HIMA

SMART SAFETY.

Protocol Manual

ISOfast

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

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

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

Contact

HIMA contact details:

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 800 464 D, Rev. 1.02 (1818)	German original document
HI 800 465 E, Rev. 1.02.00 (1821)	English translation of the German original document

Table of Contents

1 Introduction

The ISOfast manual describes the properties of the ISOfast protocol and its configuration in SILworX for the safety-related HIMatrix controller systems.

Knowledge of regulations and the proper technical implementation of the instructions detailed in this manual performed by qualified personnel are prerequisites for planning, engineering, programming, installing, starting up, operating and maintaining the HIMatrix controllers.

HIMA shall not be held liable for severe personal injuries, damage to property or the environment caused by any of the following: unqualified personnel working on or with the devices, de-activation or bypassing of safety functions, or failure to comply with the instructions detailed in this manual (resulting in faults or impaired safety functionality).

HIMatrix automation devices have been developed, manufactured and tested in compliance with the pertinent safety standards and regulations. They may only be used for the intended applications under the specified environmental conditions.

1.1 Structure and Use of This Manual

The manual contains the following chapters:

- Introduction
- Safety
- Product description
- Description of how to configure the ISOfast protocol in SILworX

Additionally, the following documents must be taken into account:

Name	Content	Document no.
HIMatrix safety manual	Safety functions of the HIMatrix system.	HI 800 023 E
HIMatrix system manual	Hardware description of the HIMatrix system.	HI 800 141 E
SILworX first steps manual	Introduction to SILworX.	HI 801 103 E
Communication manual	Communication and description of the controller's Ethernet interfaces.	HI 801 101 E

Table 1: Additional Applicable Manuals

The current manuals can be downloaded from the HIMA website at www.hima.com. The revision index in the footer can be used to compare the manuals in use with the Internet edition and determine if they are up to date.

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 SILworX.
Italics	System parameters and variables.
`Courier`	Literal user inputs.
RUN	Operating states are designated by capitals.
Chapter 1.2.3	Cross-references are hyperlinks even if they are not specially 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 specially marked.

1.3.1 Safety Notices

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

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

⚠ SIGNAL WORD

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

The signal words have the following meanings:

- Warning indicates hazardous situations which, if not avoided, could result in death or serious injury.
- Caution indicates hazardous situation 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.

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.

2 Safety

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

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

2.1 Intended Use

To use the HIMatrix controllers, all pertinent requirements must be met, see Table 1 in the corresponding manuals.

2.2 Residual Risk

No imminent risk results from a HIMatrix system itself.

Residual risk may result from:

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

2.3 Safety Precautions

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

2.4 Emergency Information

A HIMatrix system is a part of the safety equipment of a plant. If the controller fails, the system enters the safe state.

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

2.5 Cyber Security for HIMA Systems

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

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

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 controller!

The controller must be protected against unauthorized access!

For example:

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

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

- Meaningful allocation of user groups.
- 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).
- Use of appropriate passwords.

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

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

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

2.6 User Requirements

To ensure that ISOfast achieves a residual error rate ≤ 1 % SIL 3, the user must comply with the following requirements.

- As long as no ISOfast connection is established through multi-port routers or gateways, they represent network limits.
- On the receiver side, the ISOfast capable devices in use may process a maximum of 1000 messages per second and connection: sample rate per connection 1000 messages/s.
- A network with ISOfast communication may contain a maximum of 1000 storing devices (such as routers, gateways or switches), through which the ISOfast connections are routed.
- The residual error rate of the storing devices used in the ISOfast network (such as routers, gateways or switches) may not exceed 10^{-3}/h.
- If the ISOfast message format TSP1 is used in a network, a maximum of 1000 non-safe devices may be connected to that network. This limit does not apply to the ISOfast message format TSP2.
- To ensure that a safety loop with ISOfast communication achieves a residual error rate ≤ 1 % SIL 3, it may include a maximum of 10 ISOfast connections.
- ISOfast supports the black-channel principle as of IEC 61508 and assumes a bit error probability of 10^{-2} in accordance with IEC 61784-3.
- The network may be shared with other subscribers if sufficient transfer capacity is available. The plant manufacturer and the operator are responsible for ensuring that the Ethernet network used for ISOfast is sufficiently protected against manipulations (e.g., from hackers). The type and extent of the measures must be agreed upon together with the responsible test authority.
- During commissioning and whenever changes are performed during operation (reload), the user must ensure for each ISOfast connection that the process values are transferred as intended prior to starting safety-related operation. Applied to ISOfast, the commissioning and change testing required in the safety manual means that the user must check the following:
  - The assignment of the process values to be transmitted between sender and receiver of a connection uniquely identified via the connection ID must match one other. For example, the user must preclude that variables or parts of variables are swapped or switched.
  - All relevant changes to the ISOfast connections of the HIMA controller are identified in SILworX by the version comparison. This also includes changed variables.

  Changes to the configuration that require such a test are for instance:
  - Changes to the assignment of variables to the input and output data of the ISOfast connection.
  - Internal offset variable shifting due to very different changes:
    - Swapped transmission sequence of ISOfast and SPC connections within an IsoTE connection due to a changed index.
    - ISOfast or SPC connections that are deleted or added within an existing IsoTE connection as well as deletion or addition of new IsoTE connections.
    - Changes to the length of SPCs.

3 Product Description

ISOfast enables HIMA controllers from the HIMatrix F family to exchange process data with third-party systems. ISOfast is certified for safety-related communication up to SIL 3 in accordance with the following standards:

- IEC 61508 Edition 2:2010
- Cat. 4/PL e in accordance with DIN EN ISO 13849-1:2008
- IEC 61784-3:2010 / DIN EN IEC 61784-3:2011

ISOfast is ready to comply with the following standards:

- IEC 61784-3 Ed 3.0, 65C/840/FDIS, 2015-12-18
- IEC 61784-3 Ed 3.0 Amendment 1, 65C/838/CDV, 2016-02-05

The ISOfast protocol supports the black-channel principle as of IEC 61508. To achieve SIL 3, specific requirements must be met, refer to Chapter 2.6 for details.

3.1 System Requirements for Operating ISOfast

Element	Description
Controller and operating system	HIMA controller of the HIMatrix F family CPU operating system ≥ V12.8
Programming tool	SILworX ≥ V8.34
Activation	Software activation code required, see Chapter 8.1.

Table 2: System Requirements for Operating ISOfast

4 Protocol Overview

The ISOfast protocol is used for safety-related communication. ISOfast itself does not depend on the transmission medium used, but requires a subordinate transport protocol for transferring data via Ethernet. These relationships are depicted in Figure 1.

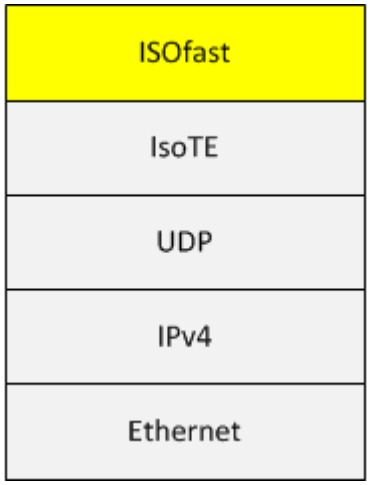


Figure 1: Protocol Layers during ISOfast Transport via Ethernet

An ISOfast connection exchanges data between precisely two nodes. The nodes within the ISOfast connection assume either the role of the master or of the slave; refer to Chapter 4.1 for details.

IsoTE serves as a container for all ISOfast connections between two endpoints, i.e., if multiple ISOfast connections are operated between two devices, they are embedded into one or multiple subordinate IsoTE protocols. Additionally, IsoTE can transfer non-safe data using SPC (standard process container). In turn, IsoTE itself is transported over Ethernet via UDP and IPv4 (with no options or fragmentation).

As long as sufficient transfer capacity is available, other protocols may also be used via the established Ethernet network.

4.1 Master and Slave Roles

The master of an ISOfast connection is responsible for establishing communication. In turn, the slave represents the passive side, i.e., it waits for the master to establish communication.

Additionally, through its configuration, the master determines the essential properties, such as communication timing.

In principle, a device may use several ISOfast nodes, but an ISOfast connection must always have matching master and slave roles.

The roles supported by a device are manufacturer-specific and have to be determined by consulting the respective device manufacturer's documentation.

i HIMA controllers only support the master role.

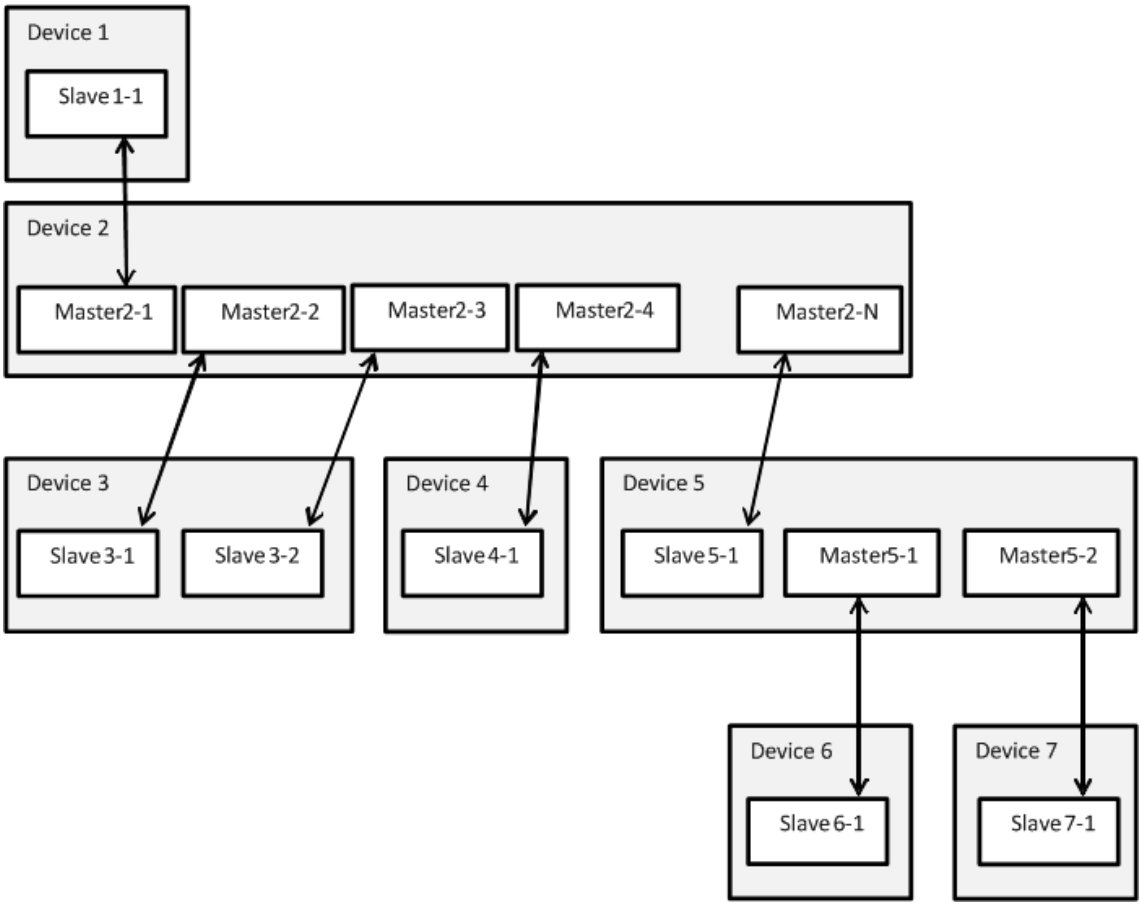


Figure 2: Communication Roles

Figure 2 exemplifies various communication roles within a device.

- Devices 1, 4, 6 and 7 include a single individual slave each.
- Device 2 represents an ISOfast multi-master.
- Device 3 includes two slaves and is therefore an ISOfast multi-slave.
- Device 5 can assume both communication roles.

HIMA controllers support multi-master operation as described for Device 2 in the example.

4.2 Establishing the Connection to ISOfast

The master always initiates the connection to ISOfast by transmitting an open indication to the slave. The open indication contains the slave's parameter settings. The transfer of the open indication may require several messages depending on the output data length. On its part, the slave checks the received open indication and responds with an open response. This, in turn, may require several messages depending on the input data length. This open response contains the result of this check, see Table 9.

To ensure that the connection is rapidly established, the open indication is transferred without the optional data of a slave configuration. Only when the slave requests a slave configuration via the result (CONFIG_DIFFER), the master attempts to establish a new connection with slave configuration transfer.

4.3 Message Formats

ISOfast differentiates between two message formats: TSP1 and TSP2. These two formats differ in the range of values of their parameters, in the transported user data length and in the management information (overhead).

4.4 General User Requirements

During start-up, the user must ensure that the assignment of the slave variables transported via ISOfast and SPC connections to the master variables is implemented as requested.

5 ISOfast

This chapter describes the properties of ISOfast. In particular, the topics of configuration parameters, diagnostics, statuses and response times, as well as the user requirements to be met, are dealt with in greater detail.

5.1 Parameters

This chapter describes the parameters of a single ISOfast connection.

These parameters are set in the SILworX programming tool and loaded into the HIMA controller, see Chapter 7 and Chapter 8.

If a device supports the slave role, the device manufacturer must provide an IDD (ISOfast device description) file. The IDD describes the properties supported by that device. Parts of the parameters specified in Table 3 can therefore be limited by the corresponding IDD. IDD files must not be modified.

Parameter	Description
ConnectionId	Unique ID for a connection between a master and a slave. This must be unique within a communication domain, regardless of the user message format (see below). A communication domain is defined as a logic network within which the safety-related messages are transported. Messages may not be transported beyond this network. Additionally, this unique ID is used to identify the connection and can therefore no longer be changed after its generation, see Chapter 7. Range of values for TSP1 message format: 1…2046 Range of values for TSP2 message format: 1…65534
Message Format	Defines the message format to be used for the connection. Range of values: TSP1 TSP2
OpenTMO [s]	Time in seconds (s) while establishing the connection, within which a valid message must have been received by the connection partner, otherwise the connection is interrupted. Range of values: 2…32 and 512
ActiveWDT [ms]	Time in milliseconds (ms) after successful connection, within which a valid message must have been received by the connection partner, otherwise the connection will be closed. In this case, the associated input data is set to the safety-related initial value. Range of values: 1…500 000

<table>
<tr><td>UseSlaveConfig</td><td>Instructs the master to transfer a slave configuration to the slave when opening the connection.<table><tr><th>Value</th><th>Description</th></tr><tr><td>TRUE</td><td>Configuration process when opening the connection. A setting must be selected for the parameters Slave Configuration Length, Configuration Parameter Signature and Slave Configuration.</td></tr><tr><td>FALSE</td><td>No configuration process when opening the connection. No setting is used for the parameters Slave Configuration Length, Configuration Parameter Signature and Slave Configuration.</td></tr></table>If a configuration process should occur when opening a connection, the configuration must also be specified in the master.</td></tr>
<tr><td>Length of the slave configuration</td><td>If UseSlaveConfig is set to TRUE, this is the length in bytes of the slave configuration.</td></tr>
<tr><td>Configuration Parameter Signature</td><td>If UseSlaveConfig is set to TRUE, this signature must be entered in accordance with the slave default.</td></tr>
<tr><td>SlaveConfiguration</td><td>If UseSlaveConfig is set to TRUE, it is the slave configuration that is transferred from the master to the slave when the connection is being established.
The system supports a maximum of 64-kB slave configurations. A single configuration, however, may use a maximum of 65 000 bytes.</td></tr>
<tr><td>SlaveConfigSignature</td><td>The signature is created during the code generation and represents the properties and configuration of the slave to that connection. This signature is used to check if the configured master and slave match one another.</td></tr>
</table>

Table 3: Parameters of an ISOfast Master

The ISOfast user data volume varies depending on the aforementioned parameters selected for a specific connection and the individual device properties of the slave used. Observe that different data volumes can be transported for each communication direction. However, only a common transport format (TSP1 or TSP2) can be used.

Properties	Description
User Data Volume	Up to the following number of process data can be transported depending on the message format and the slave used: ▪ TSP1: User data = 1…6 bytes ▪ TSP2: User data = 1…238 bytes

Table 4: ISOfast User Data Volume

An ISOfast message such as depicted in Figure 3, includes management information (overhead) and the user data.

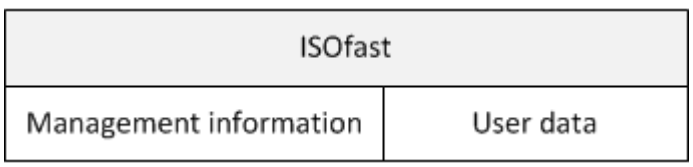


Figure 3: Abstracted ISOfast Message

The size of the management information of an ISOfast message depends on the message format used.

Message format	Overhead in bytes
TSP1	6
TSP2	12

Table 5: ISOfast Overhead

5.2 System Quantities for ISOfast

The HIMatrix system supports the following properties for ISOfast.

Properties	Description
Maximum number of ISOfast connections.	The system supports a maximum of 255 ISOfast connections.
Maximum process data volume for each direction and system	The maximum process data volume, which can be sent and received in total across all ISOfast connections, minus the standard process data (SPC), is 16 384 bytes; refer to Chapter 6.2 for details.

Table 6: System Properties for ISOfast

5.3 Diagnosis and Status

5.3.1 Diagnostic Elements of an ISOfast Connection

For each ISOfast connection, the following information is available online and/or as system variables.

<table>
<tr><th>Element</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td colspan="4">The following statuses and parameters can be assigned global variables and used in the user program.
R/W indicates whether there is only read access or also write access to the contents.</td></tr>
<tr><td>Bad-Receive-Count</td><td>UDINT</td><td>R</td><td>Bad-Receive-Count is the revolving count of rejected ISOfast messages since statistics reset, excluding the rejected resends.</td></tr>
<tr><td>Connected Count</td><td>UDINT</td><td>R</td><td>Connected-Count is the revolving count of how often the protocol stack has successfully established a connection with the ISOfast slave since statistics reset.</td></tr>
<tr><td>ISOfast Control</td><td>BYTE</td><td>W</td><td>This system variable can be used to control the ISOfast connection from within the user program.
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>AUTOCONNECT
(0x00)</td><td>Default value:
After an ISOfast communication loss, the controller automatically attempts to re-establish the connection.</td></tr>
<tr><td>Toggle Mode 0 (0x10)
Toggle Mode 1 (0x11)</td><td>The connection is still disabled after communication loss. The user program can change the toggle mode to re-establish the connection.
Toggle Mode 0 (0x10) set:
Set to Toggle Mode 1 (0x11) to re-establish the connection.
Toggle Mode 1 (0x11) set:
Set to Toggle Mode 0 (0x10) to re-establish the connection.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Element</th><th>Data type</th><th>R/ W</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Disabled (0x80)</td><td>Running ISOfast communication is being closed and remains disabled.</td></tr>
</table>
The value displayed in the online view is only up to date when the system is in the RUN state.
</td></tr>
<tr><td>ISOfast-State</td><td>BYTE</td><td>R</td><td>ISOfast master state for each connection, see Table 8.</td></tr>
<tr><td>ISOfast-Last-Diag</td><td>BYTE</td><td>R</td><td>Provides the last received result of this communication relation since the system has been operating in the RUN state.
The initial value is EMPTY.
Possible variables in accordance with Table 9.</td></tr>
<tr><td>OkBit-Slave</td><td>BOOL</td><td>R</td><td>Slave value transmitted depending on the ISOfast state
<table>
<tr><th>ISOfast-State</th><th>State: OkBit-Slave</th></tr>
<tr><td>0…6</td><td>FALSE</td></tr>
<tr><td>7</td><td>Received slave OkBit.</td></tr>
</table>
</td></tr>
<tr><td>OkBit-Master</td><td>BOOL</td><td>W</td><td>The value of the OkBit-Master system variable is transmitted to the slave in the states SAFE_DATA and VALID_DATA and can be used in accordance with the application, see Table 8. The value displayed in the online view is only up-to-date when the system is in the RUN state.</td></tr>
<tr><td>Response-Time [ms]</td><td>UDINT</td><td>R</td><td>Time in milliseconds (ms) between dispatch of an ISOfast message and receipt of the corresponding acknowledgment.. The minimum, maximum, last and average values are displayed.
If the minimum value is greater that the maximum value, the statistics values are invalid, i.e., the current and average values are 0.

When the statistics are reset, all the values are set to the last value received.

The accuracy of the response time measurement is affected by the fact that the time of receipt is determined in the input phase of the CPU cycle. It thus indicates a response time that is too long by up to n cycles, where n is the number of cycles that the CPU needs to completely process communication.
For further information, refer to the communication time slice described in the communication manual (HI 801 101 E).</td></tr>
<tr><td>Sequence-No</td><td>UDINT</td><td>R</td><td>The Sequence-No serves to ensure the monotone message sequence. This value is the current expectation of the master, i.e., the slave message must comply with it or the message will not be accepted.</td></tr>
<tr><td>Statistics Reset</td><td>BYTE</td><td>W</td><td>Affects the statistics of all the ISOfast and IsoTE connections. These are:
▪ Bad-Receive-Count (for each ISOfast connection)
▪ Response-Time (for each ISOfast connection)
▪ Connected-Count (for each ISOfast connection)
▪ IsoTE-Message-SentCount (for each IsoTE connection)
▪ IsoTE-Message-ReceiveCount (for each IsoTE connection)
▪ IsoTE-Messages-Dropped (for each IsoTE connection)

Reset when the edge changes from 0 to ≠ 0
Range of values: 0...255
Default value: 0

Remark
▪ The statistics are also reset when the state changes from STOP to RUN.</td></tr>
</table>

Element	Data type	R/ W	Description
			▪ The Statistic-Reset system variable may only be used to reset the statistics when the state is RUN.

Table 7: Diagnostic Elements of an ISOfast Connection

5.3.2 ISOfast State

Value	State
The connection is closed	
0	IDLE: The protocol is ready to establish a communication connection as soon as the application demands it. See Table 7 *ISOfast-Control*.
4	WAIT_FOR_REOPEN: The protocol was closed due to an error and waits for a certain time before establishing a new communication connection. This time period is 2 seconds + MAX(OpenTMO, ActiveWDT)
The connection is being opened	
1	OPEN_IND_FRAG: The master transmits the data of the opening phase to the slave.
2	OPEN_RESP_FRAG: The slave has received the data of the opening phase from the master and responds to it. Its response contains its check result. Depending on the result, communication can be aborted or the opening phase can be completed successfully.
The connection transfers process data	
6	SAFE_DATA: The protocol was opened successfully and the master has transmitted the first process data to the slave. The slave response is pending, i.e., the master has not yet received data from the slave. For this reason, the input data associated with communication is set to the safety-related initial value.
7	VALID_DATA: The master received valid data from the slave.
The connection is being closed.	
3	CLOSING_OPEN: The protocol is being closed in the opening phase after a corresponding signal from the application. See Table 7 *ISOfast-Control*.
5	CLOSING_DATA: The protocol is being closed in the data phase after a corresponding signal from the application. See Table 7Table 7 *ISOfast-Control*.
Remark	
ISOfast is not exchanging process data in the states 0…5; the associated input data is set to the safety-related initial value accordingly.	

Table 8: ISOfast State

5.3.3 Slave Result Symbols

Element	Description
0x00:	**OPEN_IND_ABORT**: General signal for connection abort.
0x02	**OPEN_IND_UNDERFLOW**: Signal for connection abort: The slave detects a faulty open indication (too few data).
0x03	**OPEN_IND_OVERFLOW**: Signal for connection abort: The slave detects a faulty open indication (too much data).
0x04	**CONFIG_MISSMATCH**: Signal for connection abort: The slave uses a configuration other than that set by the master and cannot be configured by the master.
0x05	**CONFIG_NOT_SUPPORTED**: Signal for connection abort: The slave does not support configuring by the master.
0x06	**CONFIG_DIFFER**: Signal for connection abort: The slave configuration does not match the master configuration; however, the slave can be configured by the master. Notice: As a response to this result, the master may attempt again to open a connection and transfer the slave configuration.
0x07	**CONFIG_CORRUPTED**: Signal for connection abort: The slave configuration could not be validated successfully.
0x08	**CONFIG_CANNOT_HANDLE**: Signal for connection abort: The slave configuration is rejected for application-specific reasons.
0x09	**PROTO_VERSION_NOT_SUPPORTED**: Signal for connection abort: The master's protocol version is not supported by the slave.
0x0A	**EMPTY**: Default setting.
0xAF	**ACCEPTED**: Connection establishment accepted.

Table 9: Slave Result Symbols

5.4 Response Times

This chapter discusses the safety function response time (SFRT, see Table 10) for the ISOfast protocol.

The allowed SFRT depends on the process and must be agreed upon together with the competent test authority.

5.4.1 Prerequisites

1. *Max. Com. Time Slice ASYNC [ms]* must be set so that only one communication time slice at a time is used on the HIMA controllers; refer to the communication manual (HI 801 801 E) for details.
2. The signals transmitted via ISOfast or safe**ethernet** must be processed in the corresponding controllers within one CPU cycle.
3. In the following examples, the formulas for calculating the SFRT only apply if the safety time is set as follows in the HIMatrix controllers used: Safety Time = 2 * Watchdog Time.

5.4.2 Definitions

Term	Description
ActiveWDT	See Table 3.
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 communication connections. The watchdog time (WDT) must be entered in the resource properties. All instructions on the watchdog time specified in the HIMatrix safety manual must be observed.
Safety Function Response Time	The SFRT is the maximum time that a physical output on controller B requires to issue a response to a changed physical input signal (In) on another controller A, even if errors occurred in one or several parts of the communication chain.
MaxDataAgeIn	Maximum age of the data when it is entered in the ISOfast message. This value must be specified by the device manufacturer. Consult the manufacturer documentation of the used input device to obtain this value.
MaxDataAgeOut	This value corresponds to the maximum estimate of the two following cases: ▪ Time between the receipt of an Input_Data_Response message and the effect of the contained data at the output. ▪ Time after ActiveWDT has expired and the safe values are effective at the output, under the boundary condition that the affected device has failed shortly before the effect sets in at the outputs. This value must be specified by the device manufacturer. Please consult the manufacturer documentation of the output device used to obtain this value. *In HIMatrix F*03, MaxDataAgeOut = 2 * WDT CPU + WorstCaseOff (for physical outputs)*

WorstCaseOff	Maximum time required to cause the physical outputs of an ISOfast or safe**ethernet** node to enter the safe state after it failed. This value must be specified by the device manufacturer. Please consult the manufacturer documentation of the output device used to obtain this value. *For HIMatrix F*03/HIMax, this value is specified in the data sheets; also refer to the communication manual (HI 801 101 E) for details.*

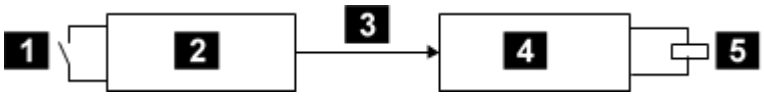
Table 10: Definitions of the Elements Required for the SFRT Calculation

i The SFRT does not necessarily apply to the entire safety loop.

5.4.3 HIMatrix with a Connection to a Third-Party Device

In this scenario, SFRT refers to exactly one communication connection.

5.4.3.1 HIMatrix as Input Device

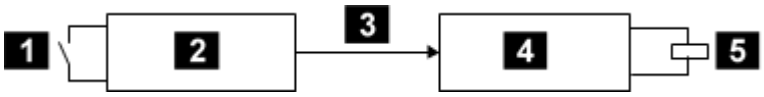


1 Input
2 HIMatrix
3 ISOfast protocol
4 Third-party device
5 Output

Figure 4: SFRT for HIMatrix as Input Device

$SFRT = MaxDataAgeIn_{HIMatrix} + 2 * ActiveWDT_{ISOfast\ Connection} + MaxDataAgeOut_{Third\text{-}Party\ Device}$

5.4.3.2 HIMatrix as Output Device



1 Input
2 Third-party device
3 ISOfast protocol
4 HIMatrix
5 Output

Figure 5: SFRT for HIMatrix as Output Device

$SFRT = MaxDataAgeIn_{Third\text{-}Party\ Device} + 2 * ActiveWDT_{ISOfast\ Connection} + MaxDataAgeOut_{HIMatrix}$

5.4.4 HIMatrix as Data Agent between Two Additional Controllers

In this scenario, a third-party device is used as input device. This device communicates via ISOfast with a HIMatrix controller that uses an additional protocol (ISOfast or safe**ethernet**) to forward the data to a further controller as output device. This means that the HIMatrix serves as data agent between input and output device; whether the HIMatrix subjects the input device data to additional processing is irrelevant as long as this is done within a cycle.

In this scenario, SFRT refers to the complete data transmission chain, i.e., with both communication connections.

5.4.4.1 ISOfast as Additional Protocol

1 Input
2 Third-party device 1
3 ISOfast connection 1
4 HIMatrix
5 ISOfast connection 2
6 Third-party device 2
7 Output

Figure 6: SFRT with ISOfast as Additional Protocol

$SFRT = MaxDataAgeIn_{Third\text{-}Party\ Device1} + 2 * ActiveWDT_{ISOfast\ Connection1} + 2 * WDT_{HIMatrix} + 2 * ActiveWDT_{ISOfast\ Connection2} + MaxDataAgeOut_{Third\text{-}Party\ Device2}$

5.4.4.2 safe**ethernet** as Additional Protocol:

The worst case response time (TR) for safe**ethernet** is specified in the communication manual. This value is required for calculating the SFRT. In this context, consider that the communication manual gives different scenarios for the communication nodes. The TR provided in the scenario with one communication connection and one HIMatrix controller as input device is the value required for the calculation used in this chapter. The output device must be used in accordance with the system required by the user.

The TR value includes two times the watchdog time of the input devices. These two cycles correspond to the two WDT-CPU cycles of the HIMatrix (data agent) in the calculation of the SFRT below. The cycles are based on the timeout detection sampling (ActiveWDT). This means that the two WDT CPU cycles are not taken into account in the SFRT since they are already included in the TR.

The communication manual does not describe a scenario in which a HIMax serves as an output device and a HIMatrix as an input device; therefore the scenario with 3 controllers (HIMax - HIMatrix - HIMax) is recommended.
Thus the calculation refers to parts of the equation presented in the communication manual. In this case, two times the value of the watchdog time is also included in the calculation.

HIMatrix as Output Device

If a HIMatrix is used as output device, the required scenario is depicted in the communication manual (HI 801 101 E), in the section on how to calculate the worst case response time of 2 HIMatrix controllers (Chapter safe**ethernet**).

1 Input
2 Third-party device
3 ISOfast connection
4 HIMatrix
5 safe**ethernet** connection
6 HIMatrix
7 Output

Figure 7: SFRT with safe**ethernet** as Additional Protocol

SFRT = $MaxDataAgeIn_{\text{Third-Party Device}} + 2 * ActiveWDT_{\text{ISOfast Connection}} + TR_{\text{safe}\textbf{ethernet}\text{ Connection}} + WorstCaseOff_{\text{HIMatrix Output Module}}$

HIMax as Output Device

If a HIMax is used as output device, the corresponding scenario is depicted in the communication manual (HI 801 101 E), in the section on how to calculate the worst case response time with 1 HIMatrix and 2 HIMax controllers (Chapter safe**ethernet**).

1 Input
2 Third-party device
3 ISOfast connection
4 HIMatrix
5 safe**ethernet** connection
6 HIMax
7 Output

Figure 8: SFRT with safe**ethernet** as Additional Protocol

SFRT = $MaxDataAgeIn_{\text{Third-Party Device}} + 2 * ActiveWDT_{\text{ISOfast Connection}} + 2 * WDT_{\text{CPU HIMatrix}} + t4_{\text{safe}\textbf{ethernet}\text{ Connection}} + t5_{\text{safe}\textbf{ethernet}\text{ Connection}} + WorstCaseOff_{\text{HIMax Output Module}}$

6 IsoTE

This chapter describes the properties of IsoTE. In particular, the topics of configuration parameters, diagnostics and statuses are dealt with in greater detail.

6.1 Basic IsoTE Structure and Resulting Quantities

IsoTE is used as transport layer for ISOfast and SPC connections via Ethernet. IsoTE transports IsoTE fragments. In turn, a fragment may include an ISOfast or an SPC frame.

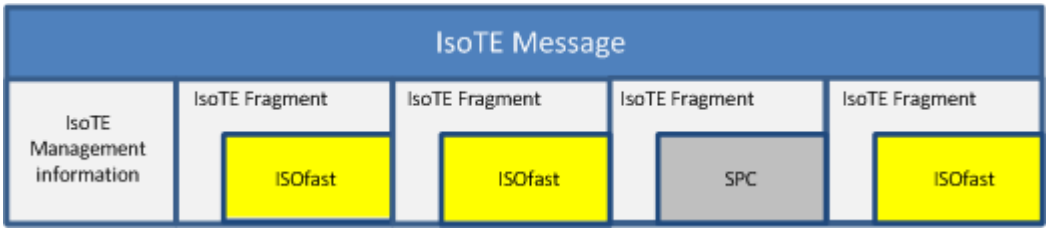


Figure 9: Basic Structure of an IsoTE Message

The following table specifies the management information (overhead) of all the components of an IsoTE message. These are needed to determine the number of user data that can be transferred with an IsoTE connection in one direction.

IsoTE components	Overhead in bytes
IsoTE management information	5
IsoTE fragment with ISOfast	1
IsoTE fragment with SPC	1

Table 11: IsoTE Overhead

The user data that can be transmitted via IsoTE must comply with two framework conditions:

1. The sum of ISOfast and SPC frames (which are not IsoTE fragments, but the frames they include) may not exceed 1300 bytes.
   This means that the user data and management information must be added for each included frame. The sum must be ≤ 1300 bytes:

   $$RL = \sum_{i=1}^{IFI}[NFAST_i + OV_i] + \sum_{j=1}^{IFS} NSPC_j \leq 1300$$

RL	Frame length
IFI	Number of IsoTE fragments with ISOfast frame
$NFAST_i$	User data of the (i) ISOfast fragment
OV_i	Overhead (management information in bytes) of the (i) ISOfast fragment, see Table 5
IFS	Number of IsoTE fragments with SPC frame
$NSPC_j$	User data of the (j) SPC fragment

2. The total length of the IsoTE message may not exceed 1458 bytes. This means that the frame length of the IsoTE fragments increased by the management information may not exceed this value:

   $$ITG = RL + \sum_{i=1}^{IF} ITO_i \leq 1458$$

ITG	IsoTE total length
RL	According to formula in point 1
IF	Number of IsoTE fragments
ITO_i	IsoTE overhead of the i. IsoTE fragment, see Table 11

6.2 Standard Process Data (SPC)

Standard process data refers to process data that is not transferred securely (as defined by the standards specified in Chapter 3). The user must be aware that this data may be faulty or outdated, e.g., due to transmission errors or time constraints. For this reason, no safety-relevant data may be transferred via SPC.

The SPC frame only includes user data and no management information. This means that the subordinate protocol has no information about the structure or semantics of the transported data.

SPC	Overhead in bytes
SPC management information	0

Tabl 12: SPC Overhead

6.2.1 System Quantities for SPCs

The HIMatrix system supports the following properties for SPCs.

Properties	Description
Maximum number of SPCs	The system supports a maximum of 255 SPCs.
Maximum standard process data volume for each direction and system	The maximum standard process data volume (SPC), which can be sent and received altogether across all SPCs, minus the ISOfast process data, is 16 384 bytes; refer to Chapter 5.2 for details.

Table 13: System Properties for SPCs

6.3 Parameters

This chapter describes the parameters of a single IsoTE connection. Additionally, it explains the resulting properties of IsoTE.

These parameters are set in the SILworX programming tool and loaded into the HIMA controller, see Chapter 7.

If a device supports the slave role, the device manufacturer must provide an IDD (ISOfast device description) file. The IDD describes the properties supported by that device. Parts of the parameters specified in Table 14 can therefore be limited by the corresponding IDD. IDD files must not be modified.

The IDD files include the following details:

- General manufacturer-specific details (serial number, order number, version, etc.), just informative for the user.
- ISOfast modules: Process data layout, ISOfast parameters (message format, etc.), default values and range of values for parameters (e.g., OpenTMO).
- SPC modules: Process data layout.
- IsoTE connections: Potential bundle of ISOfast and SPC modules.

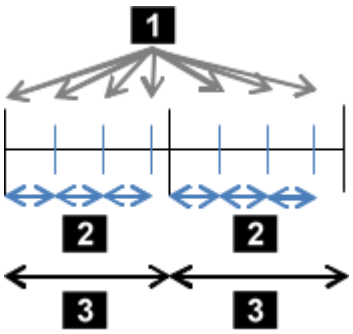
Parameter	Description
IsoTE-ConnectionId	Unique ID for a connection between two controllers. The ID must be unique within a communication domain, i.e., an IsoTE-ConnectionId must not be used for more than one connection. A communication domain is defined as a logic network within which the safety-related messages are transported. Messages may not be transported beyond this network. Additionally, this unique ID is used within HIMatrix to identify the IsoTE connection and can therefore no longer be changed after its generation, see Chapter 7. Range of values: 1…65535
IsoTE-Port	Port number used by the HIMatrix controller to receive inbound IsoTE messages. Range of values: 1…65534
IsoTE-ProductionRate [ms]	Minimum distance between two new IsoTE messages of a connection. If the value is 0, a new message is issued in each cycle, refer to Chapter 6.3.2 for details. Range of values: 0…2^{31}-1 milliseconds
IsoTE-Rate [ms]	Minimum distance of two subsequent resends of an IsoTE message, refer to Chapter 6.3.2 for details.
IsoTE-RemoteIP	Unicast IP address of the connection partner.
IsoTE-RemotePort	Port number used by the connection partner to receive inbound IsoTE messages. Range of values: 1…65534
IsoTE Resends	Displays how many times a message has been resent, refer to Chapter 6.3.1 for details.
Maximum process data volume for each direction and IsoTE connection	See Chapter 5.2.

Table 14: Parameter of an IsoTEs

6.3.1 Relationship between IsoTE Resends, IsoTE-Rate and IsoTE-ProductionRate

The number of IsoTE resends, the IsoTE rate and the IsoTE production rate are mechanisms that, on the one hand, control message losses in the network and, on the other hand, protect the network and, in particular, the IsoTE communication subscribers against too many IsoTE messages resent from one source.

i Inaccuracies may occur in connection with rates due to sampling and load shifting effects. Accordingly, messages may be sent with delay. This is a normal behavior and no system error.



1 IsoTE Resends (send time on the subordinate Ethernet)

2 IsoTE-Rate

3 IsoTE-ProductionRate

Figure 10: Relationship between IsoTE Resends, IsoTE-Rate and IsoTE-ProductionRate

IsoTE-ProductionRate indicates the update interval of the process data in send direction. This means that a new IsoTE message with new content is created every IsoTE ProductionRate milliseconds.

The IsoTE rate indicates the minimum distance between resends. A message created based on IsoTE-ProductionRate is repeated in accordance with IsoTE-Rate, but no more than IsoTE Resends.

IsoTE-ProductionsRate must be set to a value less than ((IsoTE Resends+1)*IsoTE-Rate). The inaccuracies of both the sender and the receiver must be taken into account. If this aspect is ignored, connection problems may occur at ISOfast level.

IsoTE Resends * IsoTE-Rate < min. ActiveWDT modules should apply to the ISOfast connections contained in the IsoTE message. IsoTE messages repeated in intervals longer than ActiveWDT are useless since the communication partner has either already received the message or has already closed the connection.

Similarly, IsoTE Resends * IsoTE-Rate < min. OpenTMO should apply to the ISOfast connections contained in the IsoTE message.

Remark:

1. *The system does not stop resending an IsoTE message if it has processed a response message to an ISOfast associated with this IsoTE since the evaluation of a suitable ISOfast message is too complex if several ISOfast connections are used in an IsoTE connection.*
2. *A check of whether IsoTE-ProductionRate has expired is performed once per cycle. If it has expired, a new message is sent with updated data mapping. No resends are sent in this period.*
3. *Due to the load distribution in the system and external load surcharges, the resends are likely to be sent not exactly at equidistant intervals. This means that inaccuracies as well as jitter effects with respect to the transmission times are likely to occur.*
   This does not affect the achievement of the objective mentioned above for the resends (see the chapter beginning).
4. *When configuring the IsoTE resends and the IsoTE rate, the user must observe that the system limits the number of IsoTE resends per millisecond:*
   No more than 8000 bytes are sent per millisecond.

6.3.2 Impact of Resends and Production Rate on the Subordinate Network

The number of IsoTE resends and the IsoTE production rate are two mechanisms to control message losses in the network and protect the network against too many messages. Between sent messages, IsoTE maintains the IsoTE-ProductionRate. Due to the load deferment, messages might be sent with a certain delay. This is a normal behavior and no system error.

6.4 System Quantities for IsoTE

The HIMatrix system includes the following properties for IsoTE.

Properties	Description
Number of IsoTE Connections	The system supports a maximum of 255 IsoTE connections.

Table 15: System Quantities for IsoTE

6.5 Diagnosis and Status

For each IsoTE connection, the following information is available online and/or as system variables.

Element	Data type	R/W	Description
The following statuses and parameters can be assigned global variables and used in the user program. R/W indicates whether there is only read access or also write access to the contents. A hyphen indicates that the value is not available as a system variable.			
IsoTE-Messages-Dropped	UDINT	-	IsoTE-Messages-Dropped is the revolving count of rejected IsoTE messages since statistics reset, excluding the rejected resends. Only unsuitable messages are included in this counter. This is for example the case if the IsoTE message structure configured in the communication partner is different or if the IsoTE parameters are incorrectly configured, see Chapter 6.3.1.
IsoTE-Message-Receive-Count	UDINT	-	IsoTE-Messages-ReceiveCount is the revolving count of properly received and processed messages since statistics reset, excluding their resends.
IsoTE-Message-SentCount	UDINT	-	IsoTE-Messages-SentCount is the revolving count of sent messages since statistics reset, including their resends.
IsoTE Control	BOOL	W	Use this system variable to control the IsoTE connection from within the user program.

Value	Description
TRUE	Deactivate the IsoTE connection. Neither received messages are delivered to IsoTE nor are messages sent to the communication partner. Included ISOfast connections are closed. The ISOfast connections of the communication partner are closed as soon as its ActiveWDT has expired. The input process variables in ISOfast and SPC adopt the corresponding initial values.
FALSE	Activate the IsoTE connection. Default value.

Table 16: Diagnosis and Status

7 Reload

The use of reload for changing the resource configuration must be agreed upon with the competent test authority! For further details on reload, refer to the HIMatrix safety manual (HI 800 023 E).

i The safe version comparison must be used to check changes to the ISOfast configuration **before** the program is loaded to the controller. Additionally, the general user requirements apply, see Chapter 2.6.

The ISOfast connection ID and the IsoTE connection ID are identifiers of the connections in the controller. They cannot be modified for an existing connection in the PES. If a controller loads a new configuration set for an existing connection during reload, the parameters contained in the configuration to be loaded are allocated to that connection. This means that the existing connection adopts the new parameters.

Illegal parameter changes are rejected during reload.

i In this information box, ID is used to refer to ConnectionId and IsoTE-ConnectionId.

Irrespective of whether connections in SILworX are deleted, changed or added: As soon as the controller can use the ID of an existing connection to assign the parameter set, this parameter set is adopted in the connection, if permitted.

Changing an ID in SILworX to a value not contained in the loaded configuration means that the previous connection is deleted and a new connection with changed ID is added.

i Changing the name of a connected global variable that is assigned to the system or process variables of an ISOfast, IsoTE or SPC connection causes a restart with the initial values after the reload.

7.1 ISOfast / SPC

During the reload process, ISOfast and IsoTE connections can generally be added or deleted.

The number of ISOfast connections contained in the controller during reload can be greater than configured. Not only the added ISOfast connections are held, but also the deleted ISOfast connections since they must remain active until the reload is completed.

The maximum number of simultaneous ISOfast connections during reload is limited to 300 (a maximum of 255 ISOfast connections + 45 reload buffer connections):

The following parameter settings can be changed for an existing ISOfast connection.

- ActiveWDT
- OpenTMO

i Changing the ISOfast parameters *ActiveWDT* and *OpenTMO* through a reload interrupts an existing ISOfast connection, but has no impact on other ISOfast connections. The modified ISOfast connection can be reopened with the changed parameters *ActiveWDT* and *OpenTMO*. The connection re-opening can be controlled using the system variable *ISOfast Control*, see Table 7.

i Only when the reload is acknowledged after a download, the PADT may deliver information about a possible connection interruption due to a change of at least ActiveWDT or OpenTMO.

i Changing the name of an ISOfast or SPC connections has no impact on reload.

i Changing the SPC ID causes the contained process variables to be started after reload with initial values instead of process values.

i If the variables sequence within an existing SPC module is changed through reload, the assignment will only be done properly again once the slave has been adjusted accordingly.

7.2 IsoTE

During the reload process, IsoTE connections can generally be added or deleted.

The number of IsoTE connections contained in the controller during reload can be greater than configured. Not only the added IsoTE connections are held, but also the deleted IsoTE connections since they must remain enabled until the reload is completed.

The maximum number of IsoE connections that are simultaneously held during reload is limited to 300 (a maximum of 255 IsoTE connections + 45 reload buffer connections):

The following parameter settings can be changed for an existing IsoTE connection.

- IsoTE-ProductionRate
- IsoTE-Port
- IsoTE-Rate
- IsoTE-RemoteIP
- IsoTE-RemotePort
- IsoTE Resends

i Changing *IsoTE-RemoteIP, IsoTE-RemotePort* or *IsoTE-Port* through reload may cause the ISOfast connections operated via IsoTE to be lost.

Additionally, the aggregation of ISOfast and SPC connections can change within the IsoTE connections, i.e., ISOfast and SPC connections can be added, deleted and moved within an IsoTE.

If an ISOfast connection is moved to another IsoTE connection, the process and system variables of that ISOfast connection still run with the corresponding values after a reload.

In contrast, moving SPC connections to another IsoTE connection causes the process and system variables to adopt the initial values after reload.

Changing the IsoTE aggregation through reload may cause the ISOfast connections operated via IsoTE to be lost.

A change of the aggregation can be avoided by using a new IsoTE connection.

The system issues a warning if smooth operation of an IsoTE connection cannot be ensured and offers the opportunity to abort the reload if one of the following parameters would change through the reload:

- IsoTE-RemoteIP
- IsoTE-RemotePort
- IsoTE-Port
- Aggregation of an IsoTE connection

The IsoTE connections are considered in alphabetical order when the configuration is generated. This causes a change in the ke.config (refer to the version comparator for details). The process data, however, is not initialized through reload.

8 Creating the ISOfast Protocol in SILworX

8.1 Registering and Activating the Protocol

The software activation code with the required liceses is generated on the HIMA website using the system ID of the controller (e.g., 60000). Follow the instructions provided on the HIMA website!
www.hima.com-> Products-> Registration-> Options SILworX

i The license is intrinsically bound to the system ID. A license can only be used once for a specific system ID. For this reason, only activate the code when the system ID has been uniquely defined.

A software activation code may include a maximum of 32 licenses. It is also possible to specify multiple activation codes in the license management. A maximum of 64 licenses may be loaded into one controller.

To enter the software activation code in SILworX

1. In the structure tree, select **Configuration, Resource, License Management**.
2. Right-click **License Management** and select **New, License Ke**y from the context menu.
   ☑ A new license key is created.
3. Right-click the **license key** and select **Properties** from the context menu.
4. Enter the new software activation code in the **Activation Code** field.

8.2 Creating the IDD Device Description Set in the *Library* Directory

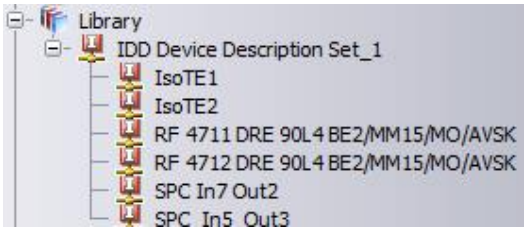


Figure 11: IDD Device Description Set in the SILworX Structure Tree

To create the IDD device description set

1. In the structure tree, select **Library**.
2. From the Library context menu, select **New**, **IDD Device Description Set** to add a new IDD device description set.
3. From the context menu of IDD Device Description Set, select **New** and read the IDD device description set file associated with the ISOfast slave.

8.3 Creating the ISOfast Protocol

ISOfast can be configured within the Protocols directory of a resource.

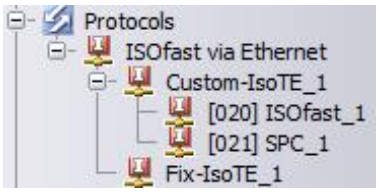


Figure 12: ISOfast Protocol in the SILworX Structure Tree

To create the ISOfast protocol via Ethernet

1. In the structure tree, select **Configuration, Resource, Protocols**.
2. Select **New, ISOfast via Ethernet** from the context menu of Protocols to add a new ISOfast protocol.
3. Select **Edit** from the context menu of *ISOfast via Ethernet* to open the *ISOfast Overview Editor* (see Chapter 9.1).
4. The following parameters must be set in the *Properties* tab:
   - *IsoTE-Port*: 1…65534
   - *Module*: Select the processor module for ISOfast master

8.4 Creating Custom-IsoTE

Custom-IsoTE means that the users can configure the bundle of ISOfast and SPC modules.

To create the Custom-IsoTE type

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**, **ISOfast via Ethernet**.
2. Select **New, Custom-IsoTE** from the context menu of *ISOfast via Ethernet* to add a new Custom-IsoTE element.
3. Select **Edit** from the context menu of *Custom-IsoTE* to open the *IsoTE Connection Editor*. The *Modules* tab includes a list of the created *ISOfast* and *SPC Modules* (refer to Chapter 9.2 for details).
4. The following parameters must be set in the *Properties* tab:
   - *IP Address (Partner)*: 1.0.0.0…223.255.255.255 (except: 127.x.x.x).
   - *IsoTE-Port (Partner)*: 1…65534 (Preset value: 740)
   - *Connection ID*: 1…65535

8.4.1 Creating the ISOfast Modules

An ISOfast module serves for transferring safe process data.

To create ISOfast

1. In the structure tree, select **Configuration, Resource, Protocols, ISOfast via Ethernet, Custom-IsoTE**.
2. Select **New, ISOfast** from the context menu of *Custom-IsoTE* to add a new ISOfast element.
3. Select **Edit** from the context menu of *ISOfast* to open the *ISOfast Module Editor*.
   The *ISOfast Module Editor* contains the tabs *Process Variables*, *System Variables* and *Properties*.
4. The following parameters must be set in the *Properties* tab:
   - *Index*: 0…2^{31}-1
   - *Connection ID:* See Table 3 (ConnectionId).
   - *ActiveWDT [ms]*: See Table 3 (ActiveWDT [ms]).

– *OpenTMO [s]*: See Table 3 (OpenTMO [s]).

8.4.1.1 Assigning the IDD Module Reference

1. In the structure tree, select **Configuration, Resource, Protocols, Custom-IsoTE**.
2. Select **Edit** from the context menu of *Custom-IsoTE* to open the *IsoTE Connection Editor*.
3. In the *Modules* tab, right-click **ISOfast** and select **Assign IDD Module Reference** from the context menu.
4. In the *Assign New IDD Module Reference* dialog box, select the IDD Module Reference associated with the *ISOfast Module* and confirm the action.

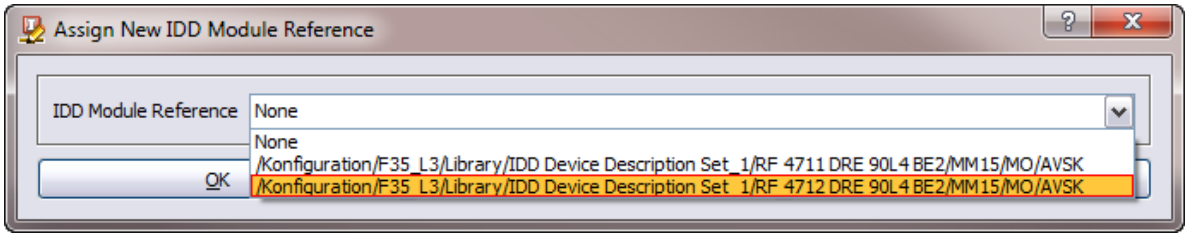


Figure 13: The Assign New IDD Module Reference Dialog Box

i The configuration file for the ISOfast module can be obtained from the manufacturer of the ISOfast slave.

8.4.1.2 Importing the Slave Configuration

It only exists in ISOfast modules with the *Use Slave Configuration* parameter set to TRUE.

1. In the **Modules** tab, right-click **ISOfast** to open the context menu.
2. Select **Import Slave Configuration** from the context menu of ISOfast and choose the `slave configuration file` for the ISOfast module.

1. In the structure tree, select **Configuration, Resource, Protocols, Custom-IsoTE**.
2. Select **Edit** from the context menu of *Custom-IsoTE* to open the *IsoTE Connection Editor*.
3. In the *Modules* tab, right-click **ISOfast** and select **Import Slave Configuration** from the context menu.
4. In the *Import Slave Configuration* dialog box, select the `file` associated with the *ISOfast Module* and confirm the action.

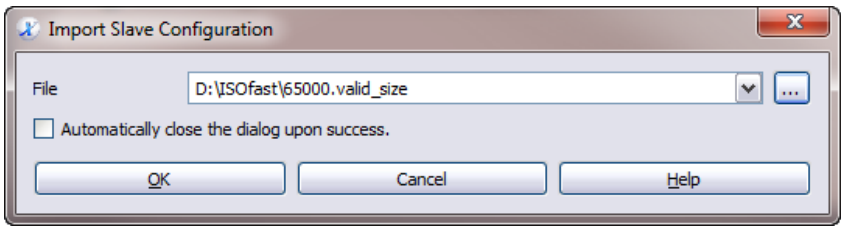


Figure 14: Import Slave Configuration

8.4.1.3 Assigning the Safe Process Variables

The safe process variables are based on the IDD module reference of the ISOfast module and fixed in the *Process Variables* tab. For use in the user program, the safe process variables can be connected to global variables.

To open the ISOfast Module Editor

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**, **ISOfast via Ethernet**, **Custom-IsoTE**, **ISOfast**.
2. Select **Edit** from the context menu of *ISOfast* to open the *ISOfast Module Editor*.
3. Select the **Process Variables** tab in the *ISOfast Module Editor.*

To connect the input signals

To connect the input signals, select the suitable global variable in the Object Panel and drag it onto the required **input signal**.

To connect the output signals

To connect the output signals, select the suitable global variable in the Object Panel and drag it onto the required **output signal**.

8.4.2 Creating the SPC Modules

An SPC module (standard process data containers module) serves for transferring non-safe process data.

To create the SPC module

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**, **ISOfast via Ethernet**, **Custom-IsoTE.**
2. Select **New, SPC** from the context menu of *Protocols* to add a new SPC.
3. Select **Edit** from the context menu of *SPC*.
4. The *SPC Module Editor* contains two tabs: the *Process Variables* and the *Properties* tabs.
5. The following parameters must be set in the *Properties* tab:
   - *Index*: 0…2^{31}-1
   - *SPC ID*: See Table 25.

8.4.2.1 Assigning the IDD Module Reference

1. In the structure tree, select **Configuration, Resource, Protocols, Custom-IsoTE**.
2. Select **Edit** from the context menu of *Custom-IsoTE* to open the *IsoTE Connection Editor*.
3. In the *Modules* tab, right-click **SPC** and select **Assign IDD Module Reference** from the context menu.
4. In the *Assign New IDD Module Reference* dialog box, select the IDD Module Reference associated with the *SPC Module* and confirm the action.

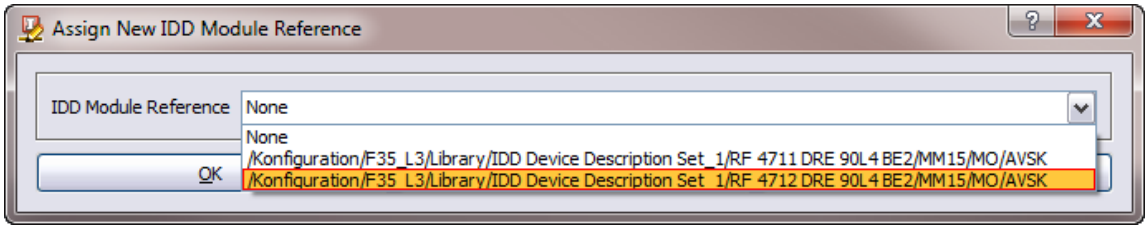


Figure 15: The Assign New IDD Module Reference Dialog Box

i The configuration file for the SPC module can be obtained from the manufacturer of the ISOfast slave.

8.4.2.2 Assign the Non-Safe Process Variables

The non-safe process variables are based on the IDD module reference of the SPC module and fixed in the *Process Variables* tab. For use in the user program, the non-safe process variables can be connected to global variables.

To open the SPC Module Editor

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**, **ISOfast via Ethernet**, **Custom-IsoTE**, **SPC**.
2. Select **Edit** from the context menu of *SPC* to open the *SPC Module Editor*.
3. Select the Process Variables tab in the *SPC Module Editor.*

To connect the input signals

To connect the input signals, select the suitable global variable in the Object Panel and drag it onto the required **input signal**.

To connect the output signals

To connect the output signals, select the suitable global variable in the Object Panel and drag it onto the required **output signal**.

8.5 Creating Fix-IsoTE

The *Fix-IsoTE* type means that the bundle of ISOfast and SPC modules is only provided by the *IDD device description*.

To create Fix-IsoTE

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**, **ISOfast via Ethernet**.
2. Select **Edit** from the context menu of *ISOfast via Ethernet* to open the *IsoTE Overview Editor*.
3. Right-click the **Fix-IsoTE** type and select **Assign IDD Device Description** from the context menu.
4. In the *Assign New IDD Device Description* dialog box, select the IDD Device Description associated with the *Fix-IsoTE* element and confirm the action.

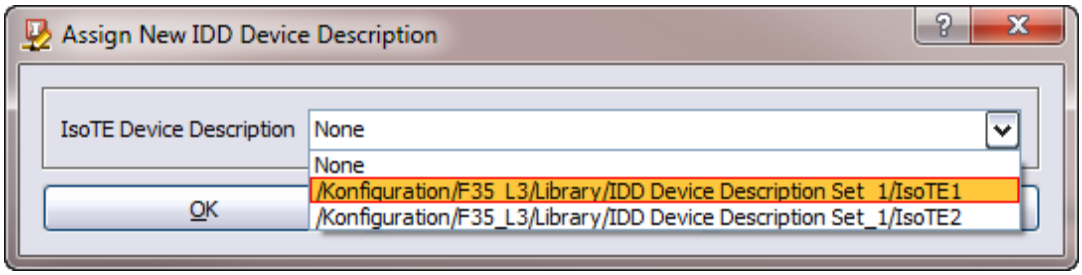


Figure 16: The Assign New IDD Device Description Dialog Box

i The configuration file can be obtained from the manufacturer of the ISOfast slave.

5. Select **Edit** from the context menu of *Fix-IsoTE* to open the *IsoTE Connection Editor*.
6. The *Modules* tab includes a list of the ISOfast and SPC modules that were assigned through the IDD device description.
7. The following parameters must be set in the *Properties* tab:
   - *IP Address (Partner)*: 1.0.0.0…223.255.255.255 (except: 127.x.x.x).
   - *IsoTE-Port (Partner)*: 1…65534
   - *Connection ID*: 1…65535

8.5.1 ISOfast and SPC Modules

The aggregation of ISOfast and SPC modules is fixed and provided by the *IDD Device Description*.

The *ISOfast Modules* and *SPC Modules* are configured as in the IsoTE type *Custom-IsoTE*, refer to Chapter 8.4.1 and Chapter 8.4.2 for details.

9 Description of the ISOfast Configuration Editors

This section describes the characteristics of the HIMA ISOfast master and the menu functions and dialog boxes required for configuring the HIMA ISOfast master in SILworX.

9.1 ISOfast via Ethernet (ISOfast Overview Editor)

ISOfast via Ethernet can be configured within the *Protocols* directory of a resource.
Select **Edit** from the context menu of *ISOfast via Ethernet* to open the *ISOfast Overview Editor*. The *ISOfast Overview Editor* contains the list of all the IsoTE connections to this master. The editor includes the tabs *Iso-TE Connections, System Variables* and *Properties*.

9.1.1 The IsoTE Connections tab

The following parameters are used for configuring the IsoTE connections.

The grayed-out fields in SILworX cannot be applied to the corresponding type.

Element (editor)	Description
Type	An IsoTE has the property IsoTE Type. The following types of IsoTE connections exist. ▪ Fix-IsoTE: The aggregation of ISOfast and SPC is only determined by the IDD device description. ▪ Custom-IsoTE: The aggregation of ISOfast and SPC is determined by the user.
Name	The name can be changed.
connection ID	See Table 14 (IsoTE-ConnectionId).
IP Address (Partner)	See Table 14 (IsoTE-RemoteIP).
IsoTE Port (Partner)	See Table 14 (IsoTE-RemotePort).
Production Rate [ms]	See Table 14 (IsoTE-Production-Rate).
Resends	See Table 14 (IsoTE Resends).
Resend Interval [ms]	See Table 14 (IsoTE-Rate).
IDD Device Description	See Glossary.

Table 17: IsoTE Connections

9.1.2 The System Variables Tab

The following system variables can be assigned global variables and used in the user program.

Element	Data type	Description
Statistics Reset	BYTE	See Table 7 (Reset).

Table 18: System Variables

9.1.3 The Properties Tab

The **Properties** tab contains the following parameters for configuring the IsoTE connections on the master side.

Element	Description
Type	ISOfast via Ethernet.
Name	ISOfast via Ethernet.
IsoTE-Port	An ISOfast root has the IsoTE-Port property. All the IsoTE connections of the protocol send and receive data via this port. Range of values: 1...65534 Default value: 739
Module	Connected processor module for ISOfast master. The ISOfast master can be assigned a processor module using a context menu.

Table 19: Properties

9.2 Custom-IsoTE (IsoTE Connection Editor)

In the structure tree, a Custom-IsoTE element is located below *ISOfast via Ethernet* and is used to configure a Custom-IsoTE.

Select **Edit** from the context menu of *Custom-IsoTE* to open the *IsoTE Connection Editor*.

The *IsoTE Connection Editor* contains the list of all the ISOfast and SPC modules associated with this Custom-IsoTE. The editor includes the tabs *Modules, System Variables* and *Properties*.

9.2.1 The Modules Tab

Right-click the ISOfast or SPC module and use the context menu to assign the *IDD Module Reference* and *Slave Configuration*.

The grayed-out fields in SILworX cannot be applied to the corresponding type (ISOfast or SPC).

Element	Description
Type	ISOfast or SPC.
Name	The name can be changed.
Index	Table 24.
Connection ID	
SPC ID	See Table 25.
ActiveWDT [ms]	See Table 3 (ActiveWDT [ms]).
OpenTMO [s]	See Table 3 (OpenTMO [s]).
Use Slave Configuration	See Table 3 (UseSlaveConfig).
Length of the configuration parameters [bytes].	See Table 3 (length of the configuration parameters [bytes]).
Signature of the configuration parameters.	See Table 3 (signature of the configuration parameters).
IDD Module Reference	Is assigned using the *Assign New IDD Module Reference* context menu function. References to an IDD module from a corresponding IDD device description set within the scope. For further information, refer to the glossary.

Table 20: Custom-IsoTE Modules

9.2.2 The System Variables Tab

Element	Data type	Description
Control	BOOL	See Table 16 (IsoTE-Control).

Table 21: Custom-IsoTE System Variables

9.2.3 The Properties Tab

Element (editor)	Description
Type	Custom-IsoTE. The aggregation of ISOfast and SPC is determined by the user.
Name	The name can be changed.
Connection ID	See Table 14 (IsoTE-ConnectionId).
IP Address (Partner)	See Table 14 (IsoTE-RemoteIP).
IsoTE Port (Partner)	See Table 14 (IsoTE-RemotePort).
Production Rate [ms]	See Table 14 (IsoTE-Production-Rate).
Resends	See Table 14 (IsoTE Resends).
Resend Interval [ms]	See Table 14 (IsoTE-Rate).

Table 22: Custom-IsoTE Properties

9.3 ISOfast Module (ISOfast Module Editor)

In the structure tree, an ISOfast module is located below the Custom-IsoTE element and is used to configure an ISOfast module for safe process data transmission.

Select **Edit** from the context menu of *ISOfast* to open the *ISOfast Module Editor*.

The editor includes the tabs *Process Variables, System Variables* and *Properties*.

9.3.1 The Process Variables Tab

The safe process variables are based on the IDD module reference of the ISOfast module and fixed in the *Process Variables* tab. For use in the user program, the safe process variables can be connected to global variables.

- To connect the input signals, select the suitable global variable in the Object Panel and drag it onto the required input signal.
- To connect the output signals, select the suitable global variable in the Object Panel and drag it onto the required output signal.

9.3.2 The System Variables Tab

The following system variables can be assigned global variables and used in the user program.

Element	Data type	Description
Bad-Receive-Count	UDINT	See Table 7.
Connected Count	UDINT	
Control	BYTE	
Last-Diag	BYTE	
OkBit-Master	BOOL	
OkBit-Slave	BOOL	
Response-Time [ms]	UDINT	
Sequence-No	UDINT	
SlaveConfigSignature	DWord	SlaveConfigSignature is calculated for each ISOfast module during code generation. This is adopted in the system configuration.
State	BYTE	ISOfast state for each connection. See Table 8.

Table 23: System Variables

9.3.3 The Properties Tab

Element (editor)	Description
Type	ISOfast or SPC.
Name	The name can be changed.
Index	Each ISOfast has a unique module index determining the position of the module within the surrounding IsoTE connections. Range of values: 1...231-1 Default value: 0
IDD Module Reference	See Table 20.
Message Format	See Table 3 (Message Format).
SafetyFunctionID	ID that is assigned by the device manufacturer with manufacturer ID and function ID, and that the PADT includes in the calculation of SlaveConfigSignature during code generation. The SafetyFunctionID is provided by the manufacturer in the IDD.
ActiveWDT [ms]	See Table 3 (ActiveWDT [ms]).

Element (editor)	Description
OpenTMO [s]	See Table 3 (OpenTMO [s]).
Use Slave Configuration	See Table 3 (UseSlaveConfig).
Length of the configuration parameters [bytes].	See Table 3 (length of the configuration parameters [bytes]).
Signature of the configuration parameters.	See Table 3 (signature of the configuration parameters).
Connection ID	See Table 3 (ConnectionId).
Input Data Length [Bytes]	Indicates the data length of the ISOfast module in input and output direction. This is provided by the IDD, see also Table 4.
Output Data Length [Bytes]	

Table 24: Properties

9.4 SPC Module (SPC Module Editor)

In the structure tree, an SPC module is located below the Custom-IsoTE element and is used to configure an SPC module for non-safe process data transmission.

The **Edit** context menu function is used to open the *SPC Module Editor*. The editor includes the tabs *Process Variables* and *Properties*.

9.4.1 The Process Variables Tab

The non-safe process variables are based on the IDD module reference of the SPC module and fixed in the *Process Variables* tab. For use in the user program, the non-safe process variables can be connected to global variables.

- To connect the input signals, select the suitable global variable in the Object Panel and drag it onto the required input signal.
- To connect the output signals, select the suitable global variable in the Object Panel and drag it onto the required output signal.

9.4.2 The Properties Tab

Element	Description
Type	SPC (standard process data containers) for non-safe process data.
Name	The name can be changed.
Index	Table 24.
IDD Module Reference	
SPC ID	The SPC ID is the identifier of the SPC module and must be unique. Range of values: 1...65534 Default value: 0
Input Data Length [Bytes]	Range of values: 2…1300 bytes Default value: 0
Output Data Length [Bytes]	

Table 25: Properties

9.5 Creating Fix-IsoTE in SILworX

The *Fix-IsoTE* type means that the bundle of ISOfast and SPC modules is only provided by the IDD device description.

In the structure tree, a *Fix-IsoTE* element is located below *ISOfast via Ethernet* and is used to configure a *Fix-IsoTE*. The Fix-IsoTE Editor is opened with the **Edit** context menu function. The editor includes the tabs *Modules, System Variables* and *Properties*.

9.5.1 The Modules Tab

The *Fix-IsoTE Overview Editor* contains the list of all the ISOfast and SPC modules associated with this *Fix-IsoTE*. The grayed-out fields in SILworX cannot be applied to the corresponding type (ISOfast or SPC).

Element	Description
Type	ISOfast or SPC
Name	The name can be changed.
Index	Not changeable
Connection ID	See Table 24.
SPC ID	See Table 25.
ActiveWDT [ms]	See Table 3 (ActiveWDT [ms]).
OpenTMO [s]	See Table 3 (OpenTMO [s]).
Use Slave Configuration	Not changeable
Length of the configuration parameters [bytes].	Not changeable
Signature of the configuration parameters.	See Table 3 (signature of the configuration parameters).
IDD module reference	See Table 24.

Table 26: Modules

9.5.2 The System Variables Tab

Element	Data type	Description
Control	BOOL	See Table 16 (IsoTE-Control).

Table 27: Fix-IsoTE System Variables

9.5.3 The Properties Tab

Element (editor)	Description
Type	Fix-IsoTE: The aggregation of ISOfast and SPC is only determined by the IDD device description.
Name	The name can be changed.
IDD Device Description	See Glossary.
IP Address (Partner)	See Table 14 (IsoTE-RemoteIP).
IsoTE Port (Partner)	See Table 14 (IsoTE-RemotePort).
Production Rate [ms]	See Table 14 (IsoTE-Production-Rate).
Resends	See Table 14 (IsoTE Resends).
Resend Interval [ms]	See Table 14 (IsoTE-Rate).

Table 28: Properties

10 Views and Diagnostics in the Control Panel

The Control Panel appears after a successful system login.

The *ISOfast* node collects the details on the *ISOfast via Ethernet* protocol operation.

10.1 IsoTE Online Pane

The IsoTE online pane displays the IsoTE connections of the *ISOfast* master:

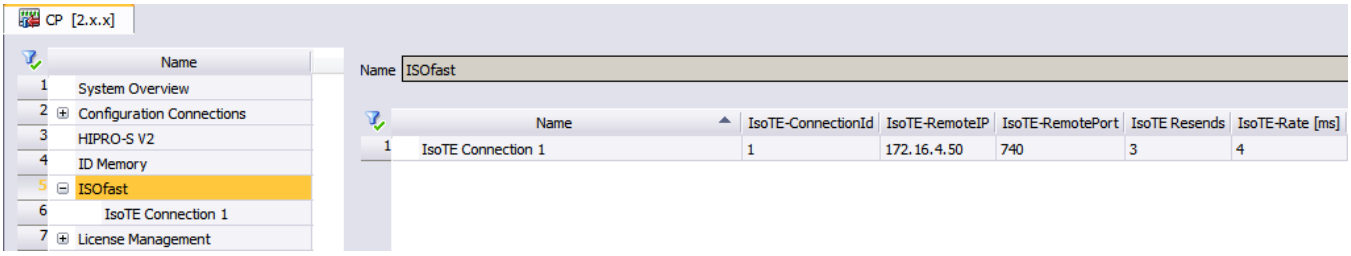


Figure 17: The IsoTE Online Pane

The following table specifies all the column elements that are available for online diagnostics of the IsoTE connections. For further details on the IsoTE connection elements, see Chapter 9.2.

Element (online)	Description
IsoTE-ConnectionName	The name can be changed.
IsoTE-ConnectionId	See Table 14.
IsoTE-RemoteIP	
IsoTE-RemotePort	
IsoTE Resends	
IsoTE-Rate	
IsoTE-Production-Rate	
IsoTE-Message-SentCount	See Table 16.
IsoTE-Message-ReceiveCount	
IsoTE-Messages-Dropped	
IsoTE Control	

Table 29: All Elements of the IsoTE Online Pane

10.2 ISOfast Modules Online Pane

For the selected IsoTE connection, the ISOfast online pane displays the ISOfast modules used for the master.

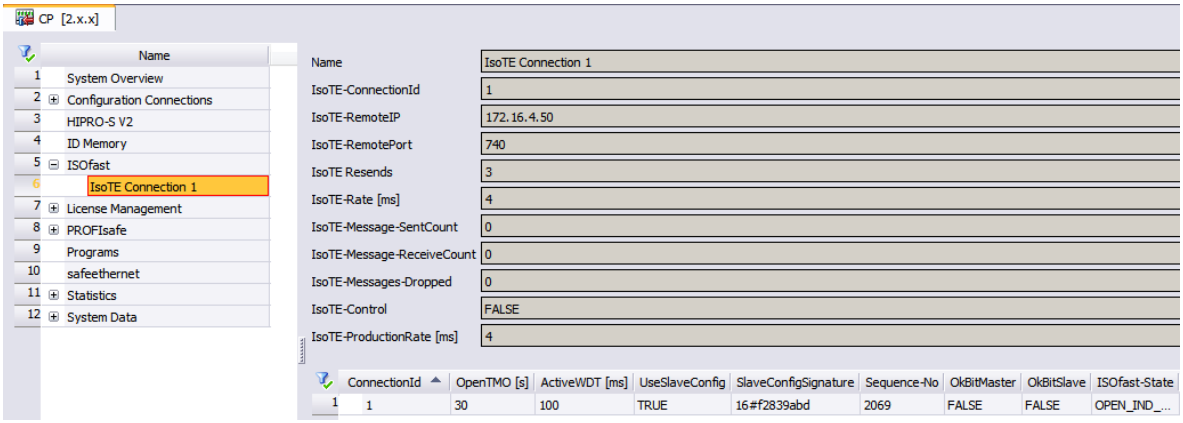


Figure 18: The ISOfast Modules Online Pane

The following tables specifies all the column elements that are available for online diagnostics of the ISOfast modules. For further details on the IsoTE connection elements, see Chapter 9.3.

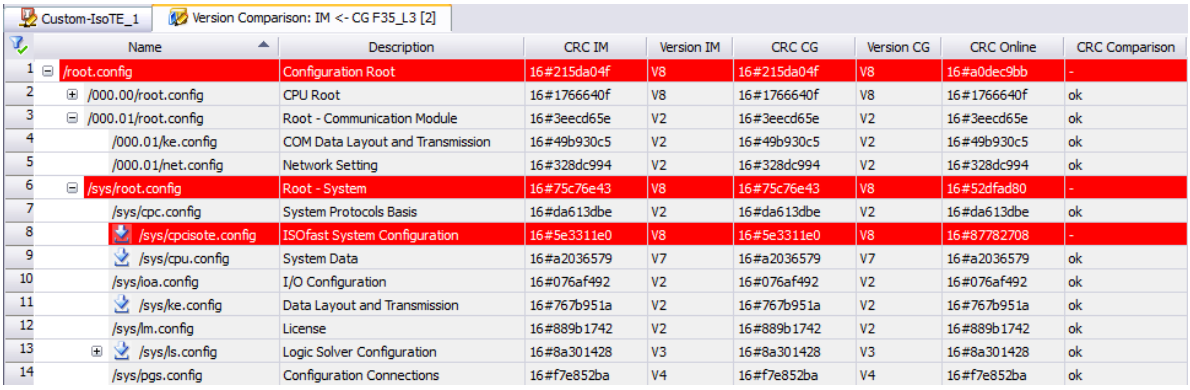
Element (online)	Description
ConnectionId	See Table 3.
OpenTMO	
ActiveWDT	
UseSlaveConfig	
Signature of the configuration parameters	
SlaveConfigSignature	
Sequence-No	See Table 7 (Sequence-No).
OkBitMaster	See Table 7 (OkBit-Master).
OkBitSlave	See Table 7 (OkBit-Slave).
ISOfast-State	See Table 7 (ISOfast-State).
ISOfast-Last-Diag	Displays the last diagnostic entry, refer to Chapter 5.3.3 for details.
Response-Time-Min	Displays the last, average, minimum and maximum response time values. See also Table 7.
Response-Time-Max	
Response-Time-Last	
Response-Time-Avg	
Bad-Receive-Count	See Table 7.
Connected Count	
ISOfast Control	

Table 30: All Elements of the ISOfast Online Pane

11 Version Comparison

The version comparison is based on the project checksums (CRCs) created by the code generator. For further information, refer to the version comparison manual (HI 801 286 E).

During a version comparison, different resource configurations are compared to one another and the differences between the individual configuration files are detected. The result of the version comparison has SIL 3 quality and is based on the configuration files describing the executable code.



	Name	Description	CRC IM	Version IM	CRC CG	Version CG	CRC Online	CRC Comparison
1	/root.config	Configuration Root	16#215da04f	V8	16#215da04f	V8	16#a0dec9bb	-
2	/000.00/root.config	CPU Root	16#1766640f	V8	16#1766640f	V8	16#1766640f	ok
3	/000.01/root.config	Root - Communication Module	16#3eecd65e	V2	16#3eecd65e	V2	16#3eecd65e	ok
4	/000.01/ke.config	COM Data Layout and Transmission	16#49b930c5	V2	16#49b930c5	V2	16#49b930c5	ok
5	/000.01/net.config	Network Setting	16#328dc994	V2	16#328dc994	V2	16#328dc994	ok
6	/sys/root.config	Root - System	16#75c76e43	V8	16#75c76e43	V8	16#52dfad80	-
7	/sys/cpc.config	System Protocols Basis	16#da613dbe	V2	16#da613dbe	V2	16#da613dbe	ok
8	/sys/cpcisote.config	ISOfast System Configuration	16#5e3311e0	V8	16#5e3311e0	V8	16#87782708	-
9	/sys/cpu.config	System Data	16#a2036579	V7	16#a2036579	V7	16#a2036579	ok
10	/sys/ioa.config	I/O Configuration	16#076af492	V2	16#076af492	V2	16#076af492	ok
11	/sys/ke.config	Data Layout and Transmission	16#767b951a	V2	16#767b951a	V2	16#767b951a	ok
12	/sys/lm.config	License	16#889b1742	V2	16#889b1742	V2	16#889b1742	ok
13	/sys/ls.config	Logic Solver Configuration	16#8a301428	V3	16#8a301428	V3	16#8a301428	ok
14	/sys/pgs.config	Configuration Connections	16#f7e852ba	V4	16#f7e852ba	V4	16#f7e852ba	ok

Figure 19: ISOfast in the Version Comparison

The relevant configuration files for the ISOfast protocol, which are specified in Table 31, are located within the *sys/root.config* configuration file.

Line	Configuration file	Description
4	/sys/root.config	Main file for the CPU module. This configuration file is referenced to subordinated configuration files and always changes if one of the subordinated file is modified.
6	/sys/cpcisote.config	ISOfast parameters, connection properties.
9	/sys/ke.config	Configuration file for assigning (using) global variables to hardware, protocols, POUs, etc. (ke = communication endpoint = global variable). View for ISOfast: ▪ ISOfast connection ID ▪ System variable name ▪ Source and target ▪ Type of change

Table 31: ISOfast Configuration Files

12 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.
Logistic+/ 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//

Appendix

Glossary

Term	Description
Aggregation	Bundle of independent objects.
CRC	Cyclic redundancy check.
Device description set	SILworX object with IDDs in the Library directory.
EN	European standard.
IDD	ISOfast device description(s) are XML files that are provided by the manufacturer of the ISOfast slave. These files must not be modified. They describe the ISOfast device and IsoTE connections, as offered by the manufacturer. ▪ IDD describes - General manufacturer-specific details (serial number, order number, version, etc.), just informative for the user. - ISOfast modules: Process data layout, ISOfast parameters (TSP level, etc.), default values and range of values for parameters (e.g., OpenTMO). - SPC modules: Process data layout. - IsoTE connections: Potential bundle of ISOfast and SPC modules. ▪ Use of IDD: - Reading of IDD files in the IDD device description set. - Deletion of IDD objects from the IDD device description set. - Use of several device description sets. - Use in various libraries. - Usage scope.
IEC	International electrotechnical commission, organization that prepares and publishes international standards for all electrical, electronic and related technologies
ISOfast connection	The ISOfast connection is the safety-related logic connection between ISOfast master and ISOfast slave
ISOfast master	In an ISOfast connection, the ISOfast master is the communication send point responsible for opening the connection
ISOfast module	The ISOfast module transports safe data via IsoTE (ISOfast slave)
ISOfast slave	In an ISOfast connection, the ISOfast slave is the communication send point that is opened by the master
ISOfast via Ethernet	ISOfast is the protocol name
IsoTE	ISOfast transport via Ethernet, transport channel for ISOfast and SPC via Ethernet
IsoTE master	The IsoTE master describes a communication partner of the IsoTE slave
IsoTE slave	The IsoTE slave describes the master's communication partner to which the master operates the ISOfast transport channel
PADT	Programming and debugging tool (in acc. with IEC 61131-3), PC with SILworX
PELV	Protective extra low voltage
PES	Programmable electronic system
R	Read
R/W	Read/Write
Rack ID	Base rack identification (number)
SELV	Safety extra low voltage
SIL	Safety integrity level, in accordance with IEC 61508
SILworX	Programming tool for HIMA systems
SPC module	The SPC module transports non-safe data via IsoTE
SW	Software
TMO	Timeout
W	Write
WD	Watchdog
WDT	Watchdog time

Index of Figures

Index of Tables

MANUAL
ISOfast protocol
HI 801 465 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/

www.hima.com