HIMA SMART SAFETY.

Manual

HIQuad® X

Safety Manual

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.

Contact

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 803 208 D, Rev. 1.00 (1825)	German original document
HI 803 209 E, Rev. 1.00.00 (1828)	English translation of the German original document

Table of Contents

1 Introduction

This manual contains information on how to operate the safety-related programmable electronic system HIQuad X 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 HIQuad X 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:

- HIQuad X operating systems in accordance with the version list.
- SILworX as of version 10.58.

1.2 Target Audience

This document is aimed at the planners, design engineers and programmers of automation systems as well as the persons authorized to start up, operate and maintain the devices and systems concerned. Specialized knowledge of safety-related automation systems is required.

1.3 Writing Conventions

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

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

Safety notices and operating tips are particularly marked.

1.3.1 Safety Notices

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

⚠ 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 the 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 cyber 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, cyber security and HIMA products can be found on HIMA's website.

Safety Lifecycle Services:	
Onsite+ / On site engineering	In close cooperation with the customer, HIMA performs changes or extensions on site.
Startup+ / Preventive maintenance	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.
Lifecycle+ / Lifecycle management	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.
Hotline+ / 24 h hotline	HIMA's safety engineers are available by telephone around the clock to help solve problems.
Standby+ / 24 h call-out service	Faults that cannot be resolved over the phone are processed by HIMA's specialists within the time frame specified in the contract.
Logistics+/ 24 h spare parts service	HIMA maintains an inventory of necessary spare parts and guarantees quick, long-term availability.

Contact details:	
Safety lifecycle services	https://www.hima.com/en/about-hima/contacts-worldwide/
Technical support	https://www.hima.com/en/products-services/support/
Seminar program	https://www.hima.com/en/products-services/seminars/

2 Use of the HIQuad X 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 HIQuad X.

The automation system is designed for controlling and regulating industrial process plants. SILworX, HIMA's programming tool, is used for programming, configuring, monitoring, operating and documenting the HIQuad X system.

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

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

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

2.1.2 Application in Accordance with the Energize to Trip Principle

The HIQuad X 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 HIQuad X systems with analog inputs are tested and certified for use in fire alarm systems in accordance with DIN EN 54-2 and NFPA 72.

The conditions of use provided in this manual must be observed, see Chapter 12.

2.1.4 Explosion Protection

The HIQuad X automation system is suitable for mounting in zone 2.

The conditions of use provided in Chapter 13 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 HIQuad X systems are safely operated in automated systems and plants.

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

2.3 ESD Protective Measures

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

NOTICE

Damage to the HIQuad X 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 the HIQuad X systems are also available:

Name	Content	Document no.
HIQuad X system manual	Hardware description of the modular system	HI 803 211 E
Certificates	Test results	
Revision list	Operating system versions certified by the TÜV	
Component-specific manuals	Description of the individual components	
Communication manual	Description of the communication protocols, ComUserTask and their configuration in SILworX.	HI 801 101 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	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. The documentation is available for registered HIMA customers in the download area https://www.hima.com/en/downloads/.

3 Safety Concept

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

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

3.1 Safety and Availability

Thanks to the 1oo2D microprocessor structure of the processor modules, the HIQuad X system is already approved for use as an automation safety-system up to safety integrity level 3 (SIL 3) in accordance with IEC 61508 as a mono system.

No imminent risk results from the HIQuad X systems.

⚠ **WARNING**

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

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

Depending on the required availability, the HIQuad X system can be equipped with redundant processor modules (F-CPU 01), redundant communication modules (F-COM 01) and redundant I/O modules.

Redundant modules increase availability. If a module fault occurs, the faulty module automatically enters the safe state and the redundant module maintains operation with no interruption.

HIMA recommends replacing failed modules as soon as possible.

If specific faults are present for longer than 24 h, additional system components are shut down for safety reasons.

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 HIQuad X system have been calculated in accordance with IEC 61508.

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

PFD = $10^{-4}...10^{-3}$

PFH = $10^{-8}...10^{-7}$ per hour.

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

3.1.2 Self-Test and Fault Diagnosis

Comprehensive self-tests are performed in the HIQuad X system at start-up and during operation.

The scope of the testing includes:

- Processors.
- Memory areas (RAM, NVRAM).
- The watchdog.
- Connections between modules.
- Individual I/O channels of the I/O modules.
- The power supply.

If the HIQuad X system detects module faults during the self-test, the affected module will enter the safe state. If a module fault is already detected during start-up, the module will not start operation at all. If a channel fault occurs and the I/O module supports channel switch-off, only the failed channel is switched off. If a channel fault is detected during initialization, the channel or module will not be activated or start up.

If a fault occurs in mono systems, either the sub-functions or the entire system is shut down. If the application has a redundant configuration instead of a mono structure, the function is performed by the redundant modules or redundant channels.

Processor modules, I/O processing modules, communication modules and power supply modules are equipped with LEDs indicating detected faults. This allows the user to quickly diagnose module faults or faults detected in the external wiring.

Additionally, the SILworX programming tool provides system variables that allow the user program to evaluate the module states.

HIQuad X carries out an extensive diagnosis of the system behavior. The diagnostic messages and detected faults are stored to the diagnostic memory of the processor module and I/O processing module. Modules with a safety-related processor system perform their own diagnosis. The diagnostic messages can also be read out after a system fault using the programming tool.

For further details on the system and module diagnosis, refer to the system manual (HI 803 211 E).

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 Redundancy

To improve availability, all parts of the system including active components can be set up redundantly and, if necessary, replaced while the system is operating.

The component redundancy does not impair the system safety. Safety integrity level 3 (SIL 3) is guaranteed.

Redundancy affects the PFD and PFH values of the HIQuad X system, see Chapter 3.1.1.

3.1.5 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.

3.1.5.1 Detection of Failed System Components

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

3.1.5.2 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 user must plan the following actions:

- Include and configure a redundant module for every I/O module.
- Every I/O module must be provided with short-circuit and open-circuit monitoring. The short-circuit and open-circuit monitoring must be configured for each channel.
- The operation of the actuators can be monitored through a position feedback.

3.1.5.3 Redundancy of Components

It may be necessary to redundantly structure the following components:

- Power supply of the controller.
- HIQuad X modules.
- Sensors and actuators.

If redundancy is lost, the controller must be repaired as soon as possible.

For details on component redundancy, refer to the system manual (HI 803 211 E).

It is not required to design the safety system modules redundantly if, in the event of a safety system failure, the required safety level can otherwise be achieved, e.g., by implementing organizational measures.

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).

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 a property of the process and describes the time interval during which the process allows faulty signals to exist without a hazardous operating state occurring.

A safety-related response of the controller including all delays due to sensors, actuators, input and output modules must occur within the process safety time.

3.2.2 The Safety Time [ms] Parameter (of the Resource)

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

$$\mathbf{t}_{RR} \leq \mathbf{t}_{SR} + \mathbf{t}_{DO\ max.}$$

$\mathbf{t}_{SR}$ The *Safety Time [ms]* parameter

$\mathbf{t}_{DO\ max.}$ Maximum shutdown time of the output modules and the F 3430 relay module itself, see

Module	$\mathbf{t}_{DO\ max.}$
F 3330	13 ms, in accordance with IEC 61131-2 Type 2
F 3331	18 ms, in accordance with IEC 61131-2 Type 2
F 3333	22 ms, in accordance with IEC 61131-2 Type 2
F 3334	21 ms, in accordance with IEC 61131-2 Type 2
F 3335	89 ms, in accordance with IEC 61131-2 Type 2
F 3349	7 ms, in accordance with IEC 61131-2 Type 2
F 3430	11 ms
F 6705	68 ms, 54 ms, current drop from 20 mA to 0/4 mA at a load of 550 Ohm

Table 2.

Module	$\mathbf{t}_{DO\ max.}$
F 3330	13 ms, in accordance with IEC 61131-2 Type 2
F 3331	18 ms, in accordance with IEC 61131-2 Type 2
F 3333	22 ms, in accordance with IEC 61131-2 Type 2
F 3334	21 ms, in accordance with IEC 61131-2 Type 2
F 3335	89 ms, in accordance with IEC 61131-2 Type 2
F 3349	7 ms, in accordance with IEC 61131-2 Type 2
F 3430	11 ms
F 6705	68 ms, 54 ms, current drop from 20 mA to 0/4 mA at a load of 550 Ohm

Table 2: Shutdown Times of the Output Modules

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.
- Configured delays in the user program, e.g., the timer function blocks TON and TOF.
- Delays due to µP modules.

If one of the µP modules F 5220, F 6217, F 6220 or F 6221 with its own processor system is used, the delay of this modules must be taken into account:

$$\mathbf{t}_{RR} \le \mathbf{t}_{SR} + \mathbf{t}_{DO\ max.} + \mathbf{t}_{D\ \mu P}$$

If several µP modules are used, then the module with the largest delay is the one to be considered, see

µP module	$\mathbf{t}_{D\ \mu P}$
F 5220	$\mathbf{t}_{SR}$ **+** 200 ms
F 6217	201 ms
F 6220	$\mathbf{t}_{SR}$ **+** 200 ms
F 6221	$\mathbf{t}_{SR}$ **+** 200 ms

Table 3.

µP module	$\mathbf{t}_{D\ \mu P}$
F 5220	$\mathbf{t}_{SR}$ **+** 200 ms
F 6217	201 ms
F 6220	$\mathbf{t}_{SR}$ **+** 200 ms
F 6221	$\mathbf{t}_{SR}$ **+** 200 ms

Table 3: Delay of the µP Modules

Example: F 6220, $\mathbf{t}_{SR}$ **=** 1000 ms, $\mathbf{t}_{DO\ max.}$ = 0

$$\mathbf{t}_{RR\ \#} \le \mathbf{t}_{SR} + \mathbf{t}_{DO\ max.} + \mathbf{t}_{D\ \mu P}$$

$$\mathbf{t}_{RR} \le \mathbf{t}_{SR} + 0 + \mathbf{t}_{SR} + 200\text{ ms}$$

$$\mathbf{t}_{RR} \le 2 \times \mathbf{t}_{SR} + 200\text{ ms}$$

$$\mathbf{t}_{RR} \le 2 \times 1000\text{ ms} + 200\text{ ms}$$

$$\mathbf{t}_{RR} \le \underline{2200\text{ ms}}$$

The *Safety Time [ms]* parameter $\mathbf{t}_{SR}$ 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.
- The *Safety Time [ms]* parameter $\mathbf{t}_{SR}$ must be adjusted if the µP modules F 5220, F 6220 or F 6221 are used.

If the µP modules F 5220, F 6220 or F 6221 are used, the following conditions apply to the *Safety Time [ms]* parameter:

$$\mathbf{t}_{SR} \ge \mathbf{4 \times t}_{WD}$$

$$\mathbf{t}_{SR} \ge \mathbf{1000\ ms}$$

$$\mathbf{t}_{WD} \ge \mathbf{50\ ms}$$

$\mathbf{t}_{WD}$ Watchdog time (of the resource)

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 (PES) 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} ≤ ½ x t_{SR}

t_{WD} Watchdog time (of the resource)

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

Condition for safety and availability:

t_{WD} ≤ 1/3 x t_{SR}

The watchdog time (of the resource) must be configured. The *Watchdog Time [ms]* parameter can be set within 6...7500 ms and is configured in the resource properties. The default setting is 200 ms.

The PADT checks the parameters *Safety Time [ms]* and *Watchdog Time [ms]* and rejects the configuration while generating it if the watchdog time is greater than ½ the value 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 oberserve 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 recommends meeting the following conditions to ensure sufficient availability of the controller:

3 x t_{WD} ≤ t_{SR} (*Safety Time [ms]* parameter*)*

3.2.5 Determining the Watchdog Time through Testing

For time-critical applications or systems including more than one controller (PES), it is necessary to determine the watchdog time $\mathbf{t}_{WD}$ during start-up. This must be done during RUN operation and under full load. To this end, all engineered modules must be inserted and all the configured communication connections (e.g., safe**ethernet** and other standard protocols) must be operating.

The maximum system load results from synchronization, when the modules are removed and reinserted. The watchdog time must be set so that synchronization at full load is always possible.

To perform the test

1. In the resource properties, set the *Safety Time [ms]* to the maximum value (22 500 ms).
2. In the resource properties, set the *Watchdog Time [ms]* to the maximum value (7 500 ms).
3. In the resource properties, set the *Maximum System Bus Latency [µs]* to the default value `System Defaults`.
4. Compile the configuration and load it into the controller by performing a download.
5. Start the resource (cold start).
6. Open the Control Panel for the resource and reset the cycle time statistics.

For the following steps, ensure that the system is operated under full load.

7. Read out the maximum cycle time in the Control Panel, wait several minutes and note down the variations and load peaks.
8. In succession, remove all I/O processing modules (F-IOP 01) from the racks. Once the last I/O processing module has been removed, read the maximum system cycle time in the Control Panel and note it down.
9. Insert the removed I/O processing modules into the racks in any order and wait for the system to properly operate again.
10. Remove the processor module with the highest slot number from the base rack and reset the cycle statistics in the Control Panel.
11. Reinsert the processor module that has been removed in the previous step into the base rack and wait for it to be completely synchronized with the existing processor module. Afterwards, read the maximum cycle time in the Control Panel and note it down.

i When a redundant processor module is added, it automatically synchronizes with the configuration of the existing processor modules. The time required for synchronization extends the controller cycle.

12. Perform steps 10 and 11 using the processor module with the lowest slot number.

13. Use the noted times in the following equation:

$$\mathbf{t}_{WD} = \mathbf{t}_{Sync} + \mathbf{t}_{Reserve} + \mathbf{t}_{Com} + \mathbf{t}_{Config} + \mathbf{t}_{Peak}$$

t_{Sync} Maximum synchronization time of the processor modules. Use the highest value resulting from steps 11 and 12.

$t_{Reserve}$ Safety margin 12 ms.

t_{Comm} = System parameter *Max. Com.Time Slice ASYNC [ms]*, which is configured in the resource properties

t_{Config} = System parameter *Max. Duration of Configuration Connections [ms]*, which is configured in the resource properties*.*

t_{Peak} Maximum load peak of the cycle time (t_{Peak}). Use the highest value resulting from steps 7 and 8.

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 803 213 E).

3.4 Safety Requirements

For using the safety-related HIQuad X automation system, the following environmental conditions must be met:

3.4.1 Product-Independent Hardware Requirements

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

- To ensure safety-related operation, approved fail-safe hardware and software components must be used. The approved components are itemized in the *Version List of Devices and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH*.
  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 (see Chapter 3.4.8) about EMC, mechanical, chemical and climatic influences must be observed.
- Non-fail-safe, interference-free hardware and software components may be used for processing non-safety-relevant signals. 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 HIQuad X 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.
- Power must be supplied by power supply units complying with SELV and PELV. For the power supply units, the following applies:
  - **24 VDC** power supply: The voltage of the power supply units may not exceed 31 V.
  - **48 VDC** power supply: The voltage of the power supply units may not exceed 62 V.
- 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 HIQuad X 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. A complete test of the logic must be performed by trial.
- 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 systems, ensure that the overall response time of the system does not exceed the worst case response time permitted for safe**ethernet** or HIPRO-S V2. All calculations must be performed in accordance with the rules given in Chapter 11.3.
- 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 factory acceptance test (FAT) and determine the access to the system by implementing administrative and technical measures.

3.4.7 Temperature Monitoring

The temperature of the following modules is measured by embedded sensors and can be displayed and used in the programming tool.

- F-CPU 01
- F-IOP 01
- F-PWR 01

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.

The temperature state may be used in connection with additional shutdown conditions.

The user must implement suitable measures to ensure that the ambient temperature limits specified for the system are met.

3.4.8 Environmental Conditions

For using the safety-related HIQuad X automation system, the following environmental conditions must be met:

General	
Protection class	Protection class II in accordance with IEC/EN 61131-2
Ambient temperature	0...+60 °C
Transport and storage temperature	-40...+70 °C
Pollution	Pollution degree II
Altitude	< 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 4: Environmental Conditions

Refer to the relevant data sheets for potential deviations.

3.5 Cyber Security

Industrial controllers (PES) must be protected against IT-specific problem sources. Typical problem sources are:

- Attackers within the company premises.
- Attackers via communication networks outside the company premises.
- Improper use of the equipment (e.g., USB sticks).
- Inadequate protection of IT equipment (e.g., open WLAN).
- Software failures.

A HIQuad X installation includes the following parts to be protected:

- The safety-related automation system HIQuad X.
- The PADT.
- The X-OPC Server: X-OPC DA, X-OPC AE (optional).
- The communication connections to external systems (optional).

HIQuad X with basic settings is already a controller fulfilling the requirements for cyber security (IT security).

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

- Each change to the user program or configuration results in a new configuration CRC.
- Online changes of the safety parameters can be deactivated in the controller. Changes to the safety parameters are only possible by performing a download or reload.
- If required, the user can set up security mechanisms in the form of user management. In the user management scheme, the user can define if an authorization is required to open the project and log in to a resource.
- The controller data can only be accessed if the PADT is operating with the current version of the user project (archive maintenance!).
- A physical connection between the PADT and the controller (PES) is not required during operation and can be interrupted. The PADT can be connected for diagnostic tasks or maintenance work at any time, also for short periods.

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

⚠ **WARNING**

Physical injury possible due to unauthorized manipulation of the controllers!

The controller must be protected against unauthorized access!

- **Change the default settings for login and password!**
- **Control the physical access to the controller and PADT!**

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

- Meaningful allocation of user groups and accounts.
- Reasonable allocation of access rights for the controllers and the PADT.
- Use of appropriate passwords.
- Maintained network maps help to ensure that secure networks are permanently separated from public networks and, if required, only a well-defined connection exists, e.g., via a firewall or a DMZ (demilitarized zone).

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

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

For more details, refer to the HIMA cyber security manual (HI 801 373 E).

3.6 Certification

The HIQuad X 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 HIQuad X 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 or obtained by sending an e-mail request to: documentation@hima.com.

3.6.2 EC Type Test Certificate

The test institute TÜV Rheinland has tested and certified the safety-related HIQuad X automation system for applications in accordance with the functional safety standards. The safety-related HIQuad X 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
HIQuad X

3.6.3 Current Standards

The HIQuad X 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, Parts 1-3:2016	SIL 3
EN / ISO 13849-1:2015	PL e
EN 62061:2005 + A1:2013 + A2:2015	SIL CL 3
EN 50156, Parts 1-2:2015	SIL 3
EN 12067-2:2004	
EN 298: 2012	
EN 60079-0:2012 + A11:2013	
EN 60079-11:2012	
EN 60079-15:2010	
NFPA 85:2015	
NFPA 86:2015	
NFPA 72:2016	
EN 61131-2:2007 + Amendment 1:2008	
EN 61131-6:2012	
EN 61326-1:2013	
EN 61326-3-1:2018	
EN 61326-3-2:2008	
EN 54-2:1997 + AC:1999 + A1:2006[1]	
EN 50130-4:2011 + A1:2014[1]	

[1] Exception: the F 3330 may not be used for applications in accordance with these standards.

Table 5: International Standards and Safety Levels

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

3.6.4 Test Conditions

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

Standard	Content
IEC/EN 61131-2	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 61326-3-2	Electrical equipment for measurement, control and laboratory use - EMC requirements Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment
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

Table 6: Standards for EMC, Climatic and Environmental Requirements

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 7: Climatic Tests

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...9 Hz / 3.5 mm 9...150 Hz / 1 g, controller in operation, 10 cycles per axis
	Shock immunity test: 15 g, 11 ms, HIQuad X in operation, 3 shocks per axis and direction (18 shocks)

Table 8: 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 unit must at least comply with one of the following standards or meet one of the following requirements: ▪ IEC 61131-2. ▪ SELV (Safety Extra Low Voltage). ▪ PELV (Protective Extra Low Voltage).
	The HIQuad X 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.
	Backup duration, withstand test: Test A, 300 h at 60 C, Goldcap for date/time.

Table 9: Verification of the DC Supply Characteristics

4 Processor Module (F-CPU 01)

The safety-related processor module is composed of two microprocessors, each with its own RAM, that simultaneously process the same programs, operating systems and the user program. A hardware comparator continuously aligns the data from the two microprocessors and those from the memories. The processor module reports detected differences and automatically enters the ERROR STOP state.

The processor module carries out additional self-tests such as the program sequence monitoring (watchdog).

4.1 Self-Tests

The operating system of the processor module 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 scope of the testing includes:

- The microprocessors.
- The redundant memories.
- The NVRAMs.
- The watchdog.
- The I/O buses inside the controller.
- The power supply.

4.2 Responses to Faults in the Processor System

If the processor module detects an internal module fault, an entry is written to the diagnostic history. Subsequently, a reboot is performed.

After the first reboot due to faults, the processor module restarts and, once all self-tests are complete, attempts to start system operation. If the internal module fault is still present, the processor module performs a second reboot.

If a further internal fault occurs within the first minute after restart, the processor module no longer participate in the system's operation.

If also the last processor module fails, the entire system stops system operation, i.e., the protocol connections are closed, I/O outputs are de-energized.

4.3 Replacing Processor Modules

Prior to replacing a processor module, ensure that the replacement will not cause a running HIQuad X system to stop.

In particular, this applies for systems running in accordance with the energize to trip principle. The failure of such systems causes the loss of the safety function.

Redundant processor modules can be replaced during operation, provided that at least one processor module is available that can maintain safety-related operation while the other module is being replaced.

NOTICE

Interruption of safety-related operation possible!

Replacing a processor module with a lit or blinking Ess **LED can result in the interruption of a controller's operation.**

Do not remove processor modules if the Ess **LED is lit or blinking.**

A lit or blinking **Ess** LED indicates that the processor module is essential for the system to function.

Even if the LED is not lit or blinking, the system redundancies, which this processor module is part of, must be checked using SILworX. The communication connections processed by the processor module must also be taken into account.

For further details on how to replace processor modules, refer to the processor module manual (HI 803 214 E) and to the system manual (HI 803 211 E).

5 Communication Module

Communication modules are used for both exchanging safety-related data with other HIMA controllers and for exchanging standard data via fieldbuses and Ethernet.

- The processor module controls the safety-related data exchange with the SIL 3-certified transmission protocols safe**ethernet** and HIPRO-S V2. The communication module forwards the data to the connected HIMA controllers. The safety-related safe**ethernet** protocol ensures that corrupted messages are detected (black-channel principle).

  This allows safety-related communication via non safety-related transmission paths, i.e., standard network components.
- The supported standard protocols are specified in

Protocol	Fieldbus	TCP/UDP
ComUserTask	X	X
Modbus Master	X	X
Modbus Slave Set	X	X
Modbus Slave Set V2	X	X
PROFIBUS DP Slave	X	-
SNTP Client	-	X
SNTP Server	-	X

- Table 17.

Refer to the following documents for further details on communication and communication modules:

- This manual, Chapter 11.1.
- Communication module manual (HI 803 223 E)
- Communication manual (HI 801 101 E).
- System manual (HI 803 211 E).

6 I/O Processing Module (F-IOP 01)

I/O processing modules within the HIQuad X system communicate with the processor modules in the base rack via the two safety-related system buses. Additionally, the I/O processing module manages the I/O bus of the rack in which it is located.

The system buses are used to transmit data via a safety-related protocol. A HIQuad X system that **only** contains **one processor module** can be operated at a reduced availability level using one system bus only.

I/O processing modules cannot be wired redundantly. If redundancy is required at the I/O level, a redundant extension rack must be used. For an overview of the different HIQuad X system concepts, refer to the system manual (HI 803 211 E).

The safety-related I/O processing module is equipped with a 1oo2D processor system (HICore 2). A hardware comparator continuously aligns the data from the internal microprocessors and those from the memories. The I/O processing module reports detected differences and automatically enters the ERROR STOP state.

The I/O processing modules test and monitor the I/O modules in one rack and report their states. Additionally, the I/O processing modules provide the watchdog signal for the output modules.

I/O processing modules provide the input values of the I/O modules in a rack to the user program. The user program's output values are sent to the I/O processing module, which writes them to the output modules. The output modules thus control the field level, e.g., the actuators.

6.1 Self-Tests

The operating system of the I/O processing module 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 scope of the testing includes:

- The microprocessors.
- The redundant memories.
- The NVRAMs.
- The watchdog.
- The I/O buses.
- The power supply.

6.2 Responses in the Event of Faults

If a failure occurs on a system bus, the bus connection is ensured via the redundant system bus, provided that both system buses have been previously configured.

If the system runs in mono operation with only one processor module, the redundant system bus is not available.

If a disturbance affects the I/O bus, no process data are transmitted. The I/O level is no longer available to the system.

The module reports faults through the LEDs on the front plate.

If faults occur, all the output modules inserted in the extension rack use the second shutdown option to enter the safe state. The input module data are no longer sent.

6.3 Responses to Faults in the Processor System

The I/O processing module reports differences detected by the hardware comparators and automatically enters the ERROR STOP state. The I/O processing module also enters the ERROR STOP state if the hardware comparator fails.

A hardware comparator within the I/O processing module constantly checks if the data from the internal microprocessor 1 are identical to the data from microprocessor 2. If they are different or if the test routines detect a fault in the I/O processing module, the I/O processing module automatically enters the ERROR STOP state.

6.4 Rack ID

The rack ID is used for unambiguously identifying the individual racks within the system. A 10-pole DIP switch on the I/O processing module is used to set the rack ID. A unique rack ID that matches the configuration in SILworX must be allocated to each rack. The rack ID of the H51X base rack is 0 since no I/O processing module is used in this rack. For a description of the rack IDs and DIP switches, refer to the I/O processing module manual (HI 803 219 E).

The rack ID is the **safety parameter** for addressing the racks and the modules inserted in them!

6.5 Service Mode

The I/O processing module is equipped with a service mode function. This allows the users to replace the I/O modules within a rack during operation without having to switch off the entire I/O level of a rack. To replace the I/O modules during operation, the service mode must be activated for the I/O processing module.

When the service mode is active, I/O module faults requiring that the affected rack is shut down, are suppressed. The system issues a warning for the affected rack. This warning is signaled via the rack connection indicators.

i If the service mode is active, the second shutdown option (via the I/O watchdog) is blocked! This option cannot be used to put the output modules in the safe state.

The service mode is either activated or deactivated using the service push-button (SERV) on the front side of the I/O processing module or via a PADT command.

The service mode stops automatically 24 h after activation, unless it was manually deactivated beforehand.

If the user deactivates the service mode, the system remains in service mode until the faulty or replaced I/O modules have been initialized and no modules report a fault after initialization is complete. After 24 h, the system deactivates the service mode.

If 24 h after activation the service mode is automatically deactivated, no I/O modules are re-initialized. If faults requiring the rack to shut down are still present in the rack (e.g., a missing output module), the I/O watchdog (second shutdown option) , is switched off and all output modules within the rack enter the safe state.

The SERV push-button can be locked using the *Deactivate service mode push-button*. If the SERV push-button is locked through the user program, then the service mode can only be controlled through a PADT command.

To replace I/O modules

1. Press the service mode push-button (SERV) on the I/O processing module (F-IOP 01) located in the rack of the I/O modules to be replaced, for 2 s to 7 s. Alternatively, select the I/O processing module with the *Start Service Mode* PADT command to switch to the module's service mode.
   ☑ The *Service Mode Active* system parameter is TRUE.

☑ Step result (optional). When the I/O processing module operates in service mode, the red LEDs *Slot* and *Chn* are blinking.

2. Completely release the fastening screws from the I/O module to be replaced.
3. Unscrew the cable plug or remove the I/O module with inserted cable plug.
4. Insert the new I/O module without cable plug and screw it in place. Observe the description provided in the system manual!
5. Plug in the cable plug and screw it in place.
6. Repeat steps 2 through 5 for each module to be replaced.
7. Press the service mode push-button (SERV) on the I/O processing module (F-IOP 01) for 2 to 7 seconds or deactivate the service mode using the *Quit Service Mode* PADT command.

   ☑ The *Service Mode Active* system parameter is FALSE.
   ☑ The LEDs of the I/O processing module report the regular module and channel diagnosis.

► The I/O modules have been replaced and are operating again without faults.

For further details on the service mode, refer to the F-IOP 01 manual (HI 803 219 E).

7 Input Modules

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

Digital input modules[1]	Channels	Safety-related	(Ex)i
F 3221	16		
F 3224A	4		X
F 3236	16	X	
F 3237	8	X	
F 3238	8	X	X
F 3240	16	X	
F 3248	16	X	
Analog input modules[1]	Channels	Safety-related	(Ex)i
F 6215	8		
F 6217	8	X	
F 6220	8	X	X
F 6221	8	X	X
Counter module[1]	Channels	Safety-related	(Ex)i
F 5220	2	X	
[1] Interference-free: When a module performing part of a safety function is not affected by other operating modules. This applies irrespective of whether the modules are safety-related or not.			

Table 10: Overview of the Input Modules

7.1 General

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 safety-related input modules F 5220, F 6217, F 6220 and F 6221 are equipped with their own 1oo2 processor system that allows for increased module complexity. The 1oo2 processor system of these modules automatically carries out safety-related tests during operation and transmits safe data to the I/O processing system.

The safety-related input modules without processor system are automatically subjected to a high-quality, cyclic self-test during operation. The input modules include wiring elements ensuring that the module function is tested with special test routines integrated in the operating system (I/O processing module). These test routines ensure the safe functioning of the corresponding input module.

Detection of faults during the self-tests automatically triggers a safety-related response of the I/O processing system and generates the corresponding error messages. The detailed error messages can be evaluated in the user program by reading out the error codes.

To ensure the module's proper operation, HIMA cable plugs must be used.

For further details on the input modules, refer to the module-specific manuals.

7.2 Response in the Event of a Fault

If a fault is detected at the signal inputs, the user program processes the input's initial value. A module fault in the input module causes the user program to process the initial value for all the inputs. The initial value of the global value must be configured in SILworX accordingly (default value = 0).

In addition to the *Slot* and *Chn* LEDs on the I/O processing modules, error and status messages are generated and saved in the processor module. These can be read out from the diagnostic memory using the PADT.

To increase availability, the safety-related input modules can also be used redundantly. Redundant input modules do not impair the system safety, see Chapter 3.1.1.

The status and error messages as well as the system variables can be used to program application-specific fault responses. For further details, refer to the module-specific manual.

7.3 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 615111 standard, Section 11.4.

7.4 I/O Noise Blanking

If noise blanking is active, the system does not respond to transient interference. In such cases, the interference does not de-energize the outputs and has no effects on the data sources.

Noise blanking only operates within the resource safety time and only if the resource safety time is ≥ 3 × resource watchdog time.

i Noise blanking is permanently active on the F 5220, F 6220 and F 6221 input modules and cannot be deactivated. The activation field in SILworX is grayed out and has no functionality.

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

The input modules read the digital signals at the inputs and provide failsafe values to the user program in every processor module cycle.

7.5.1 Test Routines

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

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

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

7.5.2 Redundancy of Digital Inputs

Digital inputs may be wired redundantly. The redundant connection is used to increase the availability of the inputs.

7.5.3 Surges on Digital Inputs

Due to the short cycle time of the HIQuad X 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 803 211 E).

7.6 Safety-Related F 5220 Counter Module

This two-channel counter module has its own 1oo2 processor system with one safety-related output for each channel. Depending on its configuration, the module can be used to gather the following process values:

- Pulse count.
- For measuring the frequency or the rotational speed via an adjustable gate time.
- For limit value monitoring through cycle-independent output operation with comparison functions.
- Detection of rotation direction.

The counter module processes pulses to the following frequency in a safety-related manner:

$$\mathbf{f_{max} = 2^{22} / (t_{RR} + 100\ ms)}$$

In *pulse counting* mode, the resource response time $\mathbf{t}_{RR}$ depends on the maximum measuring frequency $\mathbf{f}_{max}$, which the counter channels should use to operate:

$$\mathbf{t_{RR} = (2^{22} / f_{max}) - 100\ ms}$$

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

The counter module does not need the I/O watchdog signal for operation. The absence of the I/O watchdog signal has no effects on the counter module function nor on their switching outputs.

For further details, refer to the module-specific manual (HI 803 191 E).

7.6.1 Test Routines

The module has a 1oo2 processor system that automatically carries out the safety-related online tests and provides the data to the user program.

If the test routines detect a module fault, both safety-related outputs are switched off. If a channel fault occurs, the safety-related output allocated to the affected channel is switched off.

7.6.2 Behavior in the Event of Short-Circuits and Open-Circuits

If a short-circuit or open-circuit is detected at a counter input, the module switches off the corresponding safety-related output. The *Channel OK* system parameter is set to FALSE.

7.6.3 Redundancy of Counter Inputs

Counter inputs may be wired redundantly. The redundant connection increases the availability of the inputs.

The redundant connection of two counter modules must be implemented with the user program since SILworX does not support the creation of redundancy groups for counter modules.

7.7 Safety-Related Analog F 6217 Input Module

The module has a 1oo2 processor system that automatically carries out the safety-related online tests and provides the data to the user program. The analog value is available for each channel as a raw value (data type DINT) and as a scaled process value (data type REAL).

7.7.1 Test Routines

The module uses the test D/A converter to apply test values and tests these values with the A/D converter with which the input signal is digitized.

7.7.2 Redundancy of Analog Inputs

Analog inputs may be wired redundantly. The redundant connection is used to increase the availability of the inputs.

If 2 inputs are redundantly configured, the larger of the two scaled values is written to the redundant system parameter (-> *Process Value [REAL]*) This applies provided that both modules are in proper working order. If faults occur, only the value of the functional module is processed.

7.8 Safety-Related Analog F 6220 Input Module

The analog input and temperature module has 8 channels for connecting thermocouples of various types and one reference temperature input for connecting to a Pt 100 resistance thermometer. The channels are implemented with the type of protection Intrinsic Safety and are safely separated from the output and power supply circuit. The module is equipped with its own 1oo2 processor system.

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

7.8.1 Test Routines

The module has a 1oo2 processor system that automatically carries out the safety-related online tests and provides the data to the user program. Each of the (8+1) channels provides safe input values and a safe fault status.

7.8.2 Redundancy of Analog F 6220 Input Modules

Analog inputs may not be wired redundantly to connect to thermocouples. If two input modules are redundant to one another, each input channel must be connected to its own thermocouple.

The redundant connection is used to increase the availability of the inputs.

If 2 inputs are redundantly configured, the larger of the two scaled values is written to the redundant system parameter (-> *Process Value [REAL]*) This applies provided that both modules are in proper working order. If faults occur, only the value of the functional module is processed.

7.8.3 Configuration Notes

Observe the following points when engineering the module:

- Unused inputs must be short-circuited.
- The metrological accuracy outside the nominal range cannot be ensured for the channel value *-> Raw Value [1 °C / 1 mV = 10 000] [DINT]*, for this reason, the value must not be used in safety-related applications.
- The cold junction temperature for operation in accordance with SIL 3 must be taken directly from the user program or must be determined by comparing the cold junction temperatures of two modules within the user program.
- For SIL 3, the thermocouple temperature must be determined by comparing the temperatures of two different thermocouples.
- All possible deviations must be considered and taken into account when evaluating the measured values.

7.9 Safety-Related Analog F 6221 Input Module

The analog input module has eight channels to directly connect analog transmitters from the Ex zone. The channels are implemented with the type of protection Intrinsic Safety and are safely separated from the output and power supply circuit. The transmitter supply voltage can be ensured through the F 3325 supply module or another power supply in accordance with the data sheet specifications. This transmitter voltage supply must be connected to the F 6221 module for monitoring purposes.

7.9.1 Test Routines

The module has a 1oo2 processor system that automatically carries out the safety-related online tests and provides the data to the user program. Each of the 8 channels provides safe input values and a safe fault status.

7.9.2 Redundancy of Analog Inputs

Analog inputs may be wired redundantly. The redundant connection is used to increase the availability of the inputs.

If 2 inputs are redundantly configured, the larger of the two scaled values is written to the redundant system parameter (*-> Process Value [REAL]*) This applies provided that both modules are in proper working order. If faults occur, only the value of the functional module is processed.

7.9.3 Configuration Notes

Observe the following points when engineering the module:

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

7.10 Checklists for Inputs

HIMA recommends using the available checklists 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. The checklists are available for registered HIMA customers in the download area https://www.hima.com/en/downloads/.

8 Output Modules

The following table provides an overview of the HIQuad X output modules:

Digital output modules[1]	Channels	Safety-related	Load capacity
F 3322	16		≤ 0.5 A
F 3330	8	X	≤ 0.5 A
F 3331	8	X	≤ 0.5 A
F 3333	4	X	≤ 2 A
F 3334	4	X	≤ 2 A
F 3335	4 (Ex)i	X	22 V ≤ 0.053 A
Relay output modules[1]	Channels	Safety-related	Load capacity
F 3422	8		≤ 60 V ≤ 2 A
F 3430	4	X	≤ 250 V ≤ 4 A
Analog output modules[1]	Channels	Safety-related	Load capacity
F 6705	2	X	0…20 mA
F 6706	2		0…20 mA
[1] Interference-free: When a module performing part of a safety function is not affected by other operating modules. This applies irrespective of whether the modules are safety-related or not.			

Table 11: Overview of the Output Modules

8.1 General

The safety-related output modules write the values created by the user program to the outputs once per cycle. The output signals are read back and compared with the specified output data.

Additionally, all outputs for which the switched-on channels are briefly switched off and switched-off channels are briefly switched on are subject to background tests. The test pulses are present in the F 3330, F 3333, F 3335 and F3430 for 250 µs. For F 3331 and F 3334, the duration of pulse tests and the test interval can be configured, see the HIQuad X module-specific manuals.

These tests ensure that the switchability of the outputs is checked without affecting the function of the connected actuators, if these tolerate the test duration of 250 µs. As a result, the freezing (switch welding) of each output is detected, even if the output signal is static.

If inductors or lamp loads are connected, the test pulse duration configured for output modules with line monitoring must be checked and, if necessary, extended. The safe state of the outputs is 0 or an open relay contact.

To ensure the module's proper operation, HIMA cable plugs must be used.

8.2 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 sensors and actuators, refer to the IEC 615111 standard, Section 11.4.

8.3 Response in the Event of a Fault

The foreground and background tests of the output modules provide the following responses if a fault occurs:

- A module fault always causes the module and its outputs to enter the safe de-energized state.
- An undetected output module causes all the output modules within a rack to switch off since the safe state of output module can no longer be checked. To replace an output module during operation, the service mode must first be activated on the I/O processing module (F-IOP)
- If a high level is present on an output of digital output module switched off by the user program instead a low level as expected, the I/O processing module reports a module fault and the output module enters the safe de-energized state.
- If a low level is present on an output of digital output modules switched on by the user program instead of a high level as expected, the I/O processing module reports a channel fault.
- If a background test detects that an output of digital output modules with a high level cannot be switched off the I/O processing module returns a module warning. HIMA recommends removing the cause of the module warning within 24 hours since all output modules will enter the safe state HIMA after this time. On the other hand, if an output cannot be switched off when changing from high-level to low-level, the output module immediately enters the de-energized state.
- If a background test detects that an output of digital output modules with a low level cannot be switched on, the I/O processing module returns a module warning. If the module warning is still present once the background test has been completed, the output module enters the safe, de-energized state.
- If a short-circuit to L- or an overload is detected on a channel activated by a user program (within a F 3331 or F 3334 module), the I/O processing module reports a module fault and the output module enters the de-energized state. Additionally, if the system parameter *SC/OC Active* is active and *SC/OC Mode [UINT] ->* is set to 1 or 2, the system variable *LS* in the channel affected by the short-circuit is set to TRUE. Observe the hardware revision of the F 3334 output module, see Chapter 8.5.3.
- The digital output modules F 3330 through F 3335 do not support switching off individual channels. A switched-on channel for which an open-circuit has been detected causes all channels to enter the de-energized state.
- In current source mode, all faults detected in any of the modules cause the analog F 6705 output module to enter the safe, de-energized state. In current sink mode, the module can only enter the safe, de-energized state by switching off the external voltage source. The user program must shut down the voltage supply for the current loop safely.
- If an F 3330, F 3333, F 3335 or F 3430 module is shut down due to a fault and the automatic restart is activated for the module, 1 ms test pulses can be actuated in the field in intervals of 1 s!
- If an F 3331 or F 3334 module is shut down due to a fault and the automatic restart is activated for the module, test pulses can be actuated in the field in intervals of 1 s! Depending on the value configured for the *Max. Test Pulse Duration [ms]* system parameter, the following values result:
  - If the configured value is 0, the resulting maximum test pulse duration is 1 ms.
  - If the configured value is 50, the resulting maximum test pulse duration is 50 ms.
-
- If an F 6705 module is shut down due to a fault and the automatic restart is activated for the module, 10 ms test pulses can be actuated in the field in intervals of 10 s!

8.4 I/O Noise Blanking

If noise blanking is active, the system does not respond to transient interference. In such cases, the interference does not de-energize the outputs and has no effects on the data sources.

Noise blanking only operates within the resource safety time and only if the resource safety time is ≥ 3 × resource watchdog time.

8.5 Safety-Related Digital Output Modules F 3330, F 3331, F 3333, F 3334, F 3335

The output modules ensure the safety function using 3 safety switches connected in series for each channel where 2 are implemented as safety switches. If a fault is detected in the output voltage or safety switch, the safety switches causes all the outputs to enter the de-energized state.

Each safety switch can be individually switched off via the I/O bus. If a fault occurs and an output module cannot be switched off via the I/O bus, the second, independent shutdown option (I/O watchdog) is used to place the output module in the de-energized state.

If a module fault occurs, this integrated safety function safely de-energizes all the channels (de-energized state).

8.5.1 Test Routines

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

- Reading back the output signals. The switching threshold for a read-back low level is $\leq$ 6.5 V.
- Checking the integrated redundant safety shutdown.
- Applying the test patterns during the background test with configurable test intervals and maximum test pulse duration.
- Reading the line monitoring (SC/OC) for the switched-on channel, if existing.
- Reading the line monitoring (SC/OC) for all the channels during the test pattern test, if existing.

8.5.2 Redundancy of Digital Outputs

Digital outputs may be wired redundantly. The redundant connection is used to increase the availability of the outputs.

8.5.3 Engineering Notes

Open-circuit monitoring requires a minimum load of 10 mA.

The minimum load required for redundant channels is twice as high (20 mA).

As of hardware revision AS03, the F 3334 output module no longer detects short-circuits. The -> *LS [BOOL]* system variable may not be evaluated as of hardware revision AS03.

Prior to deleting an F 3330, F 3331, F 3333 or F 3334 module from the project configuration, the outputs must be set to the safe (switched-off)state, e.g., the forcing process must be stopped for outputs that are being forced to high level.

8.6 Safety-Related F 3430 Relay Module

Relay output modules are connected to the actuator under any of the following circumstances:

- Electric and galvanic separation is required.
- Higher amperages are to be connected.
- Alternating currents are to be connected.

8.6.1 Test Routines

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

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

8.6.2 Behavior in the Event of External Short-Circuit

External short-circuits cause the fuse for the relevant channel to trigger. No error message is issued.

8.6.3 Redundancy of Relay Outputs

Relay inputs may be wired redundantly. The redundant connection is used to increase the availability of the outputs.

8.6.4 Engineering Notes

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

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

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

The required tests are performed by HIMA.

8.7 Safety-Related Analog F 6705 Output Module

The analog outputs forward the values determined in the user program to the actuators.

The analog F 6705 module can be operated in current source or current sink mode. In current source mode, the de-energized state (output current = 0 ma) is the safe state.

The initial values must be set to 0 to ensure that the input variables transmit the value 0 to the user program if a fault occurs.

In current sink mode, the module can only enter the safe state if additional measures are implemented. The user program must safely shut down the supply voltage for the current loop.

8.7.1 Test Routines for Analog Outputs

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

- Reading the output signals back.
- Linearity testing of the D/A converter.
- Crosstalk testing between the outputs.
- Checking the integrated redundant safety shutdown.

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

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

8.7.3 Redundancy of Analog Outputs

Analog outputs may be wired redundantly. The analog connection is used to increase the availability of the outputs. For details on the redundant output wiring, refer to the F 6705 module manual (HI 803 196 E).

8.8 Replacing Output Modules

If a fault occurs or maintenance work is necessary and the output modules need be replaced, the service mode option on the I/O processing module (F-IOP) must be activated beforehand, see Chapter 6.5. Additionally, the *Deactivate service mode push-button* system parameter must be deactivated.

8.9 Checklist for Safety-Related Outputs

HIMA recommends using the checklists 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. The checklists are available in Microsoft® Word® format on the HIMA website.

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.

9 Software

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

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

The user program, which contains the application-specific functions to be performed by the automation device, 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.

9.1 Safety-Related Aspects of the Operating System

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 Devices and Firmware 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. The user must ensure that the operating system versions loaded in the modules are valid (see Chapter 10.2).

9.2 Operation and Functions of the Operating System

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.

9.3 Safety-Related Aspects of Programming

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

9.3.1 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 safe 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!

9.3.2 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 also be created for the numerical evaluation of formulas, e.g., 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.

The described tests must be performed within defined ranges of values, at the limits of or within invalid ranges of values.

HIMA recommend performing an active simulation with sources. This is the only way to 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.

9.3.3 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.

9.3.4 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.

9.4 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 these safety parameters correctly and verify the whole entry upon completion of the PES load from within the PES itself.

These parameters are:

- **For the rack ID, refer to the system manual (HI 803 211 E).**
- **The parameters marked as safety-related in Table 12**

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.

9.4.1 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.

System parameters	S [1)]	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), see Chapter 3.2.2. Range of values: 20...22 500 ms Default value: 600 ms (can be changed online)	Application-specific
Watchdog Time [ms]	Y	Watchdog time in milliseconds, see Chapter 3.2.3. Range of values: 6...7500 ms Default value: 200 ms (can be changed online)	Application-specific
Target Cycle Time [ms]	Y	Target or maximum cycle time, see *Target Cycle Time Mode*. Range of values: 0...7500 ms Default value: 0 ms (can be changed online) The maximum target cycle time value may not exceed the configured *Watchdog Time [ms]* minus the minimum value that can be set for *Watchdog Time [ms]* (6 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 more details, refer to Chapter 9.4.1.1.	Application-specific
Target Cycle Time Mode	N	Use of *Target Cycle Time [ms],* see Chapter 9.4.1.1. The default setting is *Fixed-tolerant* (can only be changed online).	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. Operation mode for high availability.	
		Mode 3: The processor waits until the execution time not needed by the user programs has expired, thus increasing the cycle.	
		The default setting is 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	-

<table>
<tr><th>System parameters</th><th>S 1)</th><th colspan="2">Description</th><th>Setting for safe operation</th></tr>
<tr><td>Optimized Use of Com. Time Slice</td><td>N</td><td colspan="2">The system parameter reduces the response times for communications via processor module(s).
ℹ 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).</td><td>-</td></tr>
<tr><td>Max. Duration of Configuration Connections [ms]</td><td>N</td><td colspan="2">This defines how much time within a CPU cycle is available for configuration connections.
Range of values: 2...3500 ms
Default value: 12 ms
For more details, refer to Chapter 9.4.1.2.</td><td>Application-specific</td></tr>
<tr><td>Maximum System Bus Latency [µs]</td><td>N</td><td colspan="2">Maximum delay of a message between an I/O processing module and the processor module.
Setting: Line structure or 100 µs
The default setting is line structure.
ℹ A license is required for setting the maximum system bus latency to a value ≠ <i>System Defaults</i>.</td><td>Application-specific</td></tr>
<tr><td rowspan="3">Allow Online Settings</td><td rowspan="3">Y</td><td>TRUE:</td><td><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.
The default setting is TRUE.</td><td rowspan="3">HIMA recommends using the FALSE setting.</td></tr>
<tr><td>FALSE:</td><td>The following parameters <b>cannot</b> be changed online:
▪ <i>System ID</i>
▪ <i>Autostart</i>
▪ <i>Global Forcing Allowed</i>
▪ <i>Global Force Timeout Response</i>
▪ <i>Load Allowed</i>
▪ <i>Reload Allowed</i>
▪ <i>Start Allowed</i>
The following parameters can be changed online if <i>Reload Allowed</i> is TRUE.
▪ <i>Watchdog Time</i> (for the resource)
▪ <i>Safety Time</i>
▪ <i>Target Cycle Time</i>
▪ <i>Target Cycle Time Mode</i></td></tr>
<tr><td colspan="2"><i>Allow Online Settings</i> can only be TRUE when the controller is stopped or by performing a reload.</td></tr>
<tr><td rowspan="3">Autostart</td><td rowspan="3">Y</td><td>TRUE:</td><td>If the processor module is connected to the supply voltage, the user programs start automatically.
The default setting is TRUE.</td><td rowspan="3">Application-specific</td></tr>
<tr><td>FALSE:</td><td>The user program does not start automatically after connecting the supply voltage.</td></tr>
<tr><td colspan="2">Observe the settings in the resource program properties!</td></tr>
</table>

System parameters	S[1]	Description		Setting for safe operation
Start Allowed	Y	TRUE:	Cold start or warm start permitted with the PADT in RUN or STOP. The default setting is TRUE.	Application-specific
		FALSE:	Start not allowed.	
Load Allowed	Y	TRUE:	Configuration download is allowed. The default setting is TRUE.	Application-specific
		FALSE:	Configuration download is not allowed.	
Reload Allowed	Y	TRUE:	Configuration reload is allowed. The default setting is 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. The default setting is TRUE.	Application-specific
		FALSE:	Global forcing is not permitted for this resource.	
Global Force Timeout Response	N	Specifies how the resource should behave when the global force timeout has expired: ▪ Stop Forcing Only ▪ Stop Forcing and Stop Resource Default value: Stop Forcing Only.		Application-specific
Minimum Configuration Version	N	The default setting is based on the current SILworX version. It ensures compatibility with future SILworX versions. Code is generated in accordance with SILworX V10 conventions, since HIQuad X is supported as of SILworX V10. Any setting to a SILworX version prior to V10 is rejected for HIQuad X. An error message is displayed in the logbook! For more details, refer to Chapter 9.4.1.3.		Application-specific
Fast Start-Up	N	Not applicable to HIQuad X.		-

[1] The operating system handles the system parameter in a safety-related manner, yes (Y) or no (N)

Table 12: Resource System Parameters

9.4.1.1 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.

In doing so, HIQuad X limits reload and synchronization on the redundant modules 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	If a CPU cycle is shorter than the defined Target Cycle Time, 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. i A reload or synchronization process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time).
Fixed-tolerant	Similar to *Fixed*, but with the following differences: 1. To ensure that the synchronization process can be performed successfully, the target cycle time may be violated for one CPU cycle. 2. 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). The default setting is *Fixed-tolerant*! i 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. One single cycle may be extended during synchronization.
Dynamic	The CPU processes each CPU cycle as fast as possible. This corresponds to a target cycle time of 0 ms. i A reload or synchronization 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. One single cycle may be extended during synchronization.
Dynamic-tolerant	Similar to *Dynamic*, but with the following differences: 1. If necessary, the target cycle time is automatically increased for one CPU cycle to ensure that the synchronization process can be performed successfully. 2. 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). i 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 or synchronization process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time).

Table 13: Settings for Target Cycle Time Mode

9.4.1.2 Calculating the *Maximum Duration of Configuration Connections [ms]*

If communication is not completely processed within a CPU cycle, it is resumed in the next following CPU cycle at the interruption point. This slows down communication, but it also ensures that all connections to external partners are processed equally and completely.

The value of *Max. Duration of Configuration Connections [ms]* is included in the watchdog time and must be selected so that the cyclic processor module tasks can be executed in the remaining time.

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

A temporary setting for the F-CPU 01 module can be calculated as follows:

$t_{Config} = n_{Com} + n_{PADT} + n_{RIO} * 0.25 \text{ ms} + 4 \text{ ms} + 4*(t_{Latency} * 2 + 0.8)$

t_{Config}	System parameter *Max. Duration of Configuration Connections [ms]*
n_{COM}	Number of modules with Ethernet interfaces (CPU, COM)
n_{RIO}	Number of configured remote I/Os
n_{PADT}	Maximum number of PADT connections = 5
$t_{Latency}$	To obtain the value in ms, divide the *Maximum System Bus Latency [µs]* by 1000.

If $\mathbf{t}_{Config}$ is less than 6 ms, the value must be set to 6 ms.

The calculated value $\mathbf{t}_{Config}$ must be compared with the real value derived from the online statistics of the Control Panel. The real value depends on the system structure.

If the value calculated for $\mathbf{t}_{Config}$ is greater than the real value, the remaining time will not be used for other cyclic tasks, such as the adoption of an additional CPU for redundancy operation. The remaining time is not included in the cyclic reserve time.

i If the real value is greater than the value calculated for $\mathbf{t}_{Config}$, the parameter located in the resource properties must be corrected (observe the watchdog time) and loaded into the controller by performing a download or reload. Alternatively, a direct online change is also possible. Not correcting the value causes the system handling via PADT to slow down.

9.4.1.3 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 safe SILworX version comparison can be used to determine and prove changes performed to the current project version compared to a previous one.
- For HIQuad X, *Minimum Configuration Version* must be set to *SILworX V10* or higher.

9.4.1.4 Rack 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 *System* tab located in the rack detail view of the SILworX Hardware Editor.

System variables	S [1]	Function	Setting for safe operation
Force Deactivation	Y	Prevents the forcing process from starting and terminates a running forcing process. The default setting is FALSE.	Application-specific
Emergency Stop 1...Emergency Stop 4	Y	Shuts down the controller if faults are detected by the user program. The default setting is FALSE.	Application-specific
Read-only in RUN	Y	After the controller is started, the access permissions are downgraded to *Read-Only*. Exceptions are forcing and reload. The default setting is FALSE.	Application-specific
Reload Deactivation	Y	Locks the execution of reload. The default setting is FALSE.	Application-specific

[1] Safety-related system parameter yes/no (Y/N)

Table 14: Rack 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.

9.4.1.5 Locking and Unlocking the Resource

Locking the resource 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 three system variables *Read-only in Run*, *Reload Deactivation* and *Force Deactivation* are used to lock the PES, see Table 14.

If all three 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 a global variable of type BOOL and set its initial value to FALSE.
2. Assign the global variable as output variable to the three system variables *Read-only in Run*, *Reload Deactivation* and *Force Deactivation*.
3. Assign the global variable to the channel value of a digital input.
4. Connect a key switch to the digital input.
5. Compile the program, load it 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 and other operating functions can be distributed on different keys and persons.

10 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.

10.1 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:

- Input (Function Block Editor), monitoring and documentation.
- Variables with symbolic names and different data types such as BOOL or UINT.
- Assignment of HIQuad X controllers.
- Code generator (for translating the user program into a machine code).
- Hardware configuration.
- Configuration of communication.

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

10.1.1 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.

10.1.1.1 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.

10.1.2 Programming Steps

To program HIQuad X 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.
5. Tests the user programs.

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

10.1.3 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 smaller modules into larger ones and then combining all into a single user program, the user is effectively creating a comprehensive, complex function.

10.1.4 User Program System Parameters

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

System parameters	S[1)]	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 *Code Generation Compatibility* is set to *SILworX V2*, 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 per Cycle [µs]	N	Maximum time in each processor module cycle for executing the user program. Range of values: 0…4 294 967 295 Standard 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 *Safety-related* or *Standard*; the setting is for documentation only and has no effects on the program's performance. Default value: Safety-related	Application-specific
Allow Online Settings	Y	If *Allow Online Settings* is deactivated, the settings of the reamaining program switches cannot be changed online (from within the Control Panel). Only applies if the *Allow Online Settings* switch for the resource is set to TRUE! The default setting is TRUE.	
Autostart.	Y	Enabled type of Autostart: Cold Start, Warm Start, Off. The default setting is warm start.	Application-specific
Start Allowed	Y	TRUE: The PADT may be used to start the user program. The default setting is TRUE. FALSE: The PADT may not be used to start the user program.	Application-specific

System parameters	S[1]	Description		Setting for safe operation
Test Mode Allowed	Y	TRUE:	The test mode is permitted for the user program.	Application-specific[2]
		FALSE:	The test mode is not permitted for the user program. The default setting is FALSE.	
Reload Allowed	Y	TRUE:	The user program reload is permitted. The default setting is 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. The default setting is FALSE.	
Local Force Timeout Response	Y	Behavior of the user program after the forcing time has expired: ▪ Stop Forcing Only. ▪ Stop Program. The default setting is *Stop Forcing Only*.		
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.	
		The default setting for all new projects is *SILworX V7 and higher*.		

[1] The operating system handles the system parameter in a safety-related manner, yes (Y) or no (N)

[2] Once the test mode has stopped, a cold start must be performed prior to starting a safety-related operation!

Table 15: System Parameters of the User Program

10.1.4.1 Notes on 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.

10.1.5 Code Generation

If the user programs and the resource configuration were executed without errors, 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.

10.1.6 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 details on the safe version comparison, refer to the corresponding manual (HI 801 286 E).

10.1.7 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.

10.1.8 Reload

If minor changes were performed to a project, they can be transferred to the controller by performing a reload.

If changes are performed to a user program, 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 ON and the *Reload Deactivation* system variable is set to FALSE.

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.

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!

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 *P0* 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.

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.

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.

10.1.9 Online Test

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

For more information 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).

10.1.10 Test Mode

To diagnose faults, the user programs operating in test mode 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 two 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 used if the *Test Mode Allowed* system parameter is set to TRUE in the corresponding user program.

NOTICE

Failure of safety-related operation possible!

If a user program operating in test mode is stopped, the user program does not provide a safety-related response to the inputs and does not energize the outputs! The outputs are not written to.

The test mode must not be used during safety-related operation!

For safety-related operation, the *Test Mode Allowed* parameter must be set to FALSE!

10.1.11 Changing the System Parameters during Operation

The system parameters specified in Table 16 may be changed during operation (online).

A typical application case is the temporary increase of the watchdog time to be able to perform a reload.

Prior to using an online command to set parameters, make sure that this change will not result in a dangerous state of the plant. If required, organizational and/or technical measures must be 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.

Parameters	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 Response	All

Table 16: Online Changeable Parameters

10.1.12 Forcing

When forcing a global variable, its value is replaced by a force value. A global variable obtains its current value from a physical input, communication or a logic operation. If the variable is forced, its value no longer depends on the process, but is defined by the user.

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

Refer to the system manual (HI 803 211 E) for further details on forcing.

⚠ WARNING

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

- **Forced values may affect the output values of the local controller.**
- **Forced values may also affect other systems' values through safety-related and non-safety-related communication and impact their safety function.**
- **Forcing prolongs the cycle time. This can cause the watchdog time to be exceeded.**

Forcing is only permitted after receiving consent from the test authority responsible for the acceptance test.

Forcing within a plant, e.g., on several systems or performed by several persons, must be planned, coordinated and performed accordingly by the user.

10.1.12.1 Forcing of Data Sources

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

- Physical inputs.
- Communication protocols.
- System variables.

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

1. A global variable A is assigned to one of the forced data sources and therefore the variable is forced. This actually causes the data source to be forced!
2. The assignment is removed. The data source maintains the property *Forced*.
3. The data source is assigned another global variable (global variable B).
4. A reload is performed to load the project change into the controller.

As a result, the **newly assigned** variable B is forced even though this was not intended!

Workaround: First stop forcing variable A.

The channel view of the Force Editor shows which channels have been forced.

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

10.1.13 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.

10.1.14 Multitasking

Multitasking refers to the capability of the HIQuad X 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:

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

The individual user programs operate in an interference-free manner and independently from one another. However, reciprocal influence can be caused by:

- The use of the same global variables in several user programs.
- Unpredictably long runtimes which 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 which strongly affects the user program response time and the response time of the variables written to by the user program.
- Longer evaluation times. A user program evaluates global variables written to by another user program after one CPU cycle at the earliest. 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.

For details on multitasking, refer to the system manual (HI 803 211 E).

10.1.15 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 HIQuad X system that have already been approved.

10.2 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 checklist is available in Microsoft® Word® format on the HIMA website.

11 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.

11.1 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.

11.1.1 Available Protocols and Transmission Medium

The standard protocols listed in the following table can be used in HIQuad X through the communication modules.

Protocol	Fieldbus	TCP/UDP
ComUserTask	X	X
Modbus Master	X	X
Modbus Slave Set	X	X
Modbus Slave Set V2	X	X
PROFIBUS DP Slave	X	-
SNTP Client	-	X
SNTP Server	-	X

Table 17: Available Protocols and Transmission Medium

11.2 Safety-Related safe**ethernet** Protocol

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

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

For further details on safe**ethernet**, 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 correct response from the other controller must be received.

If a correct response is not received from the communication partner within *Receive Timeout*, HIQuad X terminates the safety-related communication. The input variables of this safe**ethernet** connection respond in accordance with the preset parameter *Freeze Data on Lost Connection [ms]*. For safety-related functions, which are implemented via safe**ethernet**, 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, even in case of reload and synchronization.

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

1. **Watchdog time ≤ 1.5 x target cycle time**
2. **Receive timeout ≤ 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.

11.3 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 HIQuad X controllers.

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

Terms

Receive Timeout: Monitoring time of controller 1 (PES 1) within which a correct 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 safe**ethernet** connections. The watchdog time 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 response on the corresponding output (out) of PES 2.

Response time of the HIQuad X controller: For further details on the response time of the HIQuad X controller (resource) t_{RR}, see Chapter 3.2.2.

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.

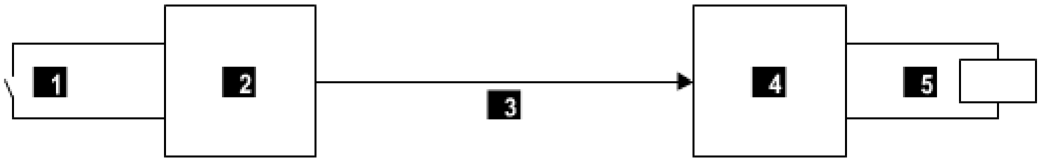
The following conditions apply to the calculations of the maximum response times specified below:

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

The calculations also apply to signals in the opposite direction.

11.3.1 Calculating the Worst Case Response Time of Two HIQuad X Controllers

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



1 Input
2 HIQuad X controller 1
3 Safety-related protocol
4 HIQuad X controller 2
5 Output

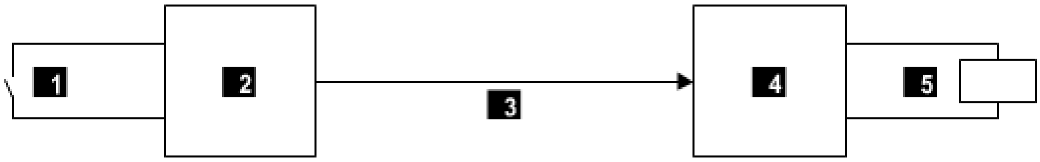
Figure 1: Response Time with Interconnection of 2 HIQuad X Controllers

$T_R = t_{RR1} + t + t_{RR2}$

T_R	Worst Case Response Time
t_{RR1}	Response time of HIQuad X controller 1
T	*Receive Timeout*
t_{RR2}	Response time of HIQuad X controller 2

11.3.2 Calculating the Worst Case Response Time with 1 HIMatrix Controller

The worst case response time T_R is the time between a change on the sensor input signal (in) of the HIQuad X controller and a response on the corresponding output (out) of HIMatrix controller. It is calculated as follows:



1 Input
2 HIQuad X controller
3 Safety-related protocol
4 HIMatrix controller
5 Output

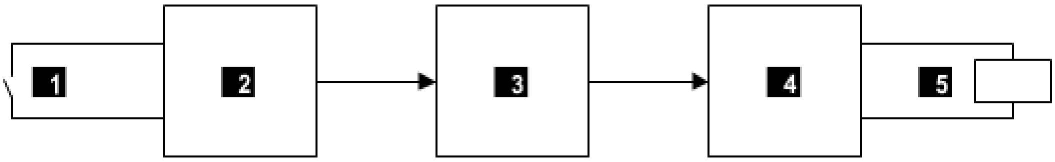
Figure 2: Response Time when 1 HIQuad X and 1 HIMatrix Controllers are Interconnected

$T_R = t_{RR} + t_1 + t_2$

T_R	Worst Case Response Time
t_{RR}	Response time of the HIQuad X controller
t_1	*Receive Timeout*
t_2	2 * Watchdog time of the HIMatrix controller

11.3.3 Calculating the Worst Case Response Time with 2 HIMatrix Controllers or Remote I/Os

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



1 Input
2 Remote I/O 1
3 HIQuad X controller
4 Remote I/O 2
5 Output

Figure 3: Response Time with 2 HIMatrix Controllers or Remote I/Os and 1 HIQuad X Controller

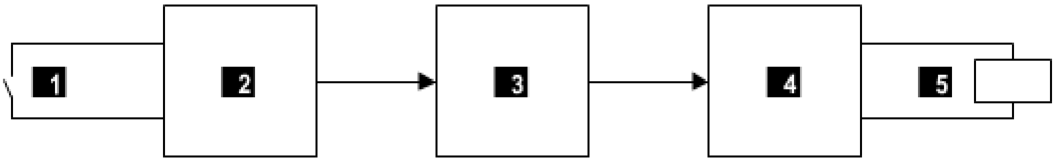
$T_R = t_1 + t_2 + t_{RR} + t_3 + t_4$

T_R Worst Case Response Time
t_1 2 * watchdog time of the HIMatrix controller or the remote I/O 1
t_2 *Receive Timeout1*
t_{RR} Response time of the HIQuad X controller
t_3 *Receive Timeout2*
t_4 2 * watchdog time of the HIMatrix controller or the remote I/O 2

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

11.3.4 Calculating the Worst Case Response Time with 2 HIQuad X and 1 HIMatrix Controllers

The worst case response time T_R is the time between a change on the sensor input signal (in) of the first HIQuad X controller and a response on the corresponding output (out) of the second HIQuad X controller. It is calculated as follows:



1 Input
2 HIQuad X controller 1
3 HIMatrix controller
4 HIQuad X controller 2
5 Output

Figure 4: Response Time with 2 HIQuad X Controllers and 1 HIMatrix Controller

$T_R = t_{RR1} + t_1 + t_2 + t_3 + t_{RR2}$

T_R	Worst Case Response Time
t_{RR1}	Response time of HIQuad X controller 1
t_1	*Receive Timeout1*
t_2	2 * watchdog time of the HIMatrix controller
t_3	*Receive Timeout2*
t_{RR2}	Response time of HIQuad X controller 2

i Both HIQuad X controllers, 1 and 2, can also be identical.
The HIMatrix controller can also be a HIQuad X controller.

11.4 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).

12 Use in Fire Alarm Systems

The HIQuad X 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 HIQuad X 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 inputs and outputs may be used:

- The digital inputs supporting line monitoring and used in the F 3237 and F 3238 input modules.
- The analog inputs supporting line monitoring and used in the F 6217 and F 6221 input modules.

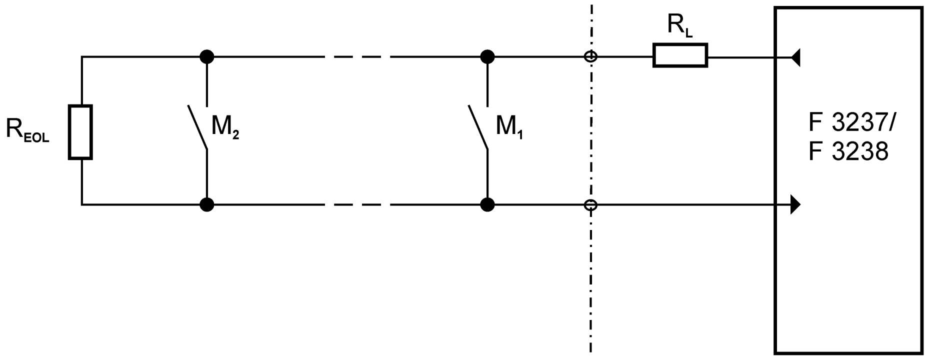
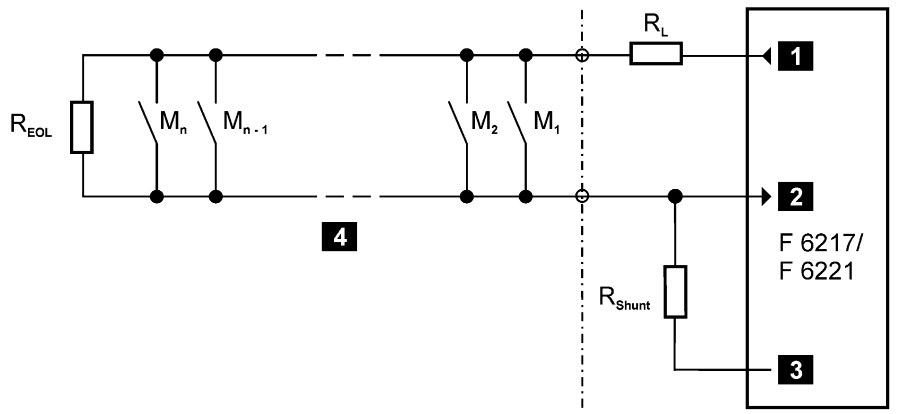


Figure 5: Wiring of Fire Detectors with Digital Inputs



1 Sensor supply	3 Reference potential
2 Analog input	4 Detection loop

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

Figure 6: Wiring of Fire Detectors with Analog Inputs

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.

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

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.

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 output modules or to transmission equipment for fault signaling must occur in accordance with the de-energize to trip principle.

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

HIQuad X 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 HIQuad X 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.

13 Use of HIQuad X Devices in Zone 2

HIQuad X components are suitable for mounting in the explosive atmospheres of zone 2. In addition to the specific conditions of use, the mounting and installation instructions provided in the system manual and in the module-specific manuals must be observed.

The declaration of conformity for HIQuad X components is available on the HIMA website, at www.hima.com/en.

HIQuad X components meet the requirements of the following directives and standards:

Directive	Standard	Description
IECEx	IEC 60079-0:2011	Explosive atmospheres - Part 0: Equipment - General requirements
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"
2014/34/EU	EN 60079-15:2010	

Table 18: Standards for HIQuad X Components in Zone 2

HIQuad X components are provided, e.g., with one of the following Ex marking and specification of the temperature range:

⟨εx⟩ II 3G Ex nA IIC T4 Gc

⟨εx⟩ II 3G Ex nA nC IIC T4 Gc

-25 °C ≤ Ta ≤ +70 °C

Marking	Description
⟨εx⟩	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 19: Ex Marking Description for HIQuad X Components

Special Conditions of Use

1. The HIQuad X components must be installed in an enclosure that fulfils the requirements of IEC 60079-0/EN 60079-0 or IEC 60079-15/EN 60079-15 with degree of protection IP54 or better.
2. The device must be provided with a warning:

   WARNING: 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. HIQuad X components are designed for operation not exceeding pollution degree 2.
4. The enclosure in use must be able to safely dissipate the generated heat.
5. The supply voltages must be taken from power supply units with protective separation. Use power supply units of type PELV or SELV only.
6. The conditions of use provided in the module-specific manuals must be observed.
7. The racks must be provided with forced cooling.

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	Supposing that two input circuits are connected to the same source (e.g., a transmitter). An input circuit is termed interference-free if it does not distort the signals of the other input circuit. In terms of functional safety, the non-safety-related-module has no influence on the safety-related modules
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
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
Rack ID	Rack identification (number)
r_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
SW	Software
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

Index of Tables

Index

MANUAL

Safety

HI 803 209 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

Learn more about HIMA solutions online:

🌐 www.hima.com/en/

HIMA SMART SAFETY.

www.hima.com