the reload.</p> <hr/>
Dynamic	<p>The CPU processes each CPU cycle as fast as possible. This corresponds to a target cycle time of 0 ms.</p> <hr/> <p><b>i</b> A reload process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time). A maximum of every fifth cycle can be extended during the reload.</p> <hr/>
Dynamic-tolerant	<p>Similar to <i>Dynamic</i>, but with the following difference: To ensure that the reload can be performed successfully, the target cycle time may be automatically increased for 1 to n CPU cycles (where n is the number of changed user programs).</p> <hr/> <p><b>i</b> After the first reload activation cycle, the values of watchdog time, target cycle time and target cycle time mode apply in accordance with the new configuration. A reload process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time).</p> <hr/>

Table 15: Settings for Target Cycle Time Mode

#### 7.4.1.2 Maximum Communication Time Slice

The maximum communication time slice is the time period in milliseconds (ms) per CPU cycle assigned to the processor module for processing the communication tasks.

If not all upcoming communication tasks can be processed within one CPU cycle, the whole communication data is transferred over multiple CPU cycles (number of communication time slices > 1). However, safety-relevant monitoring is always performed in each CPU cycle for all the protocols.

For calculating the maximum response time, the number of communication time slices must be equal to 1.

If the CPU cycle uses the communication time slice, the duration of the communication time slice must be set so that the CPU cycle cannot exceed the watchdog time specified by the process.

#### 7.4.1.3 Determining the Maximum Duration of the Communication Time Slice

For a first estimate of the maximum duration of the communication time slice, the sum of the following times must be entered in the *Max. Com. Time Slice [ms]* system parameter located in the properties of the resource.

- For each communication module (COM): 3 ms.
- For each redundant safe**ethernet** connection: 1 ms.
- For non-redundant safe**ethernet** connection: 0.5 ms.
- For each kilobyte user data of non-safety-related protocols, e.g., Modbus: 1 ms.

HIMA recommends comparing the value estimated for *Max. Com. Time Slice [ms]* with the value displayed in the Control Panel and, if necessary, correcting it in the properties of the resource. This can be done during an FAT (factory acceptance test) or SAT (site acceptance test).

##### To determine the actual duration of the maximum communication time slice

1. Operate the HIMatrix system under full load (FAT, SAT):  
All communication protocols are in operation (safe**ethernet** and standard protocols).
2. Open the **Control Panel** and select the **Com. Time Slice** structure tree folder.
3. Read the value displayed for *Maximum Com. Time Slice Duration per Cycle [ms]*.
4. Read the value displayed for *Maximum Number of Required Com. Time Slice Cycles*.

#### 7.4.1.4 Calculating the *Maximum Duration of Configuration Connections [ms]* $t_{\text{Config}}$

The *Max. Duration of Configuration Connections [ms]* system parameter corresponds to the time budget ( $t_{\text{Config}}$ ) required for the system-internal communication connections (tasks):

- PADT online connections (e.g., download/reload, OS update, online test, diagnostics).
- Remote I/O status connections (start, stop and diagnostics).
- Configuration of modules (e.g., loading of replaced modules).

If these tasks cannot be completed within one CPU cycle, the remaining tasks are processed in the next CPU cycle. This can cause unexpected delays for these tasks.

---

**i**

HIMA recommends dimensioning  $t_{\text{Config}}$  in such a way that all tasks can be processed in a single CPU cycle.

---

$t_{\text{Config}}$  for HIMatrix CPU operating systems is calculated as follows:

$$\text{HIMatrix CPU} \quad t_{\text{Config}} = (n_{\text{Com}} + n_{\text{PADT}} + n_{\text{RIO}}) * 0.25 \text{ ms} + 4 \text{ ms}$$

$t_{\text{Config}}$ :	System parameter <i>Max. Duration of Configuration Connections [ms]</i> .
$n_{\text{COM}}$ :	Number of modules with Ethernet interfaces (CPU, COM).
$n_{\text{PADT}}$ :	5, maximum number of PADT connections.
$n_{\text{RIO}}$ :	Number of configured remote I/Os.

When generating the code or converting the project, a warning message is displayed in the PADT logbook if the value defined for  $t_{\text{Config}}$  is less than the value resulting from the previous equation.

---

**i**

Setting the value for  $t_{\text{Config}}$  too low can significantly impair the performance of PADT online connections (tasks) and cause the connection to remote I/Os to be aborted.

HIMA recommends comparing the value calculated for  $t_{\text{Config}}$  with the value displayed in the Control Panel and, if necessary, correcting it in the properties of the resource. This can be done during a SAT (site acceptance test).

For test purposes,  $t_{\text{Config}}$  can also be set online in the Control Panel.

---

The value set for  $t_{\text{Config}}$  must be taken into account for dimensioning the required watchdog time. For details, refer to the section on safety-relevant time parameters.

#### 7.4.1.5 The *Minimum Configuration Version* Parameter

- The highest *Minimum Configuration Version* is always selected for new projects. Verify that this setting is in accordance with the operating system version in use.
- In a previous project converted to the current 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 configuration is still compatible with the operating systems of the modules.  
The value of *Minimum Code Generation* only needs to be increased for converted projects if additional functions of a controller should be used.
- If features requiring a higher configuration version are used in the project, SILworX automatically generates a configuration version higher than the preset *Minimum Configuration Version*. This is indicated by SILworX in the code generation logbook. The modules reject loading configurations if their version and operating system do not match.  
The safety-related SILworX version comparison can be used to determine and prove changes performed to the current project version compared to a previous one.

#### 7.4.1.6 The Fast Start-Up Parameter

The *Fast Start-Up* parameter exists for SILworX V7 and higher, and requires a resource with CPU operating system V11 or higher and a COM operating system V16 or higher. Additionally, the resource must be equipped with a CPU bootloader V11.2 or higher and a COM bootloader V16.8 or higher. The bootloader is not the same as the OS loader (emergency loader) 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 the following measures:

- Shortened self-tests.
- No detection of duplicate IP addresses.

If detection of duplicate IP addresses is deactivated and the network configuration is faulty, duplicate IP addresses might 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 reboot, the *Fast Start-Up* parameter must be set to FALSE!

### 7.4.1.7 Hardware System Variables

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

System variables	S <sup>1)</sup>	Function	Setting for safe operation
Forcing Deactivation	Y	Prevents the forcing process from starting and terminates a running forcing process. Default value: FALSE.	Application-specific
Spare 2...Spare 21	N	No function.	---
MultiForcing Denied	Y	MultiForcing can be enabled and disabled using the <i>MultiForcing Denied</i> system variable so that the associated functions can be controlled by the user program. For MultiForcing, the system variable must be set to FALSE. Default value: FALSE.	Application-specific
Emergency Stop 1... Emergency Stop 4	Y	Shuts down the controller if faults are detected by the user program. Default value: FALSE.	Application-specific
Read-only in RUN	Y	After the controller is started, the access permissions are downgraded to <i>Read-Only</i> . Exceptions are forcing and reload. Default value: FALSE.	Application-specific
Relay Contact 1... Relay Contact 4	N	Only applicable to F60! OR-linked system variables that control the relay of the FAULT contact on the F60 PS 01. The relay is a change-over contact with common contact 2, break contact 3 and make contact 1. <ul style="list-style-type: none"> <li>▪ If the F60 module is in the RUN state and the system variables <i>Relay Contact 1...Relay Contact 4</i> are FALSE, contact 1-2 is closed (contact 2-3 is open).</li> <li>▪ If the F60 module is in the RUN state and no global variables are connected to the system variables <i>Relay Contact 1...4</i>, contact 1-2 is closed (contact 2-3 is open).</li> <li>▪ If the F60 module is in the RUN state and at least one of the system variables <i>Relay Contact 1...4</i> is TRUE, contact 1-2 is open (contact 2-3 is closed).</li> <li>▪ If the F60 module is not in the RUN state, contact 1-2 is open (contact 2-3 is closed).</li> <li>▪ If the F60 module is de-energized, contact 1-2 is open (contact 2-3 is closed).</li> </ul>	Application-specific
Reload Deactivation	Y	Locks the execution of reload. Default value: FALSE.	Application-specific
User LED 1, User LED 2	N	Applicable only for special controllers! Controls the corresponding LED, if existing. Default value: 0 ms	---

<sup>1)</sup> The operating system handles the system variable in a safety-related manner, yes (Y) or no (N).

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.

### 7.4.2 Locking and Unlocking the Controller

**Locking** the controller locks all functions and prevents users from accessing them during operation. This also protects against unauthorized manipulations to the user program.

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

The system variables *Read-Only in RUN*, *Reload Deactivation*, *Forcing Deactivation* and *MultiForcing Denied* are used to lock the controller.

If all of the above system variables are TRUE, no access to the controller is possible. In this case, the controller can only enter the STOP state by restarting all processor modules. Only then can a new user program be loaded. The example describes a simple case, in which a key-operated switch is used to lock or unlock all interventions to the resource.

#### Example: To make a controller lockable

1. Define global variables of type BOOL and set initial values to FALSE.
  2. Assign the global variable as output variables to the above system variables.
  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 into the controller, and start it.
- The owner of a corresponding key-operated switch is able to lock and unlock the controller. If the corresponding digital input module fails, the controller is automatically unlocked.

This simple example can be modified using multiple global variables, digital inputs and key switches. The permissions for forcing, reload, MultiForcing and other operating functions can be distributed on different keys and persons.

## 7.5 Forcing

Forcing is the procedure of manually writing to variables with values that do not result from the process, but are defined by the user, while the controller is processing the user program.

There are different types of globally forcible data sources in a system:

- All input and status information from modules (e.g., I/O modules) and communication protocols.
- All global variables that have not been written, but have been read (VAR\_EXTERNAL).
- All global variables that have been written to by a user program (VAR\_EXTERNAL).

In addition to the globally forcible data sources in a system, there are also different types of locally (in the user program) forcible data sources:

- All user program variables that have not been written, but have been read (VAR).
- All variables from a user program that have been written (VAR).



When a variable is forced, forcing always applies to its data source! A forced variable does not depend on the process since its value is defined by the users.

---

### 7.5.1 Use of Forcing

Forcing supports users during the following tasks:

- Testing of the user program for cases that do not, or only infrequently occur during normal operation and are therefore only testable up to a certain extent.
- Simulation of sensor values, e.g., of unconnected sensors.
- Service and repair work.
- General troubleshooting.



**⚠ WARNING**

**Physical injury due to forced values is possible!**

- Only force values after consent of the person responsible for the plant and the test authority during commissioning.
- Only remove existing forcing restrictions with the consent of the person responsible for the plant and the test authority during commissioning.

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 Chapter 7.5.3 for details.

**⚠ WARNING**

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

- Forced value may lead to unexpected output values.
- Forcing prolongs the cycle time. This can cause the watchdog time to be exceeded.

Forcing can operate at two levels:

- Global forcing: Global variables are forced for all applications.
- Local forcing: Local variables are forced within a user program.

## 7.5.2 Assigning a Data Source Changed through Reload

Assigning variables to a new data source by performing a reload may have unexpected results in conjunction with the following inputs:

- Hardware.
- Communication protocols.
- System variables.

The following changes resulting from a reload lead to changed force states:

1. A global variable A is assigned to a forced data source and is thus forced itself.
2. The assignment of global variable A is removed by performing a reload. The data source maintains the property *Forced*. Global variable A is no longer forced.
3. The forced data source is assigned another global variable (global variable B).
4. During the next reload, global variable B will be forced, even if unintentionally.

### Consequence

To prevent this effect, stop forcing a variable before changing the data source. To this end, deactivate the individual force switch.

The *Inputs* tab in the Force Editor displays which channels are being forced.

### i

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

### 7.5.3 Time Limits

Different time limits can be set for global or local forcing. Once the defined time has expired, the controller stops forcing values.

The behavior of the HiMatrix system upon expiration of the time limit can be configured:

- For global forcing, the following settings can be selected:
  - *Stop Resource*.
  - *Stop Forcing Only*, i.e., the resource continues to operate.
- For local forcing, the following settings can be selected:
  - *Stop Program*.
  - *Stop Forcing Only*, i.e., the user program continues to run.

Forcing can also be used without time limit. In this case, the forcing procedure must be stopped manually.

The person responsible for forcing must clarify what effects stopping forcing have on the entire system!

### 7.5.4 Restricting the Use of Forcing

The user can limit the use of forcing; disturbed operation which may be caused by forcing, is to be avoided. The following measures can be implemented in the configuration:

- Configuration of different user profiles with or without forcing permissions.
- Explicit enabling of forcing for a resource (PES).
- Set-up of MultiForcing user accounts in the PES User Management.
- Explicit enabling of local forcing for a user program.
- Immediate stop of forcing via the *Force Deactivation* system variable using the key switch.
- Disabling of MultiForcing through the *MultiForcing Denied* system variable.

### 7.5.5 MultiForcing

Users with MultiForcing access can write force data (force values and individual force switches) for global variables in a resource if the required higher-order conditions have been met and the force permissions have been granted. To all other functions of a resource, users have Read-Only access. Starting, stopping or resetting a force process is not possible.

The use of MultiForcing is limited to a maximum of 5 users at a time. The users can be working from separate locations and also independently of each other in terms of time. The separation of the tasks performed by the individual users must be ensured by the operator through organizational measures.

#### WARNING



**Behavior that cannot be controlled by the user, is possible!**

**The operator must ensure that different Force Users do not force the same variables simultaneously and that there can be no overlaps in timing. If several Force Users write to the same variables, those force values and force switches will prevail which were written last by the firmware. Because force data are transferred in several blocks, it would otherwise be possible for the settings of different Force Users to take effect on one single controller. This behavior cannot be controlled by the user.**

**⚠ WARNING**

Existing force data is not deactivated, if *MultiForcing Denied* = TRUE!

If *MultiForcing Denied* is TRUE, users with MultiForcing access cannot modify force values or the force switches. Existing force data is not deactivated, if *MultiForcing Denied* = TRUE! Global Forcing, if allowed, is then only possible for a single user with at least Operator permissions.

Refer to the system manual (HI 800 141 E) and the SILworX online help for further details on forcing.

#### 7.5.5.1 Objectives of MultiForcing

For commissioning, normative and functional loop tests are prescribed as part of the site acceptance test, whereby a loop represents the path from the sensor to the actuator. MultiForcing makes it possible to distribute the resulting tasks to up to 5 PADTs thus processing them efficiently.

Based on loop tests, the nominal operating range is checked as well as the responses in the event of open-circuits and short-circuits. Because numerous loops must be tested frequently, the duration of site acceptance testing is a significant cost factor. MultiForcing can help to optimize these tasks.

- The behavior of actuators and linked information (e.g., end position feedback) is tested through forcing. The output signals are forced directly. This tests the wiring and the external circuit.
- In a system which is only partially functional, sensors are tested through forcing in such a way that the tests have no effect on the actuators. This approach can also be used for troubleshooting in connection with sensors.

#### 7.5.5.2 Global MultiForcing

Global MultiForcing is the simultaneous writing of force data (force values and force switches) for global variables by more than one user (Force Users).

A Force User is a person who is logged into a controller with either MultiForcing, Operator, Write or Administrator permissions. Every Force User is able to read and also at least write force data. A maximum of 5 Force Users can be logged into each controller. The number of current Force Users is displayed in the SILworX status bar.

Force values and force switches set by a Force User with MultiForcing access may only take effect if the user is logged into the controller with at least Operator permissions. Only this user can start or stop forcing.

---

**i**

To perform Global MultiForcing, Global Forcing must be allowed as well! The settings are displayed online.

---

## 7.6 Safe Version Comparison

During the code generation, SILworX creates various files. This data set is referred to as the resource configuration. The complete resource configuration is loaded to the resource whenever a download or reload is performed.

During a safe version comparison, different resource configurations are compared to one another and the differences between the individual files are detected.

Essentially, there are three types of resource configurations:

1. The created resource configuration which is the result of the last code generation.
2. The loaded resource configuration which is the configuration that was loaded into the controller by performing a reload or download.
3. An unknown resource configuration which was exported and saved. This represents any state of the resource configuration.

To verify the program changes, the safe version comparison must be started **before** the program is loaded to the controller.

The version comparison exactly determines the changed parts of the resource configuration. This facilitates testing and identifying the changes. The result has SIL 3 quality and may be submitted to the inspection authority as a piece of evidence.

Structured programming, and the use of significant names from the first resource configuration on, facilitate understanding of the comparison result.

For further details, refer to the version comparison manual (HI 801 286 E).

## 7.7 Security Measures for the Application Programming Interface (API)

SILworX API supports the following security measures:

- The use of SILworX API requires a license.
- SILworX API must be explicitly activated in the *settings.ini* file.
- Access to the SILworX API is only possible via SSL (TLS 1.2). This requires the installation of OpenSSL and a valid certificate.
- Access to projects via the SILworX API requires the same user permissions as during human interaction.
- Configurable timeouts when accessing the SILworX API ensure that projects are automatically closed if no further API queries are sent within the timeout.
- Any API activity is displayed in the SILworX status bar.
- Any actions are tracked in the SILworX logbook. This applies to both human interaction and API accesses.

---

**i**

### Important:

Users must perform a tool classification and qualification for their SILworX API application.

---

The API documentation in HTML format and a C# application example is available in the subfolder ...c3\openapi within the SILworX installation directory.

## 8 Safety-Related Aspects of User Programs

This chapter describes the safety-related aspects that are important for the user programs.

Programming goals for a user program:

- Understandable.
- Traceable.
- Testable.
- Easy to modify.

### 8.1 Safety-Related Usage

The user programs must be created with the programming tool SILworX.

SILworX can only be installed on a PC with Microsoft Windows operating system. The minimum requirements for the computer used to run SILworX are specified on the corresponding installation DVD.

The SILworX programming tool includes the following functions:

- Global Variable Editor (for creating global variables with symbolic names and data types).
- Hardware Editor (for assigning the controllers of the HIMatrix system).
- FBD Editor (for creating the user program).
- Code generator (for translating the user program into a machine code).
- Configuration of communication.
- Monitoring and documentation.

The safety requirements specified in this manual must be observed, see Chapter 3.4.

#### 8.1.1 Programming Basics

The tasks to be performed by the controller must 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 documentation depends on the control task and can be represented in two ways.

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.

#### 8.1.1.1 I/O Concept

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

Digital and analog sensors:

- 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).
- Discrepancy monitoring and response.

Actuators:

- Positioning and activation during normal operation.
- Safe response/positioning at shutdown or after power loss.

#### 8.1.2 Programming Steps

To program HIMatrix systems for safety-related applications, perform the following steps:

1. Specify the control functions.
2. Write the user programs.
3. Compile the user programs using the C code generator.
  - The user programs are free from errors and able to run.
4. Verify and validate the user programs (FAT, SAT).
5. Tests the user programs.

After these steps, the user programs are ready to start safety-related operation!

#### 8.1.3 User Program Functions

The user program functions can be freely programmed.

- Only elements complying with IEC 61131-3 together with their functional requirements are used 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.
- The user programs are 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.
- To simplify the logic, the inputs and outputs of all function blocks and variables can be inverted in any given order.
- The programmer must evaluate the fault signals from the inputs/outputs or from logic blocks.

HIMA recommends encapsulating functions to user-specific function blocks and functions based on standard functions. This ensures that user programs can be clearly structured in modules (functions, function blocks). Each module can be viewed and tested on an individual basis. By grouping modules into larger ones and combining them into a single user program, users are effectively creating a comprehensive, complex function.

## 8.1.4 User Program System Parameters

The following user parameters can be set in the *Properties* dialog box of the user programs:

System parameter	S <sup>1)</sup>	Description	Setting for safe operation
Name	N	Name of the user program. The name must be unique within the resource.	Any
Program ID	Y	ID for identifying the program when displayed in SILworX. Range of values: 0...4 294 967 295 Default value: 0 If <i>Code Generation Compatibility</i> is set to <i>SILworX V2</i> , only the value 1 is permitted.	Application-specific
Priority	Y	Priority of the user program. Range of values: 0...31 Default value: 0 (highest priority) This setting is only required if several user programs are used!	Application-specific
Program's Maximum Number of CPU Cycles	Y	Maximum number of CPU cycles that a user program cycle may take. Range of values: 1...4 294 967 295 Default value: 1 This setting is only required if several user programs are used!	Application-specific
Max. Duration for Each Cycle [μs]	N	Maximum time in each processor module cycle for executing the user program. Range of values: 0...4 294 967 295 Default value: 0 (no limitation) The safety-related response is ensured through the watchdog. This setting is only required if several user programs are used!	Application-specific
Watchdog Time [ms] (calculated)	---	Monitoring time of the user program, calculated from the product of the watchdog time of the resource and the configured maximum number of CPU cycles. Not changeable!	
Classification	N	Classification of the user program in <i>Safety-related</i> or <i>Standard</i> ; the setting is for documentation only and has no effects on the program's performance. Default value: <i>Safety-related</i> .	Application-specific
Allow Online Settings	Y	If <i>Allow Online Settings</i> is deactivated, the settings of the remaining program switches cannot be changed online (from within the Control Panel). Only applies if the <i>Allow Online Settings</i> switch for the resource is set to TRUE! Default value: TRUE.	
Autostart	Y	Enabled type of Autostart: <i>Cold Start</i> , <i>Warm Start</i> , <i>Off</i> . Default value: <i>Warm Start</i> .	Application-specific
Start Allowed	Y	TRUE: The PADT may be used to start the user program. Default value: TRUE.	Application-specific
		FALSE: The PADT may not be used to start the user program.	

System parameter	S <sup>1)</sup>	Description		Setting for safe operation
Test Mode Allowed	Y	TRUE:	The test mode is permitted for the user program.	Application-specific <sup>2)</sup>
		FALSE:	The test mode is not permitted for the user program. Default value: FALSE.	
Reload Allowed	Y	TRUE:	The user program reload is permitted. Default value: TRUE.	Application-specific
		FALSE:	The user program reload is not permitted.	
		Observe the settings in the resource properties!		
Local Forcing Allowed	Y	TRUE:	Forcing is permitted at program level.	FALSE is recommended
		FALSE:	Forcing is not permitted at program level. Default value: FALSE.	
Local Force Timeout Reaction	Y	Behavior of the user program after the forcing time has expired: <ul style="list-style-type: none"><li>▪ Stop Forcing Only.</li><li>▪ Stop Program.</li></ul> Default value: <i>Stop Forcing Only</i> .		
Code Generation Compatibility	-	Code generation is compatible with previous versions of SILworX.		Application-specific
		SILworX V2	Code generation is compatible with SILworX V2.	
		SILworX V3	Code generation is compatible with SILworX V3.	
		SILworX V4 – V6b	Code generation is compatible with SILworX V4 up to SILworX V6b.	
		SILworX V7 and higher	Code generation is compatible with SILworX V7.	
		Default value for all new projects: <i>SILworX V7 and higher</i> .		

<sup>1)</sup> The operating system handles the system parameter in a safety-related manner, yes (Y) or no (N)  
<sup>2)</sup> Once the test mode has stopped, a cold start must be performed prior to starting a safety-related operation!

Table 17: System Parameters of the User Program

### 8.1.5 Notes on the Code Generation Compatibility Parameter

Observe the following points in conjunction with the *Code Generation Compatibility* parameter:

- In a new project, SILworX selects the current setting for the *Code Generation Compatibility* parameter. This ensures that the current, enhanced features are activated and the current module and operating system versions are supported. Verify that this setting is in accordance with the hardware in use.
- In a previous project converted to the current SILworX version, the value for *Code Generation Compatibility* 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 configuration is still compatible with the operating systems of the modules.  
The value of *Code Generation Compatibility* must only be changed for converted projects if additional functions of a controller should be used.
- If a *Minimum Configuration Version* of *SILworX V4* and higher is set in the resource properties, the *Code Generation Compatibility* parameter must be set to *SILworX V7 and Higher* in every user program.



### 8.1.6 Code Generation

After completing the user programs and the resource configuration, the code generator creates a code with a typical configuration CRC.

The configuration CRC is a signature for all of the configured elements and is issued as a 32-bit, hexadecimal code.

**For safety-related operation, the user program must be compiled twice. The two checksums generated during compilation must be identical!**

By compiling the user program twice and comparing the checksums of the generated code, the user can detect potential corruptions of the user programs resulting from random faults in the hardware or operating system of the PC in use.

The result of the CRC comparison is displayed in the logbook.

### 8.1.7 Loading and Starting the User Program

A resource configuration can only be loaded into a controller through download if the controller is in the STOP state.

The user program can be started after successful resource configuration download.

---

**i**

The PADT is only able to operate the controller, e.g., by performing a reload and forcing, if the project matching the resource configuration is opened in SILworX.

HIMA recommends archiving the project after each download or reload.

SILworX stores all a project's data to a single file. For reasons of data security, HIMA recommends additionally storing the project on an external medium.

The backup ensures that the project data matching the resource configuration remains available even if the PADT fails.

---

### 8.1.8 Reload

If changes were performed to a project, they can be transferred to the controller by performing a reload. After being tested by the operating system, the modified project is activated and assumes the control task.

The reload can only be performed if the *Reload Allowed* system parameter is set to TRUE and the *Reload Deactivation* system variable is set to FALSE.

---

**i**

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

---

---

**i**

**Observe the following points when reloading sequence chains:**

The reload information for sequence chains does not take the current sequence status into account. A reload can therefore cause the sequence to change setting it to an undefined state. The user is responsible for properly performing the reload.

Examples:

- Deletion of the active step causes all the steps within the step sequence to lose the *active* state!
  - Renaming an initial step while another step is active leads to a step sequence with two active steps!
-

**i****Observe the following points when reloading actions:**

During the reload, actions are loaded with their complete 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 output 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.
- Removing a PO action qualifier set to TRUE actuates the trigger function.

Prior to performing a reload, the operating system checks if the required additional tasks would increase the cycle time of the current user programs to such an extent that the defined watchdog time is exceeded. In this case, the reload process is aborted with an error message and the controller continues operation with the previous resource configuration.

**i****The controller can abort a reload.**

Reload can be performed successfully by planning a sufficient reserve for the reload when determining the watchdog time or temporarily increasing the controller watchdog time by a reserve.

Any temporary increases in the watchdog time must be agreed upon with the competent test authority.

Exceeding the target cycle time can also lead to an abort of the reload.

**i**

The user is responsible for ensuring that the watchdog time includes a sufficient reserve time. This should allow the user to manage the following situations:

- Variations in the user program's cycle time.
- Sudden, strong cycle loads, e.g., due to communication.
- Expiration of time limits during communication.

### 8.1.9 Online Test

Online test fields (OLT fields) can be used in the user program logic to display variables while the controller is operating.

For further details on how to use OLT fields, use OLT field as keyword in the SILworX online help and refer to the SILworX first steps manual (HI 801 103 E).

### 8.1.10 Test Mode

SILworX offers a test mode for punctual troubleshooting. In test mode, the user program can be run in single steps, i.e., cycle by cycle. Each cycle is triggered by a command from the PADT. In the period between 2 cycles, the global variables written to by the user program remain **frozen**. The assigned physical outputs and communication data then no longer respond to changes in the process!

The test mode can be configured individually for each user program by activating or deactivating the *Test Mode Allowed* parameter.

<i>Test Mode Allowed</i>	Description
Deactivated	Test mode deactivated (default setting).
Activated	Test mode activated.

Table 18: User Program Parameter *Test Mode Allowed*

**NOTICE**

**Failure of safety-related operation possible!**

**If a user program operating in test mode is stopped, it cannot provide a safety-related response to changes on the inputs and cannot control the outputs!**

**Test mode is therefore not permitted in safety-related operation!**

**For safety-related operation, the *Test Mode Allowed* parameter must be deactivated!**

### 8.1.11 Changing the System Parameters during Operation

The system parameters specified in Table 19 may be changed during operation (online).

A typical application case is the temporary increase of the watchdog time 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 implemented 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 controller!

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 controller.

Parameter	Can be changed in the following controller 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	TRUE -> FALSE: All FALSE -> TRUE: STOP
Autostart	All
Start Allowed	All
Load Allowed	All
Reload Allowed	All
Global Forcing Allowed	All
Global Force Timeout Reaction	All
Global MultiForcing Allowed	All

Table 19: Online Changeable Parameters

### 8.1.12 Project Documentation for Safety-Related Applications

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

- Interface declaration.
- Signal list.
- Logic.
- Description of data types.
- Configurations for system, modules and system parameters.
- Network configuration.
- List of signal cross-references.

This documentation is required for the factory acceptance test (FAT) of a system subject to approval by a test authority, e.g., TÜV.

### 8.1.13 Multitasking

Multitasking refers to the capability of the HIMatrix system 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 module cycles. This can be controlled with the resource and user program parameters. SILworX uses these parameters to calculate the user program watchdog time:

$$\text{Watchdog Time}_{\text{User program}} = \text{Watchdog Time}_{\text{Processor module}} * \text{Maximum Number of Cycles}$$

The individual user programs operate in an interference-free manner and independently from 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 no limit is configured with *Max. Duration for Each Cycle*.
- The distribution of user program cycles over processor module cycles strongly affects the user program response time and the response time of the variables written to by the user program!
- A user program evaluates global variables written to by another user program at the earliest one CPU module cycle later. Depending on the value set for *Program's Maximum Number of CPU Cycles* in the program properties, the evaluation process may be prolonged by many CPU cycles, which also causes a delayed response.

Refer to the system manual (HI 800 141 E) for further details on multitasking.

### 8.1.14 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 system that have already been approved.

## 8.2 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 can be used as a planning document and also serves as proof of careful planning.

The current checklists can be obtained upon request by sending an e-mail to: [documentation@hima.com](mailto:documentation@hima.com). Registered customers can download the product documentation from the HIMA Extranet.

## 9 Configuring Communication

In addition to using the physical input and output variables, variable values can also be exchanged with other systems through a data connection. In this case, the variables are declared with SILworX, in the Protocols area of the corresponding resource.

### 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 non-safe import data!**

**Do not use data imported from non-safe sources for the user program's safety functions.**

The standard protocols listed in the communication manual are available for HIMatrix.

### 9.2 Safety-Related safeethernet Protocol

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

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

For further details on **safeethernet**, refer to the communication manual (HI 801 101 E).

**i**

**The safe state may be entered inadvertently!**

***Receive Timeout* and *Production Rate* are safety-related parameters!**

*Receive Timeout* is the monitoring time within which a valid response from another controller must be received.

If a correct response is not received from the communication partner within *Receive Timeout*, HIMatrix terminates the safety-related communication. The input variables of this **safeethernet** connection respond in accordance with the preset parameter *Freeze Data on Lost Connection [ms]*. For safety-related functions, which are implemented via **safeethernet**, the setting **Use Initial Value** must be used.

In the following equations for determining the worst case response time, the target cycle time can be used instead of the watchdog time, if it is guaranteed that the process module maintains the target cycle time, in case of reload as well.

In this case, the following requirements apply to the *Fixed-tolerant* or *Dynamic-tolerant* settings of *Target Cycle Time Mode*:

1. **Watchdog time**  $\geq$  **1.5 x target cycle time**
2. **Receive timeout**  $\geq$  **5 x target cycle time + 4 x latency**

Latency refers to the delay on the transport path.

3. For reload, there is either just one user program or several user programs, the cycle of which is limited to a single processor module cycle.

## 9.2.1 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 transport path must be set and a suitable safe**ethernet** profile must be selected.

The preset *Response Time* affects the configuration of all the safe**ethernet** connection parameters and is calculated as follows:

$$\text{Response Time} \leq \text{Receive Timeout} / n$$

$$n = 2, 3, 4, 5, 6, 7, 8 \dots$$

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 transport path.

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

$$\text{Min. Response Time} \leq \text{Receive Timeout} / 2 \geq 2 * \text{Delay} + 2.5 * \text{Max. Cycle Time}$$

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 noise-free network. However, this is not a safety problem for the processor module!

i

Make sure that the communication system complies with the configured response time!

If this condition 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.

**NOTICE**

In the following examples, the formulas for calculating the worst case response time only apply for a connection with HIMatrix controllers if the safety time in these HIMatrix controllers is set as follows:

$$\text{safety time} = 2 \times \text{watchdog time}$$

### 9.3 Worst Case Response Time for safeethernet

In the following examples, the formulas for calculating the worst case response time only apply for a connection with HiMatrix controllers if their programming does not include noise blanking. These formulas always apply to HiMax and HiQuad X controllers.

**i**

The allowed worst case response time depends on the process and must be agreed upon together with the competent test authority.

The following table describes the parameters and conditions that must be taken into account in SILworX to calculate the worst case response time:

Terms	Description
Receive Timeout	Monitoring time of controller 1 (PES 1) within which a valid response from controller 2 (PES 2) must be received. Otherwise, safety-related communication is terminated after the time has expired.
Production Rate	Minimum interval between two data transmissions.
Watchdog Time	Maximum duration permitted for a controller's RUN cycle. The duration of the RUN cycle depends on the complexity of the user program and the number of safeethernet connections. The watchdog time (WDT) must be entered in the resource properties.
Worst Case Response Time	The worst case response time is the time between a change in a physical input signal (in) of PES 1 and a change in the physical output signal (out) of PES 2.
Response Time of the HiMatrix controller	For further details on the response time of the HiMatrix controller (resource) $t_{RR}$ , see Chapter <i>Safety-Relevant Time Parameters</i> .
Delay	Delay of a transport path, e.g., when a modem or satellite connection is used. For direct connections, an initial delay of 2 ms can be assumed. The responsible network administrator can measure the actual delay on a transport path.

Table 20: safeethernet Parameter Description and Conditions

The following conditions apply to the calculations of the maximum response times specified below:

- The signals transmitted over safeethernet must be processed in the corresponding controllers within one CPU cycle.
- The response times of the sensors and the actuators must also be added up.

The calculations also apply to signals in the opposite direction.

### 9.3.1 Calculating the Worst Case Response Time

The worst case response time  $T_R$  is the time between a change on the input signal of controller 1 and a response on the corresponding output of controller 2. It is calculated as follows:

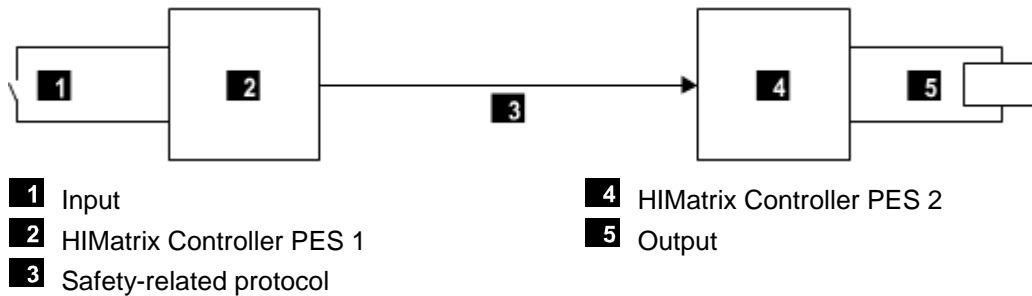


Figure 3: Response Time when 2 HiMatrix Controllers are Interconnected

$$T_R = t_1 + t_2 + t_3$$

$T_R$  Worst case response time

$t_1$  2 \* Watchdog time of HiMatrix controller 1

$t_2$  Receive Timeout

$t_3$  2 \* Watchdog time of HiMatrix controller 2

The allowed worst case response time depends on the process and must be agreed upon together with the competent test authority.

### 9.3.2 Calculating the Worst Case Response Time with 2 Remote I/Os

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

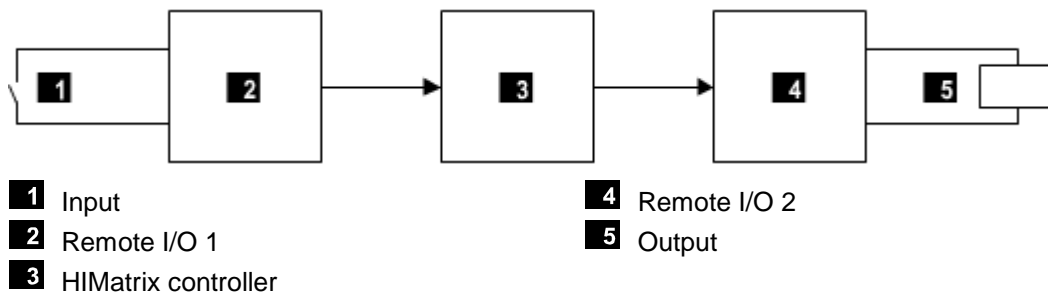


Figure 4: Response Time with Remote I/Os

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

$T_R$  Worst case response time

$t_1$  2 \* Watchdog Time of Remote I/O 1

$t_2$  Receive Timeout<sub>1</sub>

$t_3$  2 \* Watchdog time of the HiMatrix controller

$t_4$  Receive Timeout<sub>2</sub>

$t_5$  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 one or two HiMatrix controllers are used instead of one or two remote I/Os.



### 9.3.3 Connections to HIMax Controllers

Refer to the HIMax safety manual (HI 801 003 E) and the communication manual (HI 801 101 E) for a description of the connections between HIMatrix and HIMax controllers.

## 9.4 Safety-Related HIPRO-S V2 Protocol

The HIPRO-S V2 protocol is used for safety-related SIL 3 communication between HIQuad controllers and HIQuad X, HIMax or HIMatrix controllers.

For further information, refer to the HIPRO-S V2 manual (HI 800 723 E).

- For HIMax controllers, operating system as of V8.
- For HIQuad X controllers.
- For HIQuad controllers with an operating system release as of BS41q/51q V7.0-8 (08.xx).
- For HIMatrix 03 controllers with an operating system release as of V12 (CPU) / V16.10 (COM).

The HIPRO-S V2 protocol may only be used for connecting HIQuad controllers to one another or to HIMax controllers. Connections between HIMax controllers with one another and with HIMatrix controllers must be established with **safeethernet**.

For further information, refer to the HIPRO-S V2 manual (HI 800 723 E).

## 9.5 Safety-Related PROFIsafe Protocol

For further details on PROFIsafe, refer to the communication manual (HI 801 101 E).

## 9.6 Safety-Related ISOFAST Protocol

For further details on ISOFAST, refer to the ISOFAST manual (HI 801 465 E)

## 10 Use in Fire Alarm Systems

The HIMatrix systems may be used in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72, if line monitoring is configured for the inputs and outputs.

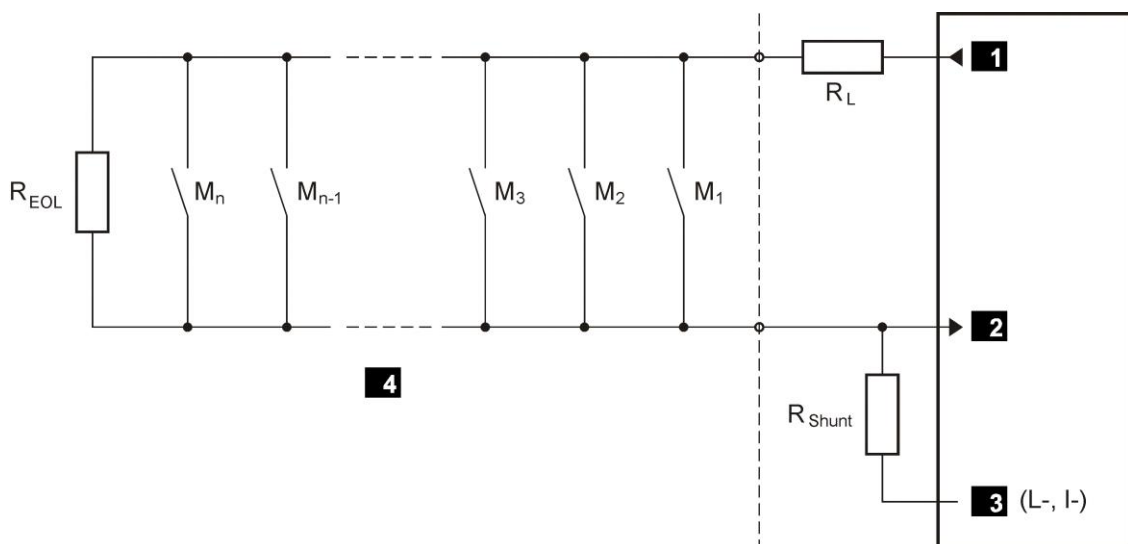
In this case, the user program must fulfill the requirements specified for fire alarm systems in accordance with the standards previously mentioned.

DIN EN 54-2 requires 10 s as the maximum cycle time allowed for fire alarm systems. This value can be easily met with the HIMA systems since the cycle time for these systems is in the milliseconds range. This also applies to the safety time of 1 s (fault response time) required in certain cases.

According to DIN EN 54-2, the fire alarm system must enter the fault report state within 100 s after the HIMatrix system has received the fault message.

The connection to fire detectors is implemented based on the energized to trip principle with line monitoring (short-circuit and open-circuit monitoring). To this end, the following devices may be used:

- The digital and analog inputs of the F35 03 controller.
- The analog inputs of the F3 AIO 8/4 01 remote I/O.
- The digital inputs and outputs of the F3 DIO 16/8 01 and F3 DIO 8/8 01 remote I/Os.
- The AI 8 01 and MI 24 01 input modules of the F60 controller.



<b>1</b> Sensor supply	$M$ Fire detectors
<b>2</b> Analog input	$R_{EOL}$ Terminating resistor on the last loop sensor
<b>3</b> Reference potential	$R_L$ Limitation of the maximum permissible loop current
<b>4</b> Detection loop	$R_{Shunt}$ Shunt

Figure 5: Wiring of Fire Detectors

For the application, the  $R_{EOL}$ ,  $R_L$  and  $R_{Shunt}$  resistors must be calculated as dictated by the sensors in use and the number of sensors per detection loop. Refer to the data sheet from the sensor manufacturer for the necessary data.

The alarm outputs for activating lamps, sirens, horns etc. are operated in accordance with the energize to trip principle. These outputs must be monitored for short-circuits and open-circuits. This can be done by returning the output signals directly from the actuator to the inputs.

The current in the actuator circuit can be monitored via an analog input using an appropriate shunt. Z-diodes and series resistor connected in series protect the input against overvoltage if a short-circuit occurs.

For an explicit detection of open-circuits (with de-energized DO outputs), a transmitter supply is required in addition to the analog inputs (see draft below):

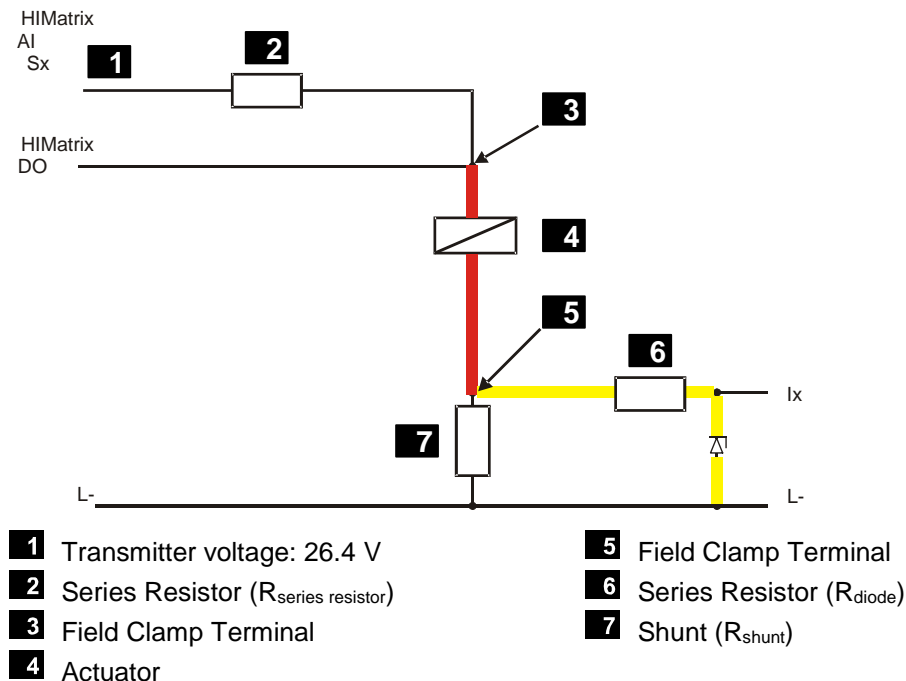


Figure 6: Example for Line Monitoring (Short-Circuits and Open-Circuits) of Digital Outputs

■ Line monitoring range (short-circuits and open-circuits)

■ Protective circuit with short-circuit

For an example of how to configure the open-circuit and short-circuit monitoring of actors using analog inputs, refer to the HI Matrix F35 03 manual (HI 800 477 E).

A user program can be adjusted to tailor the activation of the visual display systems, indicator light panels, LED indicators, alphanumeric displays, audible alarms, etc.

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

Fire alarms can be transmitted from one HI Matrix system to a different system using the existing Ethernet communication standard (OPC). Any communication loss must be reported.

HI Matrix systems that are used as fire alarm systems must have a redundant power supply. Additionally, precautionary measures must be implemented against power supply drops, e.g., the use of a battery-powered horn. Continuous operation must be ensured while switching from the main power supply to the backup power supply. Voltage drops for up to a duration of 10 ms are permitted.

If a system failure occurs, the operating system writes to the system variables defined in the user program. This allows the user to program fault signaling for faults detected by the system. If a fault occurs, the HI Matrix system switches off the safety-related inputs and outputs with the following effects:

- The low level is processed in all channels of the faulty inputs.
- All channels of the faulty outputs are switched off.

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

## 11 ATEX-Conform Use as Safety, Controlling and Regulating Device

The HIMatrix F35 03 controller and the F3 AIO 8/4 01 remote I/O are suitable for the intended use, i.e., for detecting and measuring flammable gases.

The specified HIMatrix devices were tested in accordance with the following standards:

- EN 50271:2010
- EN 50495:2010
- IEC / EN 60079-0:2012 + A11:2013
- IEC / EN 60079-29-1:2008

The specified controllers meet the requirements of ATEX Directive 2014/34/EU and are safety devices, controlling devices and regulating devices in accordance with it.

The specified devices are suitable for monitoring ignition hazards in potentially explosive atmospheres as associated equipment or, as stationary gas detection systems, for detecting and measuring flammable gases.

The hardware and software of the devices was tested for compliance with the requirements of EN 60079-29-1 and EN 50271.

Gas sensors meeting the requirements of EN 60079-29-1 must be connected to the 4...20 mA signal inputs. The gas sensors must be wired in compliance with the documentation and the EU type examination certificate.

The safety-relevant user program must be created using the SILworX programming tool and taking the safety manual into account.

The safety-related function must be proved by verification and validation.

Specific safety information and operating instructions in accordance with ATEX Directive 2014/34/EU, Annex II (1.0.6) have to be created for the safety facility or gas warning system to be assembled. In an additional conformity assessment procedure, a complete EU type examination certificate has to be issued for the safety facility or gas warning system under consideration of the above-mentioned points.

## 12 Use of HiMatrix Devices in Ex Zone 2

HiMatrix devices (the modular F60 controller, compact controllers and remote I/Os) are suitable for mounting in the explosive atmospheres of zone 2. In addition to the specific conditions, the mounting and installation instructions provided in the system manual and in the device-specific manuals must be observed.

The declaration of conformity for the HiMatrix devices is available on the HIMA website, at [www.hima.com](http://www.hima.com).

HiMatrix devices meet the requirements of the following directives and standards:

Directive	Standard	Description
IECEX	IEC 60079-0:2011	Explosive atmospheres - Part 0: Equipment - General requirements
ATEX 2014/34/EU	EN 60079-0:2012 + A11:2013	
IECEX	IEC 60079-15:2010	Explosive atmospheres - Part 15: Equipment protection by degree of protection "n"
ATEX 2014/34/EU	EN 60079-15:2010	

Table 21: Standards for HiMatrix Devices in Zone 2

The HiMatrix devices are provided with one of the following Ex marking:



II 3G Ex nA IIC T4 Gc



II 3G Ex nA nC IIC T4 Gc

Marking	Description
	Explosion protection marking complying with the relevant directive.
II	Equipment group, for all areas with explosive atmosphere, other than underground mines.
3G	Equipment category, for use in areas where explosive gas atmosphere is unlikely to occur or, if it does occur, will persist for a short period only.
Ex	Explosion protection marking complying with the relevant standard.
nA	Type of protection for non-sparking equipment.
nC	Type of protection for sparking, sealed equipment.
IIC	Gas group for explosive gas atmospheres, typical gas is hydrogen.
T4	Temperature class T4, with a maximum surface temperature of 135 °C.
Gc	Equipment protection level, corresponds to ATEX equipment category 3G.

Table 22: Ex Marking Description for HiMatrix Devices

### Special Conditions

1. The HIMatrix device must be installed in an enclosure that fulfils the requirements of the IEC 60079-15/EN 60079-15 with degree of protection IP54 or better.
2. The enclosure must be provided with the following label:

**"Work is only permitted in the de-energized state"**

Exception:

If a potentially explosive atmosphere has been precluded, work can also be performed when the device is under voltage.

3. The HIMatrix devices are designed for operation not exceeding pollution degree 2.
4. The enclosure in use must be able to safely dissipate the generated heat. Refer to the corresponding device-specific manuals for further details on power dissipation in HIMatrix systems.
5. The 24 VDC power must come from a power supply unit with protective separation. Use power supply units of type PELV or SELV only.
6. HIMatrix devices must be protected with fuses as described in the device-specific manuals.
7. The conditions specified in the device-specific manuals must be observed as well.

Applicable standards:

IEC 60079-14: 2013	Explosive atmospheres - Part 14: Electrical installations design, selection and erection
EN 60079-14: 2014	

The requirements for type of protection "n" must be observed.

## 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 standard
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
HW	Hardware
ICMP	Internet control message protocol, network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Inputs are designed for interference-free operation and can be used in circuits with safety functions
MAC	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 ground
PELV	Protective extra low voltage
PES	Programmable electronic system
R	Read, the variable is read out
R/W	Read/Write (column title for system variable type)
$I_P$	Peak value of a total AC component
SC/OC	Short-circuit/open-circuit
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
SNTP	Simple network time protocol (RFC 1769)
SRS	System.Rack.Slot, addressing of a module
SSL	Secure sockets layer, see TLS
SW	Software
TLS	Transport layer security, hybrid cryptographic protocol
TMO	Timeout
W	Write, the variable receives a value, e.g., from the user program
WD	Watchdog, device for monitoring the system's correct operation Signal for fault-free process
WDT	Watchdog time

**Index of Figures**

<b>Figure 1:</b>	<b>Line Control</b>	<b>36</b>
<b>Figure 2:</b>	<b>Pulsed Signals T1, T2</b>	<b>36</b>
<b>Figure 3:</b>	<b>Response Time when 2 HIMatrix Controllers are Interconnected</b>	<b>72</b>
<b>Figure 4:</b>	<b>Response Time with Remote I/Os</b>	<b>72</b>
<b>Figure 5:</b>	<b>Wiring of Fire Detectors</b>	<b>74</b>
<b>Figure 6:</b>	<b>Example for Line Monitoring (Short-Circuits and Open-Circuits) of Digital Outputs</b>	<b>75</b>



**Index of Tables**

<b>Table 1:</b>	<b>Overview of the System Documentation</b>	<b>13</b>
<b>Table 2:</b>	<b>Environmental Requirements</b>	<b>24</b>
<b>Table 3:</b>	<b>International Standards and Safety Levels</b>	<b>28</b>
<b>Table 4:</b>	<b>Standards for EMC, Climatic and Environmental Requirements</b>	<b>29</b>
<b>Table 5:</b>	<b>Noise Emission Tests</b>	<b>29</b>
<b>Table 6:</b>	<b>Climatic Tests</b>	<b>30</b>
<b>Table 7:</b>	<b>Mechanical Tests</b>	<b>30</b>
<b>Table 8:</b>	<b>Verification of the DC Supply Characteristics</b>	<b>31</b>
<b>Table 9:</b>	<b>Overview of the HIMatrix System Inputs</b>	<b>34</b>
<b>Table 10:</b>	<b>Analog Inputs of the F35 03 Controller</b>	<b>37</b>
<b>Table 11:</b>	<b>Analog Inputs of the F3 AIO 8/4 01 Remote I/O</b>	<b>37</b>
<b>Table 12:</b>	<b>Analog Inputs of the F60 Controller</b>	<b>37</b>
<b>Table 13:</b>	<b>Overview of the HIMatrix System Outputs</b>	<b>40</b>
<b>Table 14:</b>	<b>Resource System Parameters</b>	<b>50</b>
<b>Table 15:</b>	<b>Settings for Target Cycle Time Mode</b>	<b>51</b>
<b>Table 16:</b>	<b>Hardware System Variables</b>	<b>55</b>
<b>Table 17:</b>	<b>System Parameters of the User Program</b>	<b>64</b>
<b>Table 18:</b>	<b>User Program Parameter <i>Test Mode Allowed</i></b>	<b>66</b>
<b>Table 19:</b>	<b>Online Changeable Parameters</b>	<b>67</b>
<b>Table 20:</b>	<b>safeethernet Parameter Description and Conditions</b>	<b>71</b>
<b>Table 21:</b>	<b>Standards for HIMatrix Devices in Zone 2</b>	<b>77</b>
<b>Table 22:</b>	<b>Ex Marking Description for HIMatrix Devices</b>	<b>77</b>

**Index**

Automation security .....	25	PADT .....	15
Communication time slice .....	52	Process safety time.....	17
CRC.....	65	Proof test .....	21
De-energize to trip principle .....	11	Response time.....	20
Energize to trip principle.....	11	Safety concept .....	46
ESD protection.....	12	Safety Time.....	17
Fast start-up.....	54	Special Conditions .....	78
Fault response		Supply voltage .....	31
Inputs .....	35	Surge.....	35
Outputs .....	41	Test requirements .....	29
Fire alarm systems.....	74	Climatic .....	30
Fire detectors.....	74	EMC .....	30
Functional test of the controller .....	46	Mechanical .....	30
Hardware Editor .....	55	To make a controller lockable .....	56
Line monitoring .....	74	Watchdog time	
Maintenance .....	23	estimation.....	19
Multitasking.....	68	resource .....	18
Online test field .....	66		



MANUAL  
**HIMatrix Safety Manual**

---

HI 800 023 E


For further information, please contact:

**HIMA Paul Hildebrandt GmbH**

Albert-Bassermann-Str. 28  
68782 Brühl, Germany

Phone +49 6202 709-0  
Fax +49 6202 709-107  
E-mail [info@hima.com](mailto:info@hima.com)

Learn more about HIMatrix online:

 [www.hima.com/en/products-services/himatrix/](http://www.hima.com/en/products-services/himatrix/)



[www.hima.com](http://www.hima.com)