COMMITTENTE:

RFI RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE

ALTA SORVEGLIANZA:

ITALFERR
GRUPPO FERROVIE DELLO STATO ITALIANE

GENERAL CONTRACTOR:

IRICAV2

INFRASTRUTTURE FERROVIARIE STRATEGICHE DEFINITE DALLA LEGGE OBIETTIVO N. 443/01

LINEA A.V. /A.C. TORINO – VENEZIA Tratta VERONA – PADOVA

Lotto funzionale Verona – Bivio Vicenza

PROGETTO ESECUTIVO

Telecomando Periferico - STES

UCP 2

Manuali Apparecchiature Principali

GENERAL CONTRACTOR		DIRETTORE LAVORI	
IL PROGETTISTA INTEGRATORE Ing. **Giovanni MALAVENDA** *ALBO INGEGNERI PROV. DI MESSINA* n. **4503** Data: 01/08/2022	Consorzio Iricav Due Ing. Paolo Carmona Data: 01/08/2022	Valido per costruzione Data:	SCALA: n/a

COMMESSA	LOTTO	FASE	ENTE	TIPO DOC.	OPERA/DISCIPLINA	PROGR.	REV.	FOGLIO
IN17	12	E	I2	MI	TP0000	K20	A	001 DI 395

CONSORZIO SATURNO
High Speed Railway Technologies

VISTO CONSORZIO SATURNO	
Firma	Data
A.M. DE SIMONE	01/08/2022

Progettazione :

Rev	Descrizione	Redatto	Data	Verificato	Data	Approvato	Data	IL PROGETTISTA
A	Prima Emissione	C.DeLosSantos	01/08/2022	G. Melli	01/08/2022	M. Albertini	01/08/2022	ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MILANO DOTT. ING. MANTA NICOLA Sez. A Settori: n° A 29[illegible] Data: 01/08/2022
B								
C								

CIG. 8377957CD1	CUP: J41E91000000009	File: IN1712EI2MITP0000K20A00.doc
		Cod. origine:

Progetto cofinanziato dalla Unione Europea

Applicabilità

Il presente documento si applica ai quadri UCP 2 degli impianti STES delle gallerie da realizzarsi presso la Linea A.V./A.C. Torino-Venezia Tratta Verona- Padova Lotto funzionale Verona-Bivio Vicenza.
In particolare, il presente documento è da ritenersi applicabile alle seguenti WBS/Gallerie.

WBS	Descrizione	Competenza
TP02	TELECOMANDO PERIFERICO - STES - Galleria San Martino Buon Albergo	COLAS

Tabella 1 – Elenco WBS

Allegati

La tabella seguente fornisce l'elenco degli allegati al presente documento.

Codice	Descrizione	Pag.
19056_T00_M_202_02	Sistema STES - 3kV UCP 2 - Manuali apparecchiature principali	3÷395

Tabella 2 – Elenco Allegati

COLAS RAIL

ITALIA

Sistema STES - 3kV

UCP 2
MANUALI APPARECCHIATURE PRINCIPALI

Categoria	**RISERVATO**
Codifica	19056_T00_M_202
Revisione	02
Data	08/06/2022
Pagine	393

IL PROGETTISTA

Data: 08/06/2022

G. MELLI	08/06/2022	A. TOSCANI	08/06/2022	N. MANTA	08/06/2022
Redatto	**Data**	**Verificato**	**Data**	**Approvato**	**Data**

Indice

INDICE DELLE TABELLE

INDICE DELLE FIGURE

Non applicabile

1 INTRODUZIONE

1.1 SCOPO

Il presente documento raccoglie i manuali dei principali componenti impiegati nel quadro UCP 2.

1.2 APPLICABILITÀ

Questo documento si applica ai quadri UCP 2 del Sistema STES di COLAS Rail. Tale documento è da ritenersi applicabile sia all'applicazione generica sia all'applicazione specifica.

1.3 TERMINI, ACRONIMI E ABBREVIAZIONI

La tabella seguente fornisce la definizione dei termini, degli acronimi e delle abbreviazioni impiegati nel presente documento.

Acronimo	Definizione
COLAS	Colas Rail Italia S.p.A.
IS	Impianti di Segnalamento e Sicurezza
TE	Trazione Elettrica
STES	Sezionamento elettrico e messa a terra di sicurezza della linea di contatto
UCP	Unità di Comando e controllo Principale per TE
UCS-QS	Unità di Comando e controllo Secondaria per QS
UCS-DMBC	Unità di Comando e Controllo Secondaria per DMBC/DMQC e QCC
UCS-IMS	Unità di Comando e controllo Secondaria per IMS

Tabella 1 – Termini, acronimi e abbreviazioni

1.4 DOCUMENTI DI RIFERIMENTO

1.4.1 Leggi norme

Ref.	Ente	Codice	Rev.	Titolo
N01	CEI EN	CEI EN 50126-1	01/10/2019	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS). Parte 1 Processo generale RAMS
N02	CEI EN	CEI EN 50126-2	01/05/2019	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS). Parte 2 Approccio di sistema per la sicurezza

Ref.	Ente	Codice	Rev.	Titolo
N03	CEI EN	CEI EN 50128	01/11/2011	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane Sistemi di telecomunicazione, segnalamento ed elaborazione - Software per sistemi ferroviari di comando e di protezione.
N04	CEI EN	CEI EN 50128/EC	01/08/2014	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane Sistemi di telecomunicazione, segnalamento ed elaborazione - Software per sistemi ferroviari di comando e di protezione. Errata corrige
N05	CEI EN	CEI EN 50128/A1	01/07/2020	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane Sistemi di telecomunicazione, segnalamento ed elaborazione - Software per sistemi ferroviari di comando e di protezione. Addendum 1
N06	CEI EN	CEI EN 50129	01/04/2020	Applicazioni ferroviarie, tranviarie, filo tramviarie e metropolitane Sistemi di comunicazione, segnalamento ed elaborazione – Sistemi elettronici di sicurezza per il segnalamento.
N07	CEI EN	CEI EN 50159	01/02/2012	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane Sistemi di telecomunicazione, segnalamento ed elaborazione - Comunicazioni di sicurezza in sistemi di trasmissione.
N08	CEI EN	CEI EN 50159/A1	01/12/2020	Applicazioni ferroviarie, tranviarie, filoviarie e metropolitane Sistemi di telecomunicazione, segnalamento ed elaborazione - Comunicazioni di sicurezza in sistemi di trasmissione.
N09	CEI EN	CEI EN 61508-6	02/2011	Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza Parte 6: Linee guida per l'applicazione della IEC 61508-2 e della IEC 61508-3

Tabella 2 – Leggi/Norme

1.4.2 Specifiche RFI

Rif.	Ente	Codice	Rev.	Data	Titolo
n/a	n/a	n/a	n/a	n/a	n/a

Tabella 3 – Specifiche RFI

Per le specifiche RFI fare riferimento al documento citato al § 1.4.3 del presente documento.

1.4.3 Documenti

Rif.	Ente	Codice	Rev.	Titolo
D01	COLAS	19056_T00_X_001	-	Sistema STES – 3kV Elenco elaborati
D02	COLAS	19056_T00_S_000	-	Sistema STES – 3kV Specifiche RFI di riferimento

Tabella 4 - Documenti

1.5 DESCRIZIONE DELLE MODIFICHE RISPETTO ALLA REVISIONE PRECEDENTE

Rev. 01

Non applicabile alla prima versione.

Rev. 02

Aggiornamento a seguito commenti BV ricevuti in data 08/06/2022 - Aggiunto doc. HIMA Communication - Configuration in SILworX.

2 MANUALI APPARECCHIATURE PRINCIPALI

01 - ALIMENTAZIONE			
Descrizione	***Produttore***	***Cod.***	***Pag.***
Alimentatore QUINT4-PS/1AC/24DC/10	PHOENIX CONTACT	2904601	8÷58
Buffer capacitivo QUINT4-CAP/24DC/10/8KJ	PHOENIX CONTACT	2320571	59÷90
Modulo ridondanza QUINT4-S-ORING/12-24DC/1X40	PHOENIX CONTACT	2907752	91÷111
02 - INTERRUTTORI			
n/a - Riferirsi al doc. 19056_T00_M_201			
03 - GESTIONE DATI			
Descrizione	***Produttore***	***Cod.***	***Pag.***
PLC SIL 4 - 20 DI + 8 DO + 4 ETH	HIMA	F30 034	112÷361
▪ Safety-Related Controller Manual F30 03	HIMA	F30 034	112÷157
▪ Safety Manual Railway Applications	HIMA	F30 034	158÷235
▪ Maintenance Manual Railway Applications	HIMA	F30 034	236÷255
▪ Communication - Configuration in SILworX	HIMA	F30 034	256÷361
Switch di rete 8 ETH + 2 f.o.	WESTERMO	L110-F2G	362÷393
04 - RELE'/INTERFACCE			
n/a - Riferirsi al doc. 19056_T00_M_201			
05 - SELETTORI/PULSANTI			
n/a - Apparecchiature non presenti nel quadro UCP 2			

Tabella 5 – Manuali

QUINT4-PS/1AC/24DC/10

Power supply unit

Data sheet
107100_en_02

1 Description

QUINT POWER power supplies with SFB Technology and preventive function monitoring ensure superior system availability.

Powerful

- SFB Technology: 6 times the nominal current for 15 ms
- Power reserves:
  Static boost of up to 125% (P_N) for a sustained period
  Dynamic boost of up to 200% (P_N) for 5 s

Robust

- Mains buffering ≥ 20 ms
- High degree of electrical immunity, thanks to integrated gas discharge tube (6 kV)

Preventive

- Comprehensive signaling:
  Analog signal, digital signal, relay contact, LED bar graph

Can be ordered pre-configured

- Perform configuration online and order 1 or more units

Long service life

- Well over 15 years

Technical data (short form)	
Input voltage range	100 V AC ... 240 V AC -15 % ... +10 %
Mains buffering	typ. 42 ms (120 V AC) typ. 44 ms (230 V AC)
Nominal output voltage (U_N)	24 V DC
Setting range of the output voltage (U_{Set})	24 V DC ... 29.5 V DC
Nominal output current (I_N) Static Boost ($I_{Stat.Boost}$) Dynamic Boost ($I_{Dyn.Boost}$) Selective Fuse Breaking (I_{SFB})	10 A 12.5 A 20 A (5 s) 60 A (15 ms)
Output power (P_N) Output power ($P_{Stat. Boost}$) Output power ($P_{Dyn. Boost}$)	240 W 300 W 480 W
Efficiency	typ. 92.5 % (120 V AC) typ. 93.4 % (230 V AC)
Residual ripple	< 80 mV_{PP}
MTBF (IEC 61709, SN 29500)	> 783000 h (40 °C)
Ambient temperature (operation)	-25 °C ... 70 °C -40°C (startup type tested) > 60 °C Derating: 2.5 %/K
Dimensions W/H/D	50 mm / 130 mm / 125 mm
Weight	0.9 kg

All technical specifications are nominal values and refer to a room temperature of 25 °C and 70 % relative humidity at 100 m above sea level.

2 Table of contents

3 Ordering data

Description	Type	Order No.	Pcs./Pkt.
Primary-switched QUINT POWER power supply with free choice of output characteristic curve, SFB (selective fuse breaking) technology, and NFC interface, input: 1-phase, output: 24 V DC/10 A	QUINT4-PS/1AC/24DC/10	2904601	1

Versions of the primary-switched QUINT POWER power supply with SFB Technology (selective fuse breaking), which are configured online, can now be ordered in batches of one or more using the following web code: phoenixcontact.net/webcode/#0852

Accessories	Type	Order No.	Pcs./Pkt.
Universal wall adapter for securely mounting the device in the event of strong vibrations. The device is screwed directly onto the mounting surface. The universal wall adapter is attached on the top/bottom.	UWA 182/52	2938235	1
2-piece universal wall adapter for securely mounting the device in the event of strong vibrations. The profiles that are screwed onto the side of the device are screwed directly onto the mounting surface. The universal wall adapter is attached on the left/right.	UWA 130	2901664	1
Assembly adapter for QUINT-PS... power supply on S7-300 rail	QUINT-PS-ADAPTERS7/1	2938196	1
Near Field Communication (NFC) programming adapter with USB interface for the wireless configuration of NFC-capable products from PHOENIX CONTACT with software. No separate USB driver is required.	TWN4 MIFARE NFC USB ADAPTER	2909681	1
Type 2/3 surge protection, consisting of protective plug and base element with screw connection. For single-phase power supply network with integrated status indicator and remote signaling. Nominal voltage 230 V AC/DC.	PLT-SEC-T3-230-FM-UT	2907919	5
Type 3 surge protection, consisting of protective plug and base element, with integrated status indicator and remote signaling for single-phase power supply networks. Nominal voltage 24 V AC/DC.	PLT-SEC-T3-24-FM-UT	2907916	5
Type 2/3 surge protection, consisting of protective plug and base element with Push-in connection. For single-phase power supply network with integrated status indicator and remote signaling. Nominal voltage 230 V AC/DC.	PLT-SEC-T3-230-FM-PT	2907928	5
Type 3 surge protection, consisting of protective plug and base element, with integrated status indicator and remote signaling for single-phase power supply networks. Nominal voltage 24 V AC/DC.	PLT-SEC-T3-24-FM-PT	2907925	5
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBMC E4 24DC/1-4A NO	2906031	1

Accessories	Type	Order No.	Pcs./Pkt.
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBMC E4 24DC/1-10A NO	2906032	1
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBMC E4 24DC/1-4A+ IOL	2910410	1
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBMC E4 24DC/1-10A IOL	2910411	1
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBM E4 24DC/0.5-10A NO-R	2905743	1
Electronic device circuit breaker, number of positions: 1, mounting type: DIN rail: 35 mm, Color: light grey RAL 7035	CBM E8 24DC/0.5-10A NO-R	2905744	1

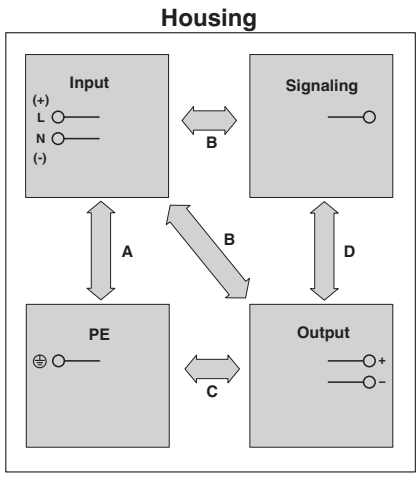
The range of accessories is being continuously extended. The current range of accessories can be found in the download area for the product.

4 Technical data

Input data	
Unless otherwise stated, all data applies for 25°C ambient temperature, 230 V AC input voltage, and nominal output current (I_N).	
Input voltage range	100 V AC ... 240 V AC -15 % ... +10 % 110 V DC ... 250 V DC -18 % ... +40 %
Electric strength, max.	300 V AC 60 s
Frequency range (f_N)	50 Hz ... 60 Hz -10 % ... +10 %
Frequency (f_R) for railway power supply systems	16.7 Hz (acc. to EN 50163)
Railway power supply systems can be operated at 16.7 Hz. Use conditions and technical data on request.	
Current draw typ.	3.4 A (100 V AC) 2.8 A (120 V AC) 1.5 A (230 V AC) 1.5 A (240 V AC) 3 A (110 V DC) 1.3 A (250 V DC)
The specified values for current consumption apply for operation in the static boost (P_N x 125%).	
Discharge current to PE typical	< 3.5 mA 0.7 mA (264 V AC, 60 Hz)
Mains buffering	typ. 42 ms (120 V AC) typ. 44 ms (230 V AC)
Switch-on time	< 1 s
Typical response time from SLEEP MODE	300 ms
Protective circuit	Transient surge protection Varistor, gas-filled surge arrester
Inrush current limitation after 1 ms	12 A
Inrush current integral (I^2t)	< 0.7 A^2s
Input fuse slow-blow, internal	8 A
During the first few microseconds, the current flow into the filter capacitors is excluded.	
The SCCR value (short-circuit current rating) of the power supply unit corresponds to the SCCR value of the backup fuse (see input protection table).	
The external backup fuse must be approved for the (AC) supply voltage used and the voltage level.	

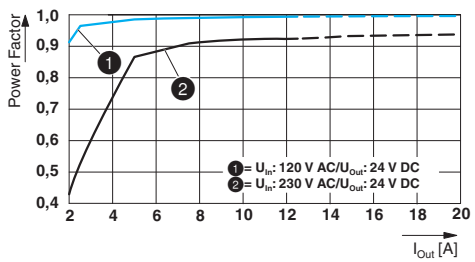
Input protection , AC (to be connected externally upstream)							
Input current I_{In} Input protection	Circuit breaker					Neozed fuse or equivalent	Power switch
Characteristics	A	B	C	D	K	gG	≤ 13 x I_{In} (maximum magnetic tripping)
4 A	-	-	-	✓	✓	✓	✓
6 A	-	-	✓	✓	✓	✓	✓
8 A	-	-	✓	✓	✓	✓	✓
10 A	-	✓	✓	✓	✓	✓	✓
13 A	-	✓	✓	✓	✓	✓	✓
16 A	✓	✓	✓	✓	✓	✓	✓

Electric strength of the insulation



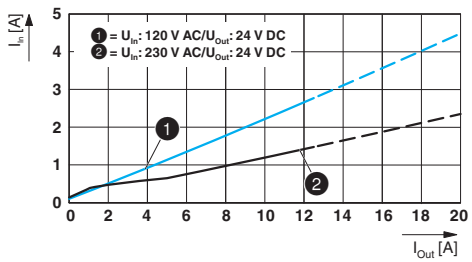
	A	B	C	D
Type test (IEC/EN 60950-1)	2.5 kV AC	4 kV AC	0.5 kV DC	0.5 kV DC
Production test	2 kV AC	2 kV AC	0.5 kV DC	0.5 kV DC
Field test (with gas-filled surge arrester)	0.8 kV AC 1.1 kV DC	0.8 kV AC 1.1 kV DC	0.5 kV DC	0.5 kV DC
Field test (gas-filled surge arrester de-contacted)	2 kV AC 2.83 kV DC	2 kV AC 2.83 kV DC	0.5 kV DC	0.5 kV DC

POWER factor



Crest factor	120 V AC	230 V AC
	typ. 1.50	typ. 1.67

Input current vs. output current



Input connection data	
Connection method	Screw connection
Conductor cross section, solid	0.2 mm² ... 2.5 mm²
Conductor cross section, flexible	0.2 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section AWG	24 ... 14
Stripping length	6.5 mm
Tightening torque	0.5 Nm ... 0.6 Nm

Output data	
Nominal output voltage (U_N)	24 V DC
Setting range of the output voltage (U_{Set}) (constant capacity)	24 V DC ... 29.5 V DC
Nominal output current (I_N)	10 A
Static Boost ($I_{Stat.Boost}$)	12.5 A
Dynamic Boost ($I_{Dyn.Boost}$)	20 A (5 s)
Selective Fuse Breaking (I_{SFB})	60 A (15 ms)
Magnetic circuit breaker tripping	A1...A6 / B2...B6 / C1...C3 / Z1...Z6
Control deviation Static load change 10 % ... 90 %	< 0.5 %
Control deviation Dynamic load change 10 % ... 90 %, (10 Hz)	< 4 %
Control deviation change in input voltage ±10 %	< 0.25 %
Short-circuit-proof	yes
No-load proof	yes
Residual ripple (with nominal values)	< 80 mV_{PP}
Connection in parallel	Yes, for redundancy and increased capacity
Connection in series	yes

Output data	
Feedback voltage resistance	≤ 35 V DC
Protection against overvoltage at the output (OVP)	≤ 32 V DC
Rise time typical	< 1 s (U_{Out} = 10 % ... 90 %)

Output connection data	
Connection method	Screw connection
Conductor cross section, solid	0.2 mm² ... 2.5 mm²
Conductor cross section, flexible	0.2 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section AWG	24 ... 14
Stripping length	6.5 mm
Tightening torque	0.5 Nm ... 0.6 Nm

LED signaling	
P_{Out} > 100%	LED lights up yellow, output power > 240 W
P_{Out} > 75%	LED lights up green, output power > 180 W
P_{Out} > 50%	LED lights up green, output power > 120 W
U_{Out} > 0.9 x U_{Set}	LED lights up green
U_{Out} < 0.9 x U_{Set}	LED flashes green

Signal contact (configurable)	
Signal output (configurable) Out 1	
Digital	0 / 24 V DC , 20 mA
Default	24 V DC , 20 mA (24 V DC for U_{Out} > 0.9 x U_{Set})
Signal output (configurable) Out 2	
Digital	0 / 24 V DC , 20 mA
Analog	4 mA ... 20 mA ± 5 % (Load ≤400 Ω)
Default	24 V DC , 20 mA (24 V DC for P_{Out} < P_N)
Relay contact (configurable) 13/14	
Function	N/O contact
Default	closed (U_{out} > 0.9 U_{Set})
Maximum contact load	24 V DC 1 A , 30 V AC/DC 0.5 A
Control input (configurable) Rem	
Function	Output power ON/OFF (SLEEP MODE)
Default	Output power ON (>40 kΩ/24 V DC/open bridge between Rem and SGnd)
Signal ground SGnd	Reference potential for Out1, Out2, and Rem

Signal connection data	
Connection method	Push-in connection
Conductor cross section, solid	0.2 mm² ... 1 mm²
Conductor cross section, flexible	0.2 mm² ... 1.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.2 mm² ... 0.75 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.2 mm² ... 1.5 mm²
Conductor cross section AWG	24 ... 16
Stripping length	8 mm

Reliability	230 V AC
MTBF (IEC 61709, SN 29500)	> 1251000 h (25 °C) > 783000 h (40 °C) > 377000 h (60 °C)

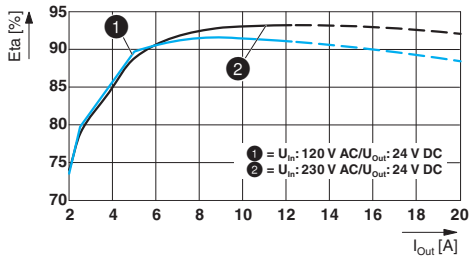
Life expectancy (electrolytic capacitors) Output current (I_{Out})	120 V AC	230 V AC
5 A	> 286000 h (40 °C)	> 283000 h (40 °C)
10 A	> 133000 h (40 °C)	> 160000 h (40 °C)
10 A	> 377000 h (25 °C)	> 454000 h (25 °C)

The expected service life is based on the capacitors used. If the capacitor specification is observed, the specified data will be ensured until the end of the stated service life. For runtimes beyond this time, error-free operation may be reduced. The specified service life of more than 15 years is simply a comparative value.

Switching frequency	Min.	Max.
PFC stage	35 kHz	700 kHz
Auxiliary converter stage	90 kHz	110 kHz
Main converter stage	50 kHz	245 kHz

General data	
Degree of protection	IP20
Protection class	I
Inflammability class in acc. with UL 94 (housing / terminal blocks)	V0
Side element version	Aluminum
Hood version	Stainless steel X6Cr17
Dimensions W / H / D (state of delivery)	50 mm / 130 mm / 125 mm
Dimensions W / H / D (90° turned)	122 mm / 130 mm / 53 mm
Weight	0.9 kg

Power dissipation	120 V AC	230 V AC
Maximum power dissipation in no-load condition	< 3 W	< 3 W
Power dissipation SLEEP MODE	< 3 W	< 3 W
Power loss nominal load max.	< 20 W	< 17 W

Efficiency	120 V AC	230 V AC
	typ. 92.5 %	typ. 93.4 %

Ambient conditions	
Ambient temperature (operation)	-25 °C ... 70 °C (> 60 °C Derating: 2.5 %/K)

The ambient temperature (operation) refers to UL 508 surrounding air temperature.

Ambient temperature (start-up type tested)	-40 °C
Ambient temperature (storage/transport)	-40 °C ... 85 °C
Max. permissible relative humidity (operation)	≤ 95 % (at 25 °C, non-condensing)
Installation height	≤ 5000 m (> 2000 m, observe derating)
Vibration (operation)	5 Hz ... 100 Hz resonance search 2.3g, 90 min., resonance frequency 2.3g, 90 min. (according to DNV GL Class C)
Shock	18 ms, 30g, in each space direction (according to IEC 60068-2-27)
Degree of pollution	2
Climatic class	3K3 (in acc. with EN 60721)
Overvoltage category EN 60950-1 EN 61010-1 EN 62477-1	 II (≤ 2000 m) II (≤ 2000 m) III (≤ 2000 m)

Standards	
Safety transformers for power supply units	EN 61558-2-16 (air clearances and creepage distances only)
Electrical safety (of information technology equipment)	IEC 60950-1/VDE 0805 (SELV)
Electrical safety (of control and regulation devices)	IEC 61010-1
SELV	IEC 60950-1 (SELV) EN 60204-1 (PELV)
Limitation of mains harmonic currents	EN 61000-3-2
Network version/undervoltage	SEMI F47-0706; EN 61000-4-11
Rail applications	EN 50121-3-2 EN 50121-4 EN 50121-5 EN 50163 IEC 62236-3-2 IEC 62236-4 IEC 62236-5
EMC requirements, power plant	IEC 61850-3 EN 61000-6-5
HART FSK Physical Layer Test Specification Compliance	Output voltage U_{Out} compliant

Approvals	
UL	UL Listed UL 508 UL/C-UL Recognized UL 60950-1 UL ANSI/ISA-12.12.01 Class I, Division 2, Groups A, B, C, D (Hazardous Location)
CSA	CAN/CSA-C22.2 No. 60950-1-07 CSA-C22.2 No. 107.1-01
SIQ	BG (type approved)
Shipbuilding	DNV GL, PRS, BV, LR, ABS

Electromagnetic compatibility		
Noise emission according to EN 61000-6-3 (residential and commercial) and EN 61000-6-4 (industrial)		
CE basic standard	**Minimum normative requirements**	**Higher requirements in practice (covered)**
Conducted noise emission EN 55016	EN 61000-6-4 (Class A)	EN 61000-6-3 (Class B)
Noise emission EN 55016	EN 61000-6-4 (Class A)	EN 61000-6-3 (Class B)
Harmonic currents EN 61000-3-2	EN 61000-3-2 (Class A)	EN 61000-3-2 (Class A)
Flicker EN 61000-3-3	not required	EN 61000-3-3

Noise emission for marine approval	**Minimum normative requirements of DNV GL**	**Higher requirements in practice of DNV GL (covered)**
DNV GL conducted noise emission	Class A Area power distribution	Class A Area power distribution
DNV GL noise radiation	Class A Area power distribution	Class B Bridge and deck area

Immunity according to EN 61000-6-1 (residential), EN 61000-6-2 (industrial), and EN 61000-6-5 (power station equipment zone), IEC/EN 61850-3 (energy supply)		
CE basic standard	**Minimum normative requirements of EN 61000-6-2 (CE) (immunity for industrial environments)**	**Higher requirements in practice (covered)**
Electrostatic discharge EN 61000-4-2		
Housing contact discharge	4 kV (Test Level 2)	8 kV (Test Level 4)
Housing air discharge	8 kV (Test Level 3)	15 kV (Test Level 4)
Comments	Criterion B	Criterion A
Electromagnetic HF field EN 61000-4-3		
Frequency range	80 MHz ... 1 GHz	80 MHz ... 1 GHz
Test field strength	10 V/m (Test Level 3)	20 V/m (Test Level 3)
Frequency range	1.4 GHz ... 2 GHz	1 GHz ... 6 GHz
Test field strength	3 V/m (Test Level 2)	10 V/m (Test Level 3)
Frequency range	2 GHz ... 2.7 GHz	1 GHz ... 6 GHz
Test field strength	1 V/m (Test Level 1)	10 V/m (Test Level 3)
Comments	Criterion A	Criterion A
Fast transients (burst) EN 61000-4-4		
Input	2 kV (Test Level 3 - asymmetrical)	4 kV (Test Level 4 - asymmetrical)
Output	2 kV (Test Level 3 - asymmetrical)	4 kV (Test Level 4 - asymmetrical)
Signal	1 kV (Test Level 3 - asymmetrical)	4 kV (Test Level 4 - asymmetrical)
Comments	Criterion B	Criterion A

Immunity according to EN 61000-6-1 (residential), EN 61000-6-2 (industrial), and EN 61000-6-5 (power station equipment zone), IEC/EN 61850-3 (energy supply)		
CE basic standard	**Minimum normative requirements of EN 61000-6-2 (CE) (immunity for industrial environments)**	**Higher requirements in practice (covered)**
Surge voltage load (surge) EN 61000-4-5		
Input	1 kV (Test Level 3 - asymmetrical) 2 kV (Test Level 3 - asymmetrical)	typ. 3 kV (Test Level 4 - symmetrical) typ. 6 kV (Test Level 4 - asymmetrical)
Output	0.5 kV (Test Level 2 - symmetrical) 0.5 kV (Test Level 1 - asymmetrical)	1 kV (Test Level 3 - symmetrical) 2 kV (Test Level 3 - asymmetrical)
Signal	1 kV (Test Level 2 - asymmetrical)	4 kV (Test Level 4 - asymmetrical)
Comments	Criterion B	Criterion A
Conducted interference EN 61000-4-6		
Input/Output/Signal	asymmetrical	asymmetrical
Frequency range	0.15 MHz ... 80 MHz	0.15 MHz ... 80 MHz
Voltage	10 V (Test Level 3)	10 V (Test Level 3)
Comments	Criterion A	Criterion A
Power frequency magnetic field EN 61000-4-8		
	50 Hz , 60 Hz (30 A/m)	16.7 Hz , 50 Hz , 60 Hz (100 A/m 60 s)
	not required	50 Hz , 60 Hz (1 kA/m , 3 s)
	not required	0 Hz (300 A/m , DC, 60 s)
Comments	Criterion A	Criterion A
Voltage dips EN 61000-4-11		
Input voltage (230 V AC , 50 Hz)		
Voltage dip	70 % , 25 periods (Test Level 2)	70 % , 0.5 / 1 / 25 / 30 periods (Test Level 2)
Comments	Criterion C	Criterion A: 0.5 / 1 / 25 / 30 periods
Voltage dip	40 % , 10 periods (Test Level 2)	40 % , 5 / 10 / 50 periods (Test Level 2)
Comments	Criterion C	Criterion A
Voltage dip	0 % , 1 period (Test Level 2)	0 % , 0,5 / 1 / 5 / 50 / 250 periods (Test Level 2)
Comments	Criterion B	Criterion A: 0.5 / 1 period Criterion B: 5 / 50 / 250 periods

Additional basic standard EN 61000-6-5 (immunity in power station), IEC/EN 61850-3 (energy supply)		
Basic standard	**Minimum normative requirements of EN 61000-6-5**	**Higher requirements in practice (covered)**
Pulse-shape magnetic field EN 61000-4-9		
	not required	1000 A/m
Comments	none	Criterion A
Damped oscillating magnetic field EN 61000-4-10		
	not required	100 kHz 110 A/m
	not required	1 MHz 110 A/m
Comments	none	Criterion A
Attenuated sinusoidal oscillations (ring wave) EN 61000-4-12		
Input	not required	2 kV (Test Level 4 - symmetrical)
	not required	4 kV (Test Level 4 - asymmetrical)
Comments	none	Criterion A
Asymmetrical conducted disturbance variables EN 61000-4-16		
Input, Output, Signals	15 Hz ... 150 Hz , 10 V on 1 V 150 Hz ... 1.5 kHz , 1 V 1.5 kHz ... 15 kHz , 1 V on 10 V 15 kHz ... 150 kHz , 10 V (Test Level 3)	15 Hz ... 150 Hz , 30 V on 3 V 150 Hz ... 1.5 kHz , 3 V 1.5 kHz ... 15 kHz , 3 V on 30 V 15 kHz ... 150 kHz , 30 V (Test Level 4)
	50 Hz , 60 Hz , 10 V (Permanent) 50 Hz , 60 Hz , 100 V (1 s) (Test Level 3)	16.7 Hz , 50 Hz , 60 Hz , 30 V (Permanent) 150 Hz , 180 Hz , 30 V (Permanent) 16.7 Hz , 50 Hz , 60 Hz , 300 V (1 s) (Test Level 4)
Comments	Criterion A	Criterion A
Attenuated oscillating wave EN 61000-4-18		
Input, Output	1 MHz 1 kV (Test Level 3 - symmetrical)	100 kHz , 1 MHz , 1 kV (Test Level 3 - symmetrical)
	10 MHz , 1 kV 1 MHz 2.5 kV (Test Level 3 - asymmetrical)	10 MHz , 1 kV 100 kHz , 1 MHz , 2.5 kV (Test Level 3 - asymmetrical)
Signals	1 MHz , 1 kV (Test Level 3 - symmetrical)	100 kHz , 1 MHz , 1 kV (Test Level 3 - symmetrical)
	1 MHz , 2.5 kV (Test Level 3 - asymmetrical)	100 kHz , 1 MHz , 2.5 kV (Test Level 3 - asymmetrical)
Comments	Criterion B	Criterion A

Key	
Criterion A	Normal operating behavior within the specified limits.
Criterion B	Temporary impairment to operational behavior that is corrected by the device itself.
Criterion C	Temporary adverse effects on the operating behavior, which the device corrects automatically or which can be restored by actuating the operating elements.

5 Safety and installation notes

5.1 Symbols used

Instructions and possible hazards are indicated by corresponding symbols in this document.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible personal injuries.

There are different categories of personal injury that are indicated by a signal word.

WARNING

This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

The following symbols are used to indicate potential damage, malfunctions, or more detailed sources of information.

NOTE

This symbol together with the signal word NOTE and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

5.2 Safety and warning notes

WARNING: Danger to life by electric shock!

- Only skilled persons may install, start up, and operate the device.
- The power supply must be switched off from outside (e.g. via the line protection on the primary side).
- Never carry out work when voltage is present.
- Establish connection correctly and ensure protection against electric shock.
- Cover termination area after installation in order to avoid accidental contact with live parts (e. g., installation in control cabinet).

CAUTION: Hot surface

Depending on the ambient temperature and load on the power supply, the housing can become hot.

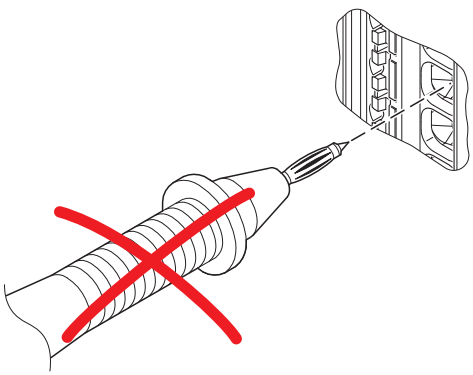
NOTE

- Observe the national safety and accident prevention regulations.
- Assembly and electrical installation must correspond to the state of the art.
- The power supply is a built-in device and is designed for mounting in a control cabinet.
- The IP20 degree of protection of the device is intended for use in a clean and dry environment.
- Observe mechanical and thermal limits.
- Ensure minimum clearances to external heat sources.
- Mount the power supply in the standard installation position. Position of the connection terminals ⏚/N/L below.
- Connect the housing to ground via protective conductor device terminal block ⏚.
- Ensure that the primary-side wiring and secondary-side wiring are the correct size and have sufficient fuse protection.
- Use copper cables for operating temperatures of
  >75 °C (ambient temperature <55 °C)
  >90 °C (ambient temperature <75 °C).
- For the connection parameters for wiring the power supply, such as the required stripping length with and without ferrule, refer to the technical data section.
- The power supply is approved for the connection to TN, TT and IT power grids (star networks) with a maximum phase-to-phase voltage of 240 V AC
- If the device is connected to the IT system, a two-pos. miniature circuit breaker is required in the application.
- Protect the device against foreign bodies penetrating it, e.g., paper clips or metal parts.
- The power supply is maintenance-free. Repairs may only be carried out by the manufacturer. The warranty no longer applies if the housing is opened.
- The power supply may only be used for its intended use.
- Relay contact 13/14 can be used to max. 30 V AC/ 24 V DC.

The continuous total output power may not exceed P_N at 60 °C ambient temperature and $P_{Stat.\ Boost}$ at 40°C ambient temperature. Observe all the maximum output powers for all operating conditions.

NOTE: Damage to the Push-in connection terminal blocks is possible

Do not plug test pins into the Push-in connection terminal blocks. The maximum pluggable depth of the Push-in connection terminal blocks is limited. In addition, when the test pin is plugged in, the unlocking button (pusher) is covered to such an extent that unlocking is not possible or only possible to an insufficient extent. If you do not push the unlocking button (pusher) down completely when you are pulling the test pin out, then the Push-in connection terminal block will become damaged.



6 High-voltage test (HIPOT)

This protection class I power supply is subject to the Low Voltage Directive and is factory tested. During the HIPOT test (high-voltage test), the insulation between the input circuit and output circuit is tested for the prescribed electric strength values, for example. The test voltage in the high-voltage range is applied at the input and output terminal blocks of the power supply. The operating voltage used in normal operation is a lot lower than the test voltage used.

High-voltage tests up to 0.8 kV AC / 1.1 kV DC can be performed as described.

For high-voltage tests > 0.8 kV AC / 1.1 kV DC, the gas-filled surge arrester must be disconnected.

The test voltage should rise and fall in ramp form. The relevant rise and fall time of the ramp should be at least two seconds.

6.1 High-voltage dielectric test (dielectric strength test)

In order to protect the user, power supplies (as electric components with a direct connection to potentially hazardous voltages) are subject to more stringent safety requirements. For this reason, permanent safe electrical isolation between the hazardous input voltage and the touch-proof output voltage as safety extra-low voltage (SELV) must always be ensured.

In order to ensure permanent safe isolation of the AC input circuit and DC output circuit, high-voltage testing is performed as part of the safety approval process (type test) and manufacturing (routine test).

6.2 High-voltage dielectric test during the manufacturing process

During the manufacturing process for the power supply, a high-voltage test is performed as part of the dielectric test in accordance with the specifications of IEC/UL/EN 60950-1. The high-voltage test is performed with a test voltage of at least 1.5 kV AC / 2.2 kV DC or higher. Routine manufacturing tests are inspected regularly by a certification body.

6.3 High-voltage dielectric test performed by the customer

Apart from routine and type tests to guarantee electrical safety, the end user does not have to perform another high-voltage test on the power supply as an individual component. According to EN 60204-1 (Safety of machinery - Electrical equipment of machines) the power supply can be disconnected during the high-voltage test and only installed once the high-voltage test has been completed.

6.3.1 Performing high-voltage testing

If high-voltage testing of the control cabinet or the power supply as a stand-alone component is planned during final inspection and testing, the following features must be observed.

– The power supply wiring must be implemented as shown in the wiring diagram.
– The maximum permissible test voltages must not be exceeded.

Avoid unnecessary loading or damage to the power supply due to excessive test voltages.

For the relevant applicable test voltages and insulation distances, refer to the corresponding table (see technical data: electric strength of the insulation section).

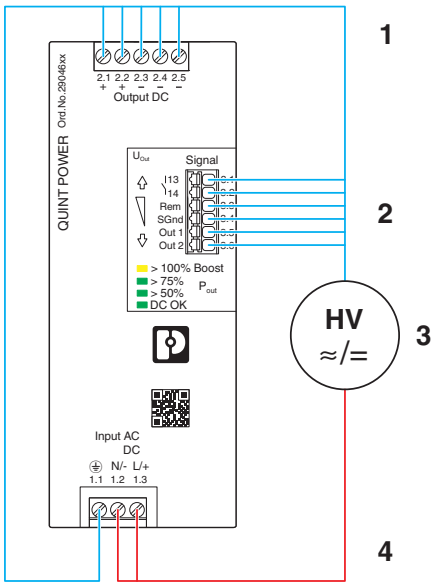


Figure 1 Potential-related wiring for the high-voltage test

Key

No.	Designation	Color coding	Potential levels
1	DC output circuit	Blue	Potential 1
2	Signal contacts	Blue	Potential 1
3	High-voltage tester	--	--
4	AC input circuit	Red	Potential 2

6.3.2 Disconnecting the gas discharge tube

The built-in gas discharge tube inside the device ensures that the power supply is effectively protected against asymmetrical disturbance variables (e.g., EN 61000-4-5).

Each surge voltage test represents a very high load for the power supply. Therefore avoid unnecessary loading or damage to the power supply due to excessive test voltages. If necessary, the gas discharge tube inside the device can be disconnected in order to use higher test voltages. Following successful completion of testing, please reconnect the gas-discharge tube.

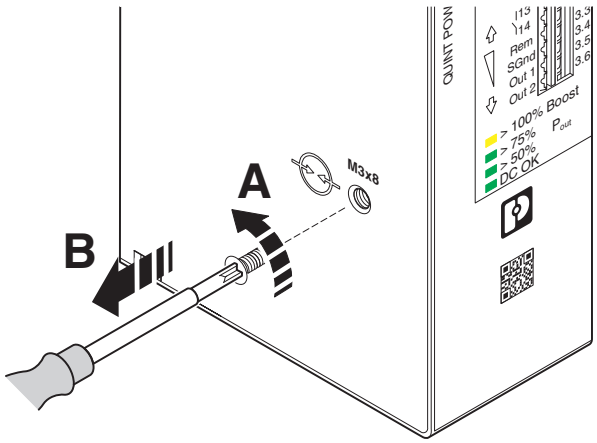


Figure 2 Disconnect gas discharge tube

To disconnect the gas discharge tube, proceed as follows:

1. Remove power from the unit.
2. Unscrew the Phillips head screw completely and keep the gas discharge tube screw in a safe place. The gas-discharge tube is now disconnected and is no longer functional.
3. Perform the surge voltage test on the power supply.
4. Following successful high-voltage testing, screw the gas discharge tube screw fully back into the power supply.

DANGER: Risk of electric shock or damage to the power supply due to using the wrong gas discharge tube screw

To connect the gas-filled surge arrester, only use the gas-filled surge arrester screw that was originally installed in the power supply.

7 Structure of the power supply

The fanless convection-cooled power supply can be snapped onto all DIN rails according to EN 60715.

7.1 Function elements

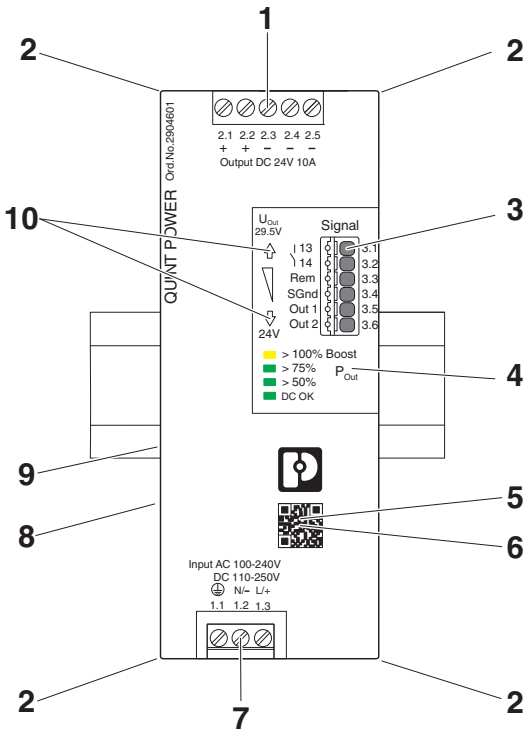


Figure 3 Operating and indication elements

Key

No.	Designation
1	DC output voltage connection terminal blocks
2	Accommodation for cable binders
3	Signaling connection terminal blocks
4	Status and diagnostics indicators
5	Position NFC interface (Near Field Communication)
6	QR code web link
7	AC input voltage connection terminal blocks
8	Gas discharge tube for surge protection (left side of housing)
9	Universal DIN rail adapter (rear of housing)
10	Output voltage button ⬇(-) / ⬆(+)

7.2 Device dimensions

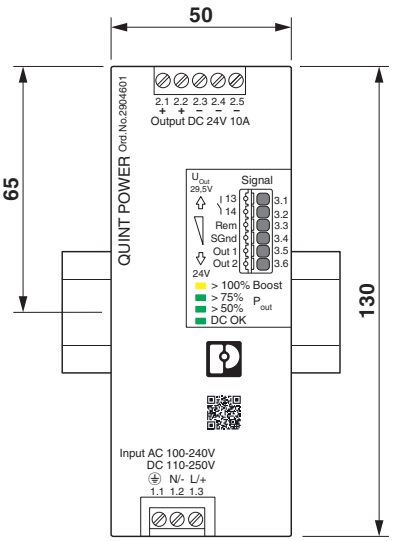


Figure 4 Device dimensions (dimensions in mm)

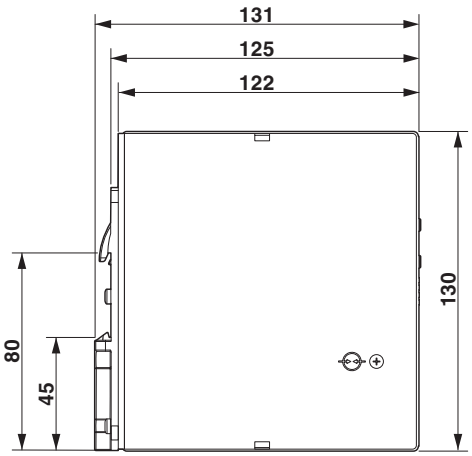


Figure 5 Device dimensions (dimensions in mm)

7.3 Keep-out areas

Nominal output capacity	Spacing [mm]		
	a	b	c
< 50 %	0	40	20
≥ 50 %	5	50	50

If adjacent components are active and the nominal output power ≥ 50%, there must be lateral spacing of 15 mm.

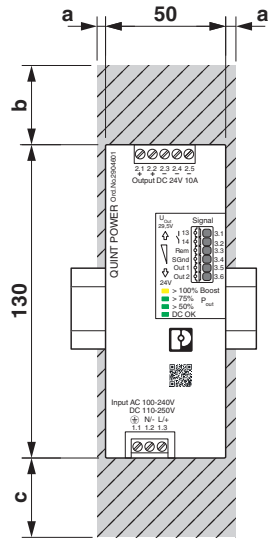


Figure 6 Device dimensions and minimum keep-out areas (in mm)

7.4 Block diagram

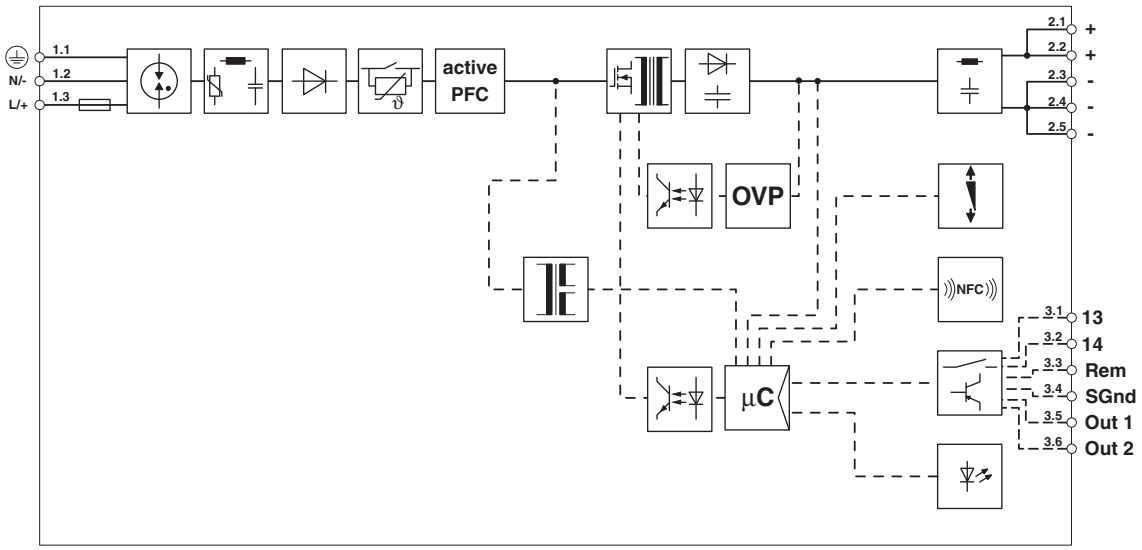


Figure 7 Block diagram

Key

Symbol	Designation
	Surge protection (gas discharge tube)
	Surge protection (varistor) with filter
	Bridge rectifier
	Inrush current limitation
active PFC	Power factor correction (PFC)
	Switching transistor and main transmitter (electrically isolating)
	Secondary rectification and smoothing
	Filter
	Auxiliary converter (electrically isolating)

Symbol	Designation
	Optocoupler (electrically isolating)
OVP	Additional regulatory protection against surge voltage
	Relay contact and signal contacts
µC	Microcontroller
NFC	Passive NFC interface (Near Field Communication)
	Output voltage button ⬇(-) / ⬆(+)
	Signal/display LEDs (P_{Out}, DC OK)

8 Mounting/removing the power supply

8.1 Mounting the power supply unit

Proceed as follows to mount the power supply:

1. In the normal mounting position the power supply is mounted on the DIN rail from above. Make sure that the universal DIN rail adapter is in the correct position behind the DIN rail (A).
2. Then press the power supply down until the universal DIN rail adapter audibly latches into place (B).
3. Check that the power supply is securely attached to the DIN rail.

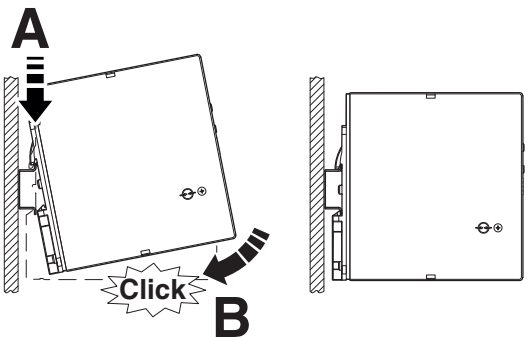


Figure 8 Snapping the power supply onto the DIN rail

8.2 Removing the power supply unit

Proceed as follows to remove the power supply:

1. Take a suitable screwdriver and insert this into the lock hole on the universal DIN rail adapter (A).
2. Release the lock by lifting the screwdriver (B).
3. Carefully swivel the power supply forward (C) so that the lock slides back into the starting position.
4. Then separate the power supply from the DIN rail (D).

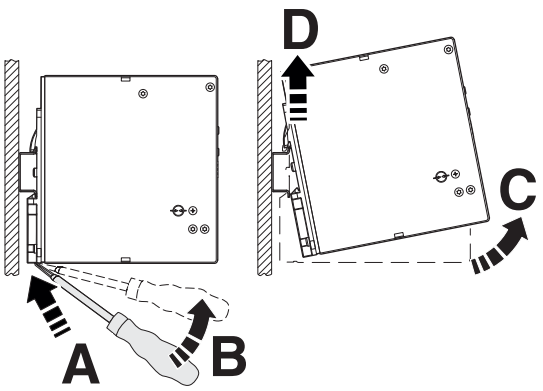


Figure 9 Removing the power supply from the DIN rail

8.3 Retrofitting the universal DIN rail adapter

For installation in horizontal terminal boxes it is possible to mount the power supply at a 90° angle to the DIN rail.

No additional mounting material is required.

Use the Torx screws provided to attach the universal DIN rail adapter to the side of the power supply.

8.3.1 Disassembling the universal DIN rail adapter

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Separate the universal DIN rail adapter from the rear of the power supply.

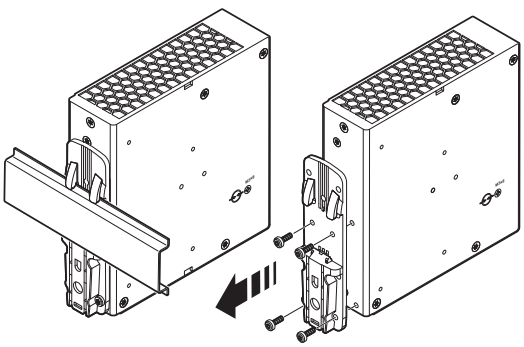


Figure 10 Disassembling the universal DIN rail adapter

8.3.2 Mounting the universal DIN rail adapter

To mount the universal DIN rail adapter on the left side of the device, proceed as follows:

1. Position the universal DIN rail adapter on the left side of the housing so that the mounting holes are congruent with the hole pattern for the mounting holes.
2. Insert the Torx screws that were removed earlier into the appropriate hole pattern on the universal DIN rail adapter so that the necessary drill holes on the power supply can be accessed.
3. Screw the universal DIN rail adapter onto the power supply.

The maximum tightening torque of the Torx screw (Torx® T10) is 0.7 Nm.

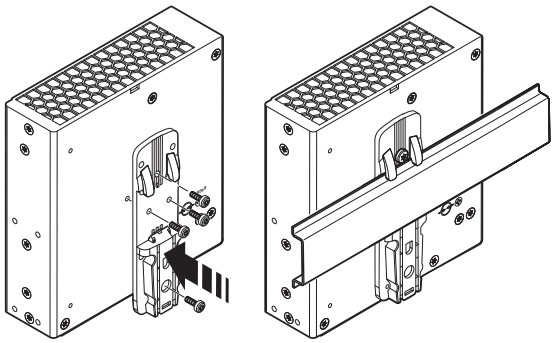


Figure 11 Mounting the universal DIN rail adapter

8.4 Retrofitting the universal wall adapter

The UWA 182/52 universal wall adapter (Order No. 2938235) or UWA 130 universal wall adapter (Order No. 2901664) is used to attach the power supply directly to the mounting surface.

The use of universal wall adapters is recommended under extreme ambient conditions, e.g., strong vibrations. Thanks to the tight screw connection between the power supply and the universal wall adapter or the actual mounting surface, an extremely high level of mechanical stability is ensured.

The power supply is attached to the UWA 182 or UWA 130 universal wall adapter by means of the Torx screws of the universal DIN rail adapter.

8.4.1 Mounting the UWA 182/52 universal wall adapter

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Separate the universal DIN rail adapter from the rear of the power supply.
3. Position the universal wall adapter in such a way that the keyholes or oval tapers face up. The mounting surface for the power supply is the raised section of the universal wall adapter.
4. Place the power supply on the universal wall adapter in the normal mounting position (input voltage connection terminal blocks below).
5. Insert the Torx screws into the appropriate hole pattern on the universal wall adapter so that the necessary mounting holes on the power supply can be accessed.
6. Screw the universal wall adapter onto the power supply.

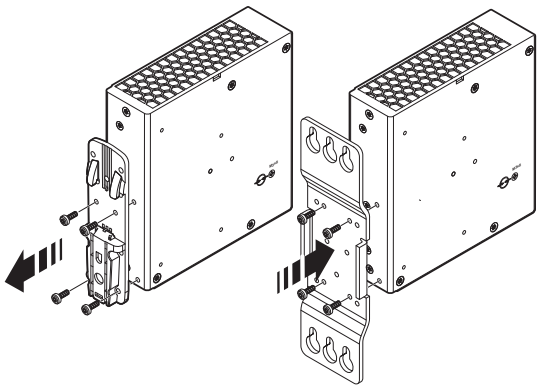


Figure 12 Mounting the UWA 182/52 universal wall adapter

The maximum tightening torque of the Torx screw (Torx® T10) is 0.7 Nm.

Make sure you use suitable mounting material when attaching to the mounting surface.

8.4.2 Mounting the UWA 130 2-piece universal wall adapter

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Separate the universal DIN rail adapter from the rear of the power supply.
3. Position the universal wall adapter. The mounting surface for the power supply is the raised section of the universal wall adapter.
4. Place the power supply on the universal wall adapter in the normal mounting position (input voltage connection terminal blocks below).
5. Insert the Torx screws into the appropriate hole pattern on the universal wall adapter so that the necessary mounting holes in the side flanges of the power supply can be accessed.
6. Screw the two-piece universal wall adapter onto the power supply.

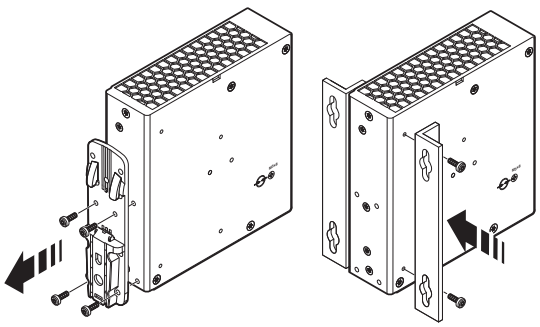


Figure 13 Mounting the UWA 130 universal wall adapter

8.5 Fix connection wiring to the power supply

Two receptacles for the bundled attachment of the connection wiring are integrated in the left and right housing panel. Use cable binders to secure the connection wiring (optional PKB 140X3,6 - Order No. 1005460).

Proceed as follows to secure the connection wiring:

– Wire the power supply with sufficient connection reserve (input terminal blocks, output terminal blocks, signal terminal blocks)
– Bundle and set up the connection wiring so that the cooling grilles on the top and bottom of the housing are covered as little as possible.
– Thread the cable binders into the necessary receptacles for the cable binders.

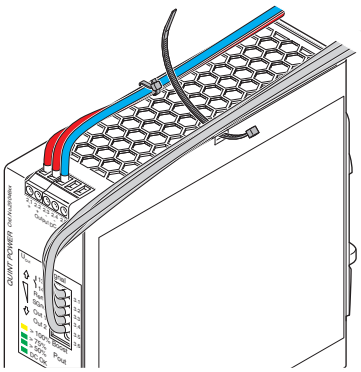


Figure 14 Lay and align connection wiring

– Secure the connection wiring with the cable binders. Make sure that the connection wiring is attached safely and securely without damaging the connection wiring.

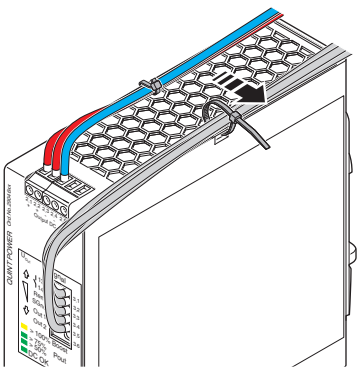


Figure 15 Secure connection wiring with cable binder

– Shorten the excess length of the cable ties.
– Then check again that the connection wiring is properly secured.

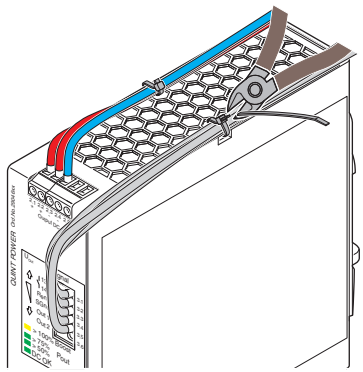


Figure 16 Shorten protruding ends of the cable binder

NOTE: Mechanical damage to the connection wiring caused by friction

In extreme ambient conditions, e.g., strong vibrations, protect the connection wiring against mechanical damage using additional insulation material. The additional insulation material for protecting the connection wiring is limited to the area where the cable binders are attached.

9 Device connection terminal blocks

The AC input and DC output terminal blocks on the front of the power supply feature screw connection technology. The signal level is wired without tools by means of Push-in connection technology.

For the necessary connection parameters for the connection terminal blocks, refer to the technical data section.

9.1 Input

The power supply is operated on single-phase AC systems or two outer conductors of three-phase systems. The power supply is connected on the primary side via the INPUT L/N/⏚ connection terminal blocks.

The power supply is approved for connection to TN, TT, and IT power grids with a maximum phase-to-phase voltage of 240 V AC.

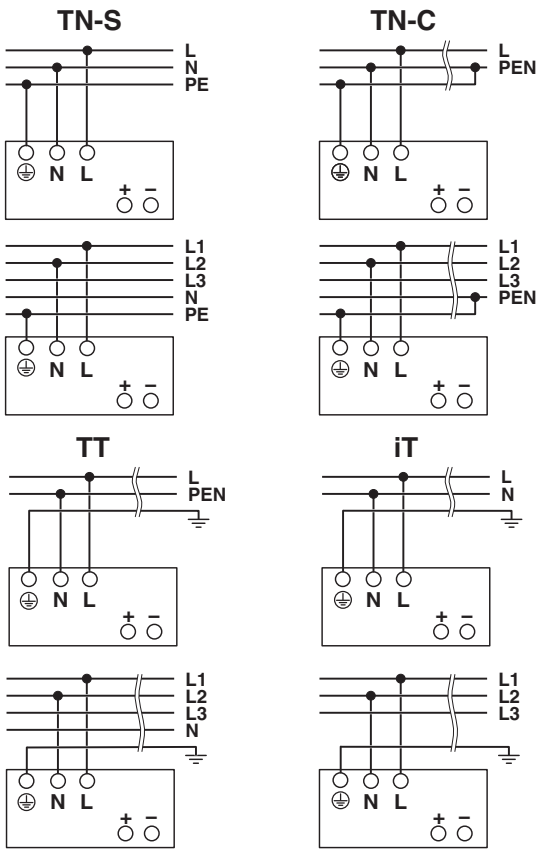


Figure 17 Network types

9.2 Protection of the primary side

Installation of the device must correspond to EN 60950-1 regulations. It must be possible to switch off the device using a suitable disconnecting device outside the power supply. The line protection on the primary side is suitable for this (see technical data section).

DANGER: Hazardous voltage

An all-pos. fuse must be present for operation on two outer conductors of a three-phase system.

Protection for AC supply

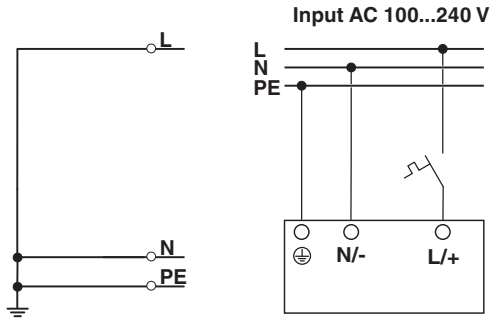


Figure 18 Pin assignment for AC supply voltage

Protection for DC supply

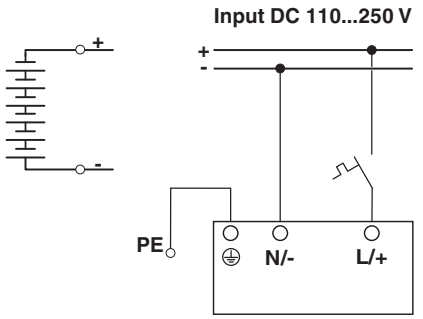


Figure 19 Pin assignment for DC supply voltage

DC applications require upstream installation of a fuse that is permitted for the operating voltage.

9.3 Output

By default, the power supply is pre-set to a nominal output voltage of 24 V DC.

The output voltage is adjusted via the two arrow keys ⬇(-) and ⬆(+) on the front of the power supply.

When you press the arrow key once briefly, the output voltage is reduced ⬇(-) or increased ⬆(+) by 3 mV. When you press the arrow key for longer, the voltage is adjusted in 100 mV increments.

9.4 Protection of the secondary side

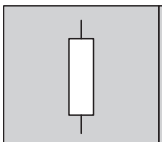
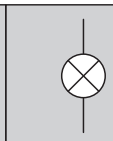
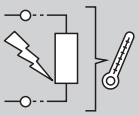
The power supply is electronically short-circuit-proof and no-load-proof. In the event of an error, the output voltage is limited

If sufficiently long connecting cables are used, fuse protection does not have to be provided for each individual load.

If each load is protected separately with its own protective device, the selective shutdown in the event of a fault enables the system to remain operational.

10 Output characteristic curves

This section describes the various output characteristic curves together with their areas of application for customization to your specific application. The U/I Advanced characteristic curve is set by default.

							
Application	Normal load	System extension	Loads with high inrush current	Energy storage charging	Selective tripping of fuses	Keeps temperatures low in the event of faults	Short circuit, non-fused
Your benefits	Reliable power supply	A stable 24 V, even in the event of a sustained overload	No over-dimensioned power supply unit required	Fast charging	Parallel loads continue working	Low thermal stress in the even of faults	Enables configuration without fuse
Characteristics							
U/I Advanced	✓	✓	✓	✓	✓	✓	–
Smart HICCUP	✓	✓	✓	✓	–	✓	–
FUSE MODE	✓	✓	–	–	–	✓	✓

Symbol	Designation
✓	Suitable for the application
–	Not suitable for the application

10.1 U/I Advanced output characteristic curve

The preset U/I Advanced output characteristic curve is optimized for the following applications:

– For selective tripping of standard circuit breakers (SFB technology). The power supply supplies up to 6 times the nominal current for 15 ms. Loads connected in parallel continue working.
– When supplying loads with high switch-on currents, such as motors. The dynamic boost of the power supply supplies up to 200% of the nominal power for 5 s. This ensures that sufficient reserve energy is available; overdimensioning of the power supply is not necessary.
– For system extension. With the static boost, up to 125% of the nominal output power is available for a sustained period (up to 40°C).
– For fast energy storage charging (e.g., of batteries) to supply a wide range of loads. The power supply operates in the nominal operating range. Energy supply to the load is ensured.

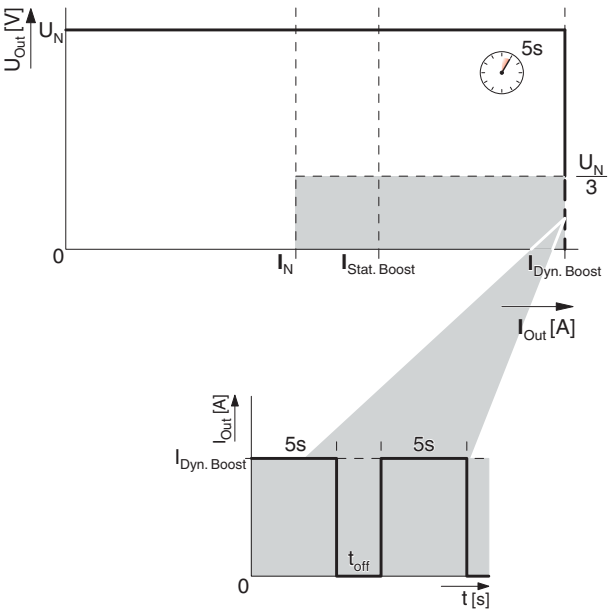


Figure 20 U/I Advanced output characteristic curve

10.2 Smart HICCUP output characteristic curve

The SMART HICCUP output characteristic curve keeps the thermal load of the connecting cables at a low level in the event of a sustained overload. If loads are not protected or are protected in a way that is not permitted, the loads are supplied for 2 s. The DC output of the power supply is then switched off for 8 s. This procedure is repeated until the cause of the overload has been remedied.

The preset Smart HICCUP output characteristic curve is optimized for the following applications:

– If only a low short-circuit current is permitted.
– If following an overload or short circuit the output voltage should be made available again automatically.

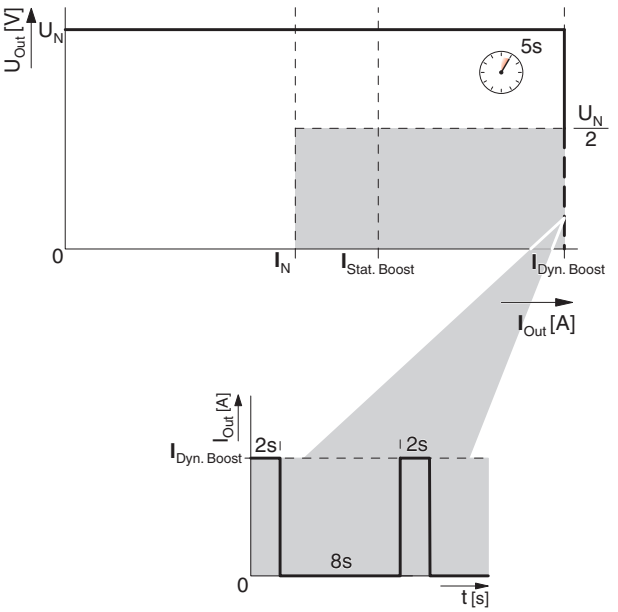


Figure 21 Smart HICCUP output characteristic curve

10.3 FUSE MODE output characteristic curve

In the event of an overload (e.g., short circuit), the power supply switches off the DC output permanently. The value of the switch-off threshold and the time period for which it may be exceeded can be freely selected. The power supply is restarted via the remote contact. As an option, the power supply can be switched on by switching the supply voltage on the primary side off and on.

Selecting the FUSE MODE output characteristic curve sets the following default values.

– t_{Fuse} = 100 ms
– I_{Fuse} = I_N

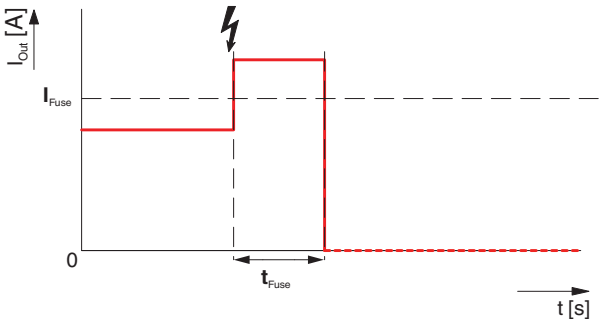


Figure 22 FUSE MODE output characteristic curve

11 Configuring the power supply

With the fourth generation of the QUINT POWER power supply, it is now possible for the first time to adapt the behavior of the power supply. In addition to setting the output voltage and selecting the output characteristic curves, you can configure signal outputs Out 1, Out 2, and floating signal contact 13/14, for example. Configuration of the remote input for controlling the power supply or specification of signal options and signal thresholds also extend the range of possible applications.

The power supply is configured via the device's internal NFC (near field communication) interface. This is located behind the QR code on the front.

The power supply behaves like a passive NFC tag. An auxiliary power source is required in order to supply the power supply with configuration data.

11.1 Configuration with PC software

In order to configure the power supply via the NFC interface, the following hardware and software requirements must be met:

- PC or notebook (as of Windows 7, Microsoft.Net Framework 4.5, USB 2.0 interface, 50 MB hard disk capacity, QUINT POWER software).
- Programming adapter:
  TWN4 MIFARE NFC USB ADAPTER (Order No. 2909681) is plugged into the USB interface.
- Programming software: the QUINT POWER software has been successfully installed.

11.2 Configuring the power supply

To configure the power supply, proceed as follows:

- Before you can configure the power supply, it should either be disconnected from the supply voltage or switched to SLEEP MODE.
- To switch the power supply to SLEEP MODE, use one of the external circuits. The following connection versions are possible between the Rem (remote input) and SGnd (signal ground) connection terminal blocks.

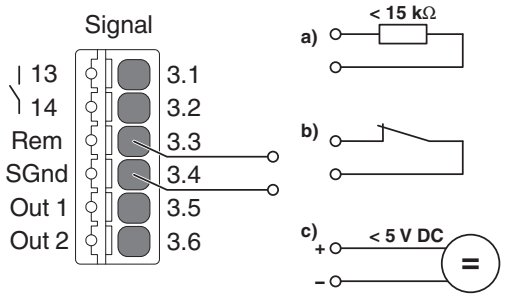


Figure 23 SLEEP MODE connection versions

- Hold the USB-PROG-ADAPTER in front of the mounted power supply such that the NFC antenna symbol is over the QR code.

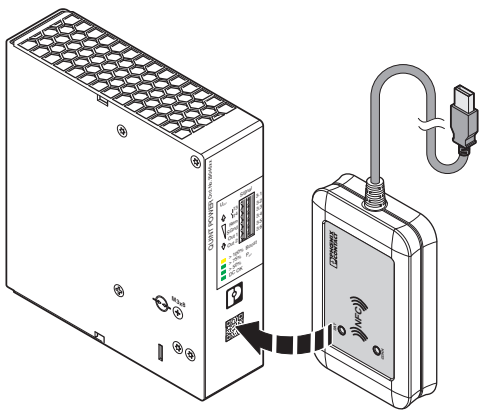


Figure 24 Configuration of the power supply

- In the programming interface of the QUINT POWER software, press the [Read] button. The current device and configuration data for the power supply is read and displayed.

If a connection cannot be established between the USB-PROG-ADAPTER and the power supply, more detailed information can be found in the user manual for the QUINT POWER software.

For information regarding the configuration of the power supply, such as selecting the characteristic curve and output parameters, refer to the user manual for the QUINT POWER software.

11.3 Configuration with NFC-capable mobile terminal device

The QUINT POWER app enables you to conveniently configure the power supply using a mobile terminal device, such as a smartphone.

In order to configure the power supply via the NFC interface, the following hardware and software requirements must be met:

– NFC-capable mobile terminal device with Android operating system as of Version 4.1.x (Jelly Bean)
– QUINT POWER app (Google Play Store)

For information regarding the configuration of the power supply, such as selecting the characteristic curve and output parameters, please refer to the QUINT POWER app.

11.4 Ordering a configured power supply

Customer-specified QUINT POWER power supplies are ordered as a KMAT item (configurable material) and are configured during the production process in the factory. The power supply is therefore supplied ready to connect for your specific application.

You can type in the the web code phoenixcontact.net/webcode/#0852 to configure and order your power supply.

12 Boost currents

The power supply provides the static boost ($I_{Stat.\ Boost}$) for a sustained load supply or the time-limited dynamic boost ($I_{Dyn.\ Boost}$).

12.1 Static Boost

For system expansion purposes, the sustained static boost ($I_{Stat.\ Boost}$) supports the load supply with up to 125 % of the nominal current of the power supply. The static boost is available at an ambient temperature of up to 40 °C.

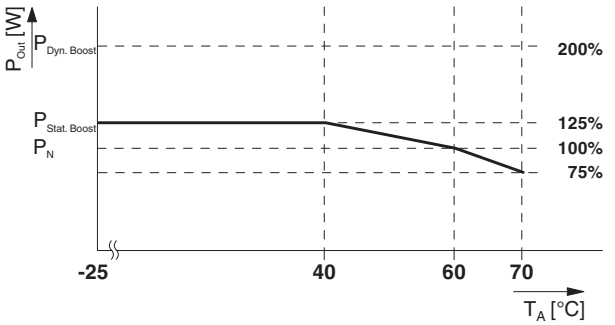


Figure 25 Performance characteristic in static boost

12.2 Dynamic Boost

Dynamic boost ($I_{Dyn.\ Boost}$) delivers up to 200 % of the power supply nominal current to supply high loads. This temporary power supply to the load lasts a maximum of 5 s at an ambient temperature of up to 60 °C. The energy supplied adaptively for the load supply and the recovery time (t_{Pause}) are calculated based on the specific load situation using algorithms (see recovery time tables).

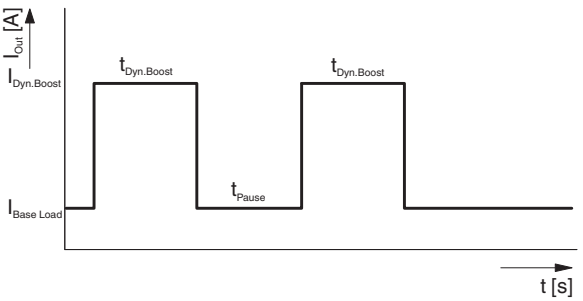


Figure 26 Basic curve of the dynamic boost process

Use the following tables to determine the required recovery time (t_{Pause}) at the maximum dynamic boost current ($I_{Dyn. Boost}$) based on the following values:

– $I_{Base Load}$
– Duration of the boost current ($t_{Dyn. Boost}$)
– Ambient temperature (40 °C or 60 °C)

If a current that is lower than the maximum available dynamic boost current ($I_{Dyn. Boost}$) is required for the same period, the recovery time may (t_{Pause}) decrease.

12.2.1 Recovery times at an ambient temperature of 40 °C

$I_{Base Load}$ [A]	$I_{Dyn. Boost}$ [A]	$t_{Dyn. Boost}$ [s]					
		1	2	3	4	5	
0	20	1,4	2,9	4,3	6	8	t_{Pause} [s]
2	20	1,5	3	4,5	6	8	
4	20	1,7	3,3	5	7	9	
6	20	1,9	3,8	6	8	10	
8	20	2,4	4,9	8	10	13	
10	20	3,7	8	12	15	19	
12,5	20	23	46	68	91	114	

Figure 27 Required recovery times at ≤ 40°C

12.2.2 Recovery times at an ambient temperature of 60 °C

$I_{Base Load}$ [A]	$I_{Dyn. Boost}$ [A]	$t_{Dyn. Boost}$ [s]					
		1	2	3	4	5	
0	20	2,3	4,6	7	10	12	t_{Pause} [s]
2	20	2,5	5	8	10	13	
4	20	2,8	6	9	12	15	
6	20	3,5	7	11	15	18	
8	20	6	11	16	22	27	
10	20	15	29	43	57	72	

Figure 28 Required recovery times at ≤ 60°C

12.2.3 Example: Determining the recovery time (t_{Pause})

At an output current ($I_{Base Load}$) of 4 A, the dynamic output current ($I_{Dyn. Boost}$) of 20 A increases for 2 s ($t_{Dyn. Boost}$). After a recovery time (t_{Pause}) of 3.3 s, the dynamic boost is available once again.

$I_{Base Load}$ [A]	$I_{Dyn. Boost}$ [A]	$t_{Dyn. Boost}$ [s]					
		1	2	3	4	5	
0	20	1,4	2,9	4,3	6	8	t_{Pause} [s]
2	20	1,5	3	4,5	6	8	
4	20	1,7	3,3	5	7	9	
6	20	1,9	3,8	6	8	10	
8	20	2,4	4,9	8	10	13	
10	20	3,7	8	12	15	19	
12,5	20	23	46	68	91	114	

Figure 29 Example recovery time for ≤ 40°C

13 SFB Technology

SFB Technology (selective fuse breaking) can be used to quickly and reliably trip miniature circuit breakers and fuses connected on the secondary side. In the event of a short circuit on the secondary side, the power supply supplies up to 6 times the nominal current for 15 ms. The faulty current path is switched off selectively.

Loads that are connected in parallel are still supplied with energy. Operation of these system parts is ensured. In order to always enable the reliable tripping of circuit breakers and fuses, certain framework conditions must be observed (see SFB configuration section).

The U/I Advanced output characteristic curve supports SFB Technology.

13.1 Tripping circuit breakers

The circuit breaker is tripped by the high SFB current of the power supply, typically within 3 to 5 ms. As a result, voltage dips at loads that are connected in parallel are avoided.

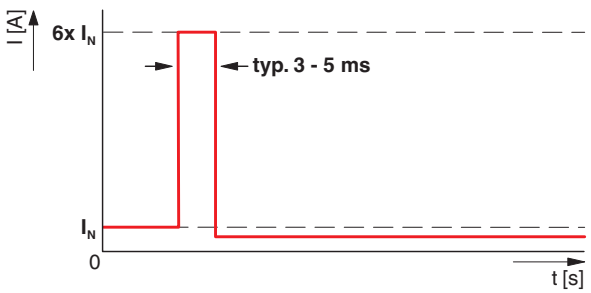


Figure 30 SFB pulse trips circuit breakers

13.2 Tripping a fuse

Fuses are tripped by melting the predetermined breaking point inside the fuse capsule. The tripping characteristic of the fuse is described by the melting integral (I^2t). A high current is crucial in order to achieve a very short tripping time.

13.3 SFB configuration

Observe the following framework conditions for determining the maximum distance between the power supply and load:

– The performance class of the power supply
– The cross section of the connecting cable
– The tripping characteristic of the fuse component

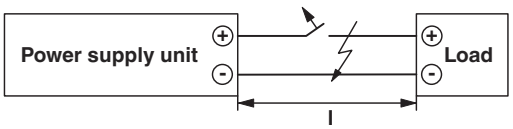


Figure 31 Schematic diagram of the maximum cable length

13.4 Maximum distance between the power supply and load

The distances given in the table are worst-case values and therefore cover the entire tolerance range for the magnetic tripping of circuit breakers. The possible distances are often greater in practice.

13.4.1 Thermomagnetic device circuit breaker, type: Phoenix Contact CB TM1 SFB

Maximum distance l [m] with device circuit breaker		Conductor cross section			
		A [mm²]	0.75	1.0	1.5	2.5
		AWG	18	(17)	16	14
Phoenix Contact	CB TM1 1A SFB P		27	36	54	91
	CB TM1 2A SFB P		18	25	37	63
	CB TM1 3A SFB P		11	15	22	38
	CB TM1 4A SFB P		6	8	13	22
	CB TM1 5A SFB P		4	5	8	14

The cable lengths determined are based on the following parameters:

Tripping:	magnetic
DC correction factor (0 Hz):	Phoenix Contact = 1,0
Characteristics:	C Characteristic C (10 times the rated current) x correction factor
Ambient temperature:	+20 °C
Internal resistance R_i of the device circuit breaker:	taken into consideration
Comments:	In addition to the short-circuit current, the power supply unit also supplies half the nominal current for load paths connected in parallel.

13.4.2 Thermomagnetic circuit breaker, type: Siemens 5SY, ABB S200

Maximum distance l [m] with circuit breaker		Conductor cross section			
		A [mm²]	0.75	1.0	1.5	2.5
		AWG	18	(17)	16	14
Siemens 5SY	A1		78	105	157	263
	A1.6		58	77	116	194
	A2		49	65	98	164
	A3		35	47	71	118
	A4		27	36	54	90
	A6		18	24	37	62
	B2		28	37	56	93
	B4		14	19	28	48
	B6		6	8	13	21
	C1		10	14	21	35
	C1.6		12	17	25	42
	C2		11	15	22	37
	C3		4	6	9	15
ABB S200	B6		5	7	11	18
	C1		3	4	6	11
	C1.6		7	10	15	25
	C2		4	6	9	15
	C3		3	4	7	11
	Z1		64	85	128	214
	Z1.6		46	62	93	156
	Z2		42	57	85	143
	Z3		33	44	66	110
	Z4		24	33	49	82
	Z6		15	20	30	51

The cable lengths determined are based on the following parameters:

Tripping:	magnetic
DC correction factor (0 Hz):	Siemens = 1.4; ABB = 1.5
Characteristics:	A, B, C, Z Characteristic A (3 times the rated current) x correction factor Characteristic B (5 times the rated current) x correction factor Characteristic C (10 times the rated current) x correction factor Characteristic Z (3 times the rated current) x correction factor
Ambient temperature:	+20 °C
Internal resistance R_i of the device circuit breaker:	taken into consideration
Comments:	In addition to the short-circuit current, the power supply unit also supplies half the nominal current for load paths connected in parallel.

13.4.3 Fuse, type: Cooper Bussmann GMA xA, GMC xA

Maximum distance l [m] with fuse		Melting integral I^2t [A^2s]	Conductor cross section			
			A [mm^2]	0.75	1.0	1.5	2.5
			AWG	18	(17)	16	14
Cooper Bussmann	GMA 1A	0.48		48	64	97	162
	GMA 1.25A	0.84		36	49	73	122
	GMA 1.5A	1.6		26	35	53	88
	GMA 1.6A	2		23	31	47	79
	GMA 2A	3.1		19	25	38	63
	GMA 2,5A	4.9		12	16	25	42
	GMA 3,15A	4.9		7	9	14	23
	GMA 3,5A	9.7		6	8	12	21
	GMA 3,5A	13		4	6	9	16
	GMC 1A	1.8		23	31	47	78
	GMC 1.25A	3.4		17	22	34	56
	GMC 1,5A	5.4		10	14	21	36
	GMC 1,6A	5.8		10	13	20	34
	GMC 2A	8.9		6	9	13	22
	GMC 2,5A	13		4	6	9	15

The cable lengths determined are based on the following parameters:

Tripping:	thermal
Characteristics:	Cooper Bussmann GMA (fast-blow - fast acting) Cooper Bussmann GMC (medium-blow - medium time delay)
Ambient temperature:	+20 °C
Internal resistance R_i of the fuse:	taken into consideration
Comments:	In addition to the short-circuit current, the power supply unit also supplies half the nominal current for load paths connected in parallel.

14 Signaling

A floating signal contact and two digital outputs are available for preventive function monitoring of the power supply. Depending on the configuration of the power supply, either the two digital outputs or one digital and one analog output can be selected. The signal outputs are electrically isolated from the input and output of the power supply.

The current device status of the power supply is signaled using four LED status indicators. The function of each LED status indicator is assigned to a fixed event.

In addition, the power supply can be switched off and on via an external circuit.

The signal outputs are configured on the software side using the QUINT POWER software or the QUINT POWER app. Upon delivery, the power supply is pre-allocated a default configuration for the signal outputs.

14.1 Location and function of the signaling elements

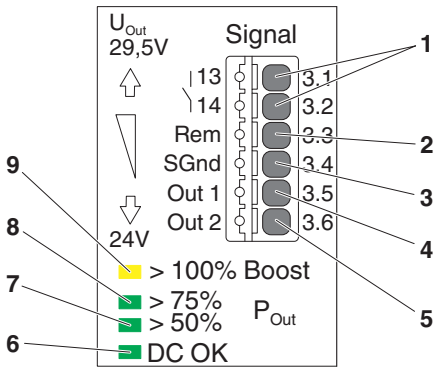


Figure 32 Position of signaling elements

Key

No.	Signaling elements
1	13/14 floating switch contact (N/O contact)
2	Rem, remote input (switch power supply off and on)
3	SGnd, signal ground (reference potential for signals Out 1, Out 2)
4	Out 1 (digital output, function depends on the signal option set)
5	Out 2 (digital or analog output, function depends on the signal option set)
6	LED status indicator DC OK
	LED on: U_{Out} > 90% x U_{Set}
	LED flashing: U_{Out} < 90 % x U_{Set}
7	LED status indicator P_{Out} >50 % (output power >120 W)
8	LED status indicator P_{Out} >75 % (output power >180 W)
9	LED status indicator P_{Out} >100 %, boost mode (output power >240 W)

14.1.1 Floating signal contact

In the default configuration, the floating switch contact opens to indicate that the set output voltage has been undershot by more than 10 % (U_{Out} < 0.9 x U_N). Signals and ohmic loads can be switched. For heavily inductive loads (e. g. a relay), a suitable protective circuit (e. g. a freewheeling diode) is necessary.

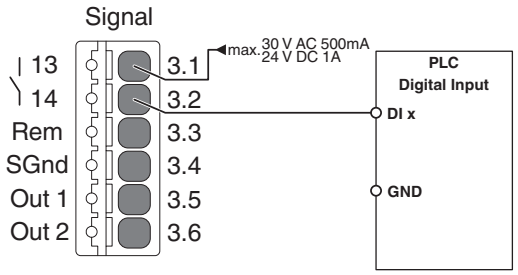


Figure 33 Signaling

14.1.2 Active signal outputs, digital

Signals are forwarded to the higher-level controller via the "Out 1" and "Out 2" signal outputs.

The 24 V DC signal is applied between the connection terminal blocks "Out 1" and "SGnd" or between "OUT 2" and "SGnd". It can carry a maximum of 20 mA.

By switching from "Active High" to "Active Low", the signal output "Out 1" indicates that the set output voltage has been undershot by more than 10 % (U_{OUT} < 0.9 x U_N).

In the default configuration, the signal output "Out 2" indicates that the nominal power has been exceeded. The power supply then switches to boost mode. Thanks to this preventive function monitoring, critical operating states can be recognized at an early stage, prior to a voltage dip occurring.

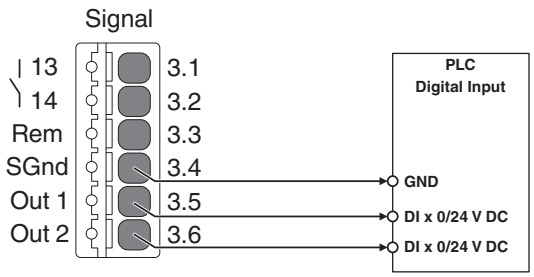


Figure 34 Signaling

14.1.3 Active analog signal output

The signal output "Out 2" can be used as an analog signal output to continuously monitor the device workload.

The 4 ... 20 mA signal is applied between the connection terminal blocks "Out 2" and "SGnd". It is proportional to the set signaling parameter.

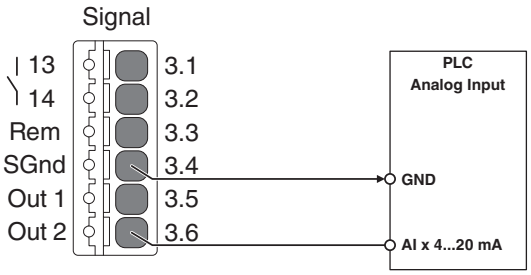


Figure 35 Signaling

If you use the same reference potential for 24 V supply and signals, wire the reference potential SGnd to the reference potential of your application.
The signal outputs of the power supply are electrically isolated from the input and output.

14.2 Preventive function monitoring

In contrast to the default signaling set upon delivery, you can customize this to the specific needs of the system. The following signal options can be selected to signal system states.

QUINT POWER default settings upon delivery			Out 1 digital 0/24 V DC 20 mA	Out 2 digital 0/24 V DC 20 mA	Relay 13/14 floating 24 V DC / ≤ 1 A 30 V AC / ≤ 0.5 A	Out 2 analog 4 ... 20 mA
Ⓥ	Output voltage	① 25 ... 135 % ② 90 %	Default	✓	Default	① 0 ... 32 V DC ② 0 ... 30 V DC
Ⓐ	Output current	① 5 ... 200 % ② 100 %	✓	✓	✓	① 0 ... 20 A ② 0 ... 10 A
Ⓟ	Output power	① 5 ... 200 % ② 100 %	✓	Default	✓	① 0 ... 480 W ② 0 ... 240 W
0 0 0 h	Operating hours	① 0 ... ∞ h ② 10 years	✓	✓	✓	--
ϑ	Early warning of high temperature	Warning of derating	✓	✓	✓	--
OVP	Voltage limitation active	Surge voltage at output	✓	✓	✓	--
AC_{OK}	Input voltage OK	10 ms after mains failure	✓	--	✓	--

Key

Symbol	Description
①	Setting range
②	Default setting of the standard item
Default	Configuration set upon delivery
✓	Configuration that can be selected
--	Configuration that cannot be selected

The simultaneous control of multiple signal outputs by means of one signal option is possible, as is the use of logic operations to link multiple signal options to one control. The power supply is configured using the QUINT POWER software or the QUINT POWER app.

14.3 Description of signaling

14.3.1 Output voltage

Signals whether the output voltage is in the preset range. If the output voltage of the power supply falls below the set threshold value, the signal state changes.

Example of use

Indicates whether the connected load is being supplied. Used to quickly detect a load circuit that is not being supplied (e.g., in the event of mains failure or short circuit in the supply line).

14.3.2 Output current

If the output current of the power supply exceeds the set threshold value, the signal state changes.

Example of use

In the case of system extensions, loads are added. This increases the utilization of the power supply. Preventive function monitoring detects critical operating states in good time. Action can be taken before system downtime occurs.

14.3.3 Output power

If the output power of the power supply exceeds the set threshold value, the signal state changes.

Example of use

In the case of system extensions, loads are added. This increases the utilization of the power supply. Preventive function monitoring detects critical operating states in good time. Action can be taken before system downtime occurs.

14.3.4 Operating hours

If the preset operating time of the power supply is exceeded, the signal state changes.

Example of use

For systems with a very long operating time, such as wind turbine generators or refineries, maintenance intervals are planned. You can even schedule the maintenance date during configuration based on the ambient temperature and utilization of the power supply.

14.3.5 Early warning of high temperature

Before the power supply protects itself through power derating in the event of an overtemperature, the signal state changes.

Example of use

Outdoor control cabinets can reach a high internal temperature depending on the position of the sun. The same is true if a control cabinet fan or cooling system fails. In the event of any form of overtemperature, the power supply provides a warning by means of this signal, well before the supply of the loads is in any danger.

Specifications regarding the available output power (see derating section).

14.3.6 Voltage limitation active

If the circuit inside the device for protecting against surge voltages is activated at the output, the signal state changes.

Example of use

Normative requirements stipulate that an upper voltage limit must be observed at the output in the event of an error. It must therefore be ensured, for example, that safety-related controllers are not supplied with an output voltage that exceeds 32 V DC, even in the event of an error. If foreign bodies (ferrules, screws, etc.) enter the power supply and generate an error, the signal state changes.

14.3.7 Input voltage OK

The power supply signals a mains failure at least 10 ms before shutting off.

Example of use

In the event of a mains failure, the power supply continues to supply the load with nominal power for at least 20 ms. Failure of the input voltage is signaled 10 ms before the output voltage falls, which means that this information is provided to the higher-level controller at an early stage. System states can therefore be stored promptly without any loss of data as a result of the unexpected failure of the supply voltage.

14.4 Remote input

The power supply is switched on and off using the digital remote input of the power supply. When switched off, power transmission is deactivated on the DC output side of the power supply. The load connected to the DC output terminal blocks is no longer supplied with energy. The operating mode where the DC output side is deactivated is called SLEEP MODE.

To switch the power supply to SLEEP MODE, select one of the external circuit versions below. The external circuit is wired between signal terminal blocks Rem (remote input) and SGnd (signal ground).

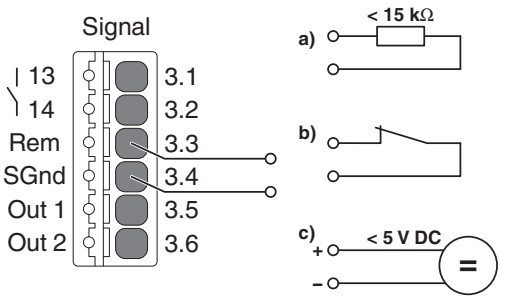


Figure 36 External wiring versions, enable SLEEP MODE

To switch the power supply back on, select one of the following external circuits between signal terminal blocks Rem and SGnd. Power transmission inside the device is activated again. As usual, the energy for supplying the loads is available at the DC output terminal blocks.

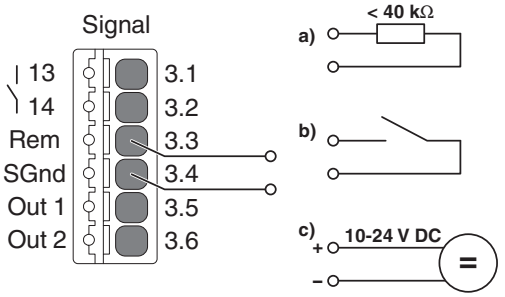


Figure 37 External wiring versions, disable SLEEP MODE

When using a PLC output, select the following external circuit version to switch the power supply to SLEEP MODE.

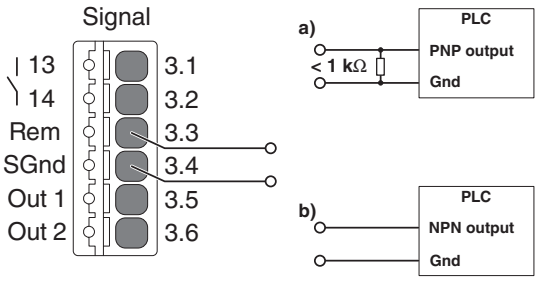


Figure 38 External wiring versions with PNP and NPN output

14.5 LED status indicators

Four LED status indicators are integrated in the front of the power supply, which indicate the current device state.

The green DC OK LED indicates the current status of the output voltage (U_{Out}). The DC OK LED is permanently on as long as the value of the output voltage U_{Out} is ≥ 0.9 x U_{Set}. If the value of the output voltage is < 0.9 x U_{Set}, the green DC OK LED flashes.

Depending on the required output power of the connected load, the three P_{Out} LEDs, which indicate the current output power, light up. Assuming that the provided output power is > 50% of the nominal output power, the > 50% LED lights up green. If the demanded power continues to increase until it is above 75%, the > 75% LED lights up green in addition to the > 50% LED. If the required output power is then greater than the nominal device power, the power supply operates in boost mode. In boost mode, the > 100% LED additionally lights up yellow.

14.6 U/I Advanced characteristic curve signaling

The following table shows the standard assignment for signaling for the U/I Advanced characteristic curves which is set by default.

		Normal operation $P_{Out} < P_N$	BOOST $P_{Out} > P_N$	Overload operation $U_{Out} < 0.9 \times U_{Set}$
LED: P_{Out} >100 %	yellow	☐	■	■
Signal Out 2: $P_{Out} < P_N$	Default	Active High	Active Low	Active Low
LED: $P_{Out} > 75$ %	green	■	■	■
LED: $P_{Out} > 50$ %		■	■	■
LED: DC OK		■	■	✳
Relay: 13/14, DC OK	Default	closed	closed	open
Signal Out 1: DC OK		Active High	Active High	Active Low

☐ LED off ■ LED on ✳ LED flashing

Figure 39 Signal image for U/I Advanced

14.7 SMART HICCUP characteristic curve signaling

The following table shows the standard assignment for signaling for the SMART HICCUP characteristic curve.

		Normal operation $P_{Out} < P_N$	BOOST $P_{Out} > P_N$	Overload operation $U_{Out} < 0.9 \times U_{Set}$
LED: P_{Out} >100 %	Yellow	☐	■	■
Signal Out 2: $P_{Out} < P_N$	Default	Active High	Active Low	Active Low
LED: $P_{Out} > 75$ %	Green	■	■	☐
LED: $P_{Out} > 50$ %		■	■	☐
LED: DC OK		■	■	✳
Relay: 13/14, DC OK	Default	Closed	Closed	Open
Signal Out 1: DC OK		Active High	Active High	Active Low

☐ LED off ■ LED on ✳ LED flashing

Figure 40 Signal image for SMART HICCUP

14.8 FUSE MODE characteristic curve signaling

The following table shows the standard assignment for signaling for the FUSE MODE characteristic curve.

		Normal operation $P_{Out} < P_N$	BOOST $P_{Out} > P_N$	FUSE MODE $I > I_{Fuse}$ for $t > t_{Fuse}$
LED: P_{Out} >100 %	Yellow			
Signal Out 2: $P_{Out} < P_N$	Default	Active High	Active Low	Active Low
LED: P_{Out} > 75 %	Green			
LED: P_{Out} > 50 %				
LED: DC OK				
Relay: 13/14, DC OK	Default	Closed	Closed	Open
Signal Out 1: DC OK		Active High	Active High	Active Low

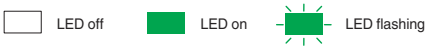


Figure 41 Signal image for FUSE MODE

14.9 SLEEP MODE signaling

In SLEEP MODE, all LEDs are off, all signals are low, and the relay switching contact is open.

14.10 Special immunity for the signal level

14.10.1 Surge protection for the high-voltage area at the power plant

Surge protection (Phoenix Contact Order No.: 2907925 or comparable protection) must be implemented for power plant applications when using signal connection types t (telecommunications area), h (high voltage area) or f (field) in accordance with IEC/EN 61850-3 or signal connection types 3 (process area) and 4 (high voltage area) in accordance with EN 61000-6-5.

When using the digital signals, a relay (Phoenix Contact Order No.: 2900299 or a comparable relay) can be implemented.

14.10.2 Surge protection for signals in railway applications

Surge protection (Phoenix Contact Order No.: 2907925 or comparable protection) must be implemented for railway applications when using signals in accordance with EN 62236-4 and EN 50121-4.

When using the digital signals, a relay (Phoenix Contact Order No.: 2900299 or a comparable relay) can be implemented.

14.10.3 Surge protection for devices in use in safety-related systems

Surge protection (Phoenix Contact Order No.: 2907925 or comparable protection) must be implemented for railway applications when using signals in accordance with EN 61000-6-7 for devices provided to perform functions in safety-related systems (functional safety) in industrial settings.

When using the digital signals, a relay (Phoenix Contact Order No.: 2900299 or a comparable relay) can be implemented.

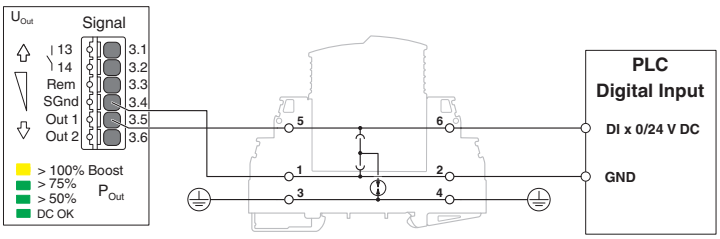


Figure 42 Schematic diagram, signal wiring with TRABTECH surge protection

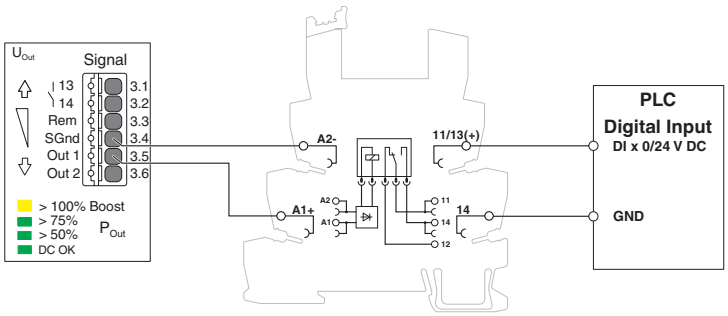


Figure 43 Schematic diagram, signal wiring with relay module

15 Operating modes

15.1 Series operation

To double the output voltage, connect two power supplies in series. Only use power supplies with the same performance class and configuration for series operation. If two 24 V DC power supplies are connected in series, an output voltage of 48 V DC is available to supply the loads.

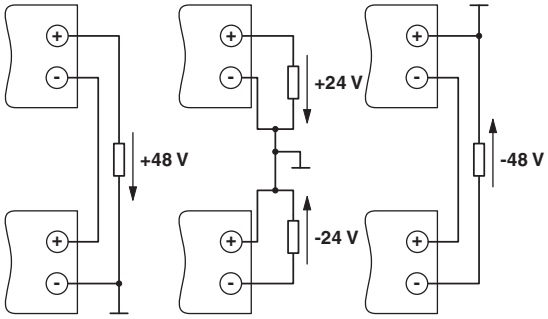


Figure 44 Schematic diagrams in series operation

15.2 Parallel operation

You can connect several power supplies in parallel in order to increase the power or to supply the loads redundantly.

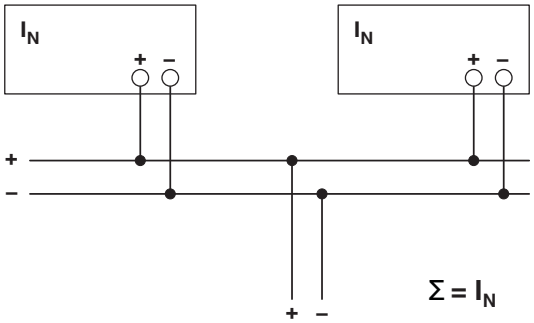


Figure 45 Schematic diagram in parallel operation

Observe the following points when carrying out parallel connection:

1. Use power supplies of the same type and performance class
2. Setting the same output voltages
3. Using the same cable cross sections for wiring
4. Using the same cable lengths for the DC convergence point
5. Operating power supplies in the same temperature environment
6. When three or more power supplies are connected in parallel, each output must be protected (e.g., with circuit breakers, fuses or decoupling modules)

We recommend the configuration "parallel operation" for a parallel connection.
For more detailed information on the operating mode for parallel operation, refer to the user manual for the QUINT POWER software or the QUINT POWER app.

15.2.1 Redundancy operation

Redundant circuits are suitable for supplying systems and system parts which place particularly high demands on operational reliability.

If energy is to be supplied to the load with 1+1 redundancy, two power supplies of the same type and performance class must be used. In the event of an error, it must be ensured that one of the power supplies is able to provide the total required power for the load. This means that in redundancy mode, two 10 A power supplies supply a load with a nominal current of 10 A, for example. During normal operation of the power supplies, each power supply therefore supplies 5 A.

Always use cables with the same cross sections and lengths when wiring the power supplies on the DC output side.

Redundancy modules can be used to 100% decouple two power supplies from one another and to ensure the supply. A distinction is made here between passive and active redundancy modules. Optimum decoupling with simultaneous monitoring and minimal power dissipation can be achieved with the QUINT ORING or QUINT S-ORING active redundancy module.

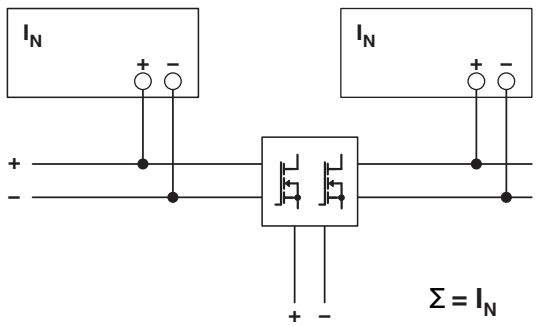


Figure 46 Schematic diagram, redundant operation with QUINT ORING

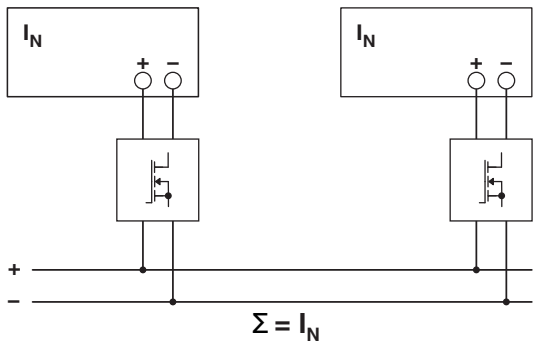


Figure 47 Schematic diagram, redundant operation with QUINT S-ORING

Certain specifications apply in redundancy operation with regard to the configuration of the keepout areas. In redundancy operation, the power supplies are operated with maximum half the nominal power. The keepout areas are therefore reduced.

Using the signaling settings, you can monitor whether both power supplies are being operated with ≤ half the nominal load. In the case of system extension, an overload is prevented if one of the power supplies fails.

15.2.2 Increased power

When n power supplies are connected in parallel, the output current is increased to n x I_N. Parallel connection for increased power is used when extending existing systems. If the individual power supply does not cover the current consumption of the most powerful load, parallel connection of power supplies is recommended.

When three or more power supplies are connected in parallel, each output must be protected separately, e.g., by a circuit breaker, fuse or decoupling module such as QUINT ORING, QUINT S-ORING or QUINT DIODE.

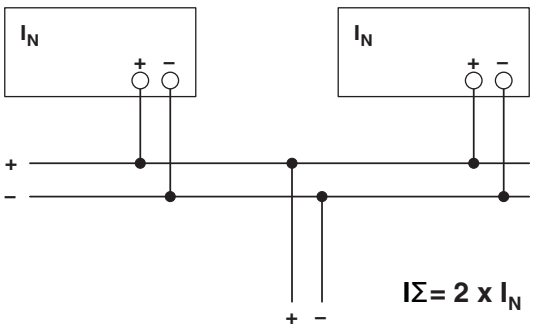


Figure 48 Schematic diagram of increased performance

16 Derating

The QUINT POWER power supply runs in nominal operation without any limitations. For operation outside the nominal range, the following points should be observed depending on the type of use.

16.1 Ambient temperature

When operating the power supply at an ambient temperature of > 60 °C, a power derating of 2.5 %/K should be observed. Up to an ambient temperature of 40 °C, the power supply can take power from the static boost for a sustained period. In the 40 °C to 60 °C temperature range, the power supply can output more than the nominal power for a sustained period.

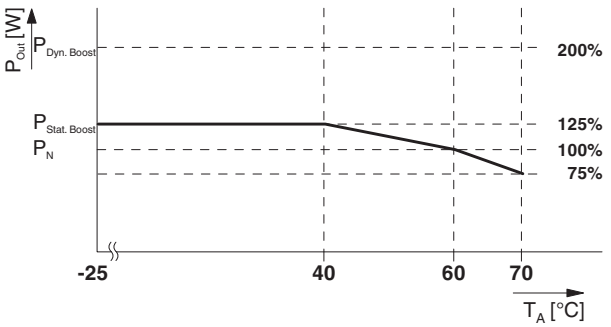


Figure 49 Output power depending on the ambient temperature

16.2 Input voltage

Derating 1 %/V			
U_{In}	T_A	I_{Out}	U_{Out}
< 100 V AC	≤ 60 °C	I_N	24 V DC
< 110 V DC			
< 115 V AC	≤ 40 °C	$I_{Stat. Boost}$	
< 110 V DC			

16.3 Installation height

The power supply can be operated at an installation height of up to 2000 m without any limitations. Different data applies for installation locations above 2000 m due to the differing air pressure and the reduced convection cooling associated with this (see technical data section). The data provided is based on the results of pressure chamber testing performed by an accredited test laboratory.

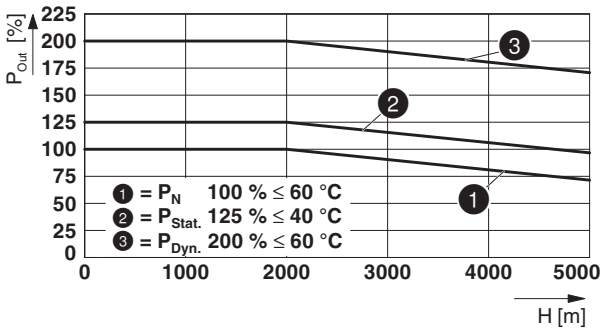


Figure 50 Output power depending on the installation height

16.4 Position-dependent derating

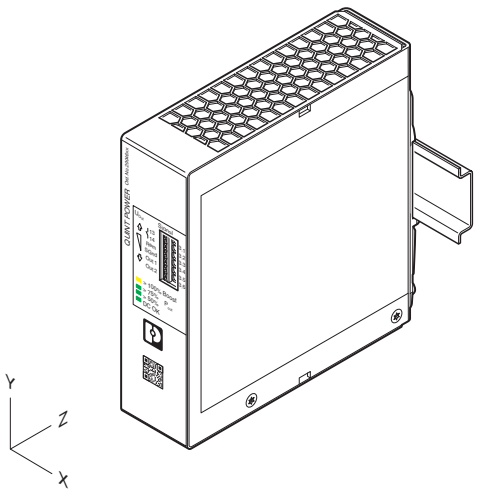
The fanless convection-cooled power supply can be snapped onto all DIN rails according to EN 60715.

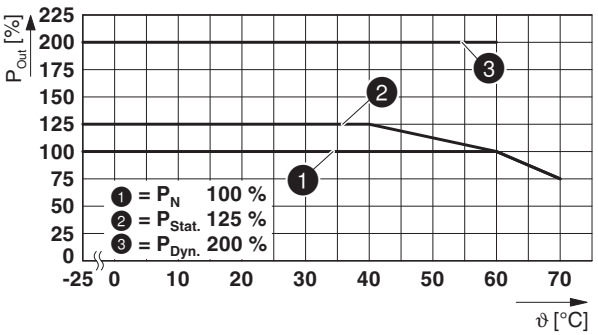
The power supply should be mounted horizontally for heat dissipation reasons (AC connection terminal blocks facing downward). Please observe the derating for any mounting other than the normal mounting position. Reduce the output power based on the prevailing ambient temperature.

The recommended output power for different mounting positions and ambient temperatures can be found in the characteristic curves below.

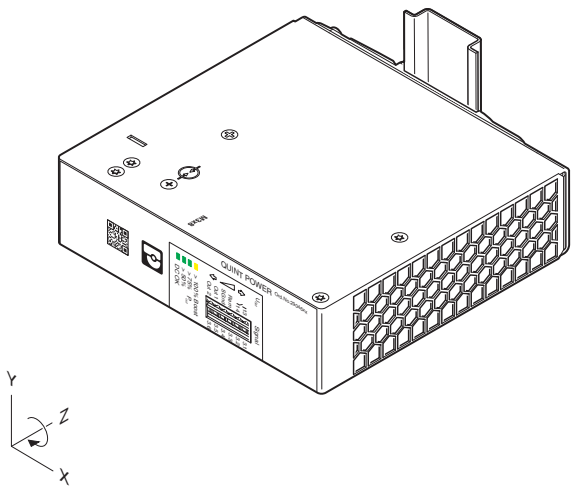
Exceeding these values will reduce the service life of the power supply.

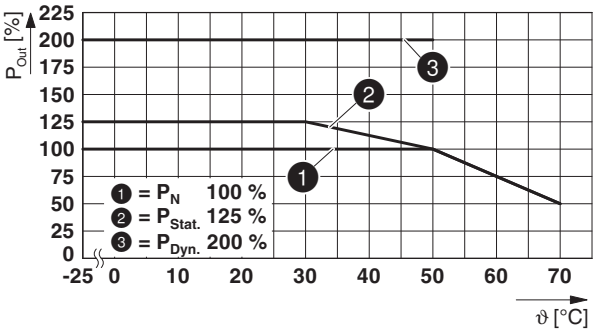
16.4.1 Normal mounting position



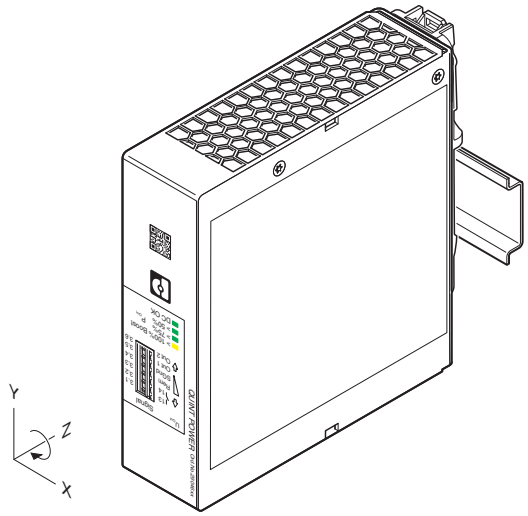


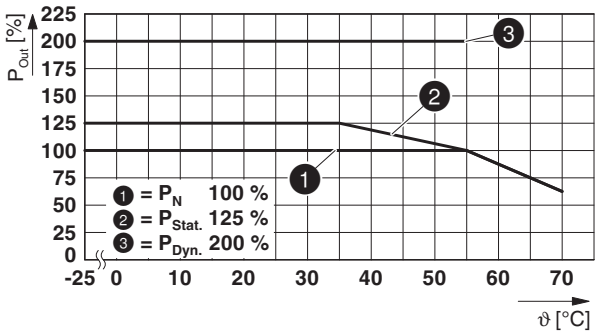
16.4.2 Rotated mounting position 90° Z-axis



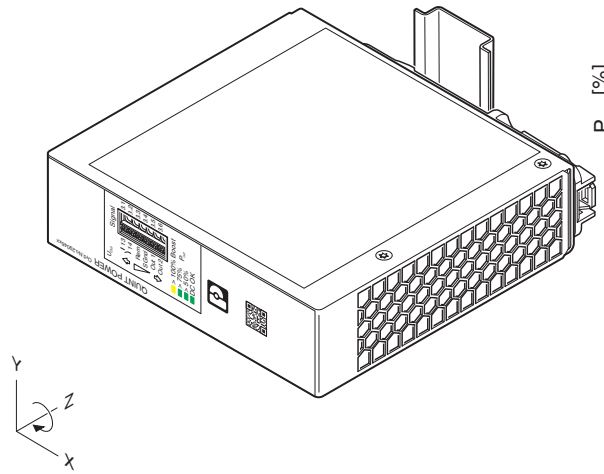


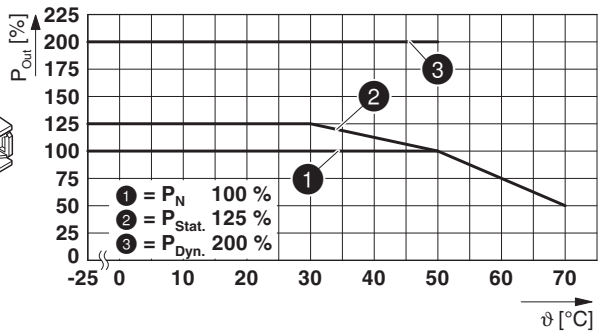
16.4.3 Rotated mounting position 180° Z-axis



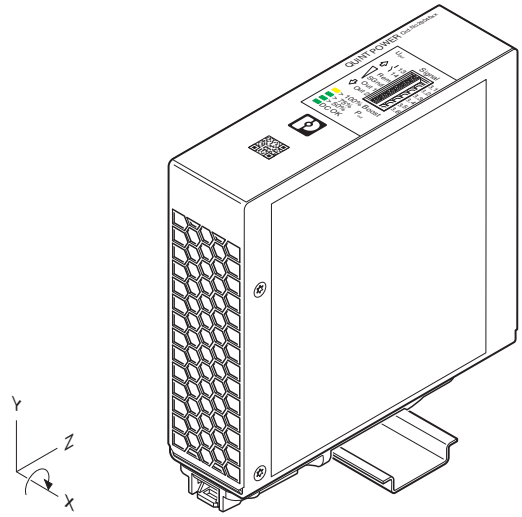


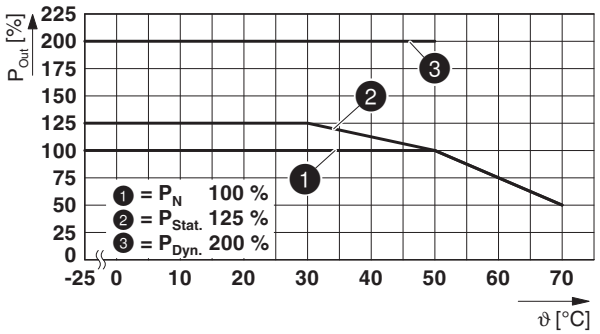
16.4.4 Rotated mounting position 270° Z-axis



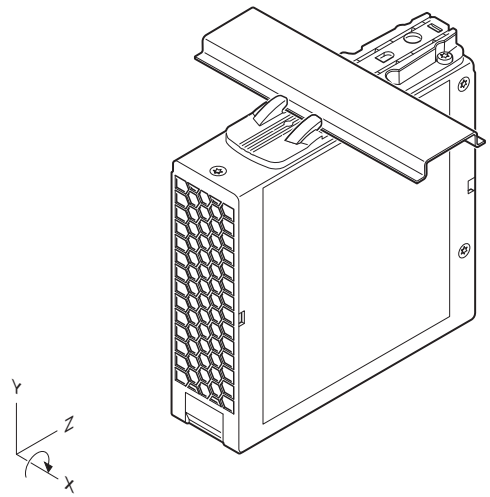


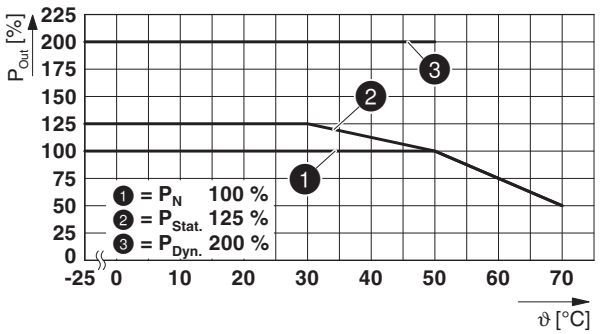
16.4.5 Rotated mounting position 90° X-axis





16.4.6 Rotated mounting position 270° X-axis





QUINT4-CAP/24DC/10/8KJ

Capacity module

Data sheet
107574_en_01

1 Description

The QUINT capacity module combines an electronic switch-over unit and energy storage in the same housing. The capacity module stores the energy required to bridge mains failures in maintenance-free double-layer capacitors. Long mains buffering is possible depending on the required load current.

- Maximum energy efficiency
- High level of system availability due to high capacitor service life
- Large temperature range
- Electronic switchover unit and energy storage device in one housing
- USB interface for connection to higher-level controllers
- Maintenance-free, thanks to double-layer capacitors
- Space savings, thanks to the compact design
- Thanks to soft start, can be used with power supplies in the low power range

Technical data (short form)	
Nominal input voltage	24 V DC (SELV)
Input voltage range	22.5 V DC ... 30 V DC
Current consumption ($I_{No\text{-}Load}$ / I_{Charge} / I_{Max})	0.1 A / 1 A / 13.5 A
Activation threshold Undervoltage Overvoltage	 < 22 V DC > 30 V DC
Buffer time	5 min. (1 A) / 30 s (10 A)
Charging time (for completely discharged capacitors)	approx. 22 min.
Recharging time	approx. 12 min.
Nominal output voltage (U_N)	24 V DC
Nominal output current I_N / $I_{Stat.\ Boost}$	10 A / 12.5 A
Efficiency (with charged energy storage device)	> 97 %
MTBF (IEC 61709, SN 29500)	2102818 h (25 °C) 1387185 h (40 °C) 697626 h (60 °C)
Ambient temperature (operation)	-25 °C ... 60 °C (> 40 °C Derating: 1 %/K)
Dimensions W/H/D	118 mm / 130 mm / 125 mm
Weight	1.6 kg

All technical specifications are nominal and refer to a room temperature of 25 °C and 70% relative humidity at 2000 m above sea level.

2 Table of contents

3 Ordering data

Description	Type	Order No.	Pcs./Pkt.
QUINT capacity module, with maintenance-free energy storage based on double-layer capacitor, DIN rail mounting, input: 24 V DC, output: 24 V DC / 10 A / 8 kJ incl. mounted UTA 107 universal DIN rail adapter. The “POWER MANAGEMENT SUITE” software (Order No. 1252232) available in the download area can be used for configuration.	QUINT4-CAP/24DC/10/8KJ	2320571	1

Accessories	Type	Order No.	Pcs./Pkt.
2-piece universal wall adapter for securely mounting the device in the event of strong vibrations. The profiles that are screwed onto the side of the device are screwed directly onto the mounting surface. The universal wall adapter is attached on the left/right.	UWA 130	2901664	1
Universal wall adapter for securely mounting the device in the event of strong vibrations. The device is screwed directly onto the mounting surface. The universal wall adapter is attached on the top/bottom.	UWA 182/52	2938235	1
Used for communication between an industrial PC and Phoenix Contact devices with USB-Mini-B connection.	MINI-SCREW-USB-DATACABLE	2908217	1
Configuration and management software	POWER MANAGEMENT SUITE	1252232	1

Our range of accessories is being continually extended, our current range can be found in the download area.

4 Technical data

Input data	
Nominal input voltage	24 V DC (SELV)
Input voltage range	22.5 V DC ... 30 V DC
Dielectric strength	max. 35 V DC (Reverse polarity protection)
Activation threshold Undervoltage Overvoltage	 < 22 V DC > 30 V DC
Voltage drop, input/output	0.5 V DC
Buffer time	5 min. (1 A) / 30 s (10 A)
Charging time ( )	approx. 22 min.
Recharging time	approx. 12 min.
Current consumption I_N (U_N, $I_{Out} = I_N$, $I_{Charge} = 0$) $I_{No\text{-}Load}$ (U_N, $I_{Out} = 0$, $I_{Charge} = 0$) I_{Charge} (U_N, $I_{Out} = 0$, I_{Charge} = max) I_{Max} (U_N, $I_{Out} = I_{Stat.Boost}$, I_{Charge} = max)	 13.5 A (max.) 0.1 A 1 A 13.5 A
Power consumption P_N (U_N, $I_{Out} = I_N$, $I_{Charge} = 0$) $P_{No\text{-}Load}$ (U_N, $I_{Out} = 0$, $I_{Charge} = 0$) P_{Charge} (U_N, $I_{Out} = 0$, I_{Charge} = max) P_{Max} (U_N, $I_{Out} = I_{stat.Boost}$, I_{Charge} = max)	 245 W 2.5 W 24 W 324 W
Inrush current	≤ 7 A (≤ 4 ms)
Internal input fuse	no
Switch-on time in buffer mode	1 ms

Input connection data	
Connection method	Screw connection
Conductor cross section, rigid	0.2 mm² ... 2.5 mm²
Conductor cross section, flexible	0.2 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.25 mm² ... 2.5 mm²
2 conductors with same cross section, solid	0.2 mm² ... 0.75 mm²
2 conductors with same cross section, stranded	0.2 mm² ... 0.75 mm²
Two conductors with the same cross section, flexible, with TWIN ferrule with plastic sleeve	0.5 mm² ... 1.5 mm²
Conductor cross section AWG	30 ... 12
Stripping length	6.5 mm
Torque	0.5 Nm ... 0.6 Nm

Output data (mains operation)	
Nominal output voltage U_N (depending on the input voltage)	24 V DC
Nominal output current I_N / $I_{Stat.\ Boost}$	10 A / 12.5 A
Output power P_N (U_N, $I_{Out} = I_N$, $I_{Charge} = 0$) $P_{Stat.Boost}$ (U_N, $I_{Out} = I_{Stat.Boost}$, $I_{Charge} = 0$)	 240 W 300 W
Power dissipation No load (U_N, $I_{Out} = 0$, $I_{Charge} = 0$) Nominal load (U_N, $I_{Out} = I_N$, $I_{Charge} = 0$)	 2.5 W 6 W
Short-circuit-proof	yes (with input fuse)
No-load proof	yes
Output data (buffer mode)	
Nominal output voltage U_N (typical)	22 V DC
Nominal output current I_N / $I_{Stat.\ Boost}$	10 A / 12.5 A
Output power P_N (U_N, $I_{Out} = I_N$, $I_{Charge} = 0$) $P_{Stat.Boost}$ (U_N, $I_{Out} = I_{Stat.Boost}$, $I_{Charge} = 0$)	 240 W 300 W
Short-circuit-proof	yes
No-load proof	yes
Efficiency	
with charged energy storage device	> 97 %
MTBF (IEC 61709, SN 29500)	
	2102818 h (25 °C) 1387185 h (40 °C) 697626 h (60 °C)
Output connection data	
Connection method	Screw connection
Conductor cross section, rigid	0.2 mm² ... 2.5 mm²
Conductor cross section, flexible	0.2 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.25 mm² ... 2.5 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.25 mm² ... 2.5 mm²
2 conductors with same cross section, solid	0.2 mm² ... 0.75 mm²
2 conductors with same cross section, stranded	0.2 mm² ... 0.75 mm²
Two conductors with the same cross section, flexible, with TWIN ferrule with plastic sleeve	0.5 mm² ... 1.5 mm²
Conductor cross section AWG	30 ... 12
Stripping length	6.5 mm
Torque	0.5 Nm ... 0.6 Nm

Signal state U_{In} OK	
Connection labeling	3.1, 3.2
Channel	DO (digital output)
Switch contact (floating 13/14)	Electronic relays (OptoMOS)
State (configurable)	U_{In} OK
State condition (configurable)	U_{IN} > 22.5 V DC, U_{IN} < 30 V DC
Output voltage	max. 30 V
Output can be loaded	300 mA
State - signal assignment	active - high
LED status indicator	green (U_{In} OK)
Alarm signal state	
Connection labeling	3.3
Channel	DO (digital output)
Switching output	Transistor
State (configurable)	Group alarm
State condition (configurable)	Alarm
Output voltage	24 V (U_N - 1 V (typical))
Output can be loaded	max. 20 mA
State - signal assignment	active - low
Reference potential	3.6 (SGnd, identical to 1.2, 2.2)
LED status indicator	red (Alarm)
Ready signal state	
Connection labeling	3.4
Channel	DO (digital output)
Switching output	Transistor
State (configurable)	Ready
State condition (configurable)	State of charge = 100% or buffer mode
Output voltage	24 V (U_N - 1 V (typical))
Output can be loaded	max. 20 mA
State - signal assignment	active - high
Reference potential	3.6 (SGnd, identical to 1.2, 2.2)
LED status indicator	Green (state of charge - SOC)
Remote signal state	
Connection labeling	3.5
Channel	DI (digital input)
State (configurable)	Remote
State condition	Remote
Low signal High signal	<3 kΩ to SGnd open (>470 kΩ between Remote and SGnd)
Signal - state assignment	low - active
Reference potential	3.6 (SGnd, identical to 1.2, 2.2)

Signal ground SGnd	
Connection labeling	3.6
Switching voltage	0 V
Current carrying capacity	max. 60 mA
Function	Signal ground
Reference potential	3.3 Alarm, 3.4 Ready, 3.5 Remote

Signal connection data	
Connection method	Push-in connection
Conductor cross section, rigid	0.2 mm² ... 1.5 mm²
Conductor cross section, flexible	0.2 mm² ... 1.5 mm²
Conductor cross section flexible, with ferrule with plastic sleeve	0.2 mm² ... 0.75 mm²
Conductor cross section flexible, with ferrule without plastic sleeve	0.2 mm² ... 1.5 mm²
Conductor cross section AWG/kcmil	24 ... 18
Stripping length	8 mm

Data interface	
Interface designation	USB (Modbus/RTU)
Connection labeling	5.1
Number of interfaces	1
Connection method	MINI-USB Type B
Locking	Screw
Transmission physics	USB 2.0
Topology	Point-to-point
Transmission speed	9600 baud
Transmission length	max. 5 m
Access time	≤ 2 s
Chipset	Silicon Labs CP2104-F03-GM
Electrical isolation	Yes, UL approved

General data	
Storage medium	Double-layer capacitor
Insulation voltage input, output / housing	500 V
Degree of protection	IP20
Protection class	III (SELV)
Inflammability class in acc. with UL 94 (housing / terminal blocks)	V0
Overvoltage category UL 60950-1	II
Connection in parallel	no
Connection in series	no
Mounting position	horizontal DIN rail NS 35, EN 60715
Installation height	≤ 4000 m
Dimensions W / H / D (state of delivery)	118 mm / 130 mm / 125 mm
Weight	1.6 kg

Ambient conditions	
Ambient temperature (operation)	-25 °C ... 60 °C (> 40 °C Derating: 1 %/K)
Ambient temperature (start-up type tested)	-40 °C
Ambient temperature (storage/transport)	-40 °C ... 60 °C
Max. permissible relative humidity (operation)	≤ 95 %
Degree of pollution	2
Vibration (operation)	0,7g
Shock	30g, 18 ms per spatial direction (in accordance with IEC 60068-2-27)
Climatic class	3K3 (in acc. with EN 60721)

Standards	
Protective extra-low voltage	UL 61010-2-201

Approvals	
UL	cULus Listed: UL/C-UL Listed UL 508 CAN/CSA-C22.2 No. 107.1-01 UL/C-UL Recognized UL 60950-1 UL ANSI/ISA-12.12.01 Class I, Division 2, Groups A, B, C, D (Hazardous Location)
CB Scheme	UL 60950-1

Current approvals/permissions for the product can be found in the download area under phoenixcontact.net/products

Electromagnetic compatibility / Conformance with EMC Directive 2014/30/EU		
Noise emission in accordance with EN 61000-6-3 and EN 61000-6-4		
CE basic standard	**Minimum normative requirements**	**Higher requirements in practice (covered)**
Noise emission EN 55016	EN 61000-6-4	EN 61000-6-3

Device immunity in accordance with EN 61000-6-2		
CE basic standard	**Minimum normative requirements**	**Higher requirements in practice (covered)**
Electrostatic discharge EN 61000-4-2		
Housing contact discharge	4 kV (Test Level 2)	6 kV (Test Level 3)
Housing air discharge	8 kV (Test Level 3)	8 kV (Test Level 3)
Comments	Criterion B	Criterion B
Electromagnetic HF field EN 61000-4-3		
Frequency range	80 MHz ... 1 GHz	80 MHz ... 6 GHz
Test field strength	10 V/m	10 V/m
Comments	Criterion A	Criterion A
Fast transients (burst) EN 61000-4-4		
Input	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 3 - asymmetrical)
Output	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 3 - asymmetrical)
Comments	Criterion B	Criterion B
Surge voltage load (surge) EN 61000-4-5		
Input/Output	1 kV (Test Level 2 - symmetrical) 2 kV (Test Level 3 - asymmetrical)	1 kV (Test Level 2 - symmetrical) 2 kV (Test Level 3 - asymmetrical)
Comments	Criterion B	Criterion B
Conducted interference EN 61000-4-6		
Frequency range	0.15 MHz ... 80 MHz	0.15 MHz ... 80 MHz
Voltage	10 V	10 V
Comments	Criterion A	Criterion A

Signal immunity in accordance with EN 61000-6-2		
CE basic standard	**Minimum normative requirements**	**Higher requirements in practice (covered)**
Fast transients (burst) EN 61000-4-4		
Signal	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 3 - asymmetrical)
Comments	Criterion B	Criterion B
Surge voltage load (surge) EN 61000-4-5		
Signal	1 kV (Test Level 2 - asymmetrical)	1 kV (Test Level 2 - asymmetrical)
Comments	Criterion B	Criterion B
Conducted interference EN 61000-4-6		
Frequency range	0.15 MHz ... 80 MHz	0.15 MHz ... 80 MHz
Voltage	10 V	10 V
Comments	Criterion A	Criterion A

Key	
Criterion A	Normal operating behavior within the specified limits.
Criterion B	Temporary impairment to operational behavior that is corrected by the device itself.

5 Safety regulations and installation notes

5.1 Symbols used

Instructions and possible hazards are indicated by corresponding symbols in this document.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible personal injuries.

There are different categories of personal injury that are indicated by a signal word.

WARNING

This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This indicates that the device can be hot and should not be touched without taking care.

The following symbols are used to indicate potential damage, malfunctions, or more detailed sources of information.

NOTE

This symbol together with the signal word NOTE and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

5.2 Safety and warning notes

WARNING: Danger to life by electric shock!

- Only skilled persons may install, start up, and operate the device.
- Never carry out work when voltage is present.
- Only remove equipment when it is disconnected and not in the potentially explosive area.
- Establish connection correctly and ensure protection against electric shock.
- Ensure cables are the correct size for the maximum input/output current and have fuse protection.
- Cover termination area after installation in order to avoid accidental contact with live parts (e. g., installation in control cabinet).
- Keep flames, embers or sparks away from the module.
- If the capacity module is disconnected from the power supply, there may still be a residual charge/voltage.

CAUTION: Hot surface

The housing can become hot, depending on the ambient temperature and device load.

NOTE

- Observe the national safety and accident prevention regulations.
- Assembly and electrical installation must correspond to the state of the art.
- The capacity module is a built-in device. The IP20 degree of protection of the device is intended for use in a clean and dry environment.
- The device must be installed in a control cabinet that can be locked and only opened by specialist staff.
- Observe mechanical and thermal limits.
- Horizontal mounting (terminals on top)
- Ensure sufficient convection (minimum gap above/ below: 50 mm). Housing can become hot.
- Use copper cables for operating temperatures of >75 °C.
- Refer to the corresponding table for the connection parameters, such as the necessary stripping length for wiring with and without ferrule (see section Device connection).
- Use ferrules for flexible cables.
- Protect the device against foreign bodies penetrating it, e.g., paper clips or metal parts.
- The device may only be used for its intended use.
- Improper use invalidates the device protection.
- The capacity module is maintenance free and may not be opened.
- Before transport, the capacity module must be completely discharged.
- A suitable fire and electrical enclosure must be provided in the end application.

More follows

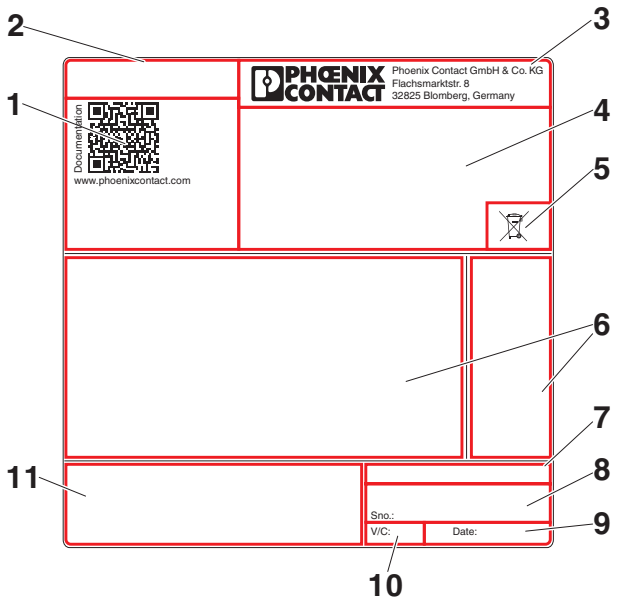
- Do not exceed max. input/output current of 16 A. Use current-limited source, e. g., QUINT POWER or suitable fuse.
- Keep these instructions in a safe place – this data sheet contains important safety notes which must be observed during installation and maintenance of the device.

6 Design

6.1 Rating plate

The rating plate for the capacity module is located on the right-hand side of the housing (viewed from the front).

Figure 1 Rating plate information

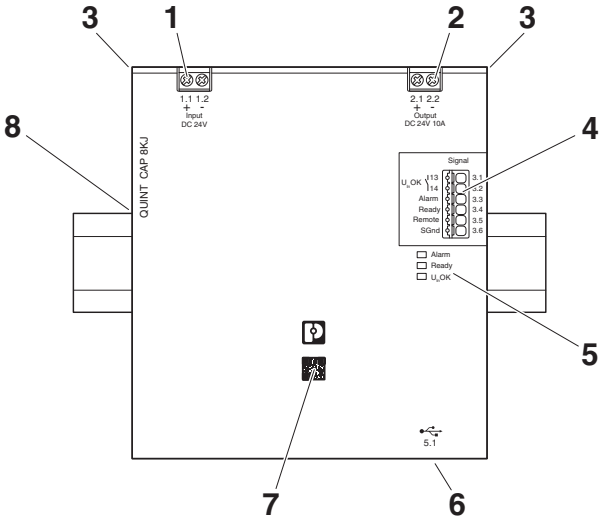


Key

No.	Designation
1	QR code as web link to the device documentation
2	Device designation and order number
3	Identification of the provider
4	Device connection data
5	Note on disposal
6	Device approvals
7	Production site of the Phoenix Contact Group
8	Bar code and serial number for device identification
9	Date of manufacture
10	Device version
11	Warning notice and note on device documentation accompanying the product

6.2 Function elements

Figure 2 Position of the function elements



Key

No.	Designation	Connection labeling
1	Connection terminal blocks for DC input (Input + / -)	1.1, 1.2
2	Connection terminal blocks for DC output (Output + / -)	2.1, 2.2
3	Accommodation for cable binders	
4	Signaling connection terminal blocks	3.1 ... 3.6
5	Status and diagnostics indicators	
6	USB interface MINI type B (bottom of device)	5.1
7	QR code web link	
8	Universal DIN rail adapter (rear of housing)	

6.3 Device dimensions and keep-out areas

Figure 3 Keep-out areas

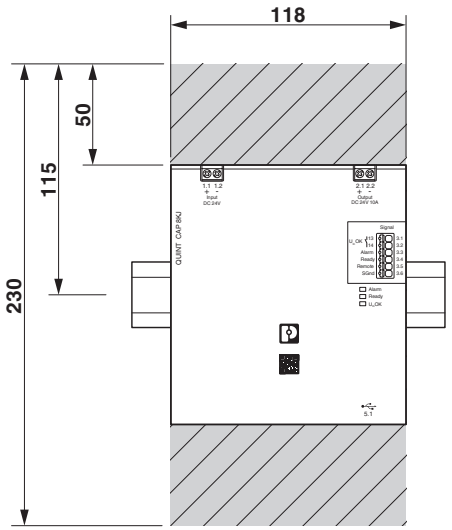
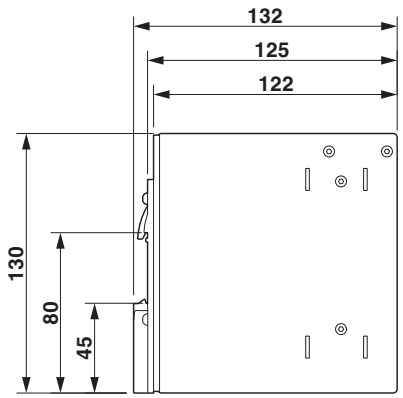
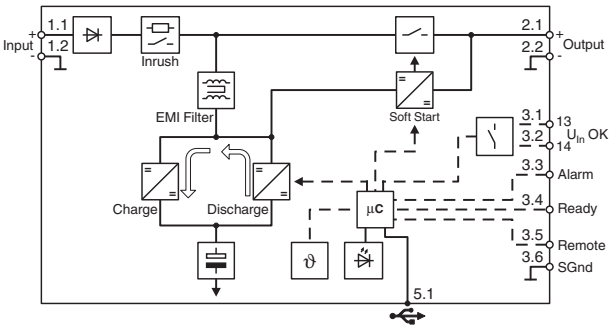


Figure 4 Device dimensions



6.4 Block diagram

Figure 5 Block diagram



Key

Symbol	Meaning
	Reverse polarity protection
	Inrush current limitation
	Switch
	EMI filter
	Electrolytic capacitor
	DC/DC converter
µC	Microprocessor
	Temperature sensor
	LED

7 Mounting and removing

The device must be installed in a control cabinet that can be locked and only opened by specialist staff.

7.1 Convection

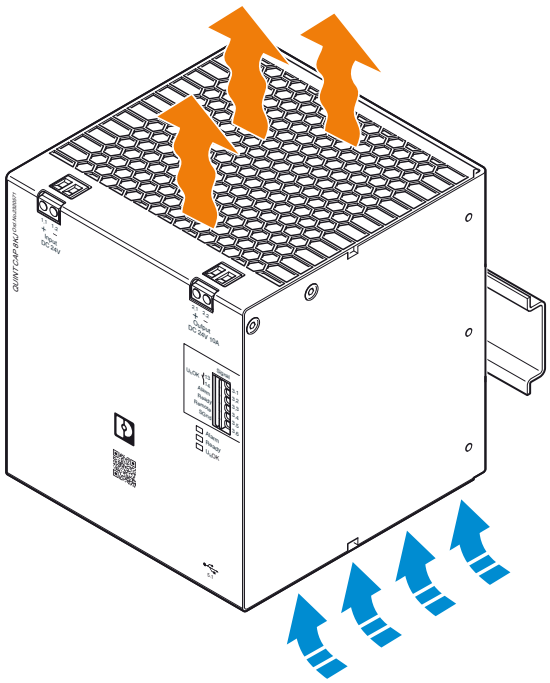
CAUTION: Hot surface

The housing can become hot, depending on the ambient temperature and device load.

NOTE: enable convection

In order to ensure sufficient convection, we recommend a minimum vertical distance of 50 mm to the other devices.

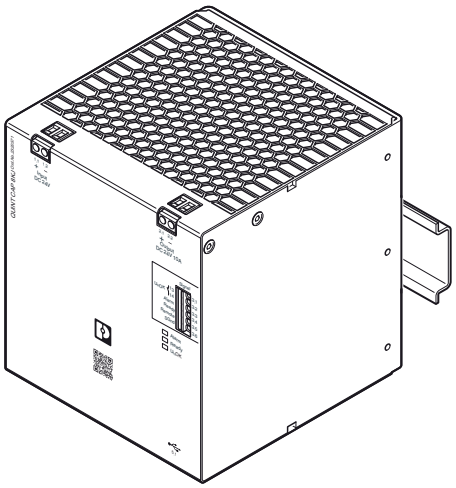
Figure 6 Convection



7.2 Normal mounting position

The device can be snapped onto all DIN rails according to EN 60715 and should only be mounted in the normal mounting position.

Figure 7 Normal mounting position

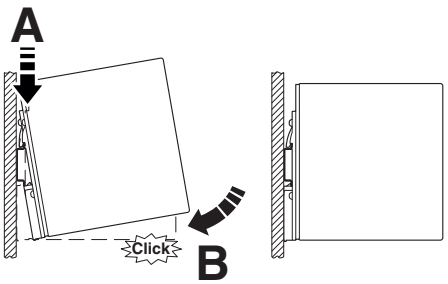


7.3 Mounting the capacity module

Proceed as follows to mount the device:

1. In the normal mounting position the device is mounted on the DIN rail from above. Make sure that the universal DIN rail adapter is in the correct position behind the DIN rail (A).
2. Then press the device down until the universal DIN rail adapter audibly latches into place (B).
3. Check that the device is securely attached to the DIN rail.

Figure 8 Snapping onto the DIN rail



7.4 Removing the capacity module

WARNING:Never carry out work when voltage is present!

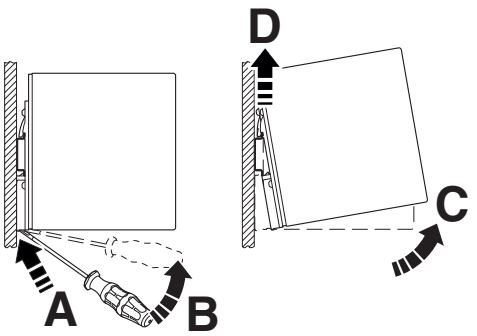
Switch off the supply voltage and ensure it cannot be switched on again!

Disconnect the connecting cables before you remove the device.

Proceed as follows to remove the device:

1. Take a suitable screwdriver and insert this into the lock hole on the universal DIN rail adapter (A).
2. Release the lock by lifting the screwdriver (B).
3. Carefully swivel the device forward (C) so that the lock slides back into the starting position.
4. Then separate the device from the DIN rail (D).

Figure 9 Removing from the DIN rail



7.5 Wall mounting

The UWA 182/52 universal wall adapter (Order No. 2938235) or UWA 130 universal wall adapter (Order No. 2901664) is used to attach the device directly to the mounting surface.

The use of the universal wall adapter is recommended under extreme ambient conditions, e.g., strong vibrations. Thanks to the tight screw connection between the device and the universal wall adapter or the actual mounting surface, an extremely high level of mechanical stability is ensured.

The maximum tightening torque of the Torx screw (Torx® T10) is 0.9 Nm.

Make sure you use suitable mounting material when attaching to the mounting surface.

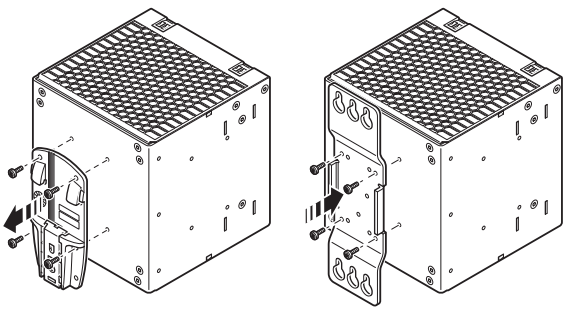
7.5.1 Mounting the UWA 182/52 universal wall adapter

The UWA 182/52 universal wall adapter (Order No. 2938235) is attached to the device by means of the Torx screws of the universal DIN rail adapter.

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Remove the universal DIN rail adapter from the rear of the device.
3. Position the universal wall adapter in such a way that the keyholes or oval tapers face up. The mounting surface for the device is the raised section of the universal wall adapter.
4. Insert the Torx screws into the appropriate hole pattern on the universal wall adapter so that the necessary mounting holes of the device can be accessed.
5. Screw the universal wall adapter onto the device.

Figure 10 Mounting the UWA 182/52 universal wall adapter



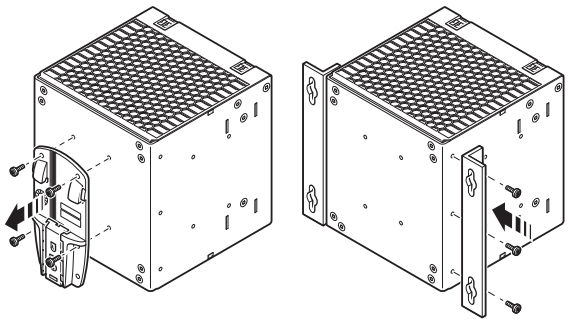
7.5.2 Mounting the UWA 130 2-piece universal wall adapter

The UWA 130 universal wall adapter (Order No. 2901664) is attached to the device using the Torx screws provided.

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Remove the universal DIN rail adapter from the rear of the device.
3. Position the two-piece universal wall adapter on the right and left side of the housing.
4. Insert the Torx screws into the appropriate hole pattern on the universal wall adapter so that the necessary mounting holes of the device can be accessed.
5. Screw the two-piece universal wall adapter onto the device.

Figure 11 Mounting the UWA 130 universal wall adapter

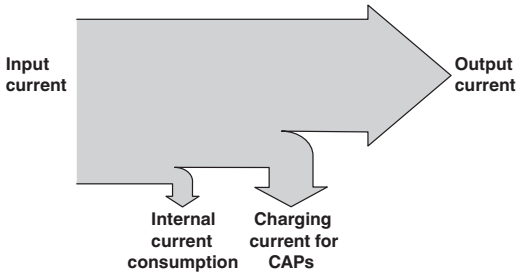


8 Device connection

8.1 Electrical installation design

When designing the electrical installation of the capacity module, take the technical data on charging current, self-consumption and loads to be supplied into consideration.

Figure 12 Electrical installation layout



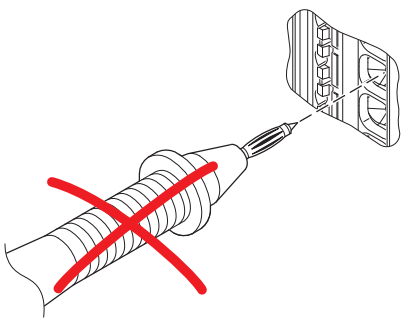
8.2 Connection parameters

For the connection parameters, including the required stripping length for wiring with and without ferrule, refer to the Section: Technical data.

9 Device connection terminal blocks

NOTE: Damage to the Push-in connection terminal blocks is possible

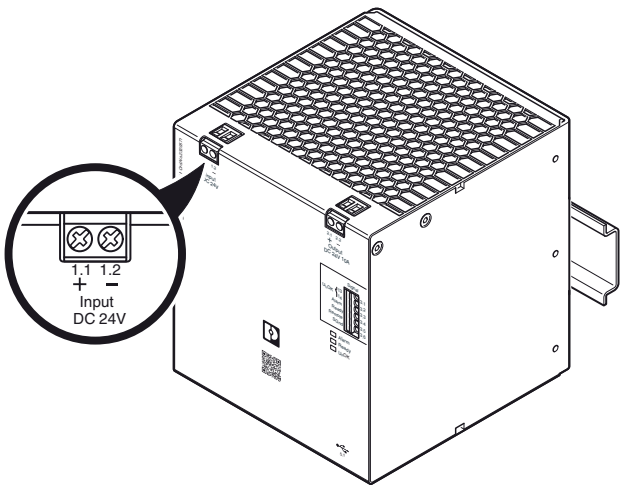
Do not plug test pins into the Push-in connection terminal blocks. The maximum pluggable depth of the Push-in connection terminal blocks is limited. In addition, when the test pin is plugged in, the unlocking button (pusher) is covered to such an extent that unlocking is not possible or only possible to an insufficient extent. If you do not push the unlocking button (pusher) down completely when you are pulling the test pin out, then the Push-in connection terminal block will become damaged.



9.1 DC input connection terminal blocks

The supply voltage is connected via the Input + / - connection terminal blocks.

Figure 13 Input voltage connection terminal blocks: Input +/- (1.1, 1.2)



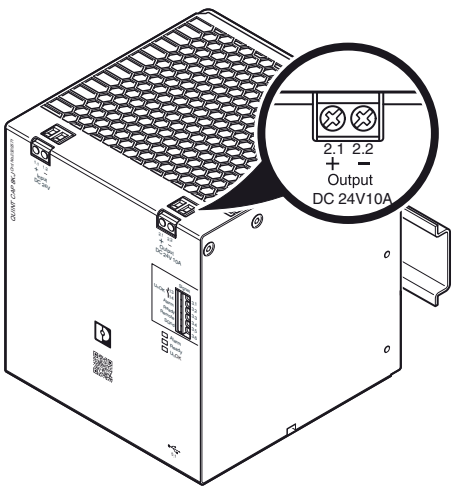
9.1.1 Protection of the primary side

Do not exceed max. input/output current of 16 A. Use current-limited source, e. g., QUINT POWER or suitable fuse.

9.2 DC output connection terminal blocks

The output voltage is connected via the "Output" connection terminal blocks.

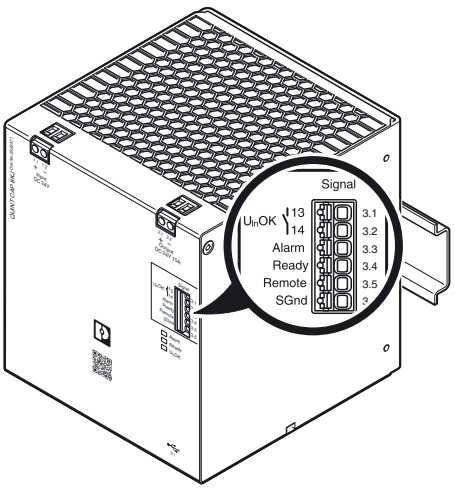
Figure 14 Output voltage connection terminal blocks: Output +/- (2.1, 2.2)



9.3 Connection terminal block signaling

The signals are connected via the Push-in connection terminal blocks for signaling.

Figure 15 Connection terminal block signaling (3.1 ... 3.6)



9.4 Securing the connection wiring

NOTE: Mechanical damage to the connection wiring caused by friction

In the event of extreme ambient conditions, e.g. strong vibrations, friction can be generated between the connection wiring and cable tie. Protect the connection wiring against mechanical damage using additional insulation material. The additional insulation material for protecting the connection wiring is limited to the area where the cable ties are attached.

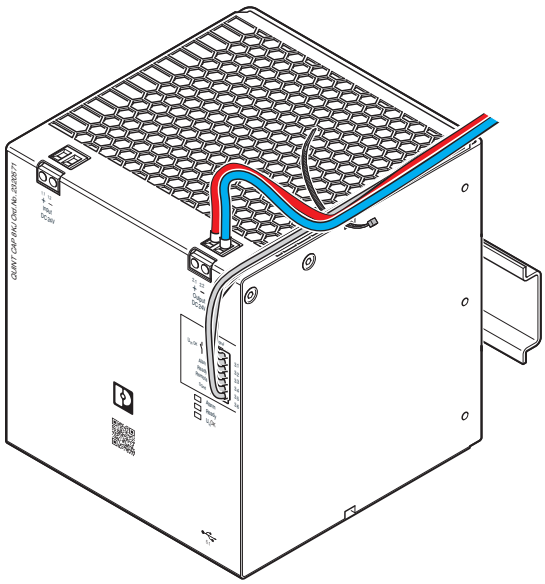
NOTE:

When wiring or disconnecting the connections, observe the bend radii specified by the manufacturer.

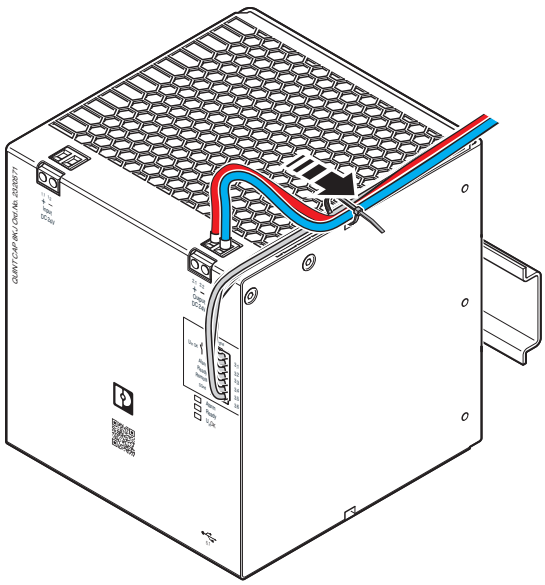
Two receptacles for the bundled attachment of the connection wiring are integrated in the left and right housing panel. Use cable ties to secure the connection wiring (optional WT-HF 3,6X140 - Order No. 3240744).

Secure the connection wiring as follows:

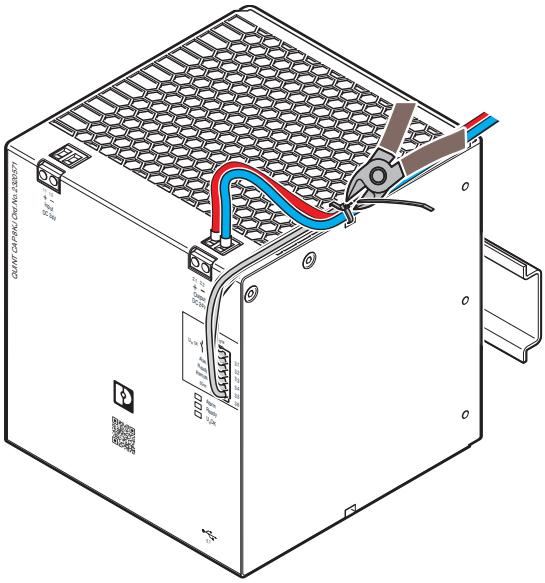
– Wire the device with sufficient connection reserves (input terminal blocks and output terminal blocks).
– Bundle and lay out the connection wiring such that the ventilation slots on the top of the housing are covered as little as possible
– Thread the cable tie through the opening provided on the top of the housing



– Tighten the cable tie
– When doing so, ensure that the connection wiring is attached safely and securely without damaging the connection wiring



– Shorten the excess length of the cable ties.

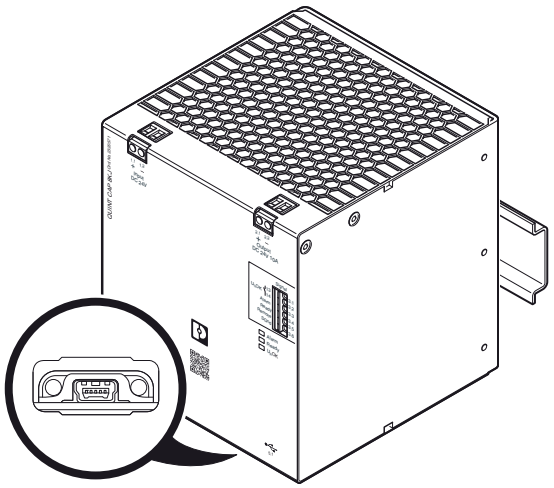


10 Communication interface

10.1 Communication via the USB interface

The capacity module is equipped with a USB Mini type B interface for data transmission.

Figure 16 Service USB interface Mini type B (device bottom) (5.1)



You can set individual parameters and perform a controlled shutdown of the PC via the USB interface. To do so, connect the capacity module to the PC using the USB connection cable.

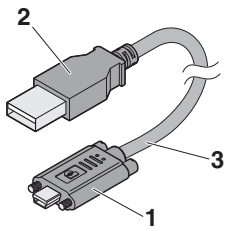
In this case of point-to-point coupling (Modbus/RTU protocol), the connected PC will continue to operate after a mains failure. Buffer mode guarantees availability until all of the data from the PC buffer has been saved. The PC subsequently performs a controlled shutdown. The PC is restarted when the mains voltage is restored.

The optional USB connection cable (MINI-SCREW-USB-DATACABLE, Order No. 2908217) is required for controlled shutdown in PC mode.

10.1.1 MINI-SCREW-USB-DATACABLE

The device is connected to the USB interface on the PC via the USB Mini type B interface with data cable MINI-SCREW-USB-DATACABLE (order number 2908217).

Figure 17 MINI-SCREW-USB-DATACABLE

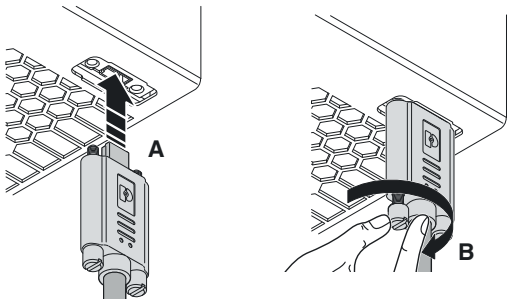


No.	Designation
1	Mini type B USB connector with screw connection
2	USB plug type A
3	Cable length: 3 m

NOTE: Damage

Tighten the screws with your fingers. If you use a tool instead, do not exceed a maximum torque of 0.2 Nm.

Figure 18 Connecting USB data cables



10.2 Modbus/RTU

The Modbus protocol is a communication protocol based on a client/server or controller/device architecture. Modbus/RTU is a point-to-point connection via USB interface.

To communicate with the capacity module, you must connect the device to the PC via the USB interface. Use the MINI-SCREW-USB-DATACABLE (Order No. 2908217) for this.

Observe the following settings for communication with a Modbus protocol:

Parameter setting for the virtual COM port via the USB interface

Order No.	Designation	Baud rate
2320571	QUINT4-CAP/24DC/10/8KJ	9600 baud

Parameter	Settings
Start bit	1
Data Bits	8
Parity	Even
Stop Bits	1

In the POWER MANAGEMENT SUITE software, these settings are already specified as default values.

Detailed information on Modbus/RTU is available in the download area in the supplementary document: Modbus/RTU communication for CAP modules.

11 Device operation

11.1 Functions in buffer mode

The capacity module provides the following functions in buffer mode:

1. Time-limit mode
2. PC mode

11.1.1 Time-limit mode (default setting)

You can activate the time-limit mode function via the POWER MANAGEMENT SUITE software.
The capacity module supplies the connected loads for the time set. After this time expires, the device switches off. Once the mains voltage returns, the device output switches on. This only happens in buffer mode.

11.1.2 PC mode

The PC mode function enables the controlled shutdown and startup of the PC connected via USB at the times set. You can set these times via the POWER MANAGEMENT SUITE software.

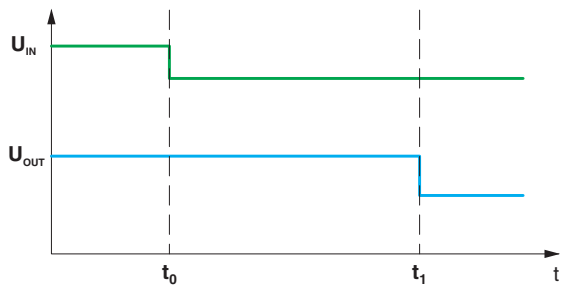
11.2 Setting the buffer time

You can set the required buffer time in the POWER MANAGEMENT SUITE software. To do this, activate the “Buffer time Custom” control field. In this setting, buffer mode is ended after the entered amount of time. If the configuration is 0 (mm:ss), all the capacity module’s available power is supplied.

Default setting: 0 (mm:ss)

Particularly with respect to cyclical applications, the recharging time is reduced when configuring the buffer time because a corresponding level of power remains in the storage capacitors (depending on the buffer time).

Figure 19

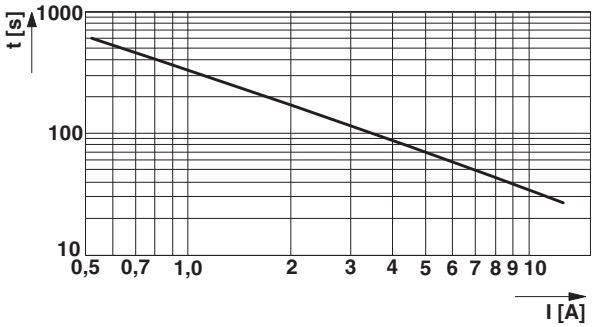


t_0: mains power failure

t_1: after the preset buffer time has expired, the output is switched off

Refer to the following diagram for possible buffer times for varying discharge currents.

Figure 20 Buffer time/discharge current diagram



11.2.1 PC mode configuration

In PC mode, you can individually configure the buffer mode’s chronological sequence using the POWER MANAGEMENT SUITE software.

Activate the "PC mode" control field to switch to the PC mode of the capacity module:

The following components are required for the PC mode function:

Data cable MINI-SCREW-USB-DATACABLE (Order No. 2908217)

POWER MANAGEMENT SUITE software (Order No. 1252232)

In the event of a mains failure, one PC can continue to work, perform a controlled shutdown, and restart automatically.

You can set the following times in the POWER MANAGEMENT SUITE software:

1: Delay time

If the mains supply is not restored during the delay time, the PC is shut down.

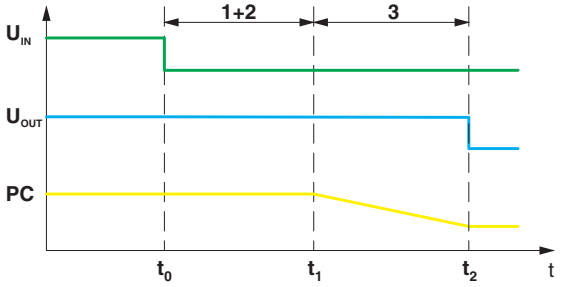
2: Program runtime

After the delay time has expired, it is possible to start a program.

3: PC shut-down

The time required for PC shutdown is set here.

Figure 21



t_0: mains power failure

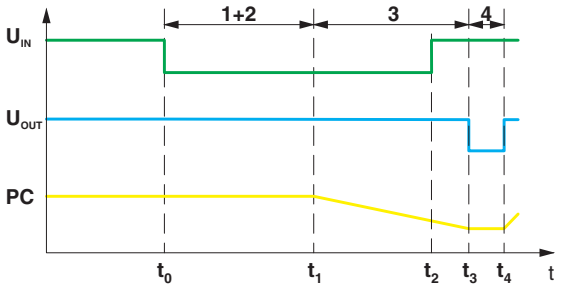
t_1: delay time and program runtime have expired, PC will be shut down

t_2: the PC has shut down, the output will be switched off

4: PC no-load time

Only if the PC is shut down and the mains supply is restored in the meantime is the output voltage interrupted for the PC standby time and the PC then started automatically.

Figure 22



t_0: mains power failure

t_1: delay time and program runtime have expired, PC will be shut down

t_2: mains restored while PC is shutting down

t_3: the PC has shut down and the output will be switched off, PC no-load time starts

t_4: the PC no-load time has expired, PC is starting back up

11.3 Remote

You can use the Remote signal terminal to:

1. Deactivate buffer mode
2. Shut down the PC immediately
3. Shut down the PC immediately in buffer mode
4. Switch on/off the output of the capacity module

To perform these steps, you must connect the Remote signal terminal to the SGnd signal terminal.

You can set the various functions in the POWER MANAGEMENT SUITE software. To do this, activate the corresponding radio buttons.

1. Remote disables buffer mode

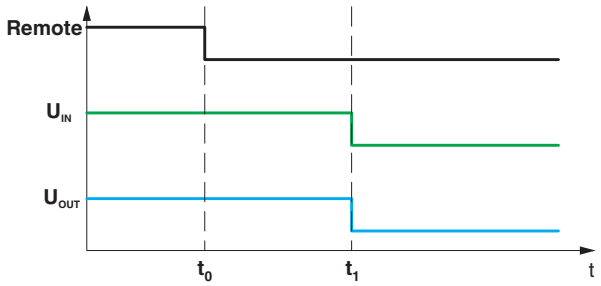
You can deactivate buffer mode using this function. This function is always active when a buffer time has been preset.

This function is the default setting in PC mode.

In mains operation, the remote signal is indicated by the flashing green LED (see section: Signaling).

In the event of mains failure, buffer mode is not started.

Figure 23

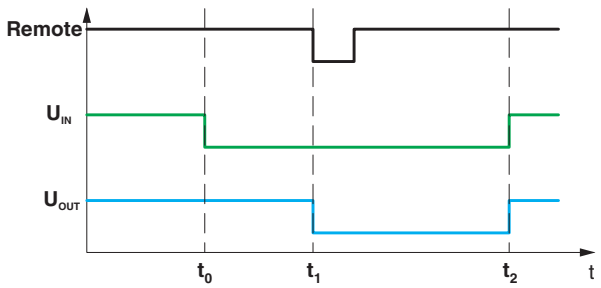


t_0: remote signal is set in mains operation

t_1: no input voltage, output will be switched off

If the remote signal is set in buffer mode, then buffer mode is exited immediately. The output of the capacity module is switched off. This procedure cannot be reversed. The capacity module is only activated once the input voltage is applied.

Figure 24



t_0: mains power failure

t_1: remote signal is set in buffer mode, the output is switched off

t_2: input voltage restored, output will be switched on

2. Remote starts undelayed PC-Shutdown

You can shut down the PC immediately via the POWER MANAGEMENT SUITE software.

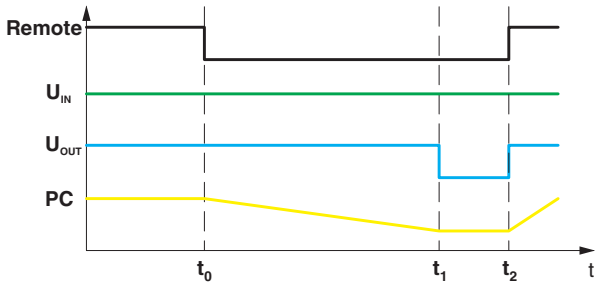
This setting only applies in PC mode.

The remote signal is indicated by the flashing green LED (see section: Signaling).

The PC shuts down, and the delay time under Item 1 is skipped (see PC mode section).

Once the PC has shut down, the capacity module output is switched off. When input voltage is present, the capacity module remains charged and the system is ready to use. When you reset the remote signal, the capacity module output is switched on again.

Figure 25



t_0: remote signal is set during mains operation, PC will be shut down

t_1: PC has shut down, output will be switched off

t_2: remote signal will be reset, output will be switched back on

Once the PC has shut down in buffer mode, the capacity module output is switched off. This procedure cannot be reversed. The capacity module is only activated once the input voltage is applied.

3. Remote starts undelayed PC-Shutdown only in buffer mode

You can shut down the PC immediately upon going into buffer mode using the POWER MANAGEMENT SUITE software.

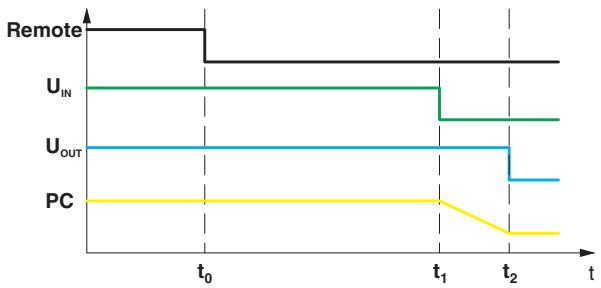
This setting only applies in PC mode.

The remote signal is indicated by the flashing green LED (see section: Signaling).

If the remote signal is set in mains operation, the PC is shut down when buffer mode is entered. The delay time under Item 1 is skipped (see “PC mode” section).

Once the PC has shut down in buffer mode, the capacity module output is switched off. This procedure cannot be reversed. The capacity module is only activated once the input voltage is applied.

Figure 26



t_0: remote signal is set in mains operation

t_1: no input voltage, PC shutdown begins immediately

t_2: the PC has shut down, the output will be switched off

4. Remote switches the output

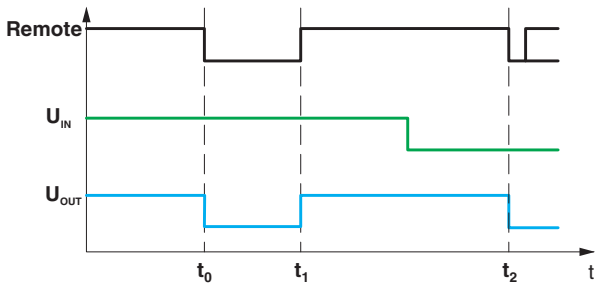
You can use this function to switch on/off the output of the capacity module.

This function is only available if a buffer time has been set.

The remote signal is indicated by the flashing green LED (see section: Signaling).

If the remote signal is set in buffer mode, then buffer mode is exited immediately. The output of the capacity module is switched off. This procedure cannot be reversed. The capacity module is only activated once the input voltage is applied.

Figure 27



t_0: remote signal is set in mains operation, output will be switched off

t_1: the remote signal will be reset, output will be switched back on

t_2: remote signal is set in buffer mode, the output is switched off

11.4 Switch-on delay

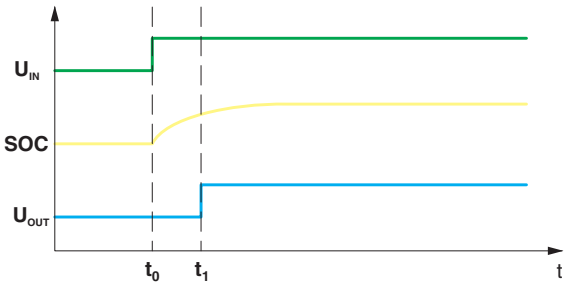
You can use this function to switch on the capacity module output based on the charging state of the storage capacitors.

The "buffer-ready threshold value" refers to the charging state of the storage capacitors and also has an effect on signaling.

You can use the corresponding selection fields in the POWER MANAGEMENT SUITE software to activate and configure parameters for this function.

The switch-on delay ensures that a system does not switch on until a certain level of power is available in the storage capacitors. As a result, a mains failure can be bypassed for a specific amount of time.

Figure 28



t_0: the input voltage is present, the storage capacitors are charged

t_1: the configured support bar has been reached, the output is switched off

11.5 Bypass function (default setting)

You can activate the bypass function via the POWER MANAGEMENT SUITE software.

As soon as the critical external temperature ≥80°C is reached, the capacity module automatically blocks and signals an alarm. The red LED indicator alarm flashes permanently. The device output remains switched off until the external temperature drops to <75°C. The module remains blocked.

The blocked capacity module continues to be supplied via the grid. The load supply is maintained via the bypass function of the capacity module.

The manufacturer can analyze the device and unlock it.

You can find detailed information on the signal states in Section: Signaling. Further information on protection against overtemperature is to be found in Section: Safety functions.

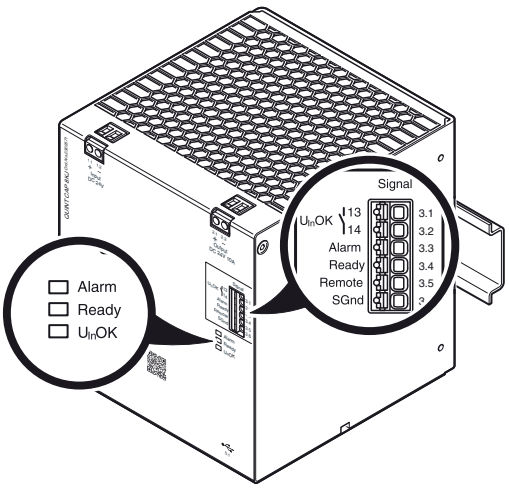
12 Signaling

Information on the software setting for signaling via the POWER MANAGEMENT SUITE is available in the Section: Software.

Various LED indicators are available for visual function monitoring of the module. Active signal outputs can be used to forward this data to a higher-level control system.

12.1 Connection terminal block signaling

Figure 29 Connection terminal block signaling (3.1 ... 3.6)



Key

Connection labeling	Designation	Function
3.1, 3.2	U_{In} OK: 13/14	Mains voltage OK
3.3	Alarm	Alarm
3.4	Ready	Buffer Ready
3.5	Remote	Start/stop buffer mode
3.6	SGnd	Signal ground

12.2 LED status indicators

On the right side of the device front, three LEDs (Alarm, Ready, U_{In} OK) signal the device status of the capacity module.

Figure 30 LED status indicators for device status

Alarm

Ready

U_{In} OK

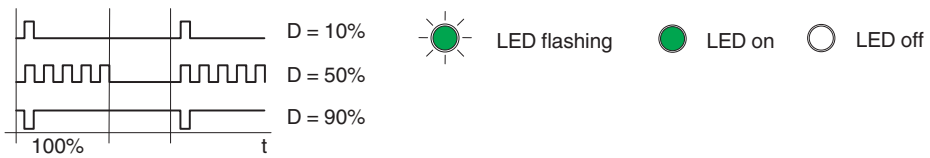
For module signaling and the corresponding states, please refer to the following tables.

12.3 Signaling in operation

Figure 31

Status LED			Switching OUTPUT			Note
U_{In} OK (green)	READY (green)	ALARM (red)	U_{In} OK	READY	ALARM	
○	○	○	open	low	low	Device off.
●	●	●	open	low	low	Initialization, LED test (~3 sec.)
●	●	○	closed	high	high	Mains operation, buffer is ready. The SOC* of the double layer capacitors is above READY threshold.
	☀ D = 50%	○	closed	low	high	Mains operation, charging in process. The SOC* of the double layer capacitors is below READY threshold.
	☀ D = 50%	●	closed	low	low	Mains operation, ALARM. The SOC* of the double layer capacitors is below READY threshold.
	●	●	closed	high	low	Mains operation, ALARM. The SOC* of the double layer capacitors is above READY threshold.
○	●	○	open	high	high	Buffer mode.
	●	●	open	high	low	Buffer mode, ALARM due to over temperature > 70°C.
	○	●	open	low	low	Buffer mode, ALARM.
	○	●	closed	low	low	Start-up, ALARM.
☀ D = 90%	●	○	closed	high	high	Mains operation, REMOTE contact shorted to SGnd, buffer is ready.
	☀ D = 50%	○	closed	low	high	Mains operation, REMOTE contact shorted to SGnd, charging in process.
☀ D = 10%	☀ D = 50%	○	closed	low	high	Mains operation, REMOTE contact shorted to SGnd or output delay on enabled, charging in process or CAP is fully charged**
	☀ D = 50%	●	closed	low	low	Mains operation, REMOTE contact shorted to SGnd or output delay on enabled, charging in process or READY, ALARM.

*SOC = State of Charge
**Delay for the flashing READY-LED maximum 10 sec.



12.4 Signaling the bypass function

Status LED			Switching OUTPUT			Note
U_{In} OK (green)	READY (green)	ALARM (red)	U_{In} OK	READY	ALARM	
○	○	D = 50%	open	low	low	The device is locked due to over temperature less or higher than 80 °C. No input, the device output is OFF.
●	○	D = 50%	closed	low	low	The device is locked. The temperature is less than 80 °C. The device output is ON.
D = 10%	○	D = 50%	closed	low	low	The device is locked. The temperature is less or higher than 80 °C, or BYPASS function is disabled. The device output is OFF.

12.5 Signal outputs

U_{In} OK (13/14)

If the input voltage is in the valid range, the signal output is active (closed). The signal status can be inverted via the POWER MANAGEMENT SUITE software.

A floating N/O contact (implemented with a photorelay) is available as a signal contact.

This signal is indicated visually by a green LED.

You can assign other additional information to this signal output using the POWER MANAGEMENT SUITE software.

Ready

When the storage capacitors are fully charged or the device is in buffer mode, the signal output is active (High level). The signal status can be inverted via the POWER MANAGEMENT SUITE software.

A digital transistor output is available as a signal contact.

This signal is indicated visually by a green LED.

You can assign other additional information to this signal output using the POWER MANAGEMENT SUITE software.

Alarm

When an alarm is present, the signal output is active (low level). The signal status can be inverted via the POWER MANAGEMENT SUITE software.

A digital transistor output is available as a signal contact.

This signal is indicated visually by a red LED.

Possible alarms include:

– Device overheated
– Error in the storage capacitor
– Disconnection in the event of overload in buffer mode

12.6 Signal input

Remote

You can activate and trigger various functions using the remote signal input. For further information, refer to the “Remote device operation” section.

You can invert the signal state using the POWER MANAGEMENT SUITE software.

A change made to the remote function using the POWER MANAGEMENT SUITE software is not applied until a corresponding status change of the remote signal input or device restart has been carried out.

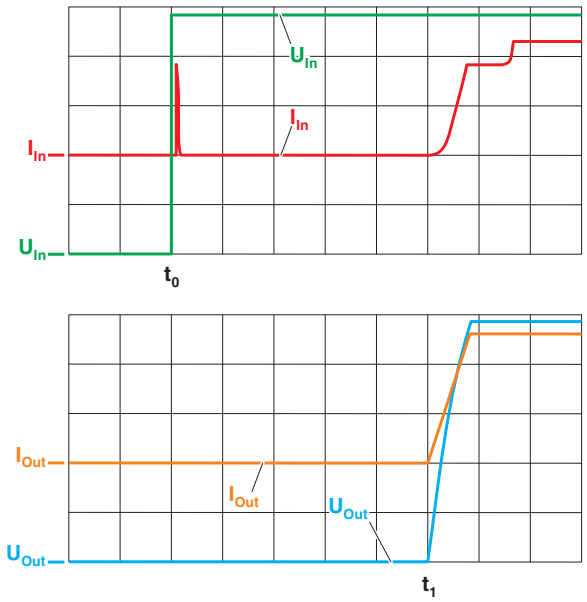
13 Switch-on and switching behavior

13.1 Switch-on behavior

The QUINT capacity module features a soft startup. The output is switched on by ramping up instead of abruptly. This makes the QUINT capacity module also suitable for use in power supplies in the low power range.

How to adjust the switch-on behavior is described in the section Switch-on delay.

Figure 32 Switch-on behavior



U_{In}: 5V/div I_{In}: 2A/div Time: 1s/div
U_{Out}: 5V/div I_{Out}: 2A/div

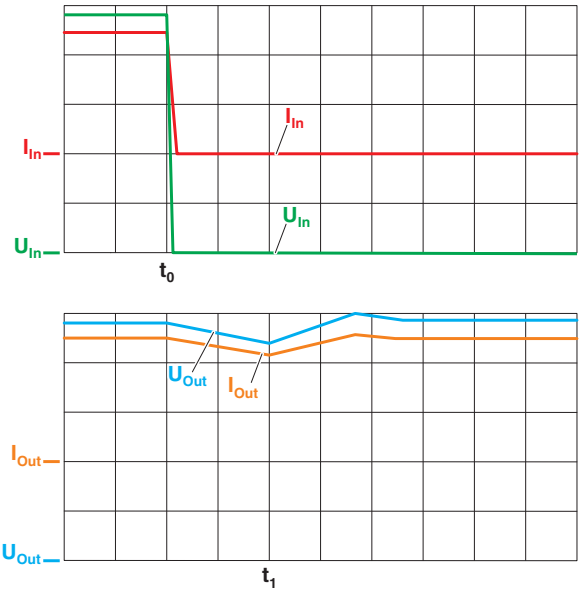
t_0: input voltage is present

t_1: the output is switched on approximately 5 seconds later

13.2 Switching behavior

The output voltage remains present without interruption when switching over from grid to buffer mode.

Figure 33 Switching behavior



U_{In}: 5V/div I_{In}: 2A/div Time: 5ms/div
U_{Out}: 5V/div I_{Out}: 2A/div

t_0: mains power failure

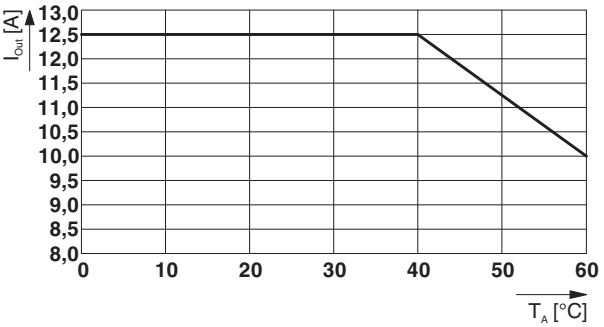
t_1: the output voltage does not drop below 20 V in the switchover phase

14 Derating

14.1 Ambient temperature

At an ambient temperature of up to +40°C, the device supplies the output current $I_{Stat. Boost}$.

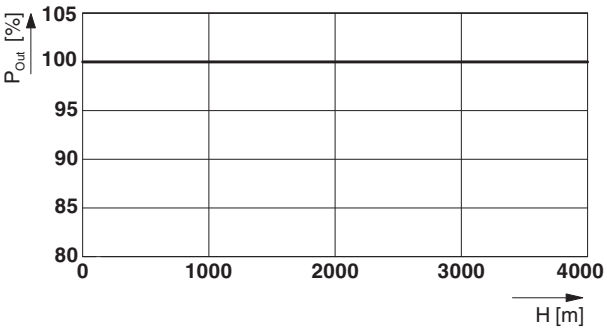
Figure 34 Temperature-dependent derating



14.2 Installation height

The device can be operated at an installation height of up to 4000 m without any limitations.

Figure 35 Altitude-dependent derating

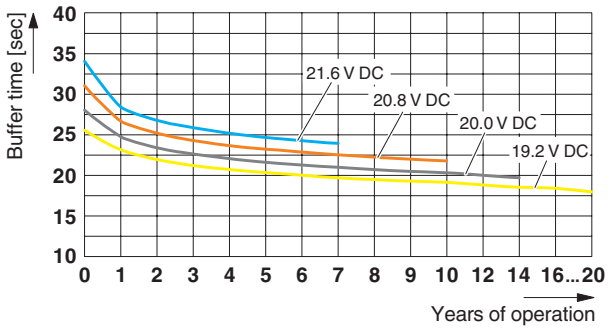


14.3 Service life

You can affect the service life of the capacity modules by configuring the charging voltage of the storage capacitors. You can parameterize this function via the corresponding selection fields in the POWER MANAGEMENT SUITE software.

Reducing the charging voltage leads to an increase in the service life and simultaneous reduction of the possible buffer time.

The specifications in the illustrated diagram are based on an operating temperature of T_A= 40°C with 10 A load.



*30 % capacitance degradation of SCAPs is considered as the end of life (EOL)

**up to a maximum humidity (rH) of 43 % rH, no impacts on the SCAPs are expected

***calculations are based on technical reference data from SCAPs manufacturer

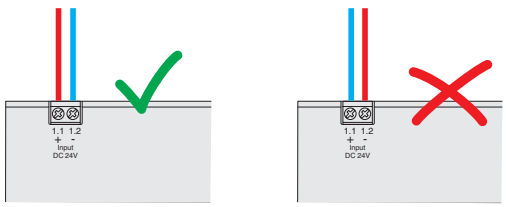
15 Safety functions

Integrated safety functions protect the capacity module against potential system errors and ensure stable, reliable system operation.

15.1 Reverse polarity protection

An integrated reverse polarity protection diode protects the device against mismatching during installation. If the positive and negative poles are connected in reverse, all visual LEDs remain off.

Figure 36 Schematic diagram, wiring of the input terminal blocks



15.2 Line protection

Protect incoming lines with suitable miniature circuit breakers or fuses.

An appropriate overcurrent protection device is necessary upstream of the capacity module if the current sources have a high short-circuit current.

Observe the technical data and the connection cross-section of the cable manufacturer.

15.3 Short-circuit protection

The capacity module is protected against internal device errors. After a short circuit in the device, the device shuts down and displays an alarm. Charging and buffer processes are disconnected automatically.

15.4 Overload protection

Numerous overload protection mechanisms are integrated into the capacity module. The device monitors the charging current. In the event of an error, the charging process is stopped. The device indicates an alarm.

15.5 Undervoltage and surge protection

The device constantly monitors the input voltage. After over- or undervoltages, the device disconnects and attempts to restart after specified interaction loops.

15.6 Protection against overtemperature

The capacity module features an additional function for internal temperature monitoring. If the external temperature exceeds a threshold value of 70°C, the module first switches the charger off. At the same time, the red alarm LED lights up and the alarm signal is active “high”.

Buffer mode is switched of at an external temperature of 75°C. The red alarm LED lights up and the alarm signal is active “high”.

If the temperature reaches a critical value of ≥ 80°C for a few seconds, the module shuts down. At the same time, the red alarm LED lights up permanently and the digital alarm signal is off.

The manufacturer can analyze the device and unlock it.

This safety function protects the module itself and prevents internal component overloads.

16 Software

The latest software version is to be found in the product download area.

POWER MANAGEMENT SUITE software (Order No. 1252232)

Configuration software UPS-CONF (Order No. 2320403)

The UPS-CONF software supports QUINT CAP modules up to production batch 05.

16.1 Software installation

You can configure the capacity module individually via the POWER MANAGEMENT SUITE software. To be able to configure the module, install the POWER MANAGEMENT SUITE PC software as follows:

1. Open the software in the download area of the item.
2. Next, extract the ZIP file.
3. Depending on the application, you can install individual modules.

You can select the following modules:

- POWER MANAGEMENT SUITE server: Communication interface between Phoenix Contact power supply systems and PC. Manages all data provided by the device.
- POWER MANAGEMENT SUITE Client: Display of data delivered by the server. Configuration and management of the system. Includes service for controlled PC shutdown.
- POWER MANAGEMENT SUITE Agent: Service for controlled PC shutdown.

4. Connect the capacity module to your PC via the USB interface and start the POWER MANAGEMENT SUITE. The software detects the connected device automatically.

Comprehensive information on the POWER MANAGEMENT SUITE as well as application examples are available in the user manual and the download area.

Further information on configuring the capacity module is available in Section: Device operation.

16.2 Software settings for signaling

16.2.1 Assignment of signal terminals

You can assign different states to the individual signal terminals using the software. The following table describes the possible combinations:

Alarm Default	U_{In} OK Default	Ready Default	Comment
1	0	0	Negation BIT
1	0	0	Alarm CAP
1	0	0	Device fail
x	0	1	Buffer mode
x	0	0	Charger
x	0	0	Status remote
x	0	0	Status buffer delayed 1
x	0	0	Status buffer delayed 2
x	0	0	Status buffer delayed 3
x	0	1	Status buffer ready
x	1	0	Input OK

Key

1 = default (factory setting)

0 = not assigned (assignment via POWER MANAGEMENT SUITE possible)

x = assignment not possible

QUINT4-S-ORING/12-24DC/1X40

Redundancy module

Data sheet
107633_en_00

1 Description

QUINT S-ORING is the active redundancy module from the QUINT POWER product range. The redundancy module can be used to 100% decouple power supplies.

Consistent redundancy

– Separate structure for redundant and monitored wiring of the power supply up to the load.

Preventive

– Comprehensive signaling by LED indicators and switch output.

Minimum power dissipation

– The use of MOSFETs enables a very small voltage drop and therefore low power dissipation.

Technical data (short form)	
Input voltage range	8 V DC ... 30 V DC
Voltage drop, input/output	0.1 V (U_{MOSFET})
Output voltage	U_{In} - 0.1 V
Nominal output current (I_N) Static Boost ($I_{Stat.Boost}$) Dynamic Boost ($I_{Dyn.Boost}$) Selective Fuse Breaking (I_{SFB})	40 A 45 A 60 A (5 s) 240 A (15 ms)
Maximum power dissipation	6.5 W (I_{OUT} = 40 A)
Efficiency	typ. 99.1 % (12 V DC) typ. 99.3 % (24 V DC)
MTBF (IEC 61709, SN 29500)	> 15153000 h (40 °C)
Ambient temperature (operation)	-40 °C ... 70 °C > 60 °C Derating: 2.5 %/K
Dimensions W/H/D	32 mm / 130 mm / 125 mm
Weight	0.55 kg

All technical specifications are nominal values and refer to a room temperature of 25 °C and 70 % relative humidity at 100 m above sea level.

2 Table of contents

3 Ordering data

Description	Type	Order No.	Pcs./Pkt.
Active QUINT single redundancy module for DIN rail mounting, input: 12 - 24 V DC, output: 12 - 24 V DC/1 x 40 A, incl. mounted UTA 107/30 universal DIN rail adapter	QUINT4-S-ORING/12-24DC/1X40	2907752	1

Accessories	Type	Order No.	Pcs./Pkt.
Universal wall adapter for securely mounting the power supply in the event of strong vibrations. The power supply is screwed directly onto the mounting surface. The universal wall adapter is attached at the top/bottom.	UWA 182/52	2938235	1
Universal DIN rail adapter	UTA 107/30	2320089	100
Assembly adapter for QUINT-PS... power supply on S7-300 rail	QUINT-PS-ADAPTERS7/1	2938196	1

The range of accessories is being continuously extended. The current range of accessories can be found in the download area for the product.

4 Technical data

Input data	
Unless otherwise stated, all data applies for 25°C ambient temperature, 24 V DC input voltage, and nominal output current (I_N).	
Nominal input voltage range	12 V DC ... 24 V DC
Input voltage range	8 V DC ... 30 V DC
Voltage drop, input/output typ.	0.1 V (U_{MOSFET})
Reverse polarity protection	< 60 V
Typical current consumption (for nominal values) Static Boost ($I_{Stat.Boost}$) Dynamic Boost ($I_{Dyn.Boost}$) Selective Fuse Breaking (I_{SFB})	40 A 45 A 60 A (5 s) 240 A (15 ms)
The SCCR value (short-circuit current rating) of the redundancy module corresponds to the SCCR value of the backup fuse (see input protection table).	

Input protection , DC (to be connected externally upstream if a current limiting source is not used)							
Input current I_{In} Input protection	**Circuit breaker**					**Neozed fuse or equivalent**	**Power switch**
Characteristics	**A**	**B**	**C**	**D**	**K**	**gG**	**≤ 13 x I_{In} (maximum magnetic tripping)**
20 A	-	✓	✓	-	-	✓	✓
25 A	-	✓	✓	-	-	✓	✓
32 A	✓	✓	✓	-	-	✓	✓
40 A	✓	✓	✓	-	-	-	✓

Electric strength of the insulation	
Type test (IEC/EN 60950-1)	0.5 kV AC
Production test	0.71 kV DC

Input connection data	
Connection method	Screw connection
Conductor cross section, solid	0.5 mm² ... 16 mm²
Conductor cross section, flexible	0.5 mm² ... 16 mm²
Stranded conductor cross section with ferrule	0.5 mm² ... 16 mm²
Conductor cross section AWG	20 ... 6
Stripping length	10 mm
Tightening torque	1.2 Nm ... 1.5 Nm

Output data	
Nominal output voltage (U_N)	U_{In} - 0.1 V (U_{MOSFET})
Nominal output current (I_N)	40 A
Static Boost ($I_{Stat.Boost}$)	45 A
Dynamic Boost ($I_{Dyn.Boost}$)	60 A (5 s)
Selective Fuse Breaking (I_{SFB})	240 A (15 ms)
Connection in series	No

Output connection data	
Connection method	Screw connection
Conductor cross section, solid	0.5 mm² ... 16 mm²
Conductor cross section, flexible	0.5 mm² ... 16 mm²
Stranded conductor cross section with ferrule	0.5 mm² ... 16 mm²
Conductor cross section AWG	20 ... 6
Stripping length	10 mm
Tightening torque	1.2 Nm ... 1.5 Nm

LED signaling (Description)	Relay contact 13/14	Status
LED off, input voltage not present or short circuit at redundancy module output	open	U_{In} < 8 V DC
LED lights up green, input voltage present	closed	U_{In} > 8 V DC
LED lights up red, redundancy module needs to be factory tested	open	Redundancy modul faulty

For floating switch contact 13/14, observe the maximum contact load: 30 V AC/DC, 100 mA

Signal connection data	
Connection method	Plug connection
Conductor cross section, solid	0.2 mm² ... 1.5 mm²
Conductor cross section, flexible	0.2 mm² ... 1.5 mm²
Stranded conductor cross section with ferrule	0.2 mm² ... 1.5 mm²
Conductor cross section AWG	24 ... 16
Stripping length	8 mm

Reliability	24 V DC
MTBF (IEC 61709, SN 29500)	> 25297000 h (25 °C) > 15153000 h (40 °C) > 7449000 h (60°C)

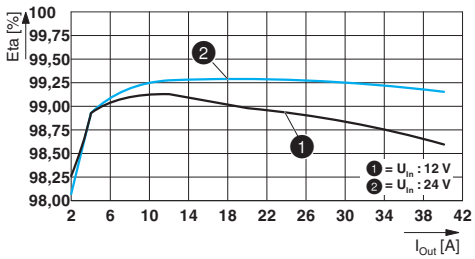
Life expectancy (electrolytic capacitors) Output current (I_{Out})	12 V DC	24 V DC
40 A	> 186000 h (40 °C)	> 123000 h (40 °C)

The expected service life is based on the capacitors used. If the capacitor specification is observed, the specified data will be ensured until the end of the stated service life. For runtimes beyond this time, error-free operation may be reduced. The specified service life of more than 15 years is simply a comparative value.

General data	
Degree of protection	IP20
Protection class	III
Inflammability class in acc. with UL 94 (housing / terminal blocks)	V0
Type of housing	Aluminum (AlMg3)
Hood version	Galvanized sheet steel, free from chrome (VI)
Weight	0.55 kg

Power dissipation	12 V DC	24 V DC
Power loss nominal load max.	6.5 W	6 W

Efficiency	12 V DC	24 V DC
	typ. 99.1 %	typ. 99.3 %



Ambient conditions	
Ambient temperature (operation)	-40 °C ... 70 °C (> 60 °C Derating: 2.5 %/K)
The ambient temperature (operation) refers to UL 508 surrounding air temperature.	
Ambient temperature (storage/transport)	-40 °C ... 85 °C
Max. permissible relative humidity (operation)	≤ 95 % (at 25 °C, non-condensing)
Installation height	≤ 5000 m (> 2000 m, observe derating)
Vibration (operation)	< 15 Hz, amplitude ±2.5 mm (according to IEC 60068-2-6) 15 Hz ... 150 Hz, 2.3g, 90 min.
Shock	18 ms, 30g, in each space direction (according to IEC 60068-2-27)
Degree of pollution	2
Climatic class	3K3 (in acc. with EN 60721)

Standards	
Electrical safety (of information technology equipment)	EN 60950-1/VDE 0805 (SELV)
SELV	IEC 60950-1 (SELV) and EN 60204-1 (PELV)

Approvals	
UL	UL/C-UL listed UL 508 UL/C-UL Recognized UL 60950-1 UL ANSI/ISA-12.12.01 Class I, Division 2, Groups A, B, C, D (Hazardous Location)
Shipbuilding	DNV GL

Electromagnetic compatibility		
Noise emission according to EN 61000-6-3 (residential and commercial) and EN 61000-6-4 (industrial)		
CE basic standard	**Minimum normative requirements**	**Higher requirements in practice (covered)**
Conducted noise emission EN 55016	EN 61000-6-4 (Class A)	EN 61000-6-3 (Class B)
Noise emission EN 55016	EN 61000-6-4 (Class A)	EN 61000-6-3 (Class B)

Noise emission for marine approval	**Minimum normative requirements of DNV GL**	**Higher requirements in practice of DNV GL (covered)**
DNV GL conducted noise emission	Class A Area power distribution	Class A Area power distribution
DNV GL noise radiation	Class A Area power distribution	Class B Bridge and deck area

Immunity according to EN 61000-6-1 (residential), EN 61000-6-2 (industrial), and EN 61000-6-5 (power station equipment zone)		
CE basic standard	**Minimum normative requirements of EN 61000-6-2 (CE) (immunity for industrial environments)**	**Higher requirements in practice (covered)**
Electrostatic discharge EN 61000-4-2		
Housing contact discharge	4 kV (Test Level 2)	8 kV (Test Level 4)
Housing air discharge	8 kV (Test Level 3)	15 kV (Test Level 4)
Comments	Criterion B	Criterion B
Electromagnetic HF field EN 61000-4-3		
Frequency range	80 MHz ... 1 GHz	80 MHz ... 1 GHz
Test field strength	10 V/m (Test Level 3)	20 V/m (Test Level 3)
Frequency range	1.4 GHz ... 2 GHz	1 GHz ... 6 GHz
Test field strength	3 V/m (Test Level 2)	10 V/m (Test Level 3)
Frequency range	2 GHz ... 2.7 GHz	1 GHz ... 6 GHz
Test field strength	1 V/m (Test Level 1)	10 V/m (Test Level 3)
Comments	Criterion B	Criterion A
Fast transients (burst) EN 61000-4-4		
Input	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 4 - asymmetrical)
Output	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 4 - asymmetrical)
Signal	2 kV (Test Level 3 - asymmetrical)	2 kV (Test Level 4 - asymmetrical)
Comments	Criterion B	Criterion A

Immunity according to EN 61000-6-1 (residential), EN 61000-6-2 (industrial), and EN 61000-6-5 (power station equipment zone)		
CE basic standard	**Minimum normative requirements of EN 61000-6-2 (CE) (immunity for industrial environments)**	**Higher requirements in practice (covered)**
Surge current loads (surge) EN 61000-4-5		
Input	1 kV (Test Level 3 - symmetrical) 2 kV (Test Level 3 - asymmetrical)	1 kV (Test Level 4 - symmetrical) 2 kV (Test Level 4 - asymmetrical)
Output	0.5 kV (Test Level 1 - symmetrical) 0.5 kV (Test Level 1 - asymmetrical)	1 kV (Test Level 2 - symmetrical) 2 kV (Test Level 3 - asymmetrical)
Signal	0.5 kV (Test Level 1 - asymmetrical)	1 kV (Test Level 2 - asymmetrical)
Comments	Criterion B	Criterion A
Conducted interference EN 61000-4-6		
Input/Output/Signal	asymmetrical	asymmetrical
Frequency range	0.15 MHz ... 80 MHz	0.15 MHz ... 80 MHz
Voltage	10 V (Test Level 3)	10 V (Test Level 3)
Comments	Criterion A	Criterion A
Power frequency magnetic field EN 61000-4-8		
	50 Hz , 60 Hz (30 A/m)	16.67 Hz , 50 Hz , 60 Hz (30 A/m , 60 s)
Comments	Criterion A	Criterion A

Key	
Criterion A	Normal operating behavior within the specified limits.
Criterion B	Temporary impairment to operational behavior that is corrected by the device itself.

5 Safety and installation notes

Only qualified electricians may install, start up, and operate the device. Observe the national safety and accident prevention regulations.

Check the device for damage before startup.

CAUTION: Before startup, observe the following

Preferably mount the redundancy module in the normal mounting position.

Make sure that the redundancy module wiring on the primary side and the secondary side is adequately dimensioned and protected.

The redundancy module is a built-in device. The IP20 degree of protection of the redundancy module is intended for use in a clean and dry environment. The redundancy module is mounted in a control cabinet.

For the connection parameters for wiring the redundancy module, such as the required stripping length with and without ferrule, refer to the technical data section.

To avoid accidental contact with live parts, always cover the termination area (e.g., installation in the control cabinet).

The redundancy module does not require maintenance. Repairs may only be carried out by the manufacturer. Opening the housing invalidates the warranty.

CAUTION: Hot surface

The housing can become hot, depending on the ambient temperature and redundancy module load.

The redundancy module may only be used for its intended use.

6 High-voltage test (HIPOT)

This protection class III redundancy module is subject to the Low Voltage Directive and is factory tested. During the HIPOT test (high-voltage test), the insulation between the input and output circuit and the housing is tested for the prescribed electric strength values, for example. The test voltage in the high-voltage range is applied at the input, output, and signal terminal blocks of the redundancy module. The operating voltage used in normal operation is considerably lower than the test voltage used.

High-voltage tests up to 0.71 kV DC can be performed as described.

The test voltage should rise and fall in ramp form. The relevant rise and fall time of the ramp should be at least seconds.

6.1 High-voltage dielectric test (dielectric strength test) and why must it be performed?

In order to ensure permanent safe isolation from the housing, high-voltage testing is performed as part of the safety approval process (type test) and manufacturing (routine test).

6.2 High-voltage dielectric test during the manufacturing process

During the manufacturing process for the redundancy module, a high-voltage test is performed as part of the dielectric test in accordance with the specifications of IEC/UL/EN 60950-1. The high-voltage test is performed with a test voltage of at least 0.71 kV DC or higher. Routine manufacturing tests are inspected regularly by a certification authority.

6.3 High-voltage dielectric test performed by the customer

Apart from routine and type tests to guarantee electrical safety, the end user does not have to perform another high-voltage test on the redundancy module as an individual component. As per EN 60204-1 (Safety of machinery - Electrical equipment of machines), the redundancy module can be disconnected during the high-voltage test and only installed once the high-voltage test has been completed.

6.3.1 Performing high-voltage testing

If high-voltage testing of the control cabinet or the redundancy module as an individual component is planned during final inspection and testing, the following features must be observed.

- The redundancy module wiring must be implemented as shown in the wiring diagram.
- The maximum permissible test voltages must not be exceeded.

Avoid unnecessary loading or damage to the redundancy module due to excessive test voltages.

For the relevant applicable test voltages, refer to the corresponding table (see technical data: electric strength of the insulation section).

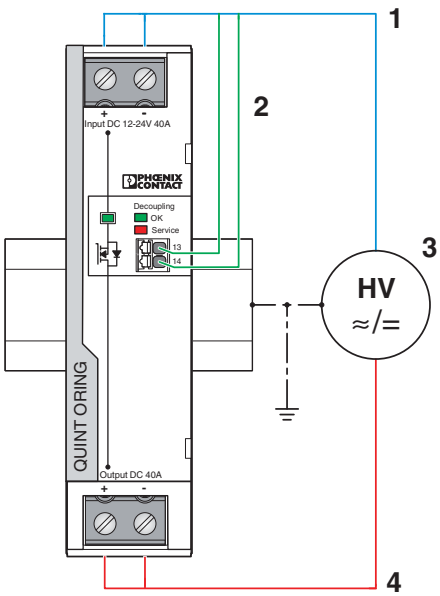


Figure 1 Potential-related wiring for the high-voltage test

Key

No.	Designation	Color coding	Potential levels
1	DC input circuit	Blue	Potential 1
2	Signal contacts	Green (optional)	Potential 2
3	High-voltage tester	--	--
4	DC output circuit	Red	Potential 3

7 Structure of the redundancy module

The convection-cooled active redundancy module can be snapped onto all DIN rails according to EN 60715.

7.1 Function elements

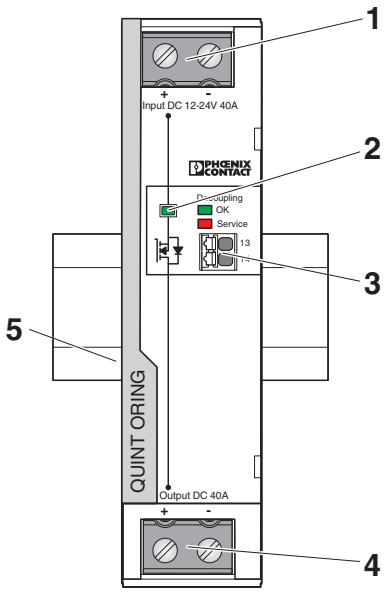


Figure 2 Operating and indication elements

Key

No.	Designation
1	DC input voltage connection terminal blocks
2	DC input voltage LED status indicators, Decoupling OK/Service
3	13/14 floating switch contact (N/O contact)
4	DC output voltage connection terminal blocks
5	Universal DIN rail adapter (rear of housing)

7.2 Device dimensions

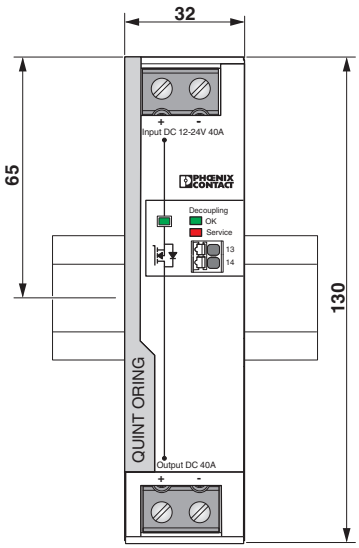


Figure 3 Device dimensions (in mm)

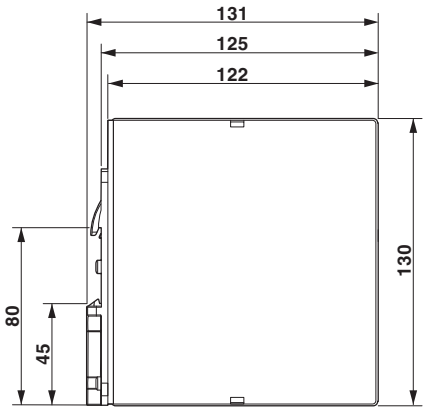


Figure 4 Device dimensions (in mm)

7.3 Locked areas

The required keepout areas for mounting vary depending on the application and ambient conditions.

Output power of the power supply	Ambient temperature	Spacing [mm]		
		a	b	c
0 ... 50 %	-25 ... 70 °C	0	40	20
≥50% ... 125%	-25 ... ≤40 °C	5	50	
≥50 % ... 100 %	>40 ... 70 °C	15		

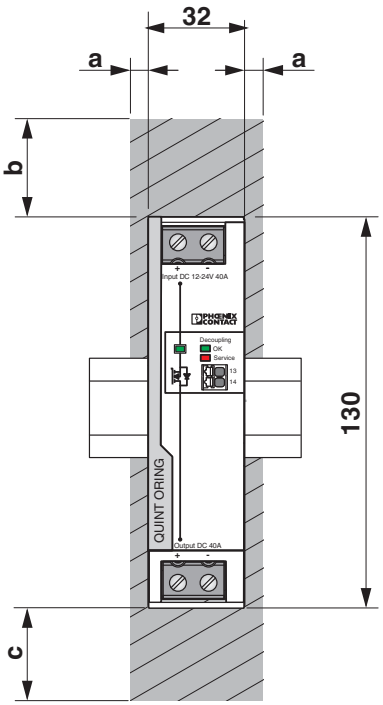


Figure 5 Device dimensions and minimum keepout areas (in mm)

7.4 Block diagram

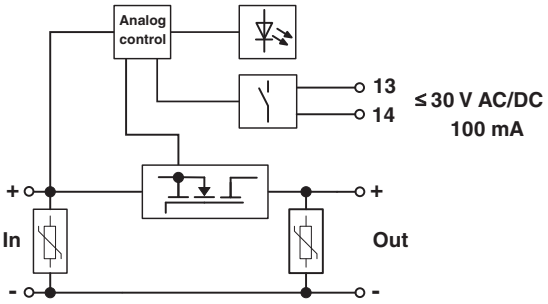


Figure 6 Block diagram

Key

Symbol	Designation
	Surge protection (varistor)
	Power semiconductor
Analog Control	Analog control equipment
	Signal/indicator LEDs (U_{In} > 8 V DC, Decoupling OK/Service)
	Floating switching output

8 Mounting/removing the redundancy module

8.1 Mounting the redundancy module

Proceed as follows to mount the redundancy module:

1. In the normal mounting position the redundancy module is mounted on the DIN rail from above. Make sure that the universal DIN rail adapter is in the correct position behind the DIN rail (A).
2. Then press the redundancy module down until the universal DIN rail adapter audibly snaps into place (B).
3. Make sure that the redundancy module is securely mounted on the DIN rail.

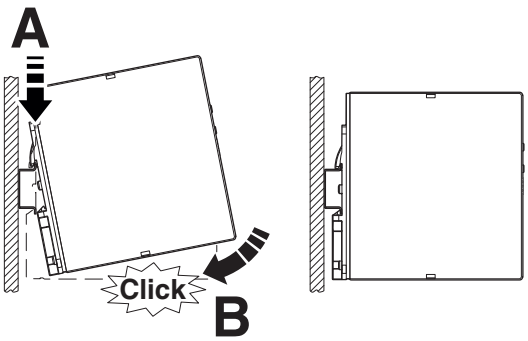


Figure 7 Snapping the redundancy module onto the DIN rail

8.2 Uninstall the redundancy module

Proceed as follows to remove the redundancy module:

1. Take a suitable screwdriver and insert this into the lock hole on the universal DIN rail adapter (A).
2. Release the lock by lifting the screwdriver (B).
3. Carefully swivel the redundancy module forward (C) so that the lock slides back into the starting position.
4. Then lift the redundancy module from the DIN rail.

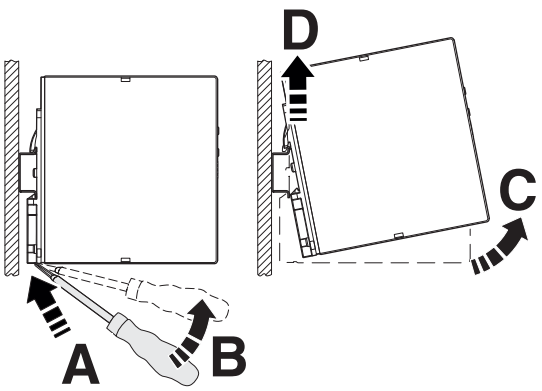


Figure 8 Removing the redundancy module from the DIN rail

8.3 Retrofitting the universal DIN rail adapter

For installation in horizontal terminal boxes it is possible to mount the redundancy module at a 90° angle to the DIN rail.

No additional mounting material is required.

Use the Torx screws provided to attach the universal DIN rail adapter to the side of the redundancy module.

8.3.1 Disassembling the universal DIN rail adapter

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Remove the universal DIN rail adapter from the rear of the redundancy module.

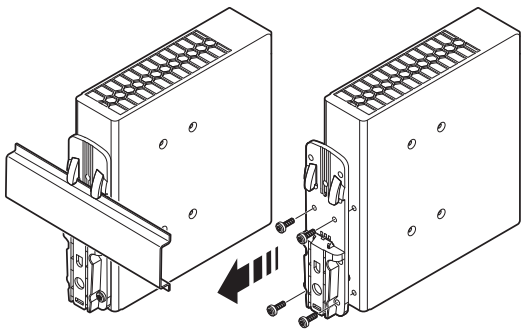


Figure 9 Disassembling the universal DIN rail adapter

8.3.2 Mounting the universal DIN rail adapter

To mount the universal DIN rail adapter on the left side of the device, proceed as follows:

1. Position the universal DIN rail adapter on the left side of the housing so that the mounting holes are congruent with the hole pattern for the mounting holes.
2. Insert the Torx screws that were removed earlier into the appropriate hole pattern on the universal DIN rail adapter so that the necessary drill holes of the redundancy module can be accessed.
3. Screw the universal DIN rail adapter onto the redundancy module.

The maximum tightening torque of the Torx screw (Torx® T10) is 0.7 Nm.

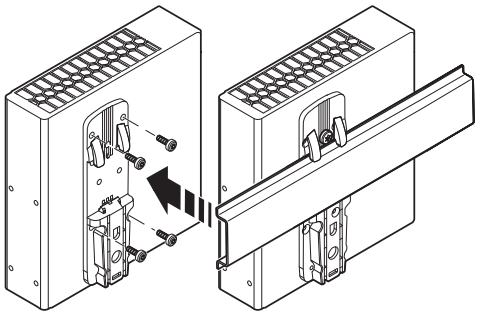


Figure 10 Mounting the universal DIN rail adapter

8.4 Retrofitting the universal wall adapter

The UWA 182/52 universal wall adapter (Order No. 2938235) or UWA 130 universal wall adapter (Order No. 2901664) is used to attach the redundancy module directly to the mounting surface.

The use of universal wall adapters is recommended under extreme ambient conditions, e.g., strong vibrations. Thanks to the tight screw connection between the redundancy module and the universal wall adapter or the actual mounting surface, an extremely high level of mechanical stability is ensured.

The redundancy module is attached to the UWA 182 or UWA 130 universal wall adapter by means of the Torx screws of the universal DIN rail adapter.

8.4.1 Mounting the UWA 182/52 universal wall adapter

Proceed as follows to disassemble the universal DIN rail adapter that comes pre-mounted:

1. Remove the screws for the universal DIN rail adapter using a suitable screwdriver (Torx 10).
2. Remove the universal DIN rail adapter from the rear of the redundancy module.
3. Position the universal wall adapter in such a way that the keyholes or oval tapers face up. The mounting surface for the redundancy module is the raised section of the universal wall adapter.
4. Place the redundancy module on the universal wall adapter in the normal mounting position (input voltage connection terminal blocks above).
5. Insert the Torx screws into the appropriate hole pattern on the universal wall adapter so that the necessary mounting holes of the redundancy module can be accessed.
6. Screw the universal wall adapter onto the redundancy module.

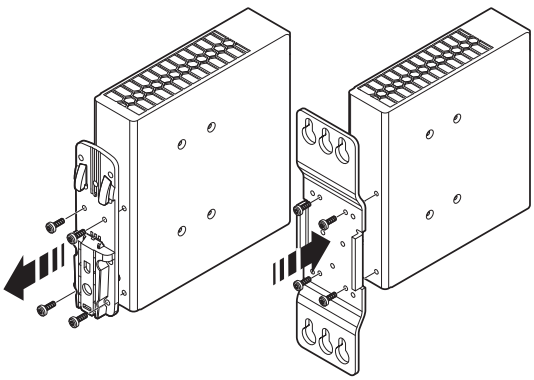


Figure 11 Mounting the UWA 182/52 universal wall adapter

The maximum tightening torque of the Torx screw (Torx® T10) is 0.7 Nm.

Make sure you use suitable mounting material when attaching to the mounting surface.

8.5 Secure the connection wiring to the redundancy module

Two receptacles for the bundled attachment of the connection wiring are integrated in the left and right housing panel. Use cable binders to secure the connection wiring (optional PKB 140X3,6 - Order No. 1005460).

Proceed as follows to secure the connection wiring:

– Wire redundancy module with sufficient connection reserve (input terminal blocks, output terminal blocks, signal terminal blocks)
– Thread the cable binders into the necessary receptacles for the cable binders.
– Bundle and set up the connection wiring so that the cooling grilles on the top and bottom of the housing are covered as little as possible.

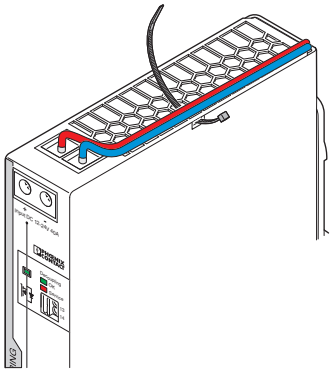


Figure 12 Lay and align connection wiring

– Secure the connection wiring with the cable binders. Make sure that the connection wiring is attached safely and securely without damaging the connection wiring.

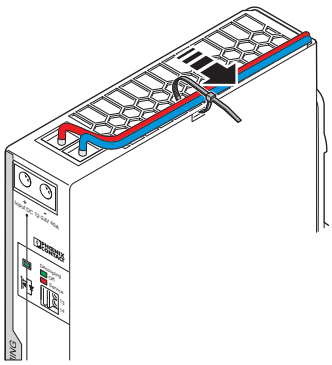


Figure 13 Secure connection wiring with cable binder

– Shorten the excess length of the cable binder ends.
– Then check again that the connection wiring is properly secured.

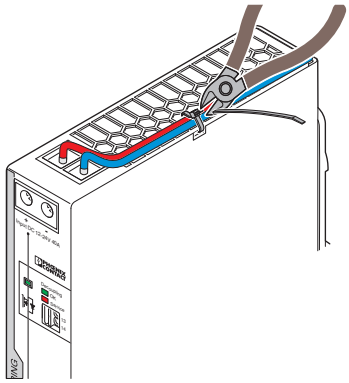


Figure 14 Shorten protruding ends of the cable binder

NOTE: Mechanical damage to the connection wiring caused by friction

In extreme ambient conditions, e.g., strong vibrations, protect the connection wiring against mechanical damage using additional insulation material. The additional insulation material for protecting the connection wiring is limited to the area where the cable binders are attached.

9 Device connection terminal blocks

The DC input terminal blocks and DC output terminal blocks on the front of the redundancy module feature screw connection technology. The signal level is wired by means of tool-free Push-in connection technology.

For the necessary connection parameters for the connection terminal blocks, refer to the technical data section.

9.1 Input

The redundancy module is operated with the DC output voltage of the upstream power supply. On the primary side, the redundancy module is connected via connection terminal blocks INPUT DC +/-.

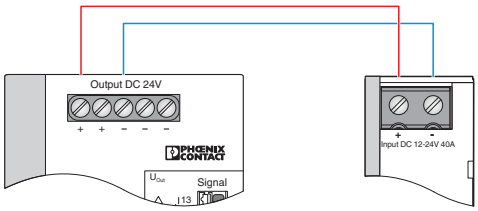


Figure 15 Schematic diagram, wiring of the input terminal blocks

Protection of the primary side

NOTE: Potential damage to the redundancy module caused by overload

If a non-current-limiting source is used to supply the load, appropriate protection must be implemented.

9.2 Output

The load to be supplied is operated with the DC output voltage of the redundancy module. On the secondary side, the redundancy module is connected via connection terminal blocks OUTPUT DC +/-.

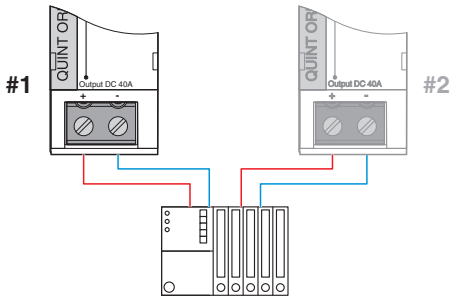


Figure 16 Schematic diagram, wiring of the output terminal blocks

10 Signaling

A floating signal contact is available for preventive function monitoring of the redundancy module.

The current device status of the redundancy module is signaled using an LED status indicator. The function of each LED status indicator is assigned to a fixed event and cannot be modified.

10.1 Location and function of the signaling elements

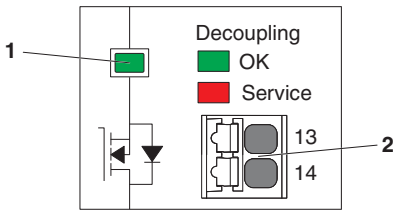


Figure 17 Position of the signaling element

Key

No.	Signaling elements
1	LED status and diagnostic indicators
2	13/14 floating switch contact (N/O contact)

10.2 Signaling table

The device status is indicated by an LED in different colors and flashing patterns.

The table below lists the possible signaling variants.

LED	Relay contact 13/14	Description
	Open	Input voltage not present or short circuit at redundancy module output
	Closed	Input voltage present
	Open	Redundancy module needs to be factory tested

Key

Symbol	Description
	LED OFF
	LED lights up green
	LED lights up red

10.3 Floating switch contact

The operating status of the redundancy module is forwarded to the higher-level controller using a floating switch contact (see signaling table section).

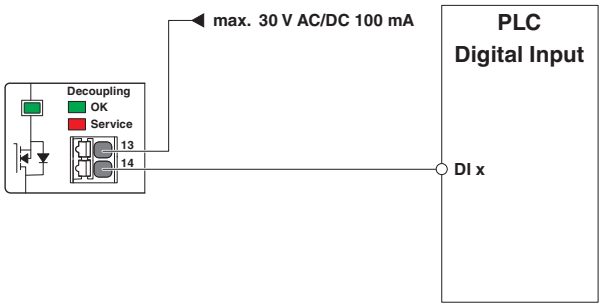


Figure 18 Schematic diagram, wiring of the floating switch contact

11 Redundancy operation

Redundant circuits are suitable for supplying systems and system parts which place particularly high demands on operational reliability.

If energy is to be supplied to the load with 1+1 redundancy, two power supplies of the same type and performance class must be used. In the event of an error, it must be ensured that one of the power supplies is able to provide the total required power for the load. This means that in redundancy mode, two 20 A power supplies supply a load with a nominal current of 20 A, for example. During normal operation of the power supplies, each power supply therefore supplies 10 A.

Always use cables with the same cross sections and lengths when wiring the power supplies on the DC output side.

11.1 Optimum structure for a redundant system

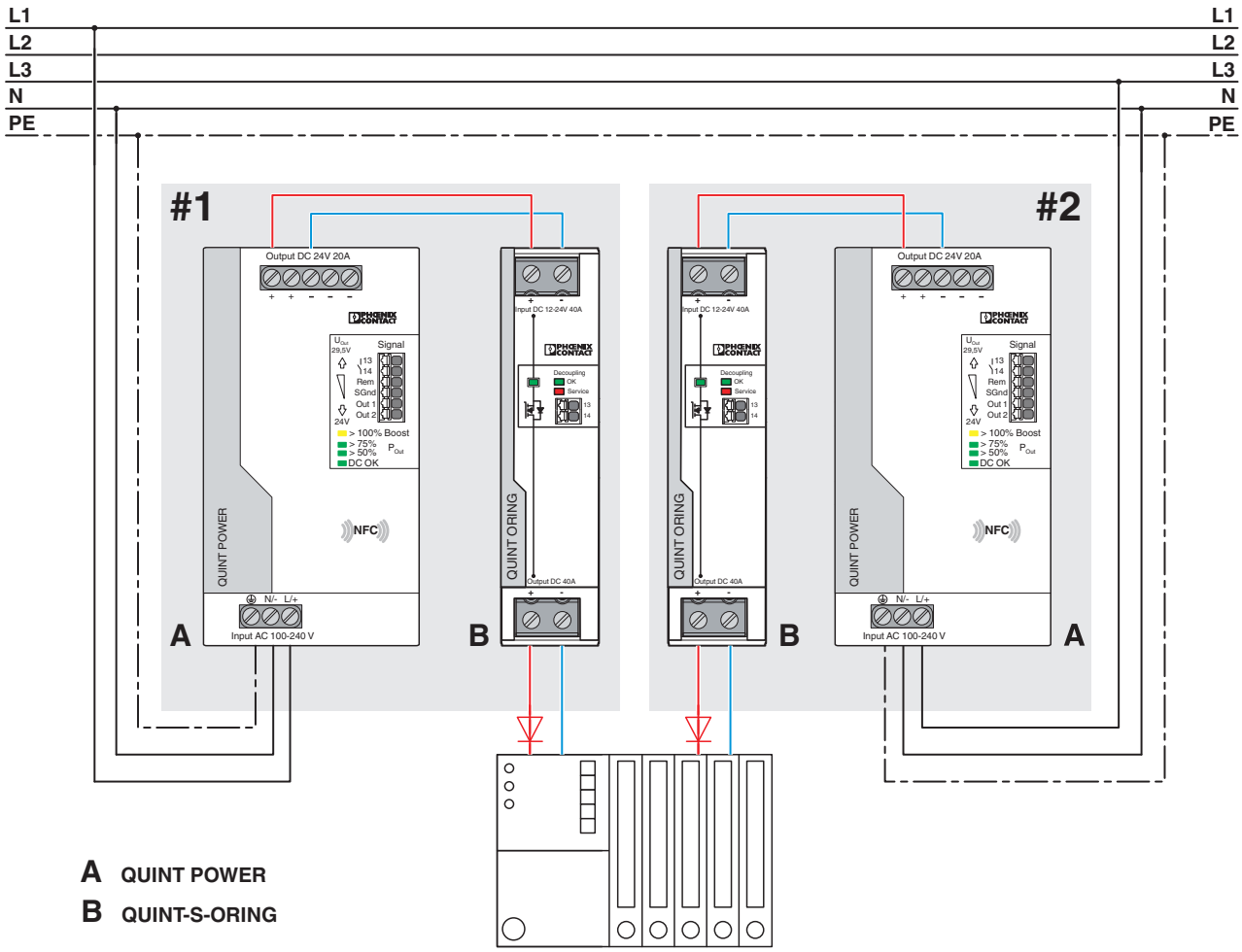


Figure 19 Structure of a redundant system

The following conditions must be met for 1+1 and n+1 redundancy operation of the power supplies in conjunction with a QUINT4-S-ORING module.

- Power supplies are connected to different phases
- Symmetrical cable routing up to the load
- Power supplies are set to the same output voltage
- Power supplies are switched to parallel operation
- Current threshold for monitoring is set to the load current

11.2 Error in a redundant system

The redundant system structure, comprising QUINT POWER power supplies and QUINT S-ORING modules, enables the complete, functional monitoring of your application.

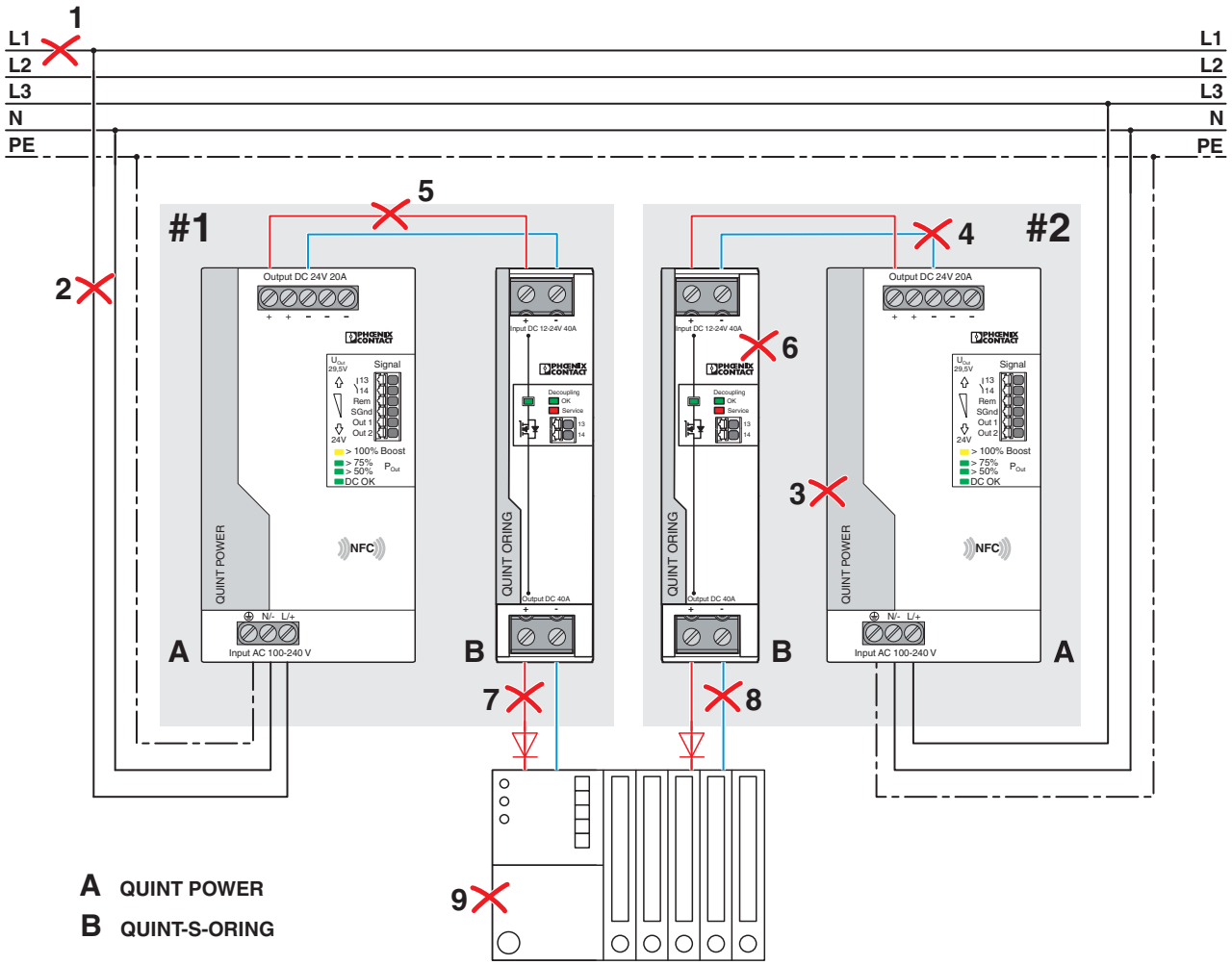


Figure 20 Schematic diagram of the monitored error scenarios

No.	Error description
1	Error in the active power grid phase
2	Supply line of the power supply interrupted or short circuited
3	Error in the active power supply
4	Short circuit in the wiring between a power supply and the connected redundancy module
5	Interruption in the wiring between a power supply and the connected redundancy module
6	Redundancy module error
7	Interruption in the wiring between a redundancy module and the load
8	Short circuit in the wiring between a redundancy module and the load
9	Load current is too high for a power supply

12 Derating

The redundancy module runs in nominal operation without any limitations. For operation outside the nominal range, the following points should be observed depending on the type of use.

12.1 Ambient temperature

When operating the redundancy module at an ambient temperature of > 60°C, a power derating of 2.5%/K should be observed. Up to an ambient temperature of 40°C, the power of the static boost can be taken from the redundancy module for a sustained period. In the 40°C to 60°C temperature range, the redundancy module can output more than the nominal power for a sustained period.

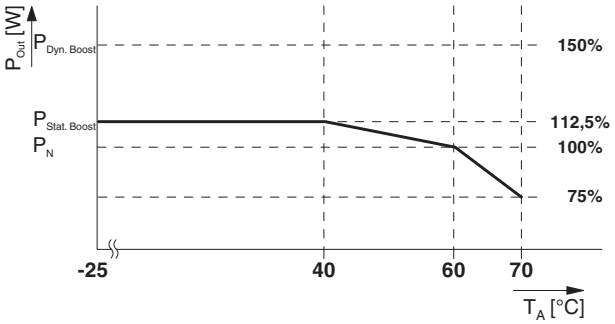


Figure 21 Output power depending on the ambient temperature

The redundancy module can be operated at an installation height of up to 5000 m without any limitations. Different data applies for installation locations above 2000 m due to the differing air pressure and the reduced convection cooling associated with this (see technical data section). The data provided is based on the results of pressure chamber testing performed by an accredited test laboratory.

12.2 Installation height

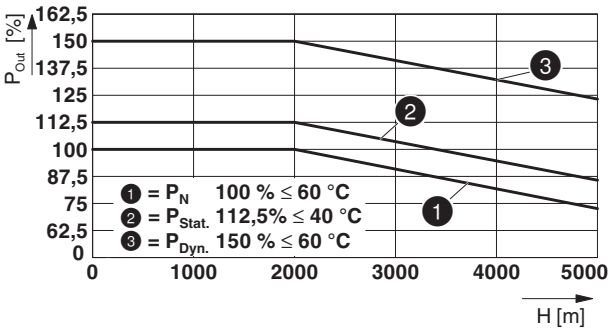


Figure 22 Output power depending on the installation height

12.3 Position-dependent derating

Position-dependent derating does not have to be taken into consideration.

HIMatrix® F

Safety-Related Controller

Manual

F30 03

SAFETY
NONSTOP

HIMA

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

Original document	Description
HI 800 472 D, Rev. 3.00 (1627)	English translation of the German original document

Table of Contents

1 Introduction

This manual describes the technical characteristics of the device and its use. It provides information on how to install, start up and configure the module in SILworX.

1.1 Structure and Use of this Manual

The content of this manual is part of the hardware description of the HIMatrix programmable electronic system.

This manual is organized in the following main chapters:

- Introduction
- Safety
- Product description
- Start-up
- Operation
- Maintenance
- Decommissioning
- Transport
- Disposal

---

i Compact controllers and remote I/Os are referred to as **devices**.

Additionally, the following documents must be taken into account:

Document	Content	Document number
HIMatrix system manual	Hardware description of the HIMatrix compact systems and the F60 modular system.	HI 800 141 E
HIMatrix safety manual	Safety functions of the HIMatrix system.	HI 800 023 E
HIMatrix safety manual for railway applications.	Safety functions of the HIMatrix system using the HIMatrix in railway applications.	HI 800 437 E
Communication manual	Description of the communication protocols, ComUserTask and their configuration in SILworX.	HI 801 101 E
SILworX online help	Instructions on how to use SILworX.	-
SILworX first steps manual	Introduction to SILworX using the HIMax system as an example.	HI 801 103 E

Table 1: Additional Relevant Documents

The latest manuals can be downloaded from the HIMA website at www.hima.de and www.hima.com. The revision index on the footer can be used to compare the current version of existing manuals with the Internet edition.

1.2 Target Audience

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

1.3 Writing Conventions

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

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

Safety notices and operating tips are particularly marked.

1.3.1 Safety Notices

The safety notices are represented as described below.

They must be strictly observed to ensure the lowest possible operating risk. The content is structured as follows:

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

⚠ SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

The signal words have the following meanings:

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

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 for additional information is located here.

Useful tips and tricks appear as follows:

TIP The tip text is located here.

2 Safety

All safety information, notices and instructions specified in this document 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. The use in the Ex zone is only permitted if additional measures are taken.

2.1 Intended Use

HIMatrix components are designed for assembling safety-related controller systems.

When using the components in the HIMatrix system, comply with the following general requirements.

2.1.1 Environmental Conditions

All the environmental conditions specified in this manual must be observed when operating the HIMatrix system. The environmental requirements are listed in the product data.

2.1.2 ESD Protective Measures

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

NOTICE

Damage to the HIMatrix system due to electrostatic discharge!

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

2.2 Residual Risk

No imminent risk results from a HIMA 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 HIMA 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 HIMA system from operating safely is permitted.

3 Product Description

The safety-related **F30 03** controller is a compact system in a metal housing with 20 digital inputs and 8 digital outputs.

The controller is available in various model variants, see Table 2.

The configuration is performed using SILworX, see Chapter 4.2.

The controller is suitable for sequence of events recording (SOE), see Chapter 4.2. The controller supports multitasking and reload. For more details, refer to the system manual (HI 800 141 E).

i A license is required to use the events recording, the multitasking and the reload features.

The device has been certified by the TÜV for safety-related applications up to SIL 3 (IEC 61508, IEC 61511 and IEC 62061), Cat. 4 and PL e (EN ISO 13849-1) and SIL 4 (EN 50126, EN 50128, and EN 50129).

Further safety standards, application standards and test standards are specified in the certificates available on the HIMA website.

3.1 Safety Function

The controller is equipped with safety-related digital inputs and outputs.

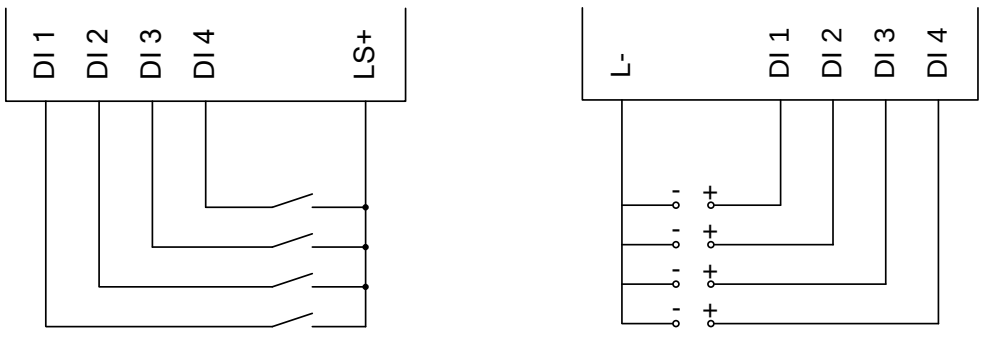
3.1.1 Safety-Related Digital Inputs

The controller is equipped with 20 digital inputs. The state (HIGH, LOW) of each input is signaled by an individual LED.

Mechanical contacts without own power supply or signal power source can be connected to the inputs.

Potential-free mechanical contacts without own power supply are fed via an internal short-circuit-proof 24 V power source (LS+). Each of them supply a group of 4 mechanical contacts. Figure 1 shows how the connection is performed.

With signal voltage sources, the corresponding ground must be connected to the input (L-), see Figure 1.



Connection of potential-free mechanical contacts

Connection of signal power sources

Figure 1: Connections to Safety-Related Digital Inputs

For the external wiring and the connection of sensors, apply the de-energize to trip principle. Thus, if a fault occurs, the input signals adopt a de-energized, safe state (low level).

If an external wire is not monitored, an open-circuit is considered as safe low level.

3.1.1.1 Reaction in the Event of a Fault

If the device detects a fault on a digital input, the user program processes a low level in accordance with the de-energize to trip principle.

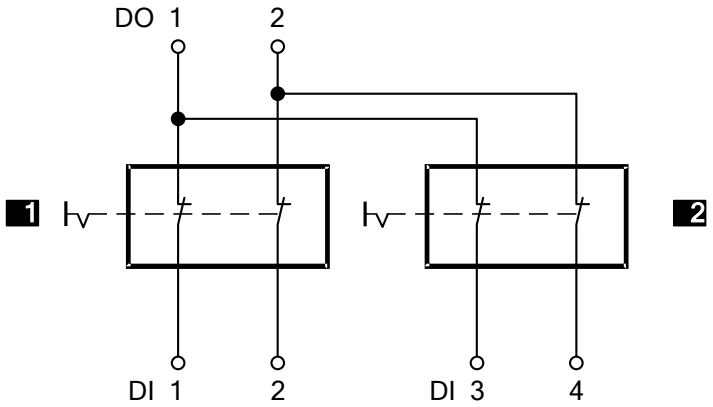
The device activates the *FAULT* LED.

For diagnostic purposes, the signal value of the channel as well as the corresponding error code must be evaluated in the user program. Using the error code, the user can configure additional fault reactions in the user program.

3.1.1.2 Line Control

Line control is used to detect short-circuits or open-circuits and can be configured for the F30 system, e.g., on EMERGENCY STOP inputs complying with Cat. 4 and PL e in accordance with EN ISO 13849-1.

To this end, connect the digital outputs DO 1...DO 8 of the system to the digital inputs (DI) of the same system as follows:



1 EMERGENCY STOP 1
2 EMERGENCY STOP 2

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

Figure 2: Line Control

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

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

- Cross-circuit between two parallel wires.
- Invalid connections of two lines (e.g., DO 2 to DI 3).
- Earth fault on one wire (with earthed ground only).
- Open-circuit or open contacts.

Refer to the HIMatrix system manual (HI 800 141 E) for a description of and further details on line control.

3.1.2 Safety-Related Digital Outputs

The controller is equipped with 8 digital outputs. The state (HIGH, LOW) of each output is signaled by an individual LED (HIGH, LOW).

At the maximum ambient temperature, the outputs 1...3 and 5...7 can be loaded with 0.5 A each; and outputs 4 and 8 can be loaded with 1 A or with 2 A at an ambient temperature of up to 50 °C.

Within a temperature range of 60…70 °C, all outputs of the F30 034 can be loaded with 0.5 A, see Table 14.

If an overload occurs, one or all digital outputs are switched off. If the overload is removed, the outputs are switched on again automatically, see Table 13.

The external wire of an output is not monitored, however, a detected short-circuit is signaled.

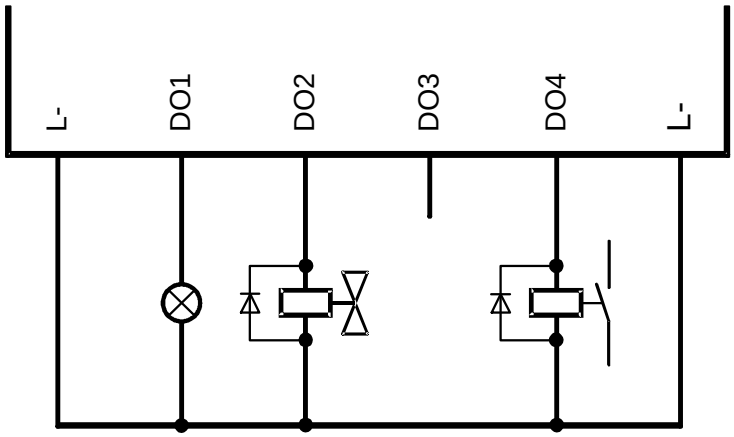


Figure 3: Connection of Actuators to Outputs

The redundant connection of two outputs must be decoupled with diodes.

⚠ WARNING

For connecting a load to a 1-pole switching output, use the corresponding L- ground of the respective channel group (2-pole connection) to ensure that the internal protective circuit can function.

Inductive loads may be connected with no free-wheeling diode on the actuator. However, HIMA strongly recommends connecting a protective diode directly to the actuator.

3.1.2.1 Reaction in the Event of a Fault

If the device detects a faulty signal on a digital output, the affected output is set to the safe (de-energized) state using the safety switches.

If a device fault occurs, all digital outputs are switched off.

In both cases, the device activates the *FAULT* LED.

For diagnostic purposes, the signal value of the channel as well as the corresponding error code must be evaluated in the user program. Using the error code, the user can configure additional fault reactions in the user program.

3.2 Equipment, Scope of Delivery

The following table specifies the available controller variants:

Designation	Description
F30 03 SILworX	Controller (20 digital inputs, 8 digital outputs) Ambient temperature: 0...+60 °C
F30 034 SILworX	Controller (20 digital inputs, 8 digital outputs) Ambient temperature: -25...+70 °C (temperature class T1) Vibration and shock tested according to EN 50125-3 and EN 50155, class 1B according to IEC 61373

Table 2: Available Variants

3.2.1 IP Address and System ID (SRS)

A transparent label for specifying the IP addresses of the CPU and the COM and the system ID (SRS, System.Rack.Slot) after a change, is delivered with the device.

Default value for CPU IP address:	192.168.0.99
Default value for COM IP address:	192.168.0.100
Default value for SRS:	60 000.0.0

The label must be affixed so that the ventilation slots in the housing are not obstructed.

Refer to the SILworX first steps manual for more information on how to modify the IP address and the system ID.

3.3 Type Label

The type label specifies the following details:

- Product name
- Bar code (1D or 2D code)
- Part no.
- Production year
- Hardware revision index (HW-Rev.)
- Firmware revision index (OS-Rev.)
- Operating voltage
- Mark of conformity

Figure 4: Sample Type Label

3.4 Structure

This chapter describes the layout and function of the controller and the connections for communication.

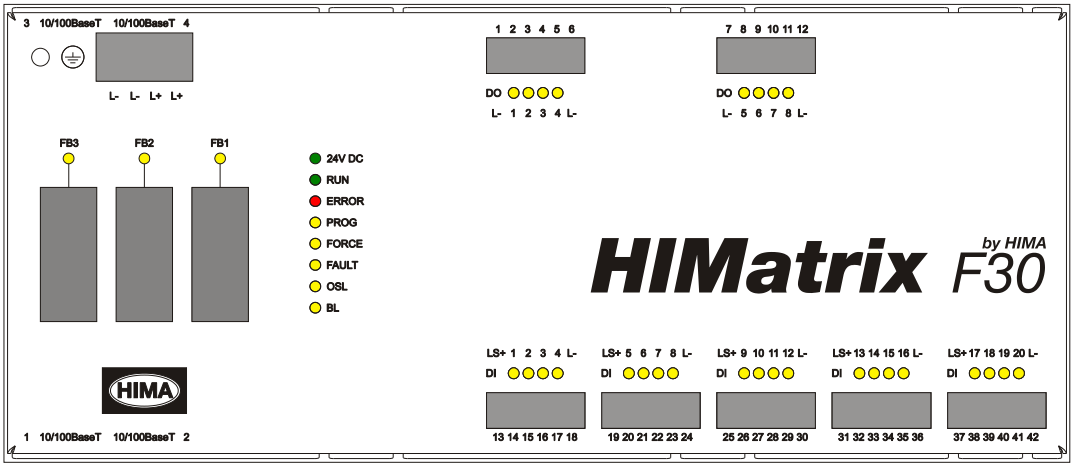
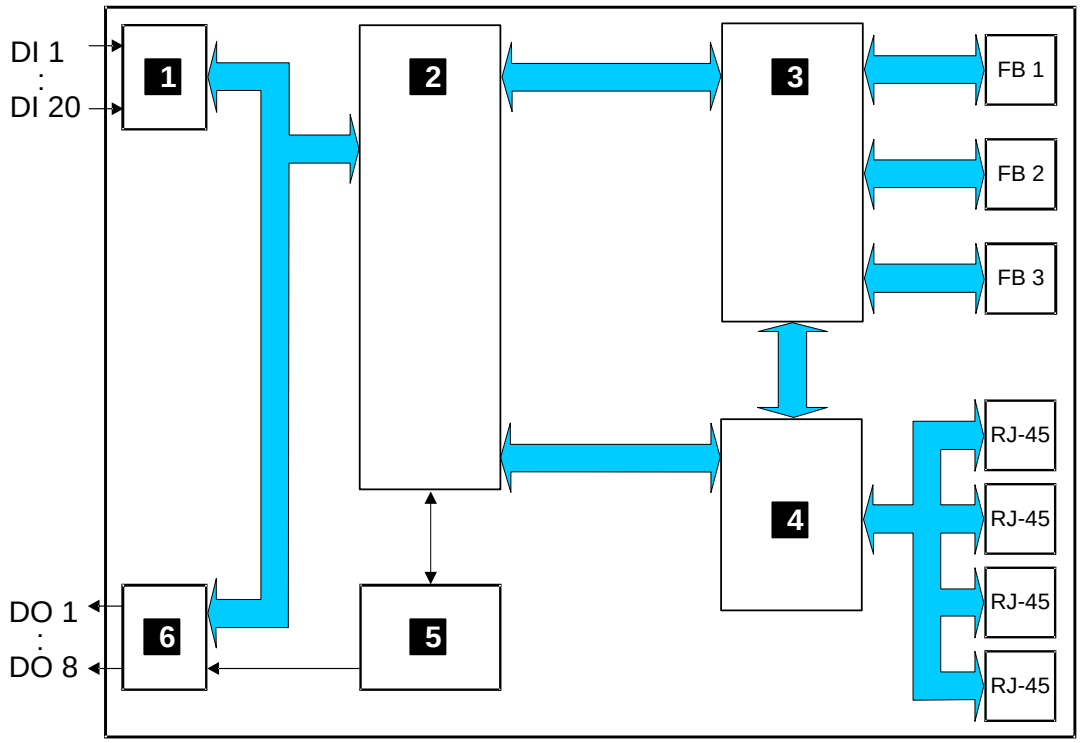


Figure 5: Front View



1 Digital inputs
2 Safety-related processor system (CPU)
3 Communication system (COM)
4 Switch
5 Watchdog
6 Digital outputs

Figure 6: Block Diagram

3.4.1 LED Indicators

The light-emitting diodes (LEDs) indicate the operating state of the controller. The LEDs are classified as follows:

- Operating voltage LED
- System LEDs
- Communication LEDs
- I/O LEDs
- Fieldbus LEDs

When the supply voltage is switched on, an LED test is performed and all LEDs are briefly lit.

Definition of blinking frequencies

The following table defines the blinking frequencies of the LEDs:

Definition	Blinking frequencies
Blinking1	Long (approx. 600 ms) on, long (approx. 600 ms) off
Blinking-x	Ethernet communication: Blinking synchronously with data transfer

Table 3: Blinking Frequencies of LEDs

3.4.1.1 Operating voltage LED

The LED signals the following states:

LED	Color	Status	Description
24 VDC	Green	On	24 VDC operating voltage present
		Off	No operating voltage

Table 4: Operating Voltage LED

3.4.1.2 System LEDs

While the system is being booted, all LEDs are lit simultaneously.

LED	Color	Status	Description
RUN	Green	On	▪ Device in RUN, normal operation. ▪ A loaded user program is being processed. ▪ The emergency loader active.
		Blinking1	▪ Device in STOP. ▪ A new operating system is being loaded.
		Off	The device is not in the RUN or STOP state.
ERR	Red	On	System warning, for example: ▪ No license for additional functions (communication protocols, re-load), test mode. ▪ Temperature warning.
		Blinking1	System error, for example: ▪ The device is in the ERROR STOP state. Internal faults detected by self-tests, e.g., hardware or voltage supply faults. The processor system can only be restarted with a command from the PADT (reboot). ▪ Fault while loading the operating system. ▪ The emergency loader active.
		Off	No faults detected.
PROG	Yellow	On	▪ The emergency loader active. ▪ A new configuration is being loaded into the device. ▪ A new operating system is being loaded. ▪ Change to watchdog time or safety time. ▪ Detection of duplicate IP address. ▪ SRS change.
		Blinking1	▪ Reload is being performed. ▪ A duplicate IP address was detected. [1)] ▪ PROFINET has received an identify request. [1)]
		Off	None of the described events occurred.
FORCE	Yellow	On	▪ Forcing prepared, but no local or global variables are currently being forced. Example: the force switch for a variable is set, the force main switch is still deactivated. The device is in the RUN or STOP state. ▪ The emergency loader active.
		Blinking1	▪ Forcing is active: At least one local or global variable has adopted the corresponding force value. ▪ A duplicate IP address was detected. [1)] ▪ PROFINET has received an identify request. [1)]
		Off	None of the described events occurred.
FAULT	Yellow	On	▪ The emergency loader active. ▪ There is a warning related to the field zone.
		Blinking1	▪ The new operating system is corrupted (after OS download). ▪ Fault while loading a new operating system. ▪ The loaded configuration is not valid. ▪ At least one fault related to the field level has occurred. ▪ A duplicate IP address was detected. [1)] ▪ PROFINET has received an identify request. [1)]
		Off	None of the described faults occurred.

LED	Color	Status	Description
OSL	Yellow	Blinking1	▪ Operating system emergency loader active. ▪ A duplicate IP address was detected. [1)] ▪ PROFINET has received an identify request. [1)]
		Off	None of the described events occurred.
BL	Yellow	On	Warning related to external process data communication.
		Blinking1	▪ OS and OSL binary defective or hardware fault, INIT_FAIL. ▪ Fault in the external process data communication. ▪ A duplicate IP address was detected. [1)] ▪ PROFINET has received an identify request. [1)]
		Off	None of the described events occurred.
[1)] If all the LEDs PROG, FORCE, FAULT, OSL and BL are blinking simultaneously.			

Table 5: System LEDs

3.4.1.3 Communication LEDs

All RJ-45 connectors are provided with a green and a yellow LEDs. The LEDs signal the following states:

LED	Status	Description
Green	On	Full duplex operation.
	Blinking1	IP address conflict, all communication LEDs are blinking.
	Blinking-x	Collision.
	Off	Half duplex operation, no collision.
Yellow	On	Connection available.
	Blinking1	IP address conflict, all communication LEDs are blinking.
	Blinking-x	Interface activity.
	Off	No connection available.

Table 6: Ethernet Indicators

3.4.1.4 I/O LEDs

The LEDs signal the following states:

LED	Color	Status	Description
DI 1…20	Yellow	On	The related channel is active (energized).
		Off	The related channel is inactive (de-energized).
DO 1…8	Yellow	On	The related channel is active (energized).
		Off	The related channel is inactive (de-energized).

Table 7: I/O LEDs

3.4.1.5 Fieldbus LEDs

LEDs FB1…FB3 are used to display the state of communication occurring via the serial interfaces. The function of the LED depends on the used protocol.

Refer to the communication manual (HI 801 101 E) for a functional description.

3.4.2 Communication

The controller communicates with remote I/Os via safe**ethernet**. Characteristics and configuration of safe**ethernet** are described in the communication manual (HI 801 101 E).

3.4.2.1 Connections for Ethernet Communication

Property	Description
Port	4 x RJ-45
Transfer standard	10BASE-T/100BASE-Tx, half and full duplex
Auto negotiation	Yes
Auto crossover	Yes
IP Address	Freely configurable [1)]
Subnet Mask	Freely configurable [1)]
Supported protocols	▪ Safety-related: safeethernet, PROFIsafe ▪ Standard protocols: Programming and debugging tool (PADT), OPC, Modbus TCP, TCP SR, SNTP, ComUserTask, PROFINET
[1)] The general rules for assigning IP address and subnet masks must be adhered to	

Table 8: Ethernet Interface Properties

Two RJ-45 connectors with integrated LEDs are located on the top and on the bottom left-hand side of the housing. Refer to Chapter 16 for a description of the LEDs' function.

The connection parameters are read based on the MAC address (media access control address) defined during manufacturing.

CPU and COM have their own MAC addresses. The CPU MAC address is specified on a label located above the two RJ-45 connectors (1 and 2).

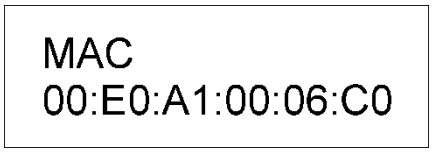


Figure 7: Sample MAC Address Label

The COM MAC address corresponds to the CPU MAC address, except for the last byte which is increased by 1.

Example:

CPU MAC address: 00:E0:A1:00:06:C0

COM MAC address: 00:E0:A1:00:06:C1

The controller is equipped with an integrated switch for Ethernet communication. For further information on switches and safe**ethernet**, refer to the system manual (HI 800 141 E).

3.4.2.2 Network Ports in Use for Ethernet Communication

UDP ports	Use
123	SNTP (time synchronization between PES and remote I/O, PES and external devices)
502	Modbus salve (can be changed by the user)
6010	safeethernet and OPC
6005 / 6012	If TCS_DIRECT was not selected in the HH network
8000	Programming and operation with SILworX
8004	Configuration of the remote I/Os using the PES (SILworX)
34 964	PROFINET endpoint mapper (required for establishing the connection)
49 152	PROFINET RPC server
49 153	PROFINET RPC client

Table 9: Network Ports (UDP Ports) in Use

TCP ports	Use
502	Modbus salve (can be changed by the user)
xxx	TCP SR assigned by the user

Table 10: Network Ports (TCP Ports) in Use

i The ComUserTask can use any port if it is not already used by another protocol.

3.4.2.3 Connections for Fieldbus Communication

The three 9-pole D-sub connectors are located on the front plate of the housing.

The fieldbus interfaces FB1 and FB2 can be equipped with fieldbus submodules. The fieldbus submodules are optional and must be installed by the manufacturer. The available fieldbus submodules are described in the communication manual (HI 801 101 E).

The fieldbus interfaces are not operational without fieldbus submodule.

Factory-made, the fieldbus interface FB3 is equipped with RS485 for Modbus (master or slave) or ComUserTask.

3.4.3 Reset Key

The controller is equipped with a reset key. The key is only required if the user name or password for administrator access is not known. If only the IP address set for the controller does not match the PADT (PC), the connection can be established with a `Route add` entry on the PC.

i Only the model variants without protective lacquer are equipped with a reset key.

The key can be accessed through a small round hole located approximately 5 cm from the upper left-hand side of the housing. The key is engaged using a suitable pin made of insulating material to avoid short-circuits within the controller.

The reset is only effective if the controller is rebooted (switched off and on) while the key is simultaneously engaged for at least 20 s. Engaging the key during operation has no effect.

⚠ CAUTION

Fieldbus communication may be disturbed!

Prior to switching on the controller with the reset key engaged, all device fieldbus connectors must be unplugged to ensure that the fieldbus communication among other stations is not disturbed.

The fieldbus plugs may only be plugged in again when the controller is in the RUN or STOP state.

Properties and behavior of the controller after a reboot with engaged reset key:

- Connection parameters (IP address and system ID) are set to the default values.
- All accounts are deactivated except for the standard account *Administrator* with empty password.
- Loading a user program or operating system with standard connection parameters is inhibited!

  Loading is only allowed after the connection parameters and the account have been configured on the controller and the controller has been rebooted.

After a new reboot with unengaged reset key, the following connection parameters (IP address and system ID) and accounts become effective:

- Those configured by the user.
- Those valid prior to rebooting with the reset key engaged, if no changes were performed.

3.4.4 Hardware Clock

In case of loss of operating voltage, the power provided by an integrated gold capacitor is sufficient to buffer the hardware clock for approximately one week.

3.5 Product Data

General	
Supply voltage L+	24 VDC, -15...+20 %, $r_P \leq 5$ % from a power supply unit with safe insulation in accordance with IEC 61131-2
Maximum supply voltage	30 V
Current consumption	max. 8 A (with maximum load) Idle: 0.5 A at 24 V
Fuse (external)	10 A time-lag (T)
Microprocessor	PowerPC
Total program and data memory for all user programs	5 MB less 64 kB for CRCs
Data memory for retain variables	Up to CPU OS V10.16: 8 kBytes CPU OS V10.32 and higher: 32 kBytes
Response time	≥ 6 ms.
Ethernet interfaces	4 x RJ-45, 10BASE-T/100BASE-Tx with integrated switch
Fieldbus Interfaces	3 x 9-pole D-sub FB1 and FB2 with fieldbus submodule pluggable FB3 with RS485 for Modbus (master or slave) or ComUserTask
Buffer for date/time	min. 5 days, gold capacitor
Protection class	Protection class III in accordance with IEC/EN 61131-2
Ambient temperature	0...+60 °C
Storage temperature	-40...+85 °C
Pollution	Pollution degree II in accordance with IEC/EN 61131-2
Altitude	< 2000 m
Degree of protection	IP20
Max. dimensions (without plug)	Width: 257 mm (with housing screws) Height: 114 mm (with fixing bolt) Depth: 66 mm (with earthing screw)
Weight	approx. 1.2 kg

Table 11: Product Data

Digital inputs	
Number of inputs	20 (non-galvanically separated)
High level: Voltage Current consumption	15...30 VDC ≥ 2 mA at 15 V
Low level: Voltage Current consumption	max. 5 VDC Max. 1.5 mA (1 mA at 5 V)
Switching point	typ. 7.5 V
Supply	5 x 20 V / 100 mA (at 24 V), short-circuit-proof

Table 12: Specifications for Digital Inputs

Digital outputs	
Number of outputs	8 (non-galvanically separated)
Output voltage	≥ L+ minus 2 V
Output current	Channels 1...3 and 5...7: 0.5 A at ≤ 60 °C The output current of the channels 4 and 8 depends on the ambient temperature. Ambient temperature / Output current < 50 °C / 2 A 50…60 °C / 1 A
Minimum load	2 mA for each channel
Internal voltage drop	max. 2 V at 2 A
Leakage current (with low level)	max. 1 mA at 2 V
Behavior upon overload	The affected output is switched off and cyclically switched on again.
Total output current	max. 7 A Upon overload, all outputs are switched off and cyclically switched on again.

Table 13: Specifications for the Digital Outputs

3.5.1 Product Data F30 034

The F30 034 model variant is intended for use in railway applications. The electronic components are coated with a protective lacquer.

F30 034	
Ambient temperature	-25…+70 °C (temperature class T1 [1)])
Output current of the digital outputs	Channels 1...3 and 5...7: 0.5 A at ≤ 70 °C The output current of the channels 4 and 8 depends on the ambient temperature. Ambient temperature / Output current < 50 °C / 2 A 50…60 °C / 1 A > 60 °C / 0.5 A
Weight	approx. 1.2 kg
[1)] For more temperature classes, refer to the HIMatrix safety manual for railway applications (HI 800 437 E)	

Table 14: Product Data F30 034

The F30 034 controller meets the vibration and shock requirements in accordance with EN 61373, Category 1, Class B.

3.6 Certified F30 03 HIMatrix

Refer to the HIMatrix safety manual for more information on the standards used to certify the HIMatrix system.

The certificate and the EC type test certificate are available on the HIMA website.

4 Start-Up

To start up the controller, it must be installed, connected and configured in SILworX.

4.1 Installation and Mounting

The HIMatrix is mounted on a 35 mm (DIN) rail such as described in the HIMatrix system manual (HI 800 141 E).

When laying cables (long cables, in particular), take appropriate measures to avoid interference, e.g., by separating the signal lines from the supply lines.

When dimensioning the cables, ensure that their electrical properties have no negative impact on the measuring circuit.

4.1.1 Connecting the Digital Inputs

Use the following terminals to connect the digital inputs:

Terminal	Designation	Function
13	LS+	Sensor supply of the inputs 1...4
14	1	Digital input 1
15	2	Digital input 2
16	3	Digital input 3
17	4	Digital input 4
18	L-	Ground
Terminal	Designation	Function
19	LS+	Sensor supply of the inputs 5...8
20	5	Digital input 5
21	6	Digital input 6
22	7	Digital input 7
23	8	Digital input 8
24	L-	Ground
Terminal	Designation	Function
25	LS+	Sensor supply of the inputs 9...12
26	9	Digital input 9
27	10	Digital input 10
28	11	Digital input 11
29	12	Digital input 12
30	L-	Ground
Terminal	Designation	Function
31	LS+	Sensor supply of the inputs 13...16
32	13	Digital input 13
33	14	Digital input 14
34	15	Digital input 15
35	16	Digital input 16
36	L-	Ground

Terminal	Designation	Function
37	LS+	Sensor supply of the inputs 17...20
38	17	Digital input 17
39	18	Digital input 18
40	19	Digital input 19
41	20	Digital input 20
42	L-	Ground

Table 15: Terminal Assignment for the Digital Inputs

4.1.1.1 Surges on Digital Inputs

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

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

1. Install shielded input wires.
2. Program noise blanking in the user program. A signal must be present for at least two cycles before it is evaluated. This measure increases the maximum response time!

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, earthing and plant wiring in accordance with the relevant standards and the instructions specified in the system manual (HI 800 141 E).

4.1.2 Connecting the Digital Outputs

Use the following terminals to connect the digital outputs:

Terminal	Designation	Function
1	L-	Ground channel group
2	1	Digital output 1
3	2	Digital output 2
4	3	Digital output 3
5	4	Digital output 4 (for increased load)
6	L-	Ground channel group
Terminal	Designation	Function
7	L-	Ground channel group
8	5	Digital output 5
9	6	Digital output 6
10	7	Digital output 7
11	8	Digital output 8 (for increased load)
12	L-	Ground channel group

Table 16: Terminal Assignment for the Digital Outputs

4.1.3 Cable Plugs

Cable plugs attached to the pin headers of the devices are used to connect to the power supply and to the field zone. The cable plugs are included within the scope of delivery of the HIMatrix devices and modules.

The devices power supply connections feature the following properties:

Connection to the power supply	
Cable plugs	4 poles, screw terminals
Wire cross-section	0.2…2.5 mm^2 (single-wire) 0.2…2.5 mm^2 (finely stranded) 0.2…2.5 mm^2 (with wire end ferrule)
Stripping length	10 mm
Screwdriver	Slotted 0.6 x 3.5 mm
Tightening torque	0.4…0.5 Nm

Table 17: Power Supply Cable Plug Properties

Connection to the field zone	
Number of cable plugs	7 piece, 6 poles, screw terminals
Wire cross-section	0.2…1.5 mm^2 (single-wire) 0.2…1.5 mm^2 (finely stranded) 0.2…1.5 mm^2 (with wire end ferrule)
Stripping length	6 mm
Screwdriver	Slotted 0.4 x 2.5 mm
Tightening torque	0.2…0.25 Nm

Table 18: Input and Output Cable Plug Properties

4.1.4 Mounting the Controller in Zone 2

The controller is suitable for mounting in the explosive atmospheres of zone 2. The special conditions X specified in the HIMatrix safety manual (HI 800 023 E) must be observed for use in zone 2.

These conditions require the controller to be mounted in an enclosure that is able to safely dissipate the generated heat.

Depending on the output load and supply voltage, the HIMatrix F30 03 has a power dissipation ranging between 12 W and 33 W.

The remote I/O must be labeled with the following Ex marking:

 II 3G Ex nA IIC T4 Gc

i When using the controller in zone 2, the permissible ambient temperature must be observed, see Chapter 3.5.

4.2 Sequence of Events Recording (SOE)

The global variables of the controller can be monitored using sequence of events recording. Global variables to be monitored are configured using SILworX; refer to the online help and the communication manual (HI 801 101 E) for further details. Up to 4000 events can be configured.

An event is composed of:

Entry data	Description
Event ID	The event ID is assigned by the PADT
Timestamp	Date (e.g., 21/11/2008) Time (e.g., 9:31:57.531)
Event state	Alarm/Normal (boolean event) LL, L, N, H, HH (scalar event)
Event quality	Quality good/ Quality bad, see www.opcfoundation.org

Table 19: Event Description

Events are recorded within the cycle of the user program. The processor system uses global variables to create the events and stores them in its non-volatile event buffer.

The event buffer includes 1000 events. If the event buffer is full, an overflow system event entry is created. Thereafter, events are no longer recorded until existing events have been read and space is once again available in the event buffer.

4.3 Configuration with SILworX

In the Hardware Editor, the controller is represented like a base plate equipped with the following modules:

- Processor module (CPU).
- Communication module (COM).
- Input module (DI 20).
- Output module (DO 8).

Double-click the module to open the Detail View with the corresponding tabs. The tabs of the I/O modules are used to assign the global variables configured in the user program to the system variables.

4.3.1 Processor Module

The following tables present the parameters for the processor module (CPU) in the same order as given in the Hardware Editor.

4.3.1.1 Tab **Module**

The **Module** tab contains the following parameters:

Parameter	Description
Name	Module name.
Activate Max. µP Budget for HH Protocol	▪ Activated: Use CPU load limit from the *Max. µP Budget for HH Protocol [%]* field. ▪ Deactivated: Do not use the CPU load limit for IP data transfer. Default setting: Deactivated
Max. µP Budget for HH Protocol [%]	Maximum module's CPU load that can be used for processing the IP data transfer. i The maximum load must be distributed among all the implemented protocols that use this communication module.
Code Generation	Up to V6: Setting compatible with existing projects. V6 and higher: Setting recommended for new projects to support safe**ethernet** reload. Default setting: V6 and higher
IP Address	IP address of the Ethernet interface. Default value: 192.168.0.99
Subnet Mask	32-bit address mask to split up the IP address in network and host address. Default value: 255.255.252.0
Standard Interface	Activated: the interface is used as standard interface for system login. Default setting: Deactivated
Default Gateway	IP address of the default gateway. Default value: 0.0.0.0

Parameter	Description
ARP Aging Time [s]	A processor or COM module stores the MAC addresses of the communication partners in a MAC/IP address assignment table (ARP cache). The MAC address remains stored in the ARP cache, if messages from the communication partner are received in a period of 1x...2x *ARP Aging Time*. The MAC address is erased from the ARP cache, if no messages from the communication partner are received in a period of 1x...2x *ARP Aging Time*. The typical value for the *ARP Aging Time* in a local network ranges from 5...300 s. The user cannot read the contents of the ARP cache. Range of values: 1...3600 s. Default value: 60 s. **Notice:** If routers or gateways are used, the *ARP Aging Time* must be adjusted (increased) due to the additional time required for two-way transmission. If the *ARP Aging Time* is too low, the processor or the COM module deletes the MAC address of the communication partner from the ARP cache and communication is either delayed or breaks down entirely. For an efficient performance, the *ARP Aging Time* value must be greater than the receive timeout set for the protocols in use.
MAC Learning	*MAC Learning* and *ARP Aging Time* are used to set how quick the Ethernet switch should learn the MAC address. The following settings are possible: ▪ Conservative (recommended): If the ARP cache already contains MAC addresses of communication partners, these are locked and cannot be replaced by other MAC addresses for at least 1 *ARP Aging Time* and a maximum of 2 *ARP Aging Time* periods. This ensures that data packets cannot be intentionally or unintentionally forwarded to external network subscribers (ARP spoofing). ▪ Tolerant: When a message is received, the IP address contained in the message is compared to the data in the ARP cache and the MAC address stored in the ARP cache is immediately overwritten with the MAC address from the message. The *Tolerant* setting must be used if the availability of communication is more important than the authorized access to the controller. Default setting: Conservative.
IP Forwarding	The function is not supported. Default setting: Deactivated

Parameter	Description
ICMP Mode	ICMP (Internet Control Message Protocol) allows the higher protocol layers to detect error states on the network layer and optimize the transmission of data packets. Message types of ICMP supported by the processor module: ▪ No ICMP Responses All the ICMP commands are deactivated. This ensures a high degree of safety against potential sabotage that might occur over the network. ▪ Echo Response If Echo Response is activated, the node responds to a ping command. It is thus possible to determine if a node can be reached. Safety is still high. ▪ Host Unreachable Not important for the user. Only used for testing at the manufacturer's facility. ▪ All Implemented ICMP Responses All ICMP commands are activated. This allows a more detailed diagnosis of network malfunctions. Default setting: Echo Response

Table 20: CPU and COM Configuration Parameters, **Module** Tab

4.3.1.2 Tab **Routings**

The **Routings** tab contains the routing table. This table is empty if the module is new. A maximum of 8 routing entries are possible.

Parameter	Description
Name	Denomination of the routing settings.
IP Address	Target IP address of the communication partner (with direct host routing) or network address (with subnet routing). Range of values: 0.0.0.0...255.255.255.255 Default value: 0.0.0.0
Subnet Mask	Define the target address range for a routing entry. 255.255.255.255 (with direct host routing) or subnet mask of the addressed subnet. Range of values: 0.0.0.0...255.255.255.255 Default value: 255.255.252.0
Gateway	IP address of the gateway to the addressed network. Range of values: 0.0.0.0...255.255.255.255 Default value: 0.0.0.1

Table 21: Routing Parameters for CPU and COM

4.3.1.3 Tab **Ethernet Switch**

The **Ethernet Switch** tab contains the following parameters:

Parameter	Description
Name	Name of the port (Eth1...Eth4) as printed on the housing; per port, only one configuration may exist.
Speed [MBit/s]	10: Data rate 10 Mbit/s 100: Data rate 100 Mbit/s Autoneg: Automatic baud rate setting. Default value: Autoneg
Flow Control	Full duplex: Simultaneous communication in both directions. Half duplex: Communication in one direction. Autoneg: Automatic communication control. Default value: Autoneg
Autoneg also with fixed values	The *Advertising* function (forwarding the speed and flow control properties) is also performed if the parameters *Speed* and *Flow Control* have fixed values. This allows other devices with ports set to *Autoneg* to recognize the HIMax port settings. Default setting: Activated
Limit	Limit the inbound multicast and/or broadcast packets. Off: No limitation Broadcast: Limit broadcast (128 kbit/s) Multicast and broadcast: Limit multicast and broadcast (1024 kbit/s). Default value: Broadcast

Table 22: Ethernet Switch Parameters

4.3.1.4 Tab **VLAN** (Port-Based VLAN)

For configuring the use of port-based VLAN.

i Should VLAN be supported, port-based VLAN should be off to enable each port to communicate with the other switch ports.

For each switch port, the user can define which other switch ports received Ethernet frames may be sent to, refer to Figure 6.

The table in the VLAN tab contains entries through which the connection between two ports can be set to active or inactive.

	Eth1	Eth2	Eth3	Eth4	COM
Eth1					
Eth2	Active				
Eth3	Active	Active			
Eth4	Active	Active	Active		
COM	Active	Active	Active	Active	
CPU	Active	Active	Active	Active	Active

Table 23: **VLAN** Tab

4.3.1.5 Tab **LLDP**

LLDP (Link Layer Discovery Protocol) periodically sends information per multicast via the own device (e.g., MAC address, device name, port number) and receives the same information from the neighboring devices.

LLDP uses the following values depending on whether PROFINET is configured on the communication module:

PROFINET on the COM module	Chassis ID	TTL (Time to Live)
Used	Device name	20 s
Not used	MAC address	120 s

Table 24: Values for LLDP

The processor and communication modules support LLDP on the Eth1, Eth2, Eth3 and Eth4 ports.

The following parameters define how a given port should work:

Off	LLDP is disabled on this port.
Send	LLDP sends LLDP Ethernet frames, received LLDP Ethernet frames are deleted without being processed.
Receive	LLDP sends no LLDP Ethernet frames, but received LLDP Ethernet frames are processed.
Send/Receive	LLDP sends and processes received LLDP Ethernet frames.

Default setting: Off.

4.3.1.6 Tab **Mirroring**

Mirroring is used to configure whether the module should duplicate Ethernet packets on a given port such that they can be read from a device connected to that port, e.g., for test purposes.

The following parameters define how a given port should work:

Off	This port does not participate to the mirroring process.
Egress	Outgoing data of this port are duplicated.
Ingress/Egress	Incoming and outgoing data of this port are duplicated.
Dest Port	This port is used to send duplicated data.

Default setting: Off.

4.3.2 Communication Module

The communication module contains the **Module** and the **Routings** tabs. Their content is identical to those of the processor module, see Table 20 and Table 21.

4.3.3 Parameters and Error Codes for the Inputs and Outputs

The following tables specify the system parameters that can be read and set for the inputs and outputs, including the corresponding error codes.

In the user program, the error codes can be read using the variables assigned within the logic.

The error codes can also be displayed in SILworX.

4.3.4 Digital Inputs for F30

The following tables present the statuses and parameters for the input module (DI 20) in the same order given in the SILworX Hardware Editor.

4.3.4.1 Tab **Module**

The **Module** tab contains the following system parameters:

System parameters	Data type	R/W	Description
DI Number of Pulsed Outputs	USINT	W	CPU OS V11 and higher: Without function Up to CPU OS V10: Number of pulsed outputs (supply outputs) Coding / Description: 0 – No pulsed output planned for detection of SC/OC [1)] 1 – Pulsed output 1 planned for detection of SC/OC [1)] 2 – Pulsed outputs 1 and 2 planned for detection of SC/OC [1)] … – … 8 – Pulsed output 1...8 planned for detection of SC/OC [1)] **Pulsed outputs must not be used as safety-related outputs!**
DI Pulse Slot	UDINT	W	Pulse module slot (detection of SC/OC [1]), set the value to 3
DI Pulse Delay [µs]	UINT	W	Waiting time for line control (detection of short-circuits or cross-circuits) Range of values 0...2000 µs Default value: 0 µs, waiting time: 400 µs
DI.Error Code	WORD	R	Error codes for all digital inputs 0x0001 – Fault within the digital inputs 0x0002 – Test of test pattern faulty
Module Error Code	WORD	R	Module error code 0x0000 – I/O processing, if required with errors See other error codes 0x0001 – No I/O processing (CPU not in RUN) 0x0002 – No I/O processing during the booting test 0x0004 – Manufacturer interface operating 0x0010 – No I/O processing: invalid configuration 0x0020 – No I/O processing: fault rate exceeded 0x0040/ 0x0080 – No I/O processing: configured module not plugged in
Module SRS	UDINT	R	Slot number (System.Rack.Slot)
Module Type	UINT	R	Type of module, setpoint: 0x00A5 [165_{dec}]

[1)] SC/OC (SC = short-circuit, OC = open-circuit)

Table 25: System Parameter for Digital Inputs, **Module** Tab

4.3.4.2 Tab **DI 20: Channels**

The **DI 20: Channels** tab contains the following system parameters.

<table>
<tr><th>System parameters</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Channel no.</td><td>---</td><td>R</td><td>Channel number, preset and not changeable</td></tr>
<tr><td>-> Error Code [BYTE]</td><td>BYTE</td><td>R</td><td>Error codes for the digital input channels
<table>
<tr><th>Coding</th><th>Description</th></tr>
<tr><td>0x01</td><td>Fault in the analog input module</td></tr>
<tr><td>0x10</td><td>Short-circuit of the channel</td></tr>
<tr><td>0x80</td><td>Intermittence between pulsed output DO and digital input DI, for instance:
▪ Open-circuit
▪ Open switch
▪ L+ undervoltage</td></tr>
<tr><td>0x90</td><td>Cross-circuit</td></tr>
</table></td></tr>
<tr><td>-> Value [BOOL]</td><td>BOOL</td><td>R</td><td>Input values for the digital input channels
0 = input de-energized
1 = input energized</td></tr>
<tr><td>Pulsed Output [USINT] -></td><td>USINT</td><td>W</td><td>Source channel for pulsed supply
<table>
<tr><th>Coding</th><th>Description</th></tr>
<tr><td>0</td><td>Input channel</td></tr>
<tr><td>1</td><td>Pulse of the 1st DO channel</td></tr>
<tr><td>2</td><td>Pulse of the 2nd DO channel</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>8</td><td>Pulse of the 8th DO channel</td></tr>
</table></td></tr>
</table>

Table 26: System Parameters for Digital Inputs, **DI 20: Channels** Tab

4.3.5 Digital Outputs for F30

The following tables present the statuses and parameters for the output module (DO 8) in the same order given in the SILworX Hardware Editor.

4.3.5.1 Tab **Module**

The **Module** tab contains the following system parameters:

System parameters	Data type	R/W	Description
DO.Error Code	WORD	R	Error codes for all digital outputs Coding: Description 0x0001: Fault within the digital outputs 0x0002: Test of safety shutdown returns a fault [1)] 0x0004: Test of auxiliary voltage returns a fault [1)] 0x0008: Test of test pattern faulty. 0x0010: Test of output switch test pattern faulty [1)] 0x0020: Test of output switch test pattern (shutdown test of the outputs) faulty [1)] 0x0040: Test: Active shutdown via WD faulty [1)] 0x0200: All outputs switched off, total current exceeded 0x0400: Test: 1st temperature threshold exceeded 0x0800: Test: 2nd temperature threshold exceeded 0x1000: Test: Monitoring of auxiliary voltage 1: Undervoltage
Module Error Code	WORD	R	Module error code. Coding: Description 0x0000: I/O processing, if required with errors See other error codes 0x0001: No I/O processing (CPU not in RUN) 0x0002: No I/O processing during the booting test 0x0004: Manufacturer interface operating 0x0010: No I/O processing: invalid configuration 0x0020: No I/O processing: fault rate exceeded 0x0040/ 0x0080: No I/O processing: configured module not plugged in
Module SRS	UDINT	R	Slot number (System.Rack.Slot)
Module Type	UINT	R	Type of module, setpoint: 0x00B4 [180_{dec}]
[1)] If the error or fault is present for longer than 24 h, the safety-related reaction is triggered			

Table 27: System Parameter for Digital Outputs, **Module** Tab

4.3.5.2 Tab **DO 8: Channels**

The **DO 8: Channels** tab contains the following system parameters.

System parameters	Data type	R/W	Description
Channel no.	---	R	Channel number, preset and not changeable
-> Error Code [BYTE]	BYTE	R	Error codes for the digital output channels Coding: 0x01 – Fault in the digital output module 0x02 – Channel shutdown due to overload 0x04 – Error while reading back the digital outputs 0x08 – Error while reading back the status of the digital outputs
Value [BOOL] ->	BOOL	W	Output value for DO channels: 1 = output energized 0 = output de-energized **Pulsed outputs must not be used as safety-related outputs!**

Table 28: System Parameters for Digital Outputs, **DO 8: Channels** Tab

5 Operation

The controller F30 is ready for operation. No specific monitoring is required for the controller.

5.1 Handling

Handling of the controller during operation is not required.

5.2 Diagnosis

A first diagnosis results from evaluating the LEDs, see Chapter 3.4.1.

The device diagnostic history can also be read using SILworX.

6 Maintenance

No maintenance measures are required during normal operation.

If a failure occurs, the defective module or device must be replaced with a module or device of the same type or with a replacement model approved by HIMA.

Only the manufacturer is authorized to repair the device or module.

6.1 Faults

Refer to Chapter 3.1.1.1, for more information on the fault reaction of digital inputs.

Refer to Chapter 3.1.2.1, for more information on the fault reaction of digital outputs.

If the test harness detects safety-critical faults, the module enters the STOP_INVALID state and will remain in this state. This means that the input signals are no longer processed by the device and the outputs switch to the de-energized, safe state. The evaluation of diagnostics provides information on the fault cause.

6.2 Maintenance Measures

The following measures are required for the device:

- Loading the operating system, if a new version is required.
- Performing the proof test.

6.2.1 Loading the Operating System

HIMA is continuously improving the operating system of the devices.

HIMA recommends using system downtimes to load a current version of the operating system into the devices.

Refer to the release list to check the impact of the new operation system version on the system!

The operating system is loaded using the programming tool.

Prior to loading the operating system, the device must be in STOP (displayed in the programming tool). Otherwise, stop the device.

Refer to the system manual (HI 800 141 E) for further details on how to load the operating systems.

6.2.2 Proof Test

HIMatrix devices and modules must be subject to a proof test in intervals of 10 years. For more information, refer to the safety manual (HI 800 023 E).

7 Decommissioning

Remove the supply voltage to decommission the device. Afterwards pull out the pluggable screw terminal connector blocks for inputs and outputs and the Ethernet cables.

8 Transport

To avoid mechanical damage, the components must be transported in packaging.

Always store the components in their original product packaging. This packaging also provides protection against electrostatic discharge (ESD). Notice that the product packaging alone is not suitable for transport.

9 Disposal

Industrial customers are responsible for correctly disposing of decommissioned hardware. Upon request, a disposal agreement can be arranged with HIMA.

All materials must be disposed of in an ecologically sound manner.

Appendix

Glossary

Term	Description
AI	Analog input
AO	Analog output
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CRC	Cyclic redundancy check
DI	Digital input
DO	Digital output
EMC	Electromagnetic compatibility
EN	European norm
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
HW	Hardware
ICMP	Internet control message protocol, network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Inputs are designed for interference-free operation and can be used in circuits with safety functions
MAC	Media access control address, hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX
PE	Protective earth
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)
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

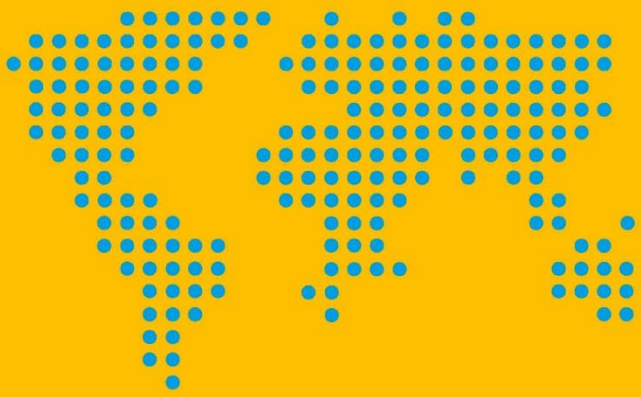
Index

HI 800 473 E

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

SAFETY
NONSTOP

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



HIMA

SMART SAFETY.

Manual

HIMatrix®F

Safety Manual

Railway Applications

Contact

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 800 436 D, Rev. 5.02 (2050)	German original document
HI 800 437 E, Rev. 5.02.00 (2050)	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 HIMatrix in the intended manner.

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

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

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

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

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

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

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

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

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

1.1 Validity and Current Version

This safety manual was created for the following versions:

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

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

1.2 Target Audience

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

1.3 Writing Conventions

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

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 specially marked. In the electronic document (PDF): When the mouse pointer hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are specially marked.

1.3.1 Safety Notices

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

The safety notices are represented as described below.

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

The signal words have the following meanings:

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

⚠ SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

NOTICE

Type and source of damage!

Damage prevention.

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

i The text giving additional information is located here.

Useful tips and tricks appear as follows:

TIP The tip text is located here.

1.4 Safety Lifecycle Services

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

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

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

Safety Lifecycle Services:	
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 HIMatrix System

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

2.1 Intended Use

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

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

The safety-related HIMatrix system can be used up to safety integrity level SIL 4 in accordance with EN 50126-1, EN 50128 and EN 50129.

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

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

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

Thus, if faults occur, the de-energized state is adopted as the safe state for inputs and outputs.

2.1.2 Application in Accordance with the Energize to Trip Principle

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

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

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

2.2 Non-Intended Use

The transfer of safety-relevant data through public networks like the Internet is permitted if additional security measures such as VPN tunnel or firewall have been implemented to increase security.

No safety-related communication can be ensured with fieldbus interfaces.

2.3 Tasks of Operators and Machine and System Manufacturers

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

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

2.3.1 Connecting to Communication Partners

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

2.3.2 Implementing Safety-Related Communications

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

The calculation basis provided in Chapter 9 and in the communication manual (HI 801 101 E) must be applied.

2.4 ESD Protective Measures

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

NOTICE

Damage to the HIMatrix system due to electrostatic discharge!

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

2.5 Additional System Documentation

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

Name	Content	Document no.
HIMatrix safety manual	Safety functions of the HIMatrix system.	HI 800 023 E
HIMatrix system manual	Hardware description of the system	HI 800 141 E
HIMatrix F60 system manual	Hardware description of the modular F60 system	HI 800 191 E
Certificates	Test results	
Revision list	Operating system versions certified by the TÜV	
Component-specific manuals	Description of the individual components	
Maintenance manual	Description of significant operational and maintenance actions.	HI 800 673 E
Communication manual	Description of safe**ethernet** communication and of the available protocols.	HI 801 101 E
Automation security manual	Description of automation security aspects related to the HIMA systems.	HI 801 373 E
SILworX first steps manual	Introduction to the use of SILworX for engineering, start-up, testing and operation.	HI 801 103 E
SILworX online help (OLH)	Instructions on how to use SILworX	

Table 1: Overview of the System Documentation

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

2.6 Mean Technical Delay for the Modules

For the HIMatrix modules described in this manual, the time for starting repair after a detected first fault can be delayed by a maximum of 64 hours.

Assuming that repair is successful within 8 hours, 72 hours instead of 8 hours are thus available for the whole restoration process.

With respect to the remote I/O F3 DIO 16/8 01(4), this applies to the inputs and to the outputs, only if these are operated in 2-pole mode (DOn+ and DOn-).

The calculated functional failure rates (FFR) specified in the corresponding HIMatrix manual (HI 800 429 E) remain valid.

3 Safety Concept

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

- Safety and availability.
- Safety-relevant time parameters.
- Safety requirements.
- Automation security.
- Additional test conditions for railway applications

3.1 Safety and Availability

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

The safety-related HIMatrix system can be used up to safety integrity level SIL 4 in accordance with EN 50126-1, EN 50128 and EN 50129.

No imminent risk results from the HIMatrix automation systems.

⚠ WARNING

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

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

3.1.1 Calculating the FFR Values

The FFR values for the HIMatrix system have been calculated in accordance with IEC 61508.

The functional failure rate (FFR) values are provided by HIMA upon request.

Within the scope of the update to the EN 50129:2018 + AC:2019 standard, the term used to designate the HR (Hazard Rate) changed to FFR (Functional Failure Rate). The calculation principles have not changed.

The safety functions, consisting of a safety-related loop (input, processing unit, output and safety communication among HIMA systems), meet the requirements described above in all combinations. The controllers, remote I/Os and F60 modules meet these requirements.

3.1.2 Self-Test and Fault Diagnostics

The controllers' operating system executes extensive self-tests at start-up and during operation.

The scope of the testing includes:

- Processors.
- Memory areas (RAM, NVRAM).
- The watchdog.
- Individual I/O channels.
- The power supply.
- If faults are detected during the tests, the operating system switches off the defective controller, module, remote I/O or the faulty I/O channel.
- In non-redundant systems, this means that sub-functions or even the entire PES may be shut down.

All HIMatrix controllers, remote I/Os and modules are equipped with LEDs to indicate that faults have been detected. This allows the user to quickly diagnose faults detected in a device or the external wiring.

Additionally, the user program can evaluate various system variables displaying the device status, e.g., the temperature range.

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

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

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

3.1.3 PADT

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

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

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

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

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

3.1.4.1 Detection of Failed System Components

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

3.1.4.2 Safety Function in Accordance with the Energize to Trip Principle

The safety function is performed when the safety system energizes one or several actuators, thus ensuring that the safe state is adopted.

The users must plan the following actions:

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

3.2 Safety-Relevant Time Parameters

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

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

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

3.2.1 Process Safety Time

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

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

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

3.2.2 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:

$\mathbf{t}_{RR}$ **≤** $\mathbf{t}_{SR}$

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

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

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

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

3.2.3 Watchdog Time (of the Resource)

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

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

Requirement for safety:

$t_{WD} \leq$ ½ x t_{SR}

t_{WD} Watchdog time (of the resource)

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

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

The PADT checks the parameters *Safety Time [ms]* and *Watchdog Time [ms]* and rejects the configuration while generating it if the watchdog time is set to a value greater than ½ 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!

i Determine the safety time and the watchdog time for the system to be controlled.

3.2.4 Estimating the Watchdog Time

HIMA strongly recommends the following setting to ensure sufficient availability:

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

3.2.5 Determining the Watchdog Time through Testing

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

Test requirements:

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

To determine the minimum value for the watchdog time

1. Operate the system under full load. Communication should also run under full load.
2. Specify input data to preferably pass through the longest program paths. To this end, input value sequences may be necessary.
3. Reset the cycle time statistics in the Control Panel.
4. Perform the reload multiple times, if required by the application.
5. In the Control Panel, observe the maximum cycle time values.
   ☑ $\mathbf{t}_{Cycle}$ is identified.
6. Determine the maximum deviation between the user program's total execution time and the average total execution time.
   ☑ $\Delta\mathbf{t}_{Peak}$ is identified.
7. Calculate the minimum watchdog time $\mathbf{t}_{WD}$ using:

$\mathbf{t}_{WD} = \mathbf{t}_{Cycle} + \mathbf{t}_{Res} + \mathbf{t}_{Com} + \mathbf{t}_{Config} + \Delta\mathbf{t}_{Peak}$, where

$\mathbf{t}_{Cycle}$	Observed maximum cycle time (basic load, already includes portions of $\mathbf{t}_{Com}$ and $\mathbf{t}_{Config}$)
$t_{Reserve}$	Safety margin 6 ms.
t_{Com}	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}) less observed basic load, see step 6.

► The value set for the watchdog time should be: determined minimum value $\mathbf{t}_{WD}$ + margin for future changes or extensions.

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

In the following cases, contact HIMA technical support:

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

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

3.2.6 Response Time

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

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

3.3 Safety Requirements

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

3.3.1 Product-Independent Hardware Requirements

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

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

3.3.2 Product-Dependent Hardware Requirements

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

- Only devices that are safely separated from the power supply may be connected to the system.
- The safe, electrically protective separation of the power supply must be guaranteed within the 24 V system supply. Only power supply units ensuring that the controllers and remote I/O modules are supplied with 24 V low voltage may be used.
- To comply with the protective provisions for electrical safety and grounding, the manufacturer of the specific application must ensure that proper measures are implemented for separating the indoor and outdoor equipment in accordance with EN 50122. This shall protect the HIMatrix systems against influences from the outdoor equipment in the overhead contact line zone or the pantograph zone, as well as against traction return currents. Power supply devices allowed for railway applications must be used.

3.3.3 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.

3.3.4 Product-Dependent Programming Requirements

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

- Compiling the program twice in SILworX and comparing the two CRCs ensures ensures that the program was properly compiled.
- 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.
- The system response to faults in fail-safe inputs and outputs must be defined in the user program in accordance with the system-specific safety-related conditions.
- The SILworX programming tool is provided with a feature that, after the user program or system configuration has changed, only displays the performed changes. The analysis of the changes (change impact analysis IA) must define the required test scope. This impact analysis must take the expected changes based on the performed modifications, the result of the SILworX comparison feature and the required regression tests into account.

3.3.5 Communication

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

- When implementing safety-related communications between various HIMA systems, ensure that the overall response time of a system does not exceed the worst case response time. All calculations must be performed in accordance with the rules given in Chapter 9.2.
- Data transmission in Category 1 and Category 2 transmission systems in accordance with EN 50159 is possible with no additional measures.
- Transmission systems (Category 3) in accordance with EN 50159 may be used, if additional measures are taken to guarantee that the transmission channel is secure (e.g., firewalls or encryption).
- At this stage, the serial interfaces may only be used for non-safety-related purposes.
- Only devices with electrically protective separation may be connected to the communication interfaces.

3.3.6 Requirements for Railway Applications

The following requirements must be observed when using the HIMatrix system in railway applications:

- The standard variants of the HIMatrix system family as specified in Table 4, can be used in containers or in buildings with controlled temperature and air humidity.
- The standard variants of the HIMatrix system family are not approved for use on railway vehicles.
- The HIMatrix variants for railway applications (see Table 3) can be used and operated in environments with pollution degree 2 and overvoltage category 2 in accordance with EN 50124-1.
- The relevant standards must be used for railway applications.
- The digital outputs are equipped with line short-circuit monitoring. Responses to detected short-circuits must be programmed in the user program.
- The users must ensure that the specified temperature ranges are maintained at the installation site. For example, the ambient temperature at the installation site can be recorded either by separate temperature sensors or by the sensors integrated in the HIMatrix systems. Based on this, appropriate measures can be taken.

  For further details on the temperature status' monitoring in HIMatrix systems, refer to the HIMatrix system manual (HI 800 141 E).
- For remote I/Os and modules with relay outputs, the maximum number of switching operations must be monitored by implementing suitable methods and measures, e.g., a counter for recording switching operations in the user program. If the maximum number of switching operations is exceeded, the remote I/O or the module must be replaced.
- Each safe**ethernet** connection is has its own error counter. The error counters can be monitored online in the Control Panel or can be evaluated in the user program.
- Error messages must be evaluated in the user program. Errors are signaled by state bits and are thus available to the user program. Additionally, errors are stored in the diagnostic memory of the controller and can be evaluated using the programming tool. For further details, refer to the HIMatrix system manual (HI 800 141 E).
- Detection of ground faults must be configured externally.

3.4 Automation Security

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

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

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

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

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

3.4.1 Product Properties

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

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

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

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

⚠ WARNING

Physical injury possible due to unauthorized manipulation of the controllers!

Protect the controllers against unauthorized access!!

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

3.4.2 Risk Analysis and Planning

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

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

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

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

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

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

3.5 Test Conditions

Refer to the HIMatrix safety manual (HI 800 023 E) for the standards used to test and certify the HIMatrix system for industrial use.

3.6 Additional Test Conditions for Railway Applications

The following tables show the HIMatrix components that are approved for railway applications:

Compact controllers
F30 03
F35 03
Remote I/Os
F1 DI 16 01
F2 DO 4 01
F2 DO 8 01
F2 DO 16 01
F2 DO 16 02
F3 AIO 8/4 01
F3 DIO 8/8 01
F3 DIO 16/8 01
F3 DIO 20/8 02
Modular F60 System
AI 8 01
CIO 2/4 01
CPU 03
DI 32 01
DIO 24/16 01
DO 8 01
GEH 01
MI 24 01
PS 01

Table 2: HIMatrix Standard Variants

All the HIMatrix standard variants listed in Table 2 are only approved for use as equipment for signaling and telecommunications in accordance with EN 50125-3.

Compact controllers
F30 034
F35 034
Remote I/Os
F1 DI 16 014
F2 DO 8 014
F2 DO 16 014
F3 AIO 8/4 014
F3 DIO 8/8 014
F3 DIO 16/8 014
F3 DIO 20/8 024
Modular F60 System
AI 8 014
CIO 2/4 014
CPU 034
DI 32 014
DIO 24/16 014
GEH 014
MI 24 014
PS 014

Table 3: HIMatrix Variants for Railway Applications

All the HIMatrix components listed in Table 3 are approved for use on railway vehicles in accordance with EN 61373, Category 1, Class B, and, as equipment for signaling and telecommunications in accordance with EN 50125-3, for the position outside the track (1…3 m from the rail). These variants of the standard components are identified by the suffix 4 in the type designation.

The HIMatrix components have been additionally developed to meet the following EMC, climatic and environmental conditions:

3.6.1 Altitude Range

The following classes in the specified altitude range apply to the HIMatrix components:

- For use in signaling applications in accordance with EN 50125-3: AX up to 2000 m.

The following classes in the specified altitude range apply to the HIMatrix components that are specified in Table 3:

- For use in signaling applications in accordance with EN 50125-3: AX up to 2000 m.
- For use on railway vehicles in accordance with EN 50125-1: AX up to 2000 m.

3.6.2 Climatic Conditions

All HIMatrix standard variants are designed and tested for a temperature range of 0…60 °C and a relative air humidity of 10…95 % (non-condensing). The following temperature classes result for railway applications in accordance with EN 50125-3:

HIMatrix	In external ambient	In control cabinet	In container		In building	
			N.T.C	T.C	N.C.C.	C.C
Standard	-	-	-	T1, T2, TX	-	T1, T2, TX

Table 4: HIMatrix Temperature Classes of the Standard Variants in Accordance with EN 50125-3

The standard variants of the HIMatrix system family as specified in Table 4, can be used in containers or in buildings with controlled temperature and air humidity.

NOTICE

The standard variants of the HIMatrix system family are not approved for use on railway vehicles in accordance with EN 50155.

3.6.2.1 Use in Signaling Applications

The HIMatrix variants for railway applications are designed for a temperature range of -25…+70 °C. All the HIMatrix variants for railway applications were tested in accordance with EN 50125-3 and can be used in the following temperature classes:

HIMatrix	In external ambient	In control cabinet	In container		In building	
			N.T.C	T.C	N.C.C.	C.C
F30 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F35 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F1 DI 16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F2 DO 16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 AIO 8/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 8/8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 16/8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
F3 DIO 20/8 024	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
PS 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
CPU 034	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
AI 8 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
CIO 2/4 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
DI 32 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
DIO 24/16 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX
MI 24 014	T1	T1	T1, T2	T1, T2, TX	T1, T2, TX	T1, T2, TX

Table 5: Temperature Classes in Accordance with EN 50125-3

3.6.2.2 Use on Railway Vehicles

All the HIMatrix variants for railway applications were tested in accordance with EN 50155 and can be used in the following temperature classes:

HIMatrix	Temperature classes
F30 034	OT3
F35 034	OT3
F1 DI 16 014	OT3
F2 DO 8 014	OT3
F2 DO 16 014	OT3
F3 AIO 8/4 014	OT3
F3 DIO 8/8 014	OT3
F3 DIO 16/8 014	OT3
F3 DIO 20/8 024	OT3
PS 014	OT3
CPU 034	OT3
AI 8 014	OT3
CIO 2/4 014	OT3
DI 32 014	OT3
DIO 24/16 014	OT3
MI 24 014	OT3

Table 6: Temperature Classes in Accordance with EN 50155

As for the extended operating temperature when powering on, class ST0 applies to the HIMatrix system family, as defined in EN 50155, Chapter 4.3.3.

With respect to fast temperature change, temperature class H1 applies, as defined in EN 50155, Chapter 4.3.4.

Since the PCB in the components of the HIMatrix system family are provided with a protective coating, they achieve the protective coating class PC2, as defined in EN 50155, Chapter 10.7.

3.6.2.3 Derating of Digital Outputs

With an operating temperature higher than 60 °C the load of the digital outputs must be derated. In this case, each output can be loaded with a maximum of 0.5 A, see the manuals of the components.

3.6.3 Mechanical Conditions

The HIMatrix components were tested in accordance with EN 50125-3 and EN 50155.

3.6.3.1 Use in Signaling Applications

All HIMatrix components were mechanically tested in accordance with EN 50125-3 for the position "from 1 m to 3 m from the rail". The following table lists the most important tests and limits for mechanical conditions:

EN 50125-3	Mechanical Tests
	Vibration immunity test: 2.3 m/s^2 between 5…2000 Hz, EUT in operation
	Shock immunity test: 20 m/s^2, 11 ms, EUT in operation

Table 7: Mechanical Conditions for Use in Signaling Applications

3.6.3.2 Use on Railway Vehicles

The components listed in Table 3 were mechanically tested in accordance with EN 50155. Testing was performed in accordance with EN 61373, Category 1, Class B.

The HIMatrix system family has no sockets for integrated circuits and/or edge connectors, which is why class K2 is complied with, as defined in EN 50155, Chapter 10.1.5.

3.6.4 EMC Conditions

The following chapters contain the tests and limit values of the EMC conditions for use in signaling technology and on railway vehicles.

3.6.4.1 Use in Signaling Applications

All HIMatrix components were successfully tested and meet the EMC conditions in accordance with EN 50121-4. The following table lists the most important tests and limits:

Test standard	Type of test	Interference immunity tests	
EN 61000-4-2	ESD test	6 kV contact discharge, 8 kV air discharge	
EN 61000-4-3	EM field	80…1000 MHz:	10 V/m
		800 … 1000 MHz:	20 V/m
		1400…2000 MHz:	10 V/m
		2000…2700 MHz:	5 V/m
		5100…6000 MHz:	3 V/m
EN 61000-4-4	Burst test	Supply voltage:	2 kV
		I/O lines:	2 kV
		Ground:	1 kV
EN 61000-4-5	Surge	Supply voltage:	2 kV CM
			1 kV DM
		I/O lines:	2 kV CM
			1 kV DM
		Shielded wires:	2 kV CM
EN 61000-4-6	Injected RF currents	Supply voltage:	10 V
		I/O lines:	10 V
		Ground:	10 V
EN 61000-4-8	Power frequency magnetic field	16 2/3 Hz, 50 Hz, 60 Hz:	100 A/m
		DC:	300 A/m

Table 8: EMC Conditions for Use in Signaling Applications in Accordance with EN 50121-4

Remarks to Surge with 2 kV (CM) / 1 kV (DM):

The following notes apply to the standard variants and the variants for railway applications, even if these are not explicitly mentioned.

The external H 7013 filter from HIMA is absolutely required if HIMatrix compact systems are used to act against the DC supply voltage surge. The supply voltage of the HIMatrix F35 03 must not be provided from outside, but must be generated within the same control cabinet.

i In the following cases, external surge filters are to be used in the F1 DI 01(4), F3 DIO 20/8 02(4), F30 03(4), F60 DIO 24/16 01(4) and F60 DI 32 01(4) for all unshielded input and output lines:

- Equipment within the 3-meter range.
- Connection to equipment within the 10-meter range with connection within the 3-meter range.
- Connection to equipment within the 10-meter range with lines that are longer than 30 m.

3.6.4.2 Use on Railway Vehicles

The HIMax components specified in Table 3 were successfully tested and met the EMC conditions in accordance with EN 50121-4 and EN 50121-3-2. The following table lists the most important tests and limits:

Test standard	Type of test	Interference immunity tests	
EN 61000-4-2	ESD test	6 kV contact discharge, 8 kV air discharge	
EN 61000-4-3	EM field	80…1000 MHz:	20 V/m
		1400…2000 MHz:	10 V/m
		2000…2700 MHz:	5 V/m
		5100…6000 MHz:	3 V/m
EN 61000-4-4	Burst test	Supply voltage:	2 kV
		I/O lines:	2 kV
EN 61000-4-5	Surge	Supply voltage:	2 kV CM
			1 kV DM
EN 61000-4-6	Injected RF currents	Supply voltage:	10 V
		I/O lines:	10 V

Table 9: EMC Conditions for Use on Railway Vehicles in Accordance with EN 50121-3-2

Remarks to Surge with 2 kV (CM) / 1 kV (DM):

The external H 7013 filter from HIMA is absolutely required if HIMatrix compact systems are used to act against the DC supply voltage surge. The supply voltage of the HIMatrix F35 034 must not be provided from outside, but must be generated within the same control cabinet.

Surge absorbers from other manufacturers may be used, if the specifications provided in the data sheets are equivalent or better.

3.6.5 Severe Conditions

The HIMatrix system must be installed in enclosures with suitable degree of protection (e.g., IP54) to ensure protection against the environmental influences as of classes 4C3, 4B1 and 4S2.

3.6.6 Supply Voltage

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

IEC/EN 61131-2	Verification of the DC supply characteristics
	Voltage range test: 24 VDC, -15…+20 %, $r_P \leq 5$ %
	Momentary external current interruption immunity test: DC, PS 2: 10 ms
	Reversal of DC power supply polarity test: Tested for 10 s

Table 10: Supply Voltage Failures Immunity Test

3.6.6.1 Supply Voltage Requirements for Use on Railway Vehicles

The HIMatrix systems are supplied from an accumulator battery with 24 V nominal voltage.

The following values apply to the HIMatrix supply voltage: 24 VDC, -15…+20 %, 5 % ripple.

This results in the following tolerance values:

- Minimum continuous voltage: 19.2 V (0.8 U_N)
- Maximum continuous voltage: 30 V (1.25 U_N)

The HIMatrix variants specified in Table 2 were tested in accordance with EN 50155, Chapter 5.1.

Taking external measures, users must ensure that the minimum continuous voltage of 0.8 U_N is maintained, since otherwise individual devices or the entire system will reboot.

Taking external measures, the user must be able to intercept voltage fluctuations above 1.25 U_N in accordance with EN 50155, Chapter 5.1.1.3.

HIMatrix systems are designed for voltage dropouts of up to 20 ms. As such, the HIMatrix meets the requirements of Class S3 in accordance with EN 50155, Chapter 5.1.1.4.

The HIMatrix system meets the requirements for DC voltage ripple factor in accordance with EN 50155, Chapter 5.1.1.6.

The requirements in accordance with EN 50155, Chapter 5.1.3, for switching two supply voltages are not met. External measures must be implemented by the user.

4 Central Functions

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

The controllers of type F60 are modular systems. In addition to a processor module and a power supply module, one controller of this type may include up to 6 I/O modules.

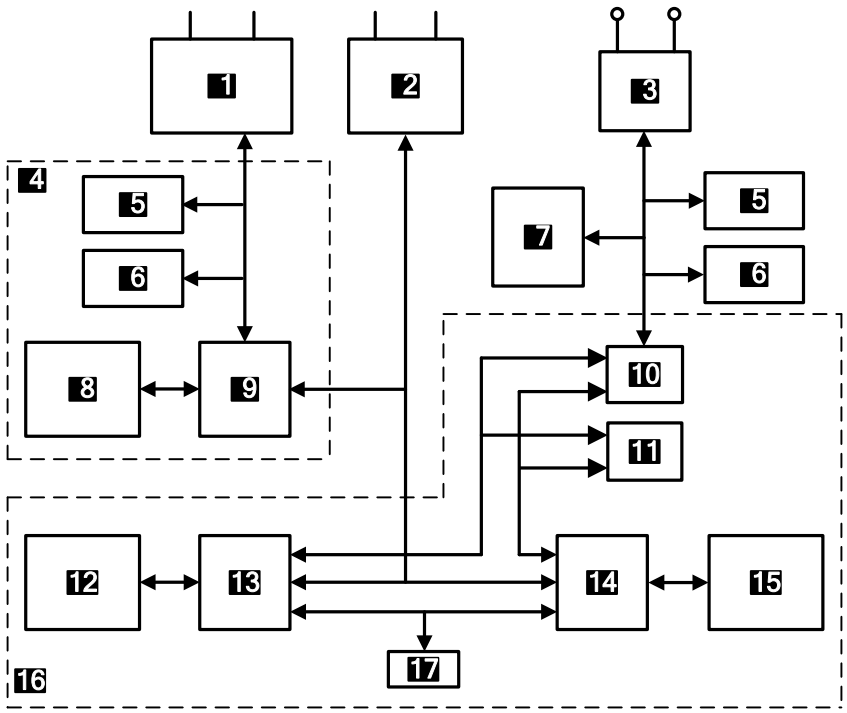
4.1 Power Supply Units

The HIMatrix systems must be supplied by power supply units ensuring a 24 V low voltage to the controllers and remote I/Os.

Observing the permitted voltage limits guarantees the controller's proper operation.

4.2 Functional Description of the Processor System

The processor system is the central component of the controller. The following figure shows the block diagram of the processor system based on the example of the CPU 03 in the F60 modular system:



1 Fieldbus interfaces
2 Ethernet interfaces
3 I/O bus submodule
4 Communication system
5 NVSRAM
6 Flash
7 V_{CC} and temperature monitoring
8 SDRAM of the communication system
9 Processor of the communication system
10 Comparator
11 Watchdog
12 SDRAM 1 of the processor system
13 Processor 1 of the processor system
14 Processor 2 of the processor system
15 SDRAM 2 of the processor system
16 Safety-related processor system
17 Real time clock

Figure 1: CPU 03 Block Diagram

Characteristics of the Processor System

- 1oo2 processor system.
- 2 synchronous microprocessors with 1 SDRAM each
- Testable hardware comparators for all external accesses of both microprocessors.
- In the event of an error, the watchdog is set to the safe state.
- Flash as the program memory for operating systems and user programs, suitable for at least 100 000 memory cycles.
- Data memory in NVSRAM.
- Gold capacitor for buffering date/time.
- Communication processor for fieldbus and Ethernet connections.
- Interface for exchanging data between devices, F60 controllers and the PADT, based on Ethernet.
- Optional interface(s) for data exchange via fieldbus.
- LEDs for indicating the system states.
- I/O bus logic for connection to I/O modules.
- Safe watchdog (WD).
- Monitoring of power supply units, testable (1.8 VDC / 3.3 VDC).
- Temperature monitoring.

4.3 Self-Tests

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

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

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

4.3.1 Microprocessor Test

The following is tested:

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

4.3.2 Memory Areas Test

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

4.3.3 Protected Memory Areas

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

4.3.4 RAM Test

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

4.3.5 Watchdog Test

The watchdog signal is switched off if it is not triggered by both CPUs within a defined time window and if the hardware comparator test fails. An additional test determines the switch-off ability of the watchdog signal.

4.3.6 Testing the I/O Bus Within the Controller

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

4.4 Responses to Faults in the Processor System

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

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

4.5 Fault Diagnostics

Each F60 module has an own LED for reporting module malfunctions or faults in the external wiring. This allows the user to quickly diagnose faults detected in a module.

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

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

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

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

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

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

5 Inputs

The notes in this chapter apply to the standard variants and the variants for railway applications, even if these are not explicitly mentioned.

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

Component	Type	Number	Safety-related	Interference-free	Galvanically separated
Compact systems					
F30 03	Digital	20	•	•	– [1]
F35 03	Digital	24	•	•	– [1]
	24-bit counter	2	•	•	– [1]
	Analog	8	•	•	– [1]
F1 DI 16 01	Digital	16	•	•	– [1]
F3 DIO 8/8 01	Digital	8	•	•	– [1]
F3 DIO 16/8 01	Digital	16	•	•	– [1]
F3 AIO 8/4 01	Analog	8	•	•	– [1]
F3 DIO 20/8 02	Digital	20	•	•	– [1]
Modulares System F60					
DIO 24/16 01	Digital	24	•	•	•
DI 32 01 (configurable for line control)	Digital	32	•	•	•
CIO 2/4 01	24-bit counter	2	•	•	•
AI 8 01	Analog	8	•	•	•
MI 24 01	Analog or digital	24	•	•	•

[1] Reference potential: L-

Table 11: Overview of the HIMatrix System Inputs

5.1 General Information

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

The controllers provide status and fault information as follows:

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

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

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

5.2 Response in the Event of a Fault

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

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

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

5.3 Safety of Sensors, Encoders and Transmitters

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

5.4 Safety-Related Digital Inputs

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

5.4.1 General Information

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

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

5.4.2 Test Routines

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

5.4.3 Surges on Digital Inputs

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

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

- 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. This measure increases the maximum response time!

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 HIMatrix system manual (HI 800 141 E).

5.4.4 Configurable Digital Inputs

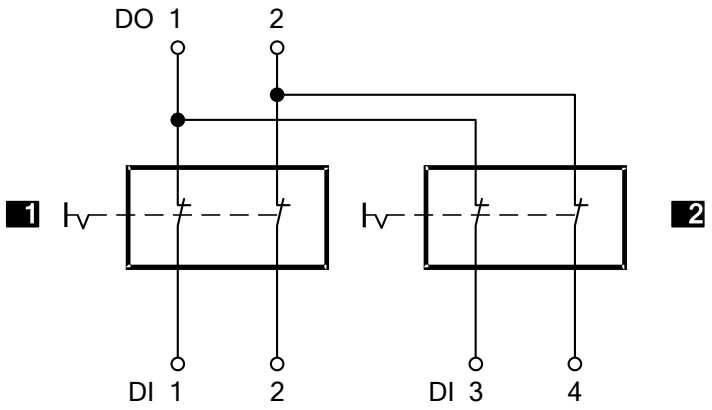
The digital inputs of the F35 03 controller and the MI 24 01 module operate as analog inputs, but return digital values due to the configuration of switching thresholds.

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

5.4.5 Line Control

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

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

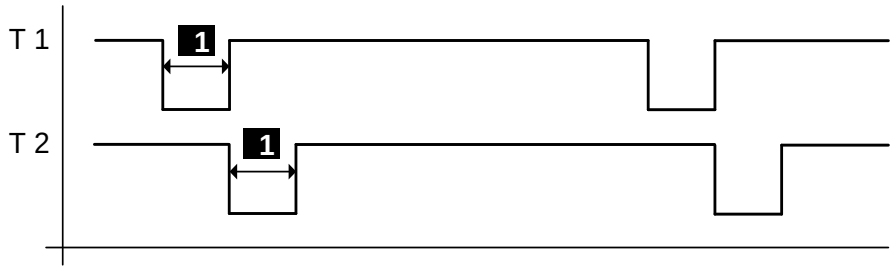


1 Emergency stop 1
2 Emergency stop 2

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

Figure 2: Line Control

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



1 Configurable 5…2000 µs

Figure 3: Pulsed Signals T1, T2

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

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

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

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

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

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

F35 03 Controller

Input channels	Measurement procedure	Current, voltage	Range of values in the application	
			FS1000 [1]	FS2000 [1]
8	Unipolar	0…+10 V	0…1000	0…2000
8	Unipolar	0…20 mA	0…500 [2] 0…1000 [3]	0…1000 [2] 0…2000 [3]

[1] Configurable by selecting the type in the PADT.

[2] With external 250 Ω shunt adapter.

[3] With external 500 Ω shunt adapter.

Table 12: Analog Inputs of the F35 03 Controller

F3 AIO 8/4 01 Remote I/O

Input channels	Measurement procedure	Current, voltage	Range of values in the application
8	Unipolar	0…+10 V	0…2000
8	Unipolar	0/4…20 mA	0…1000 [1] 0…2000 [2]

[1] With external 250 Ω shunt adapter.

[2] With external 500 Ω shunt adapter.

Table 13: Analog Inputs of the F3 AIO 8/4 01 Remote I/O

F60 Modules

Input channels	Measurement procedure	Current, voltage	Range of values in the application	
			FS1000 [1]	FS2000 [1]
AI 8 01				
8	Unipolar	-10…+10 V	-1000…1000	-2000…2000
8	Unipolar	0…20 mA	0…1000 [3]	0…2000 [3]
8	Unipolar	0…20 mA	0…500 [2]	0…1000 [2]
4	Bipolar	-10…+10 V	-1000…1000	-2000…2000
MI 24 01				
24	Unipolar	0…20 mA	0…2000 [4]	

[1] Configurable by selecting the type in the PADT (F60).

[2] With external 250 Ω shunt.

[3] With external 500 Ω shunt (accuracy 0.05 % 1 W). No longer available at HIMA.

[4] Internal shunts.

Table 14: Analog Inputs of the F60 Controller

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

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

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

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

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

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

5.5.1 Test Routines

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

5.6 Safety-Related Counters (F35 03 and F60)

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

5.6.1 General Information

A counter channel can be configured for operation as a high-speed up or down counter with 24-bit resolution or as a decoder in Gray code.

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

The counter encoders have the following resolutions:

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

A reset is possible.

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

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

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

5.7 Checklists for Inputs

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

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

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

6 Outputs

The notes in this chapter apply to the standard variants and the variants for railway applications, even if these are not explicitly mentioned.

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

Component	Type	Number	Safety-related	Galvanically separated
Compact systems				
F30 03 (configurable for line control)	Digital	8	•	–[1]
F35 03	Digital	8	•	–[1]
F1 DI 16 01	Pulse	4	-	–[1]
F2 DO 4 01 [2]	Digital	4	•	–[1]
F2 DO 8 01	Relay	8	•	•
F2 DO 16 01	Digital	16	•	–[1]
F2 DO 16 02 [2]	Relay	16	•	•
F3 DIO 8/8 01	Digital 1-pole	8	•	–[1]
	Digital 2-pole	2		
F3 DIO 16/8 01	Digital 1-pole	16	•	–[1]
	Digital 2-pole	8		
F3 AIO 8/4 01	Analog	4	-	–[1]
F3 DIO 20/8 02 (configurable for line control)	Digital	8	•	–[1]
Modular F60 System				
DIO 24/16 01 (configurable for line control)	Digital	16	•	
DO 8 01 (250 V) [2]	Relay	8	•	•
CIO 2/4 01	Digital	4	•	

[1] Reference potential L-.

[2] Only available as standard variant.

Table 15: Overview of the HIMatrix System Outputs

6.1 General Information

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

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

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

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

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

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

6.2 Response in the Event of a Fault

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

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

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

6.3 Safety of Actuators

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

6.4 Safety-Related Digital Outputs

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

6.4.1 Test Routines for Digital Outputs

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

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

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

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

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

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

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

6.4.3 Line Control

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

NOTICE

Malfunctions of the connected actuators are possible!

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

Relay outputs cannot be used as pulsed outputs.

6.5 Safety-Related 2-Pole Digital Outputs

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

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

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

  F3 DIO 16/8 01:
  - Short-circuit to L+, L-.
  - Short-circuit between 2-pole connections.
  - Open-circuit in one of the 2-pole connections.

  F3 DIO 8/8 01:
  - Short-circuit to L+, L-.

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

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

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

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

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

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

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

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

i Detection of open-circuits may be disturbed!

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

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

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

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

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

6.6 Relay Outputs

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

6.6.1 Test Routines for Relay Outputs

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

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

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

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

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

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

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

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

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

To achieve SIL 4, the output values must be read back via safety-related analog inputs and evaluated in the user program. Responses to faulty output values must be programmed in the user program as well.

6.7.1 Test Routines

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

6.8 Checklists for Outputs

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

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

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

7 Software

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

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

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

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

7.1 Safety-Related Aspects of Operating Systems

Each approved operating system is clearly identified by the revision number and the CRC signature. The valid versions of the operating system and corresponding signatures (CRCs) - approved by the TÜV for use in safety-related automation devices - are subject to a revision control and are documented in a version list.

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

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

7.2 Operation and Functions of Operating Systems

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

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

The following basic functions are also executed:

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

7.3 Safety-Related Aspects of Programming

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

7.3.1 Safety Concept of SILworX

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

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

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

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

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

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

7.3.2 Verifying the Configuration and the User Programs

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

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

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

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

SILworX can be used as test equipment for:

- Checking inputs.
- Forcing outputs.

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

7.3.3 Archiving a Project

HIMA recommends archiving the project after each download or reload.

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

7.3.4 Identifying Configuration and Programs

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

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

i During commissioning or after a change to the user program of a safety-related controller, a comprehensive functional test must be performed.

A project archive must be created.

7.4 Resource Parameters

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

⚠ WARNING

Physical injury possible due to invalid configuration!

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

These parameters are:

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

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

7.4.1 Resource System Parameters

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

Parameter	S [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), refer to the safety manual (HI 801 003 E). Range of values: 20…22 500 ms Default value: 600 ms for controllers, 400 ms for remote I/Os (can be changed online)	Application-specific
Watchdog Time [ms]	Y	For details on the watchdog time of the resource (in milliseconds), refer to the safety manual (HI 801 003 E). Range of values: 4…5000 ms Default value: 200 ms for controllers, 100 ms for remote I/Os (can be changed online)	Application-specific
Target Cycle Time [ms]	N	Target or maximum cycle time, see *Target Cycle Time Mode*. Range of values: 0…5000 ms Default value: 0 ms (can be changed online) The maximum target cycle time value may not exceed the configured *Watchdog Time [ms]* minus the minimum value that can be set for *Watchdog Time [ms]* (4 ms, see above); otherwise the entry is rejected. If the default value is set to 0 ms, the target cycle time is not taken into account. For further details, refer to the following chapters.	Application-specific
Target Cycle Time Mode	N	For details on the use of the *Target Cycle Time [ms],* see the following chapters. Default value: *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. Mode 2 The processor provides the execution time portion not needed by lower priority user programs to higher priority user programs. Mode of operation for high availability. Mode 3 The processor waits until the execution time not needed by the user programs has expired, thus increasing the cycle. Default value: *Mode 1*	Application-specific
Max. Com.Time Slice [ms]	N	Highest value in ms for the time slice used for communication during a resource cycle, see the communication manual (HI 801 101 E). Range of values: 2…5000 ms Default value: 60 ms	Application-specific

Parameter	S [1)]	Description	Setting for safe operation
Optimized Use of Com. Time Slice	N	The system parameter reduces the response times for communications via processor module(s). i This can affect the temporal utilization of *Max.Com. Time Slice ASYNC [ms]* and the system parameter *Max. Duration of Configuration Connections [ms]* such that these two times can be subject to more demands (e.g., during reload).	---
Max. Duration of Configuration Connections [ms]	N	This defines how much time within a CPU cycle is available for configuration connections. Range of values: 2...3500 ms Default value: 20 ms For further details, refer to the following chapters.	Application-specific
Maximum System Bus Latency [µs]	N	Not applicable for HIMatrix controllers! Default value: System Defaults	---
Allow Online Settings	Y	TRUE: **All** the switches/parameters listed under FALSE can be changed online using the PADT. This is only valid if the system variable *Read-only in RUN* has the value FALSE. Default value: TRUE.	HIMA recommends using the FALSE setting.
		FALSE: The following parameters **cannot** be changed online: ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global MultiForcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* The following parameters can be changed online if *Reload Allowed* is TRUE. ▪ *Watchdog Time (for the resource)* ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode*	
		Allow Online Settings can only be TRUE when the controller is stopped or by performing a reload.	

Parameter	S [1]	Description		Setting for safe operation
Autostart	Y	TRUE:	If the processor module is connected to the supply voltage, the user programs start automatically. Default value: TRUE.	Application-specific
		FALSE:	The user program does not start automatically after connecting the supply voltage.	
		Observe the settings in the resource program properties!		
Start Allowed	Y	TRUE:	Cold start or warm start permitted with the PADT in RUN or STOP. Default value: TRUE.	Application-specific
		FALSE:	Start not allowed.	
Load Allowed	Y	TRUE:	Configuration download is allowed. Default value: TRUE.	Application-specific
		FALSE:	Start not allowed.	
Reload Allowed	Y	TRUE:	Configuration reload is allowed. Default value: TRUE.	Application-specific
		FALSE:	Configuration reload is not allowed. A running reload process is not aborted when switching to FALSE.	
Global Forcing Allowed	Y	TRUE:	Global forcing is permitted for this resource. Default value: TRUE.	Application-specific
		FALSE:	Global forcing is not permitted for this resource.	
Global Force Timeout Reaction	N	Specifies how the resource should behave when the global force timeout has expired: ▪ *Stop Forcing Only*. ▪ *Stop Forcing and Stop Resource*. Default value: *Stop Forcing Only*.		Application-specific
Global Multi-Forcing Allowed	Y	TRUE:	Users with MultiForcing access can write force data (force values and individual force switches) for global variables in a resource if the required higher-order conditions have been met and the force permissions have been granted.	Application-specific
		FALSE:	Users with MultiForcing access cannot force global variables. Default value: FALSE (can be changed online)	
Minimum Configuration Version	N	With this setting, it is possible to generate code that is compatible with previous or newer HIMatrix operating system versions in accordance with the project requirements. The installed SILworX version is the default setting.		Application-specific
Fast Start-Up	Y	After connecting the supply voltage, the resource starts up faster, <10 s, see Chapter 7.4.1.4. Default value: FALSE.		Application-specific

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

Table 16: Resource System Parameters

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

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

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

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

Setting	Description
Fixed	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 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 difference: To ensure that the reload can be performed successfully, the target cycle time may be violated for 1 to n CPU cycles (where n is the number of changed user programs). Default value: *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.
Dynamic	The CPU processes each CPU cycle as fast as possible. This corresponds to a target cycle time of 0 ms. i A reload process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time). A maximum of every fifth cycle can be extended during the reload.
Dynamic-tolerant	Similar to *Dynamic*, but with the following difference: To ensure that the reload can be performed successfully, the target cycle time may be automatically increased for 1 to n CPU cycles (where n is the number of changed user programs). 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 process is rejected if the reserve time is not sufficient (target cycle time minus actual cycle time).

Table 17: Settings for Target Cycle Time Mode

7.4.1.2 Calculating the *Maximum Duration of Configuration Connections [ms]* T_{Config}

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

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

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

i HIMA recommends dimensioning $\mathbf{t}_{Config}$ in such a way that all tasks can be processed in a single CPU cycle.

$\mathbf{t}_{Config}$ for HIMatrix CPU operating systems is calculated as follows:

HIMatrix CPU $\mathbf{t}_{Config} = (\mathbf{n}_{Com} + \mathbf{n}_{PADT} + \mathbf{n}_{RIO}) * 0.25 \text{ ms} + 4 \text{ ms}$

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

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

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

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

For test purposes, $\mathbf{t}_{Config}$ can also be set online in the Control Panel.

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

7.4.1.3 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 safety-related SILworX version comparison can be used to determine and prove changes performed to the current project version compared to a previous one.

7.4.1.4 The Fast Start-Up Parameter

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

Fast start-up is only effective when the PES supply voltage is connected. Operation at SIL 4 level is still ensured.

Fast start-up is achieved through the following measures:

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

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

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

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

7.4.1.5 Hardware System Variables

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

System variables	S [1)]	Function	Setting for safe operation
Forcing Deactivation	Y	Prevents the forcing process from starting and terminates a running forcing process. Default value: FALSE.	Application-specific
Spare 2…Spare 21	N	No function.	---
MultiForcing Denied	Y	MultiForcing can be enabled and disabled using the *Multi-Forcing Denied* system variable so that the associated functions can be controlled by the user program. For MultiForcing, the system variable must be set to FALSE. Default value: FALSE.	Application-specific
Emergency Stop 1… Emergency Stop 4	Y	Shuts down the controller if faults are detected by the user program. Default value: FALSE.	Application-specific
Read-only in RUN	Y	After the controller is started, the access permissions are downgraded to *Read-Only*. Exceptions are forcing and reload. Default value: FALSE.	Application-specific
Relay Contact 1… Relay Contact 4	N	Only applicable to F60! OR-linked system variables that control the relay of the FAULT contact on the F60 PS 01. The relay is a change-over contact with common contact 2, break contact 3 and make contact 1. ▪ If the F60 module is in the RUN state and the system variables *Relay Contact 1…Relay Contact 4* are FALSE, contact 1-2 is closed (contact 2-3 is open). ▪ If the F60 module is in the RUN state and no global variables are connected to the system variables *Relay Contact 1…4*, contact 1-2 is closed (contact 2-3 is open). ▪ If the F60 module is in the RUN state and at least one of the system variables *Relay Contact 1…4* is TRUE, contact 1-2 is open (contact 2-3 is closed). ▪ If the F60 module is not in the RUN state, contact 1-2 is open (contact 2-3 is closed). ▪ If the F60 module is de-energized, contact 1-2 is open (contact 2-3 is closed).	Application-specific
Reload Deactivation	Y	Locks the execution of reload. Default value: FALSE.	Application-specific
User LED 1, User LED 2	N	Applicable only for special controllers! Controls the corresponding LED, if existing. Default value: 0 ms	---
[1)] The operating system handles the system variable in a safety-related manner, yes (Y) or no (N).			

Table 18: Hardware System Variables

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

7.4.2 Locking and Unlocking the Controller

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

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

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

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

Example: To make a controller lockable

1. Define global variables of type BOOL and set initial values to FALSE.
2. Assign the global variable as output variables to the above system variables.
3. Assign the global variable to the channel value of a digital input.
4. Connect a key switch to the digital input.
5. Compile the program, load it into the controller, and start it.

► The owner of a corresponding key-operated switch is able to lock and unlock the controller. If the corresponding digital input module fails, the controller is automatically unlocked.

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

7.5 Forcing

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

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

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

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

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

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

7.5.1 Use of Forcing

Forcing supports users during the following tasks:

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

⚠ WARNING

Physical injury due to forced values is possible!

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

When forcing values, the person in charge must take further technical and organizational measures to ensure that the process is sufficiently monitored in terms of safety. HIMA recommends setting a time limit for the forcing procedure, refer to Chapter 7.5.3 for details.

⚠ WARNING

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

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

Forcing can operate at two levels:

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

7.5.2 Assigning a Data Source Changed through Reload

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

- Hardware.
- Communication protocols.
- System variables.

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

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

Consequence

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

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

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

7.5.3 Time Limits

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

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

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

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

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

7.5.4 Restriction on the Use of Forcing

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

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

7.5.5 MultiForcing

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

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

⚠ WARNING

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

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

⚠ WARNING

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

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

For further details on forcing, refer to the system manual (HI 800 141 E) and the SILworX online help.

7.5.5.1 Objectives of MultiForcing

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

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

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

7.5.5.2 Global MultiForcing

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

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

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

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

7.6 Safe Version Comparison

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

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

Essentially, there are three types of resource configurations:

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

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

The version comparison exactly determines the changed parts of the resource configuration. This facilitates testing and identifying the changes. The result has SIL 4 quality and may be submitted to the inspection authority as a piece of evidence.

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

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

7.7 Security Measures for the Application Programming Interface (API)

SILworX API supports the following security measures:

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

Important:

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

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

8 Safety-Related Aspects of User Programs

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

Programming goals for a user program:

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

8.1 Safety-Related Usage

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

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

The SILworX programming tool includes the following functions:

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

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

8.1.1 Programming Basics

The tasks to be performed by the controller must be defined in a specification or a requirements specification. This documentation serves as the basis for checking its proper implementation in the user program.

The documentation depends on the control task and can be represented in two ways.

Combinational logic:

- Cause/effect diagram.
- Logic of the connection with functions and function blocks.
- Function blocks with specified characteristics.

Sequential controllers (sequence control system):

- Written description of the steps and their enabling conditions and of the actuators to be controlled.
- Flow charts.
- Matrix or table form of the step enabling conditions and the actuators to be controlled.
- Definition of constraints, e.g., operating modes, emergency stop.

8.1.1.1 I/O Concept

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

Digital and analog sensors:

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

Actuators:

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

8.1.2 Programming Steps

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

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

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

8.1.3 User Program Functions

The user program functions can be freely programmed.

- Only elements complying with IEC 61131-3 together with their functional requirements are used within the logic.
- The physical inputs and outputs usually operate in accordance with the de-energize to trip principle, i.e., their safe state is 0.
- The user programs are built of logic and/or arithmetic functions irrespective of the de-energize to trip principle of the physical inputs and outputs.
- The program logic should be clear and easy to understand and well documented to assist in debugging. This includes the use of functional diagrams.
- To simplify the logic, the inputs and outputs of all function blocks and variables can be inverted in any given order.
- The programmer must evaluate the fault signals from the inputs/outputs or from logic blocks.

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

8.1.4 User Program System Parameters

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

System parameter	S [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 for Each Cycle [µs]	N	Maximum time in each processor module cycle for executing the user program. Range of values: 0…4 294 967 295 Default value: 0 (no limitation) The safety-related response is ensured through the watchdog. This setting is only required if several user programs are used!		Application-specific
Watchdog Time [ms] (calculated)	---	Monitoring time of the user program, calculated from the product of the watchdog time of the resource and the configured maximum number of CPU cycles. Not changeable!		
Classification	N	Classification of the user program in *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! Default value: TRUE.		
Autostart	Y	Enabled type of Autostart: Cold Start, Warm Start, Off. Default value: *Warm Start*.		Application-specific
Start Allowed	Y	TRUE:	The PADT may be used to start the user program. Default value: TRUE.	Application-specific
		FALSE:	The PADT may not be used to start the user program.	

System parameter	S [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. Default value: FALSE.	
Reload Allowed	Y	TRUE:	The user program reload is permitted. Default value: TRUE.	Application-specific
		FALSE:	The user program reload is not permitted.	
		Observe the settings in the resource properties!		
Local Forcing Allowed	Y	TRUE:	Forcing is permitted at program level.	FALSE is recommended
		FALSE:	Forcing is not permitted at program level. Default value: FALSE.	
Local Force Timeout Reaction	Y	Behavior of the user program after the forcing time has expired: ▪ Stop forcing only. ▪ Stop program. Default value: *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.	
		Default value for all new projects: *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 19: System Parameters of the User Program

8.1.5 Notes on the *Code Generation Compatibility* Parameter

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

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

8.1.6 Code Generation

The code is generated after entering the complete user program and the I/O assignments of the controller. During these steps, the configuration CRC, i.e., the checksum for the configuration files, is created.

This is a signature for the entire configuration and is issued as a 32-bit, hexadecimal code. It includes all of the configurable or modifiable elements such as the logic, variables or switch parameter settings.

i Before loading a user program for safety-related operation, the user program must first be compiled twice. The two generated versions must have the same checksum.

By default, SILworX automatically compiles the resource configuration twice and compares the checksums.

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

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

8.1.7 Loading and Starting the User Program

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

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

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

HIMA recommends archiving the project after each download or reload.

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

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

8.1.8 Reload

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

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

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

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.

The use of reload requires a license. For further details on reload, refer to the HIMatrix system manual (HI 800 141 E).

8.1.9 Online Test

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

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

8.1.10 Test Mode

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

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

Test Mode Allowed	Description
Deactivated	Test mode deactivated (default setting).
Activated	Test mode activated.

Table 20: User Program Parameter *Test Mode Allowed*

NOTICE

Failure of safety-related operation possible!

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

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

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

8.1.11 Changing the System Parameters during Operation

The system parameters specified in Table 21 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.

Parameter	Can be changed in the following controller state
System ID	STOP
Watchdog Time (for the resource)	RUN, STOP/VALID CONFIGURATION
Safety Time	RUN, STOP/VALID CONFIGURATION
Target Cycle Time	RUN, STOP/VALID CONFIGURATION
Target Cycle Time Mode	RUN, STOP/VALID CONFIGURATION
Allow Online Settings	TRUE -> FALSE: All FALSE -> TRUE: STOP
Autostart	All
Start Allowed	All
Load Allowed	All
Reload Allowed	All
Global Forcing Allowed	All
Global Force Timeout Reaction	All
Global MultiForcing Allowed	All

Table 21: Online Changeable Parameters

8.1.12 Project Documentation for Safety-Related Applications

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

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

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

8.1.13 Multitasking

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

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

A user program cycle can take multiple processor system cycles. This can be controlled with the resource and user program parameters. SILworX uses these parameters to calculate the user program watchdog time:

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

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

- Use of the same global variables in several user programs.
- Unpredictably long runtimes can occur in individual user programs if no limit is configured with *Max Duration for Each Cycle*.
- The distribution of user program cycles over processor module cycles strongly affects the user program response time and the response time of the variables written to by the user program!
- A user program evaluates global variables written to by another user program as many processor system cycles later as the value set in the system parameter *Program's Maximum Number of CPU Cycles*. In the worst case, the following sequence is possible:
  - Program A writes to global variables needed by program B.
  - Program A stops its cycle in the same processor system cycle in which program B starts its cycle.
  - Program B is only able to read the values written to by program A when its next cycle starts.
  - The duration of the cycle just started by program B can be *Program's Maximum Number of CPU Cycles * Cycle Time*. Only at this point, program B adopts the values written to by program A.
  - It may take more than the configured *Program's Maximum Number of CPU Cycles* of the processor system until B reacts to these values!

⚠ CAUTION

Reciprocal influence of user programs is possible!

The use of the same global variables in several user programs can lead to a variety of unintentional consequences caused by the reciprocal influence of the user programs.

- **Carefully plan the use of the same global variables in several user programs.**
- **Use the cross-references in SILworX to check the use of global data. Global data may only be assigned values by one entity, either within a user program, from safety-related inputs or through safety-related communication protocols!**

The user is responsible for ensuring that operation is not disturbed by a reciprocal influence of the user programs!

For further details on multitasking, refer to the HIMatrix system manual (HI 800 141 E).

8.1.14 Factory Acceptance Test and Test Authority

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

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

8.2 Checklist for Creating a User Program

To comply with all safety-related aspects during the programming phase, HIMA recommends using the checklist prior to and after loading a new or modified program. The checklist can be used as a planning document and also serves as proof of careful planning.

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

9 Configuring Communication

In addition to physical input and output variables, variables can also be exchanged with another system via a data connection. In this case, the variables are declared with SILworX, in the Protocols area of the corresponding resource.

This data exchange can occur in either read-only or read/write mode.

9.1 Standard Protocols

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

⚠ WARNING

Physical injury possible due to usage of non-safe import data!

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

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

- SNTP
- Send/Receive TCP
- Modbus (master/slave)
- PROFIBUS DP (master/slave)
- PROFINET and PROFIsafe (as of CPU BS V7)

All standard protocols are interference-free with respect to the safe processor system.

9.2 Safety-Related safe**ethernet Protocol**

safe**ethernet** must be used for safety-related data exchange between safety-related components.

As a HIMatrix system component, safe**ethernet** is certified up to SIL 4.

Use the safe**ethernet** Editor / P2P Editor to configure how safety-related communication is monitored.

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

For safety-related functions, which are implemented via safe**ethernet**, the setting **Use Initial Value** must be used.

NOTICE

The safe state may be entered inadvertently!

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

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

9.2.1 Receive Timeout

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

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

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

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

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

Delay:	Delay on the transport path, e.g., due to switch or satellite.
Max. cycle time	Maximum cycle time of both controllers.

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

NOTICE

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

9.2.2 Response Time

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

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

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

Response Time ≤ Receive Timeout / n

n = 2, 3, 4, 5, 6, 7, 8, …

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

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

Min. response time ≤ receive timeout / 2 ≥ 2 * delay + 2.5 * max. cycle time

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

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

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

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

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

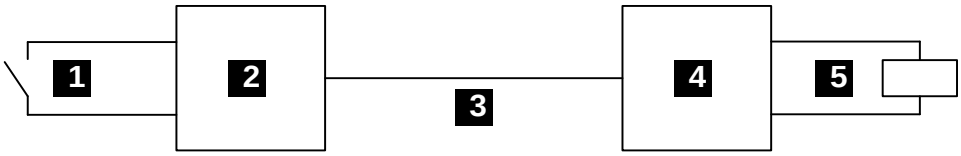
NOTICE

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

safety time = 2 * watchdog time

9.2.3 Calculating the Maximum Response Time

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



1 Input
2 Controller 1
3 Safety-related protocol
4 Controller 2
5 Output

Figure 4: Response Time when 2 HIMatrix Controllers are Interconnected

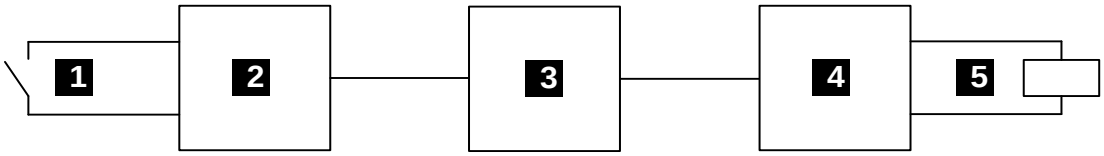
$$T_R = t_1 + t_2 + t_3$$

T_R	Worst case response time
t_1	2 ∗ watchdog time of controller 1.
t_2	Receive timeout
t_3	2 ∗ watchdog time of controller 2

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

9.2.4 Calculating the Maximum Response Time with 2 Remote I/Os

The maximum response time T_R is the time between a change on a field component input signal (in) of the first remote I/O module and a response on the corresponding output (out) of the second remote I/O module. It can be calculated as follows:



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

Figure 5: Response Time with Remote I/Os

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

T_R	Worst case response time
t_1	2 * watchdog time of remote I/O 1
t_2	Receive timeout$_1$
t_3	2 ∗ watchdog time of the controller
t_4	Receive timeout$_2$
t_5	2 * watchdog time of remote I/O 2

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

9.2.5 Terms

Receive timeout	Monitoring time of controller 1 within which a valid response from controller 2 must be received. After the time has expired, safety-related communication is terminated.
Receive timeout$_1$	Remote I/O 1 → controller
Receive timeout$_2$	Controller → remote I/O 2
Watchdog time	Maximum permissible duration of a PES RUN cycle (cycle time).
Worst case	Time between a change in a physical input (in) signal of controller 1 and a response in the corresponding output (out) of controller 2.

Data is transmitted using a safety-related protocol.

9.2.6 Assigning safe**ethernet** Addresses

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

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

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

i The operator is responsible for ensuring that the Ethernet used for safe**ethernet** communication or peer-to-peer communication 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.

Appendix

Glossary

Term	Description
AI	Analog input
AO	Analog output
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CRC	Cyclic redundancy check
DI	Digital input
DO	Digital output
EMC	Electromagnetic compatibility
EN	European standard
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
HW	Hardware
ICMP	Internet control message protocol, network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Inputs are designed for interference-free operation and can be used in circuits with safety functions
MAC	Media access control address, hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX
PE	Protective ground
PELV	Protective extra low voltage
PES	Programmable electronic system
R	Read, the variable is read out
R/W	Read/Write (column title for system variable type)
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
SSL	Secure sockets layer, see TLS
SW	Software
TLS	Transport layer security, hybrid cryptographic protocol
TMO	Timeout
W	Write, the variable receives a value, e.g., from the user program
WD	Watchdog, device for monitoring the system's correct operation Signal for fault-free process
WDT	Watchdog time

Index of Figures

Index of Tables

Index

MANUAL

HIMatrix Safety Manual for Railway Applications

HI 800 437 E

For further information, please contact:

HIMA Rail Segment Team
Phone: +49 6202 709-411

Or contact our Rail Expert Team: rail@hima.com

Learn more about HIMA solutions for railway applications online:

www.hima.com/en/industries-solutions/rail/

www.hima.com

Manual

HIMatrix®F

Maintenance Manual

Railway Applications

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 800 672 D, Rev. 2.00 (1936)	German original document
HI 800 673 E, Rev. 2.00.00 (1939)	English translation of the German original document

Table of Contents

1 Introduction

This document describes all relevant activities for servicing and operating safety-related HIMatrix controllers.

- Chapter 2 lists the activities in a table.
- Chapter 3 lists the manuals to be observed and other applicable documents.
- Chapter 4 includes maintenance action details.

1.1 Target Audience and Required Know-How

This manual is aimed at the planners, design engineers, programmers and maintenance personnel of automation systems. Specialized knowledge of safety-related automation systems is required.

Additional knowledge is necessary for maintenance activities on the HIMatrix system hardware and software, e.g., for reading and evaluating diagnostics.

For work on safety-related automation systems, the safety standards demand proof of the qualifications required for maintenance personnel.

Qualified HIMA service personnel can be requested to perform maintenance tasks in accordance with the manufacturer's instructions. HIMA also offers specific training seminars to qualify the maintenance personnel.

HIMA recommends the following seminars for performing maintenance tasks:

- **FS 101** Functional safety for maintenance and operation
- **PT 230** SILworX HIMatrix Maintenance

1.2 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 specially marked. In the electronic document (PDF): When the mouse pointer hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are specially marked.

1.2.1 Safety Notices

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

The safety notices are represented as described below.

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

The signal words have the following meanings:

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

⚠ SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

NOTICE

Type and source of damage!

Damage prevention.

1.2.2 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.

1.3 Safety Lifecycle Services

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

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

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

Safety Lifecycle Services:	
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 Operating and Maintenance Activities

The operating and maintenance activities of the individual system components are listed in the following sections.

2.1 Activities Recurring in the Short Term

The HIMatrix system must be tested by the operator at short recurring intervals in line with the Automation Security policy. The operator must specify the test details in a security risk analysis; refer to the automation security manual (HI 801 373 E).

2.2 Activities Recurring on an Annual Basis

The chapter specifies the activities recurring on an annual basis.

2.2.1 Mechanical Test (Visual Inspection)

The table specifies the maintenance activities for the mechanics:

Activity	Who	Reference
Check whether the compact systems are securely fastened to the DIN rail (DIN).	Operating company, assembler, maintenance personnel	D1
Check the module screws for firm connection, tighten if necessary (HIMatrix F60).	Operating company, assembler, maintenance personnel	D2
Check the data cables for firm connection, including to the communication interfaces.	Operating company, assembler, maintenance personnel	D1, D2
Check the fans for proper function (HIMatrix F60).	Operating company, assembler, maintenance personnel	D2

Table 1: Annual Activities for the Mechanics

2.2.2 Power Supply Test

The table specifies the maintenance activities for the power supply:

Activity	Who	Reference
Check the 230 VAC/24 VDC power supply for compliance with tolerances, 24 VDC, -15…+20 %, $r_p \leq 5$ %.	Operating company, assembler, maintenance personnel	D1, D2
Check the 24 VDC distribution. Check any existing decoupling diodes for proper function.	Operating company, assembler, maintenance personnel	D1, D2
Check the redundant supply for proper function.	Operating company, assembler, maintenance personnel	D1, D2

Table 2: Annual Activities for the Power Supply

2.3 Activities Recurring in the Long Term

The chapter specifies activities recurring in the long term.

2.3.1 Hardware

The table specifies the maintenance activities for the hardware:

Activity	Who	Reference
At an operating temperature of > 40 °C: Replace the fans every **3** years (HIMatrix F60).	Operating company, assembler, maintenance personnel	D2
At an operating temperature of ≤ 40 °C: Replace the fans every **5** years (HIMatrix F60).	Operating company, assembler, maintenance personnel	D2

Table 3: Activities for the Hardware Recurring in the Long Term

2.4 Activities as Required

The chapter specifies activities to be carried out as required.

2.4.1 Hardware

The table specifies the maintenance activities for the hardware:

Activity	Who	Reference
Replace the compact system.	Operating company, assembler, maintenance personnel	D1, D6
Replace the modules (HIMatrix F60).	Operating company, assembler, maintenance personnel	D2, D7 Chapter 4.2.2

Table 4: Activities for the Hardware to be Carried out as Required

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

NOTICE

Damage 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 component is protected from electrostatic discharge, e.g., by storing it in its packaging.**

Use a grounding strap and connect it to the ESD connection point on the control cabinet before touching the module to preclude any potential residual charge during module replacement. This also applies when inserting the plugs of cables and data lines.

If the control cabinet is not provided with an ESD connection point, get in contact with a grounded part of the control cabinet before touching the module.

Avoid any direct contact with electronic module components and their PCBs. Only touch the modules by their handles.

2.4.2 Software

The table specifies the maintenance activities for the software:

Activity	Who	Reference
Loading the user program.	Operating company, assembler, maintenance personnel	D1
Load new operating systems.	Operating company, assembler, maintenance personnel	D1, Chapter 4.3
Change the system parameters.	Operating company, assembler, maintenance personnel	D1, D2, D3, D5, D6, D7

Table 5: Activities for the Software to be Carried out as Required

3 Other Applicable Documents

The following table specifies other applicable documents.

Reference	Standard/Document ID	Description
N1	IEC 61511-1, Section 12	Functional safety - Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements
D1	HI 800 141 E	HIMatrix system manual for compact systems
D2	HI 800 191 E	HIMatrix system manual for modular systems
D3	HI 800 437 E	HIMatrix safety manual for railway applications
D4	HI 801 373 E	Automation security manual
D5	-	SILworX online help
Reference	Standard/Document ID	Description
D6	**HIMatrix manuals for compact systems**	
	HI 800 153 E	F1 DI 16 01 manual
	HI 800 155 E	F2 DO 4 01 manual
	HI 800 157 E	F2 DO 8 01 manual
	HI 800 159 E	F2 DO 16 01 manual
	HI 800 139 E	F2 DO 16 02 manual
	HI 800 161 E	F3 AIO 8/4 01 manual
	HI 800 179 E	F3 DIO 8/8 01 manual
	HI 800 177 E	F3 DIO 16/8 01 manual
	HI 800 345 E	F3 DIO 20/8 02 manual
	HI 800 473 E	F30 03 manual
	HI 800 477 E	F35 03 manual
Reference	Standard/Document ID	Description
D7	**HIMatrix manuals for the modular system**	
	HI 800 195 E	AI 8 01 manual
	HI 800 199 E	CIO 2/4 01 manual
	HI 800 479 E	CPU 03 manual
	HI 800 203 E	DI 32 01 manual
	HI 800 205 E	DIO 24/16 01 manual
	HI 800 207 E	DO 8 01 manual
	HI 800 183 E	GEH 01 manual
	HI 800 209 E	MI 24 01 manual
	HI 800 211 E	PS 01 manual

Table 6: Other Applicable Documentation

Derived variants: Variants derived from some compact devices (the corresponding manuals are specified in Table 6) were developed for special application fields. These derived variants require the same maintenance actions valid for the basic variants.

4 Maintenance Actions in Details

This chapter describes individual maintenance actions for the components of the HIMatrix system.

i Only qualified personnel may perform maintenance actions to supply, signal and data lines, taking all ESD protection measures into account. Personnel must be electrostatically discharged prior to any direct contact with these supply or signal lines!

4.1 Compact Systems

Defective compact systems must be replaced with systems of the same type.

When replacing compact systems, observe the instructions specified in the system manual for compact systems (HI 800 141 E) and safety manual (HI 800 437 E).

4.1.1 Replacing the Compact Systems

To remove compact systems from the DIN rail

1. Remove all connector plugs from the compact system:
   - Pluggable screw terminals.
   - Ethernet plugs.
   - Fieldbus plugs, if existing.
2. Insert a flathead screwdriver into the gap between the housing and the latch, using it as a lever to move the latch downward and simultaneously lift the compact system from the rail.

► The compact system is removed from the DIN rail.

To mount the compact system on the DIN rail

1. Shift the latch on the rear side of the compact system downwards, press it against the housing frame and snap it into position.
2. Attach the guiding rail located on the rear side of the compact system to the upper edge of the DIN rail.
3. Press the compact system against the rail and release the latch again to secure the compact system to the DIN rail.
4. Insert all plugs into the correct sockets:
   - Pluggable screw terminals.
   - Ethernet plugs.
   - Fieldbus plugs, if existing.

► The device is mounted on the DIN rail.

4.2 F60 Modular Systems

Modular systems may require the following maintenance actions:

- Replace the fans.
- Replace the modules.
- Replace the base plate.

4.2.1 Replacing the Fans

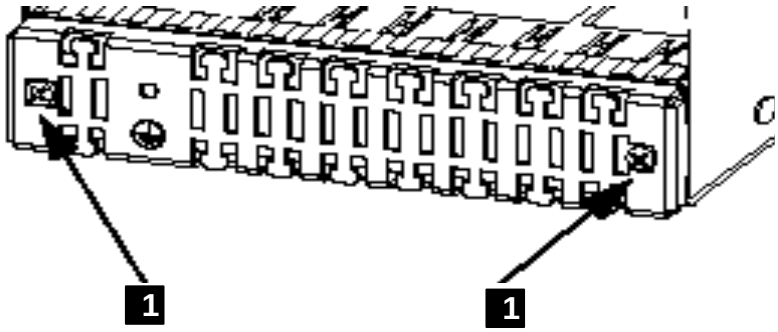
HIMA recommends replacing the fans of the HIMatrix F60 on a regular basis to prevent the fans to fail:

- At increased temperatures, > 40 °C: every 3 years.
- At normal temperatures, < 40 °C: every 5 years

The fans may be replaced while the controller is operating, the controller needs not be shut down.

To replace the fans in the base plate

1. Unscrew both fastening screws located on the left and right of the ground grid, see Figure 1.



1 Fastening Screws

Figure 1: Ground Grid with Fastening Screws

2. Position the ground grid (including the attached cables) to allow removal of the fan mounting plate located behind it.
3. Release the plugs for the fan voltage supply and remove the fan mounting plate completely.
4. Unscrew and remove the 4 fastening screws on each fan to allow replacement of the old fans.
5. Attach the new fans using the fastening screws; in doing so, pay attention the direction of the air flow.
6. Place the mounting plate with the new fans into position and plug in the connectors for the power supply of the fans.
7. Place the ground grid into position and tighten the two fastening screws.

► The fans are replaced.

4.2.2 Replacing the Modules

Defective modules must be replaced with modules of the same type or with approved replacement models.

When replacing modules, observe the instructions specified in the system manual (HI 800 191 E) and the safety manual (HI 800 437 E).

NOTICE

Damage to the controller possible!

Only replace the modules if the controller is shut down!

To remove a module from the base plate

1. Remove the plugs from the module front plate.
2. Release the locking screws located on the upper and lower end of the front plate.
3. Loosen the module using the handle located on the lower part of the front plate and remove it from the guiding rails.

► The module is removed.

To mount a module in the base plate

1. Insert the module as far as it can go – without jamming it – into the two guiding rails located on the upper and lower part of the housing.
2. Apply pressure to the upper and lower extremity of the front plate until the module plugs snap into the backplane socket.
3. Secure the module with the screws located on the upper and lower end of the front plate.
4. Depending on the type of module, insert the plugs of the communication cables or field cables into the front plate.

► The module is mounted.

4.2.3 Replacing the Base Plate of the F60

Defective base plates must be replaced with new ones.

To replace the base plate in the F60

1. Switch the voltage supply off to put the controller out of operation.
2. Remove all the modules from the base plate, see Chapter 4.2.2.
3. Remove the base plate from the support, e.g., the cabinet.
4. Mount the new base plate on the support.
5. Insert all modules into the new base plate, see Chapter 4.2.2.
6. Connect the voltage supply and restart the controller.

► The base plate is replaced.

4.3 Loading Operating Systems

The processor and communication systems have different operating systems that are stored in the rewritable flash memories and can be replaced, if necessary.

NOTICE

Interruption of safety-related operation!

The controller must be in the STOP state to enable the programming tool to load new operating systems.

During this time period, the operator must ensure the plant safety, e.g., by taking organizational measures.

i

- The programming tool prevents controllers from loading operating systems in the RUN state and reports this accordingly.
- Interruption or incorrect termination of the loading process causes the controller to be no longer functional. It is possible, however, to repeat loading.

The operating system for the processor system (CPU operating system) must be loaded before that for the communication system (COM operating system).

Operating systems for controllers differ from those for remote I/Os.

A new operating system can only be loaded, if previously stored in a directory accessible to the programming tool.

i

The current operating system versions of modules are displayed in the SILworX Control Panel. The type label specifies the delivered module version.

To load the new operating system

1. Set the controller to the STOP state, if this has not yet been done.
2. Open the online view of the hardware and log in to the controller with administrator rights.
3. Right-click the module (processor or communication module) to be loaded
4. The context menu appears. Click **Maintenance/Service->Load Module Operating System**.
5. In the *Load Module Operating System* dialog box, select the type of firmware that should be loaded.
6. A dialog box for selecting a file appears. Select the file with the operating system that should be loaded and click **Open**.

► SILworX loads the new operating system into the controller.

Appendix

Glossary

Term	Description
AI	Analog input
AO	Analog output
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses
COM	Communication module
CRC	Cyclic redundancy check
DI	Digital input
DO	Digital output
EMC	Electromagnetic compatibility
EN	European standard
ESD	Electrostatic discharge
FB	Fieldbus
FBD	Function block diagrams
HW	Hardware
ICMP	Internet control message protocol, network protocol for status or error messages
IEC	International electrotechnical commission
Interference-free	Inputs are designed for interference-free operation and can be used in circuits with safety functions
MAC	Media access control address, hardware address of one network connection
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX
PE	Protective earth
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)
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

MANUAL

HIMatrix Maintenance Manual Railway Applications

HI 800 673 E

For further information, please contact:

HIMA Rail Segment Team
Phone: +49 6202 709-411

Or contact our Rail Expert Team: rail@hima.com

Learn more about HIMA solutions for railway applications online:

https://www.hima.com/en/industries-solutions/rail/

www.hima.com

Manual

Communication

Configuration in SILworX

Contact

HIMA Paul Hildebrandt GmbH

P.O. Box 1261

68777 Brühl, Germany

Phone: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Document designation	Description
HI 801 100 D, Rev. 12.00 (2024)	German original document
HI 801 101 E, Rev. 12.00.00 (2027)	English translation of the German original document

Table of Contents

1 Introduction

The communication manual for safety-related HIMA systems provides an overview of the protocols available and the physical properties of the Ethernet and fieldbus interfaces. For protocols not described in this manual, separate manuals are available, see Table 2.

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 HIMA systems 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.

1.1 Structure and Use of This Manual

The manual contains the following chapters:

- Introduction
- Safety
- Product description
- safeethernet
- SNTP
- HART
- General

Additionally, the following documents must be taken into account:

Name	Content	Document no.
HIMax system manual	Hardware description HIMax system	HI 801 001 E
HIMax safety manual	Safety function HIMax systems	HI 801 003 E
HIMatrix safety manual	Safety function HIMatrix systems	HI 800 023 E
HIMatrix compact system manual	Hardware description HIMatrix compact system	HI 800 141 E
HIMatrix modular system manual	Hardware description HIMatrix modular F 60 system	HI 800 191 E
HIQuad X system manual	Hardware description HIQuad X system	HI 803 211 E
HIQuad X safety manual	Safety function HIQuad X system	HI 803 209 E
Automation security manual	Description of automation security aspects related to the HIMA systems	HI 801 373 E
SILworX first steps manual	Introduction to SILworX.	HI 801 103 E

Table 1: Additional Applicable Manuals

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/.

1.2 Target Audience

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

1.3 Writing Conventions

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

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 specially marked. In the electronic document (PDF): When the mouse pointer hovers over a hyperlink, it changes its shape. Click the hyperlink to jump to the corresponding position.

Safety notices and operating tips are specially marked.

1.3.1 Safety Notices

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

The safety notices are represented as described below.

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

The signal words have the following meanings:

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

⚠ SIGNAL WORD

Type and source of risk!

Consequences arising from non-observance.

Risk prevention.

NOTICE

Type and source of damage!

Damage prevention.

1.3.2 Operating Tips

Additional information is structured as presented in the following example:

i	The text giving additional information is located here.

Useful tips and tricks appear as follows:

TIP	The tip text is located here.

1.4 Safety Lifecycle Services

HIMA provides support throughout all the phases of 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 automation security.

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

Safety Lifecycle Services:	
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 Safety

All safety information, notes and instructions specified in this document 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

To use the HIMA controllers, all pertinent requirements must be met, see additionally applicable manuals listed in Table 1.

2.2 Residual Risk

No imminent risk results from a HIMA 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 HIMA system is a part of the safety equipment of an overall system. If the controller fails, the system enters the safe state.

In emergencies, no action that may prevent the HIMA system from operating safely is permitted.

2.5 Automation Security for HIMA Systems

The objectives of automation security are data confidentiality, integrity and availability. Targeted attacks are to be expected for automation security. In particular, potential targets of attacks are interfaces such as described in this manual.

⚠ WARNING

Physical injury possible due to unauthorized manipulation of the controller!

Protect the controller against unauthorized access!

Users are responsible for implementing the necessary measures in a way suitable for the plant!

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

- 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.

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

3 Product Description

Using the provided protocols, HIMA controllers can be connected to one another or to controllers from other manufacturers. The protocols are configured in the SILworX programming tool.

Manufacturer-independent standard protocols are available to ensure optimal integration of field devices and control systems into the HIMA systems. Both Ethernet and fieldbus protocols may be used. The standard protocols are interference-free with respect to the safe processor system of the HIMAsystems.

The following protocols are available for the HIMA systems:

Protocol	SIL[1)]	HIMax	HIQuad X	HIMatrix	Chapter or manual
safeethernet	4	X	X	X	Chapter 4
SNTP	-	X	X	X	Chapter 5
HART Protocol	-	X	--	--	Chapter 6
HIMA X-OPC Server[2)]	-	X	X	X	HI 801 480 E
HIMA OPC UA Server	-	X	X	X	HI 801 551 E
ISOfast	3	--	--	X	HI 801 465 E
Send/Receive TCP	-	X	--	X	HI 801 524 E
HIPRO-S V2	3	X	X	X	HI 800 723 E
PROFINET IO controller	-	X	--	X	HI 801 523 E
PROFINET IO device	-	X	--	X	
PROFIsafe host	3	X	--	X	
PROFIsafe F-device	3	X	--	X	
PROFIBUS DP master	-	X	--	X	
PROFIBUS DP slave	-	X	X	X	
Modbus master	-	X	X	X	HI 801 522 E
Modbus slave set	-	X	X	X	
Modbus slave set V2	-	X	X	X	HI 801 475 E
Synchronous serial interface (SSI)	-	X	--	X	HI 801 521 E
ComUserTask[3)]	-	X	X	X	

1) --: No SIL.
3: SIL 3 in accordance with IEC 61508-2:2010, IEC 61784-3:2019.
4: SIL 4 in accordance with IEC 61508-2:2010, IEC 61784-3:2019 and EN 50159:2010, see Chapter 4.

2) The HIMA X-OPC Server is installed on a host PC and is used as a transfer interface for up to 255 HIMA controllers and third-party systems that have an OPC interface.

3) In the ComUserTask, a C program of the user can be implemented and connected to various communication interfaces of the COM module.

Table 2: Protocols Available for the HIMA Systems

The safety-related protocols are operated on the corresponding processor module of the HIMA system. The amount of process data is limited by the available free memory for global process data on the processor module:

- HIMax, HIMatrix, HIQuad X = 512 kBytes.

i The memory for global process data is used for all variables of the HIMA system (e.g,. protocol, user program and system variables). If the available memory space is depleted, the HIMA system rejects a configuration during the download or reload and informs the user in the SILworX logbook.

Many standard protocols only ensure a non-safety-related data transmission. The non-safe data may only be used for safety-related functions under the responsibility of the user if sufficient additional measures have been taken.

⚠ WARNING

Use of non-safe import data in safety-related functions!

Physical injury possible due to usage of non-safe import data!

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

3.1 HIMA System Quantity Structure for Non-Safety-Related Protocols

Non-safety-related protocols (NSIP) are operated on the corresponding communication module (COM module) of the HIMA systems.

Properties	HIMax	HIQuad X	Description
System view			The pictures are examples of the respective system family. The figures depict a HIMax and a HIQuad X H51X.
Communication modules per HIMA controller	With X-CPU 01: 1…20 X-COM 01 With X-CPU 31: 1…4 X-COM 01	H51X: 1…10 F-COM 01 H41X: 1…2 F-COM 01	NSIP are run on the communication modules.
Ethernet and fieldbus interfaces	On the X-COM 01	On the F-COM 01	For details, refer to Table 5.
Maximum number of NSIP	▪ 201) for each HIMax controller. ▪ 61) for each X-COM module.	▪ 20[1)] for each HIQuad X. ▪ 5[1)] for each F-COM 01.	Available NSIP, see Table 2.
Process data volume[1)2)] of all NSIP within a controller	Send 128 kB Receive 128 kB	Send 64 kB Receive 64 kB	The maximum process data volume of the controller must not be exceeded. If it is exceeded, the controller configuration is rejected during the load process.

Properties	HIMatrix	Description
System view		The picture is an example of the respective system family. It shows an F30.
Communication modules per HIMA controller	Integrated communication module	NSIP are run on the communication modules.
Ethernet and fieldbus interfaces	On the controller	For details, see Table 5.
Maximum number of NSIP	6[1)]	Available NSIP, see Table 2.
Process data volume[1)2)] of all NSIP within a controller	Send 64 kB Receive 64 kB	The maximum process data volume of the controller must not be exceeded. If it is exceeded, the controller configuration is rejected during the load process.

1) X-OPC Server, SNTP client and SNTP server are not taken into account in this calculation.

2) The process data volume of non-safety-related protocols (NSIP) includes the exchanged data and the system variables of non-safety-related protocols and of PROFIsafe.

Table 3: HIMA System Quantity Structure for Non-Safety-Related Protocols

3.2 Protocol Registration and Activation

The protocols specified below are available for HIMA systems and can be activated as follows:

Protocol	Interfaces	HIMax	HIQuad X	HIMatrix
HIMA safeethernet	Ethernet	I	I	I
SNTP	Ethernet	I	I	I
HART protocol	Ethernet	I	--	--
HIMA X-OPC Server (runs on a host PC)	Ethernet	II	II	II
HIMA OPC UA Server	Ethernet	II	II	II
ISOfast	Ethernet	--	--	II
Send/Receive TCP	Ethernet	II	--	II
HIPRO-S V2	Ethernet	II	II	II
PROFINET IO controller	Ethernet	II	--	II
PROFINET IO device	Ethernet	II	--	II
PROFIsafe F-Host1)	Ethernet	II	--	II
PROFIsafe F-Device1)	Ethernet	II	--	II
PROFIBUS DP master	Fieldbus	III	--	III
PROFIBUS DP slave	Fieldbus	III	II	III
Modbus master Eth	Ethernet	II	II	II
Modbus slave Eth	Ethernet	II	II	II
Modbus master RS485	Fieldbus	IV	II	IV
Modbus slave RS485	Fieldbus	IV	II	IV
Synchronous serial interface (SSI)	Fieldbus	IV	--	IV
ComUserTask	Ethernet, Feldbus	IV	II	IV

I These protocols are activated by default.
II A license (software activation code) must be purchased for these protocols.
III These protocols are activated by installing a fieldbus submodule.
IV A license (software activation code) and, if required, the corresponding fieldbus submodule must be purchased for these protocols.

1) Additional PROFINET license needed

Table 4: Protocol Registration and Activation

The software activation code with the required licenses is generated on the HIMA website using the system ID of the controller. To this end, follow the instructions provided on the HIMA website www.hima.com-> Products & Services -> Product 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.

i If a Modbus master RS485 is operated on one COM through multiple interfaces, it is still considered a single Modbus master instance. It requires therefore only one license.

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 Key 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.

i Order the license on time!
All functions requiring a license (e.g., protocols) can be tested without license for 5000 operating hours.
If functions are operated with no valid license, the Error LED (for HIMax/HIMatrix and HIQuad X) is lit.
After 5000 operating hours, the function (e.g., protocols) continues until the controller is stopped. Afterwards, the user program cannot be started without a valid license for the features used in the project (faulty configuration).

3.3 Ethernet Interfaces

The Ethernet interfaces of CPU and COM in the HIMA systems can be used for communication with external systems and programming. The Ethernet interfaces can simultaneously process multiple protocols, excepted from the system bus interfaces of the X-SB 01, X-CPU 31 and F-IOP 01 modules.

The use of these interfaces is described in the respective system manual.

Each CPU and COM module has a a freely configurable IPv4 address and an Ethernet switch.

To transfer data, the Ethernet switch establishes a targeted connection between two communication partners. This prevents collisions and reduces the load on the network.

For targeted data forwarding, a MAC/IP address assignment table (ARP cache) is generated in which the MAC addresses are assigned to specific IP addresses. From now on, data packets are only forwarded to the IP addresses specified in the ARP cache.

i Replacement of CPU or COM module with identical IP address.
If a device has its ARP Aging Time set to 5 minutes and its MAC Learning set to Conservative, its communication partner does not adopt the new MAC address until a period of 5 to 10 minutes after the module is replaced. Until the new MAC address has been adopted, no communication is possible using the replaced device.
In addition to the configurable ARP Aging Time, the user must wait at least the non-configurable MAC Aging Time of the switch (approx. 10 seconds) before the replaced device is able to communicate again.

3.3.1 HIMax Ethernet Interfaces

The following table shows the HIMax Ethernet interfaces for communication with external system:

Property	HIMax X-CPU 01	HIMax X-CPU 31	HIMax X-COM 01
Ports	4	2 for protocols 2 for system bus UP/DOWN	4
Transmission standard	10/100/1000 Base-T, half and full duplex	10/100 Base-T Half and full duplex	
Autonegotiation	Yes		
Autocrossover	Yes		
Connection socket	RJ45		
IP address	Freely configurable[1)]		
Subnet mask	Freely configurable[1)]		
Supported protocols	safeethernet, X-OPC (DA & A+E), HIPRO-S V2 Programming and debugging tool (PADT), SNTP		
	--	--	Standard protocols[2)]

[1)] The general rules for assigning IP address and subnet masks must be adhered to.
[2)] In this manual, the term standard protocols designates protocols that are used to connect to external systems.

Table 5: HIMax Ethernet Interfaces

3.3.2 HIQuad X and HIMatrix Ethernet Interfaces

The following table shows the HIQuad X and HIMatrix Ethernet interfaces for communication with external system.

Property	HIQuad X F-CPU 01	HIQuad X F-COM 01	HIMatrix Steuerung
Ports	2	2	4
Transmission standard	10BASE-T/ 100BASE-Tx, Half and full duplex		
Autonegotiation	Yes		
Autocrossover	Yes		
Connection socket	RJ45		
IP Address	Freely configurable[1)]		
Subnet Mask	Freely configurable[1)]		
Supported protocols	safeethernet, X-OPC (DA & A+E), HIPRO-S V2 Programming and debugging tool (PADT), SNTP		
	--	Standard protocols[2)]	Standard protocols[2)]

[1)] The general rules for assigning IP address and subnet masks must be adhered to.
[2)] In this manual, the term standard protocols designates protocols that are used to connect to external systems.

Table 6: HIQuad X and HIMatrix Ethernet Interfaces

3.3.3 Configuring the Ethernet Interfaces

The Ethernet interfaces are configured in SILworX in the detail view of the CPU or COM module.

For HIMA systems, the Speed Mode and Flow Control Mode parameters are set to Autoneg by default.

i Communication loss!

With an inappropriate Ethernet parameters setting, the device might no longer be reachable. Reset the device!

To open the CPU/COM module detail view

1. In the structure tree, select Configuration, Resource, Hardware.
2. Right-click and select Edit from the context menu to open the Hardware Editor.
3. Right-click CPU/COM Module and select Detail View from the context menu to open the detail view.

i The parameters set in the properties of the CPU/COM module are not available for the HIMA system communication, until they have been re-compiled with the user program and transferred to the controller.

3.3.3.1 The Module Tab

The Module tab contains the following parameters:

Designation	Description
Name	Module name.
Activating Max. µP Budget for HH Protocol	▪ Activated: Use CPU load limit from the *Max. µP Budget for HH Protocol [%]* field. ▪ Deactivated: Do not use the CPU load limit for safeethernet.
Max. µP Budget for HH Protocol [%]	Maximum CPU load of the module that can be used for processing the safeethernet protocol. i The maximum load must be distributed among all the implemented protocols that use this communication module.
Code Generation	This parameter can only be set for HIMax and HIMatrix systems since HIQuad X is only available as of V10. Prior to V6: Setting compatible with existing projects. V6 and higher: Recommended setting for new projects, especially if safeethernet connections are routed via this communication module. Changes to the safeethernet connection can be loaded by performing a reload.
IP Address	IP address of the Ethernet interface. Default value: 192.168.0.99
Subnet Mask	32-bit address mask to split up the IP address into network and host address.
Standard Interface	Activated: The interface is used as standard interface for system login. Default setting: Deactivated
Default Gateway	IP address of the default gateway. Default value: 0.0.0.0

Designation	Description
ARP Aging Time [s]	A processor or COM module stores the MAC addresses of the communication partners in a MAC/IP address assignment table (ARP cache). The MAC address remains stored in the ARP cache if messages from the communication partner are received within 1x…2x *ARP Aging Time*. The MAC address is erased from the ARP cache if no messages from the communication partner are received within 1x…2x *ARP Aging Time*. The typical value for the *ARP Aging Time* in a local network ranges from 5…300 s. The contents of the ARP cache cannot be read out. Range of values: 1…3600 s Default value: 60 s **Note:** If routers or gateways are used, the *ARP Aging Time* must be adjusted (increased) due to the additional time required for two-way transmission. If the *ARP Aging Time* is too low, the MAC address of the communication partner is erased from the ARP cache and communication is delayed or interrupted. For an efficient performance, the *ARP Aging Time* value must be greater than the receive timeout set for the protocols in use.
MAC Learning	*MAC Learning* and *ARP Aging Time* are used to set how quick the Ethernet switch should learn the MAC address. The following settings are possible: ▪ Conservative (recommended) If the ARP cache already contains MAC addresses of communication partners, these are locked and cannot be replaced by other MAC addresses for at least 1 *ARP Aging Time* and a maximum of 2 *ARP Aging Time* periods. ▪ Tolerant When a message is received, the IP address contained in the message is compared to the data in the ARP cache, and the MAC address stored in the ARP cache is immediately overwritten with the MAC address from the message. Tolerant must be used if the availability of communication is more important than the authorized access to the controller. Default setting: Conservative
ICMP Mode	The Internet Control Message Protocol (ICMP) allows the higher protocol layers to detect error states on the network layer and optimize the transmission of data packets. Message types of Internet Control Message Protocol (ICMP) supported by the CPU module: ▪ No ICMP Responses All ICMP commands are deactivated. This ensures a high degree of safety against potential sabotage that might occur over the network. ▪ Echo Response If Echo Response is activated, the node responds to a ping command. It is thus possible to determine if a node can be reached. Safety is still high. ▪ Host Unreachable Not important for the user. Only used for testing at the manufacturer's facility. ▪ All Implemented ICMP Responses All ICMP commands are activated. This allows a more detailed diagnosis of network malfunctions. Default setting: Echo Response

Table 7: Configuration Parameters

3.3.3.2 The Routings Tab

The Routings tab contains the routing table. This table is empty if the module is new. A maximum of 8 routing entries are possible.

Designation	Description
Name	Designation of the routing settings.
IP Address	Target IP address of the communication partner (with direct host routing) or network address (with subnet routing). Range of values: 0.0.0.0…255.255.255.255 Default value: 0.0.0.0
Subnet Mask	Define the target address range for a routing entry. 255.255.255.255 (with direct host routing) or subnet mask of the addressed subnet. Range of values: 0.0.0.0…255.255.255.255 Default value: 255.255.255.255
Gateway	IP address of the gateway to the addressed network. Range of values: 0.0.0.0…255.255.255.255 Default value: 0.0.0.1

Table 8: Routing Parameters

3.3.3.3 The Ethernet Switch Tab

The Ethernet Switch tab contains the following parameters:

Designation	Description
Name	Port number as printed on the housing; per port, only one configuration may exist. Range of values: 1…4
Speed [MBit/s]	10 Mbit/s: Data rate 10 Mbit/s 100 Mbit/s: Data rate 100 Mbit/s 1000 Mbit/s: Data rate 1000 Mbit/s (X-CPU 01 module only). Autoneg (10/100/1000): Automatic baud rate setting. Default value: Autoneg
Flow Control	Full duplex: Simultaneous communication in both directions. Half duplex: Communication in one direction. Autoneg: Automatic communication control. Default value: Autoneg
Autoneg also with Fixed Values	The Advertising function (forwarding the speed and flow control properties) is also performed if the parameters Speed and Flow Control have fixed values. This allows other devices whose ports are set to Autoneg to detect the port setting.
Limit	Limit the inbound multicast and/or broadcast packets. Off: No limitation. Broadcast: Limit broadcast (128 kbit/s). Multicast and Broadcast: Limit multicast and broadcast packets (1024 kbit/s). Default value: Broadcast

Table 9: Ethernet Switch Parameters

3.3.3.4 The VLAN Tab (Port-Based VLAN)

For configuring the use of port-based VLAN, see also Chapter 3.3.5.

i If VLAN is to be supported, port-based VLAN must be off to enable each port to communicate with the other switch ports.

For each port of a switch, the user can define to which other ports of the switch received Ethernet frames may be sent to.

The table in the VLAN tab contains entries through which the connection between two ports can be set to active or inactive.

Name	Eth1	Eth2	Eth3	Eth4
Eth1				
Eth2	Active			
Eth3	Active	Active		
Eth4	Active	Active	Active	
CPU	Active	Active	Active	Active

Table 10: VLAN Tab

Default setting: All connections between ports are set to Active

3.3.3.5 The LLDP Tab

LLDP (Link Layer Discovery Protocol) periodically sends information on the own device via multicast (e.g., MAC address, device name, port number) and receives the same information from the neighboring devices.

LLDP uses the following values depending on whether PROFINET is configured on the communication module:

PROFINET on the COM module	Chassis ID	TTL (Time to Live)
Used	Device name	20 s
Not used	MAC Address	120 s

Table 11: LLDP Values for Profinet

The processor and communication modules support LLDP on the Eth1, Eth2, Eth3 and Eth4 ports.

The following parameters define how a given port should work:

Off	LLDP is disabled on this port.
Send	LLDP sends LLDP Ethernet frames, received LLDP Ethernet frames are deleted without being processed.
Receive	LLDP sends no LLDP Ethernet frames, but received LLDP Ethernet frames are processed.
Send/Receive	LLDP sends and processes received LLDP Ethernet frames.

Default setting: Off.

3.3.3.6 The Mirroring Tab

Mirroring is used to configure whether the module should duplicate Ethernet packets on a given port such that they can be read from a device connected to that port, e.g., for test purposes.

The following parameters define how a given port should work:

Off	This port does not participate in the mirroring process.
Egress:	Outgoing data of this port are duplicated.
Ingress:	Incoming data of this port are duplicated.
Ingress/Egress:	Incoming and outgoing data of this port are duplicated.
Dest Port:	Duplicated data are sent to this port.

Default setting: Off.

3.3.4 Network Ports in Use for Ethernet Communication

UDP ports	Use
123	SNTP (time synchronization between controller and remote I/O, and external devices).
502	Modbus salve (can be changed by the user).
6010	safeethernet and OPC.
8000	Programming and operation with SILworX..
8001	Port on the remote I/O for configuring the remote I/O using the controller.
8004	Port on the controller for configuring the remote I/O using the controller.
34964	PROFINET endpoint mapper (required for establishing the connection).
49152	PROFINET RPC server.
49153	PROFINET RPC client.
Xxx	ComUserTask assigned by the user. May not be used with another protocol.

Table 12: Network Ports (UDP Ports) in Use

TCP ports	Use
502	Modbus salve (can be changed by the user).
Xxx	TCP SR assigned by the user.
Xxx	ComUserTask assigned by the user. May not be used with another protocol.

Table 13: Network Ports (TCP Ports) in Use

3.3.5 Separating Switch Ports via VLAN

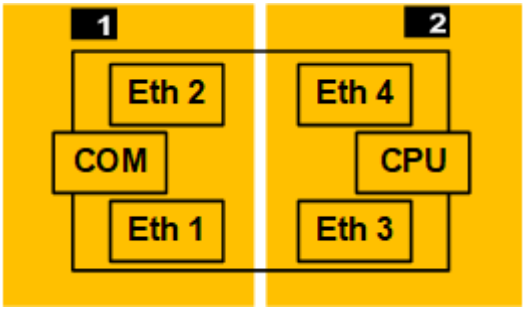
VLAN settings can be used to divide the available switch ports according to the required application. It is therefore possible in HIMatrix to establish a connection with two IP addresses or to separate safe communication through the CPU from non-safe communication through the COM.

The switch port is configured in SILworX in the detail view of the CPU or COM module, see Chapter 3.3.3.

For HIMatrix, HIMA recommends separating the CPU and COM. The example below can be adapted to the application-specific requirements.

	Eth1	Eth2	Eth3	Eth4	COM
Eth1					
Eth2	Active				
Eth3	Inactive	Inactive			
Eth4	Inactive	Inactive	Active		
COM	Active	Active	Inactive	Inactive	
CPU	Inactive	Inactive	Active	Active	Inactive

Table 14: VLAN Tab



1 Eth 1 and Eth 2 in the unprotected area via the COM for non-safety-related protocols.

2 Eth 3 and Eth 4 in the protected area via the CPU for safeethernet communication with the remote I/Os and other HIMA PES..

Figure 1: Example of Switch Ports Separated via VLAN

i If all the Ethernet port connections to the processor of the controller have been blocked by the VLAN configuration, the controller must be reset. Afterwards, the controller is once again accessible via the default IP address.

i Connection blockades in networks separated via VLAN if these networks are not completely separated, e.g.,connected through a common external switch.
The internal switch in HIMatrix controllers includes a common MAC<->switch port assignment table for the CPU and the COM. When Ethernet frames arrive from a network that is not completely separated, the MAC<->switch port assignment table of the internal switch must be continuously relearned. This results in alternating blockades of the corresponding Ethernet frames to the CPU and the COM.

3.4 Fieldbus Interfaces

The fieldbus submodules allow communication via the fieldbus interfaces of the HIMax X-COM 01, HIQuad X, F-COM 01, as well as the HIMatrix controllers F30, F35 and the F60 CPU 01.

For the HIMax and HIMatrix controllers, the fieldbus submodules are optional and must be installed by the manufacturer. Ex-factory, the FB3 fieldbus interface of the HIMatrix controllers includes an RS485 for Modbus (master or slave) or ComUserTask.

Users can configure the fieldbus interface transmission standards in SILworX for the HIQuad X controllers. The pins for the FB1and FB2 interfaces of the F-COM 01 module are automatically assigned once this configuration has been loaded into the HIQuad X controller.

The fieldbus protocols may only be used for safety-related functions under the responsibility of the user if sufficient additional measures have been taken.

The system does not support programming using these interfaces.

3.4.1 Registration and Activation

The communication options are activated in accordance with the protocol, see Chapter 3.2.

3.4.2 Installation of the Fieldbus Submodules

The fieldbus submodules are optional and must be installed by the manufacturer. Additionally, the protocols used must be activated. Additionally, the protocols used must be partially activated.

3.4.2.1 Part Number Structure

The following sections present how the part number for the HIMax X-COM 01 or a HIMatrix controller changes if fieldbus interfaces are used.

Numbers are allocated to the fieldbus to create the part numbers, see Table 15.

Options for FB1 and FB2	Designation	Fieldbus submodule description
0	--	No fieldbus submodule inserted.
1	RS485 module	RS485 for Modbus (master or slave) or ComUserTask.
2	PROFIBUS master	PROFIBUS DP master.
3	PROFIBUS slave	PROFIBUS DP slave.
5	RS232 module	RS232 for use with ComUserTask.
6	RS422 module	RS422 for use with ComUserTask.
7	SSI module	SSI for use with ComUserTask.
8	CAN module	CAN for use with ComUserTask. Only available for HIMatrix.

Table 15: Options for Fieldbus Interfaces FB1 and FB2

3.4.2.2 HIMax COM Module Part Number

When the X-COM 01 is equipped with one or multiple fieldbus submodules, in addition to the the part number, the module name changes from X-COM 01 to X-COM 010 XY.

Each COM module forms a functional unit with the X-CB 001 02 connector board. Note that the connector board must be separately purchased.

The following table specifies the available components:

Designation	Description
X-COM 01	Communication module without fieldbus submodules.
X-COM 010 **XY** [1)]	Communication module with fieldbus submodule.
X-CB 001 02	Connector board.
[1)] **X**: Option for fieldbus interface FB1 in accordance with Table 15. **Y**: Option for fieldbus interface FB2 in accordance with Table 15.	

Table 16: Available HIMax Components

The designation and part number (part no.) are printed on the type label of the module.

i HIMA recommends operating the PROFIBUS DP using the FB1 fieldbus interface (maximum transfer rate 12 Mbit). The maximum transfer rate permitted for the FB2 fieldbus interface is 1.5 Mbit.

3.4.2.3 HIMatrix Controller Part Numbers

The HIMatrix controllers can be equipped with fieldbus submodules in accordance with the following table:

Controller	FB1 and FB2	FB3
F30 03z **XY**[1)]	Freely equippable in accordance with Table 15.	Integrated RS485
F35 03z **XY**[1)]	Freely equippable in accordance with Table 15.	Integrated RS485
F60 CPU 03z **XY**[1)]	Freely equippable in accordance with Table 15.	---
[1)] **X**: Option for fieldbus interface FB1 in accordance with Table 15. **Y**: Option for fieldbus interface FB2 in accordance [1)]Table 15. z: Hardware variant.		

Table 17: Equipment of HIMatrix Controllers with Fieldbus Submodules

The part number changes when the appropriate fieldbus submodule is selected:

Example: The part number for F35 030 XY is 98 22**XY**497

X: Option for fieldbus interface FB1 according to Table 15.
Y: Option for fieldbus interface FB2 according to Table 15.

3.4.3 HIMax and HIMatrix Fieldbus Interfaces

Pin assignment of the HIMax and HIMatrix fieldbus interfaces depends on the selected communication option, see Chapter 3.4.

Wiring and bus termination!
Observe the corresponding fieldbus standard when connecting the fieldbus interfaces.
- These require a suitable grounding concept.
- The shielded cables should be connected on both sides over a large area. Use the bus terminations to terminate the fieldbuses on their physical ends.

3.4.3.1 RS485 for Modbus Master, Slave or ComUserTask

One RS485 cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RxD/TxD-A	Receive/send data A.
4	CNTR-A	Control signal A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RxD/TxD-B	Receive/send data B.
9	CNTR-B	Control signal B.

Table 18: Pin Assignment of D-Sub Connectors for RS485

3.4.3.2 PROFIBUS DP Master or Slave

One PROFIBUS DP cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	-	Not used.
2	-	Not used.
3	RxD/TxD-A	PROFIBUS DP receive/send data A.
4	RTS	Control signal.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RxD/TxD-B	PROFIBUS DP receive/send data B.
9	-	Not used.

Table 19: Pin Assignment of D-Sub Connectors for PROFIBUS DP

3.4.3.3 RS232 für ComUserTask

One RS485 (RS232) cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	-	Not used.
2	TxD	Send data.
3	RxD	Receive data.
4	-	Not used.
5	DGND	Data transmission potential (ground to 5 V).
6	-	Not used.
7	RTS	Request to send.
8	-	Not used.
9	-	Not used.

Table 20: Pin Assignment of D-Sub Connectors for RS232

3.4.3.4 RS422 for ComUserTask

One RS485 (RS422) cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RxA	Receive data A.
4	TxA	Send data A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RxB	Receive data B.
9	TxB	Send data B.

Table 21: Pin Assignment of D-Sub Connectors for RS422

3.4.3.5 SSI

One RS485 (SSI) cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	D2+	Data input channel 2+.
2	D1-	Data input channel 1-.
3	CL2+/D3+	Clock output channel 2+ or data input channel 3+.
4	CL1+	Clock output channel 1+.
5	GND	Reference potential.
6	D1+	Data input channel 1+.
7	D2-	Data input channel 2-.
8	CL2-/D3-	Clock output channel 2- or data input channel 3-.
9	CL1-	Clock output channel 1-.

Table 22: Pin Assignment of D-Sub Connectors for SSI

3.4.3.6 CAN

One CAN cable must be used, see Chapter 3.7.

Connection	Signal	Function
1	-	Not used.
2	CAN-L	CAN-Low.
3	GND	Reference potential.
4	-	Not used.
5	-	Not used.
6	-	Not used.
7	CAN-H	CAN-High.
8	-	Not used.
9	-	Not used.

Table 23: Pin Assignment of D-Sub Connectors for CAN

3.4.4 HIQuad X F-COM 01 Fieldbus Interfaces

Pin assignment of the F-COM 01 fieldbus interfaces FB1/FB2 depends on the selected communication option, see Chapter 3.4.

i

Wiring and bus termination!

Observe the corresponding fieldbus standard when connecting the fieldbus interfaces.

- These require a suitable grounding concept.
- The shielded cables should be connected on both sides over a large area. Use the bus terminations to terminate the fieldbuses on their physical ends.

3.4.4.1 RS422

One RS485 (RS422) cable must be used, see Chapter 3.7.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RxD-A	Receive data A.
4	TxD-A	Send data A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RxD-B	Receive data B.
9	TxD-B	Send data B.

Table 24: Pin Assignment of the FB1 Interface with RS422

3.4.4.2 RS485 with RTS

One RS485 cable must be used, see Chapter 3.7.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RXD/TXD-A	Receive/send data A.
4	CNTR-A	Control signal A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RXD/TXD-B	Receive/send data B.
9	CNTR-B	Control signal B.

Table 25: Pin Assignment of the FB1 Interface with RS485 (with RTS)

3.4.4.3 Twice RS485 (without RTS)

One (two) RS485 cable must be used, see Chapter 3.7.

The pin assignment does not comply with the standard, since two interfaces are connected to one plug.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RxD1/TxD1-A	First receive/send data A.
4	RxD2/TxD2-A	Second receive/send data A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RxD1/TxD1-B	First receive/send data B.
9	RxD2/TxD2-B	Second receive/send data B.

Table 26: Pin Assignment of the FB1 and FB2 Interface with two RS485 (without RTS)

i The assignment Table 25 is active upon reload completion on FB1 with RS485 (with RTS).
The assignment Table 27 is active upon reload completion on FB2 with RS485 (without RTS).

3.4.4.4 FB2 with RS485 (without RTS)

One RS485 cable must be used, see Chapter 3.7.

The pin assignment does not comply with the standard.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	-	-
4	RxD2/TxD2-A	Second receive/send data A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	-	-
9	RxD2/TxD2-B	Second receive/send data B.

Table 27: Pin Assignment of the FB2 Interface with RS485 (without RTS)

3.4.4.5 PROFIBUS DP Slave

One PROFIBUS DP cable must be used, see Chapter 3.7.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	RXD/TXD-A	PROFIBUS DP receive/send data A.
4	CNTR-A	Control signal A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	RXD/TXD-B	PROFIBUS DP receive/send data B.
9	CNTR-B	Control signal B.

Table 28: Pin Assignment of the FB1 Interface with PROFIBUS DP Slave

3.4.4.6 PROFIBUS DP Slave and RS485

The pin assignment does not comply with the standard, since two interfaces are connected to one plug.

One PROFIBUS DP cable must be used for PROFIBUS DP slaves. One RS485 cable must be used for RS485, see Chapter 3.7.

Pin	Signal	Description
1	-	Not used.
2	5 V	Fieldbus supply decoupled via diode.
3	PROFIBUS DP RXD/TXD-A	PROFIBUS DP receive/send data A.
4	RS485 RxD1/TxD1-A	Receive/send data A.
5	DGND	Data transmission potential (ground to 5 V).
6	5 V	Fieldbus supply.
7	-	Not used.
8	PROFIBUS DP RXD/TXD-B	PROFIBUS DP receive/send data B.
9	RS485 RxD1/TxD1-B	RS485 receive/send data B.

Table 29: Pin Assignment of the FB1/2 Interface with PROFIBUS DP Slave and RS485

3.5 Technical Characteristics of RS485 Transmission

The following table presents the basic technical features of the RS485 transmission that is used for the PROFIBUS DP.

Element	Description
Network topology	Linear bus, active bus termination on both ends.
Medium	Shielded, twisted pair wires
Connectors	9-pin D-sub connector, see Chapter 3.4.3 and Chapter 3.4.4.
Number of bus subscribers for each segment	32 subscribers in every segment, without repeaters[1)].
Total number of bus subscribers for each bus	1 Modbus master, 3 repeaters[1)]. 121 Modbus slaves.
Max. length of a bus segment	1200 m for each segment.
Max. length of the bus	4800 m, 4 segments with 3 repeaters[1)].
Max. baud rate	115200 Bit/s

[1)] The maximum number of bus subscribers in the segment decreases by 1 for each repeater used. This means that a maximum of 31 subscribers may be operated on the segment. According to the standard, a total of three repeaters may be used so that a maximum of 121 Modbus slaves may be connected per serial interface on a Modbus master. If several interfaces are available (HIMax and HIMatrix), up to 3 interface slaves or repeaters can be connected. Internally, the system behaves like a master. The minimum number of slaves is thus 254.

Table 30: Properties of the RS485 Transmission

The cable length specified in Table 31 depends on the baud rate selected.

Baud rate	Cable length for each segment	RS485	PROFIBUS DP
300 Bit/s	1200 m	X	-
600 Bit/s	1200 m	X	-
1200 Bit/s	1200 m	X	-
2400 Bit/s	1200 m	X	-
4800 Bit/s	1200 m	X	-
9600 Bit/s	1200 m	X	X
19200 Bit/s	1200 m	X	X
38400 Bit/s	1200 m	X	-
45450 Bit/s	1200 m	-	X
57600 Bit/s	1200 m	X	-
62500 Bit/s	1200 m	X	-
76800 Bit/s	1200 m	X	-
93750 Bit/s	1200 m	-	X
115200 Bit/s	1200 m	X	-
187500 Bit/s	1000 m	-	X
500000 Bit/s	400 m	-	X
1.5 MBit/s	200 m	-	X
3 MBit/s	100 m	-	X
6 MBit/s	100 m	-	X
12 MBit/s	100 m	-	X

Table 31: Cable Length According to the Baud Rate for RS485 and PROFIBUS DP

i The cable length may be increased by using bidirectional repeaters. A maximum of three repeaters may be connected between two subscribers. In doing so, a cable length of 4.8 km may be achieved.

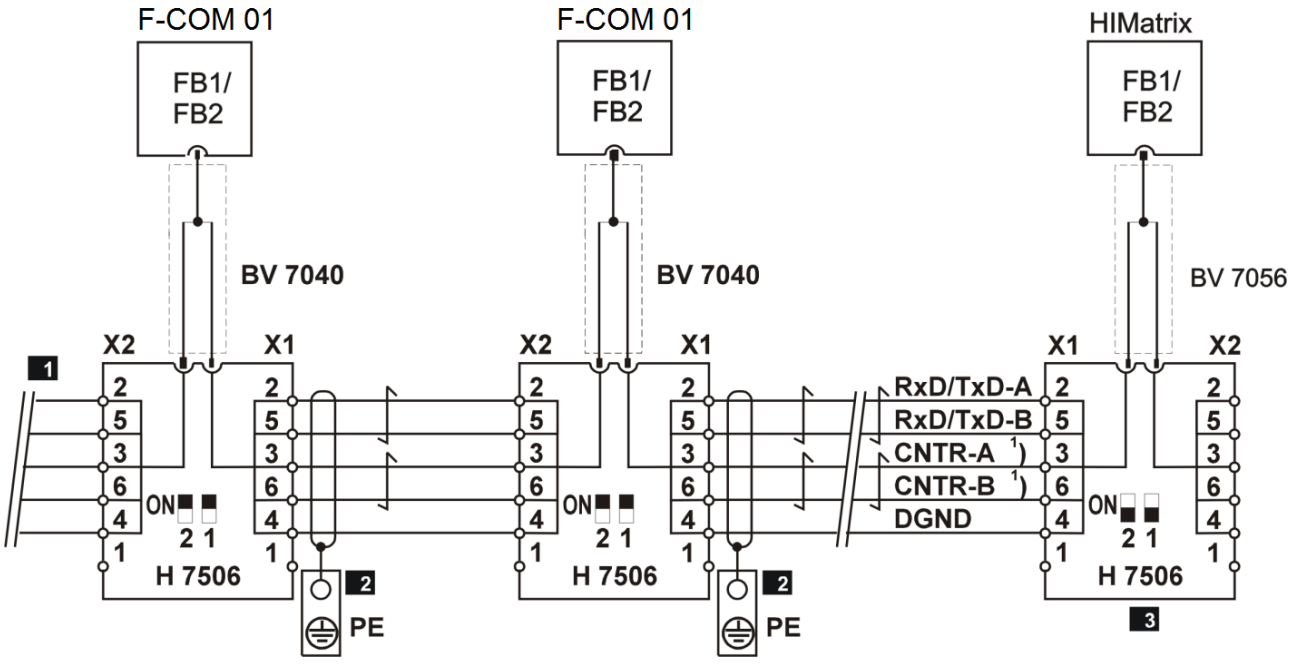
For time-critical applications, HIMA recommends connecting no more than 32 bus subscribers. For non-time-critical applications, up to 126 subscribers (with repeaters) may be used.

3.6 RS485 Bus Topology

The following picture shows a structure example of RS485 bus topology using HIMA components. H 7506 are used as bus terminals. The total bus length may not exceed 1200 m. A repeater such as the H 7505) must be used for long distances. A total of 3 repeaters may be used. The bus may thus have a maximum extension of 4800 m.

i If fiber optic cable or RS485 converters are used in the bus, H 7505 must not be used (no automatic switching of data direction).

The time until the information from a slave is available on a master increases by the number of slaves on the bus. The more slaves are connected to the bus, the worse the system response time will become.



1) Only necessary in repeater operation mode

1 Additional controllers

2 Protective conductor terminal, USLKG4 YE/GN

3 H 7506 switch position (bus termination) (switch position: both white switches set to ON)

Figure 2: RS485 Bus Topology

i Equipotential bonding should be used if the bus is extended over larger distances.

At transmission rates ≥ 1.5 MBit/s, branch lines must be strictly avoided. For this reason, use suitable bus connector plugs only.

3.6.1 H 7506 Terminal Assignment

The following table shows the terminal assignment of the HIMA H 7506 bus terminal. The HIMA BV 7040 cable connects the H 7506 to the FBx fieldbus interface of the controller.

X1/X2	Color	Description
1	-	-
2	WH	RxD/TxD-A, data cable.
3	GN	CNTR-A, control line for repeater.
4	GY	DGND
5	BN	RxD/TxD-B, data cable.
6	YE	CNTR-B, control line for repeaters.

Table 32: Terminal Assignment for H 7506

i For registered customers, the product documentation for this and other HIMA RS485 components is available at https://www.hima.com/en/downloads/.

3.6.2 Bus Connection and Bus Termination

The incoming and outgoing data cables can be directly connected in the bus connector plug. This avoids branch lines and the bus connector plug can be plugged in to and out from the field device at any time without interrupting the data traffic.

The IEC 61158 standard recommends using a 9-pole D-sub connector. Depending on the degree of protection of the field device, other slots, which are not occupied, may be used.

Figure 3 shows the pin assignment of the 9-pole D-sub connector. The bus connection to the field device is implemented as a socket.

The PROFIBUS DP bus connection includes a resistor combination that ensures a defined rest potential on the bus cable. The resistor combination is integrated in the PROFIBUS DP bus connector plugs and can be activated via bridges or switches.

Additionally, stations at which the bus terminates should provide 5 V at pin 6.

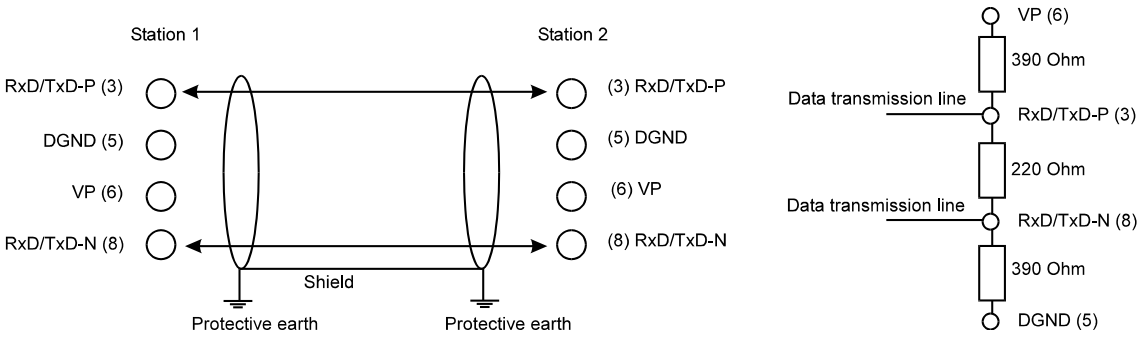


Figure 3: Bus Connection and Bus Termination, Pin Assignment of the Fieldbus Interface

3.7 Communication Cable Requirements

For communication connections running within a control cabinet, the minimum cable cross-section must be 0.2 mm².

For communication connections running outside a control cabinet, the minimum cable cross-section must be 0.5 mm². If necessary, installation cables with rigid cores must be used instead of cables with flexible cores.

Cables with the following characteristics are permitted for connecting to Ethernet or fieldbus interfaces:

- All the cables for Ethernet or fieldbus interfaces must withstand at least 500 bending cycles, if bending load is applied during the intended operating conditions.
- All the cables for Ethernet or fieldbus interfaces must withstand at least 25 bending cycles, if bending load is only applied during maintenance.
- All the cables for Ethernet or fieldbus interfaces must comply with UL94-V0.

3.7.1 Patch Cables

HIMA recommends using patch cables with the following minimum requirements: Cat.5e, RJ-45.

3.7.2 CAN Cables

As transmission medium, HIMA recommends only using CAN cables approved for CAN.

3.7.3 RS485 (RS422, RS232, SSI) Cables

As bus cables for RS485 (RS422, RS232 and SSI), HIMA recommends using shielded twisted pair wires with the following characteristics:

Element	Description
Cable type	LiYCY 3 x 2 x 0.25 mm² for RS485, RS422, RS232. LiYCY 6 x 2 x 0.25 mm² for SSI
Wire cross-section	> 0.25 mm²
Impedance	100…120 Ω

Table 33: RS485 (RS422, RS232, SSI) Bus Cables

3.7.4 PROFINET Cables

As transmission medium, HIMA recommends only using PROFINET cables approved for PROFINET.

3.7.5 PROFIBUS DP Cables

As transmission medium, HIMA recommends only using PROFIBUS DP cables approved for PROFIBUS DP with the following parameters:

Parameters	Cable type A
Impedance	135…165 Ω
Capacitance	≤ 30 pF / m
Loop impendence	≤ 110 Ω / km
Wire diameter	> 0.64 mm
Wire cross-section	> 0.34 mm²

Table 34: Parameters of the PROFIBUS DP Cable Type A

Cable type A can be used for all transfer rates up to 12 Mbit/s.

4 safeethernet

All HIMA can safely communicate via safeethernet.

i The safeethernet protocol meets all requirements for safety-related protocols in accordance with IEC 61508-2:2010, IEC 61784-3:2019 and EN 50159:2010. The TÜV has tested these features and verified the safe**ethernet** protocol as part of HIMA systems.

If the bit error probability of the transmission medium is 0.5, e.g., due to a disturbed network, the residual error rate λ_{SCL} of a safety-related function with 100 safe**ethernet** connections is less than 1 % of SIL 4 in accordance with IEC 61508-2:2010, IEC 61784-3:2019 and EN 50159:2010.
The residual error rate λ_{SCL} is applicable irrespective of the number of storing network elements, non-safety-related devices, the use of WLAN, compression and encryption.
This results in a residual error rate λ_{SCL} of less than 10^{-12}/h for the individual safe**ethernet** connection.

The corresponding Ethernet interfaces of the HIMA controllers can be also used for other protocols.

Various Ethernet network topologies can be used to ensure safe**ethernet** communication between controllers. To this end, so-called safe**ethernet** profiles suitable for the Ethernet network in use can be selected in SILworX to increase the data transmission speed and efficiency.
These safe**ethernet** profiles ensure safe**ethernet** communication, without requiring users to first become familiar with all the details involved in network configuration.

⚠ Warning

Manipulation of safety-related data transmission!

Physical injury

The plant manufacturer and the operator are responsible for ensuring that the Ethernet network used for safeethernet 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.

4.1 General Information about safeethernet

Requirements as determinism, reliability, interchangeability, expandability and above all safety, are central issues within the process and automation technology.

safe**ethernet** is a protocol for transmitting safety-related data up to SIL 4 in accordance with IEC 61508-2:2010, IEC 61784-3:2019 and EN 50159:2010 when Ethernet technology is used.

safe**ethernet** implements mechanisms that can detect and safely respond to faults.

The transmission of safety-related data occurs via standard Ethernet (IEEE 802.3) and is based on UDP/IP.

safe**ethernet** uses "unsafe data transmission channels" (Ethernet) in accordance with the black channel approach and monitors the data correctness through safety-related protocol mechanism. This allows users to use normal Ethernet network components such as switches, routers and wireless LAN devices within a safety-related network.

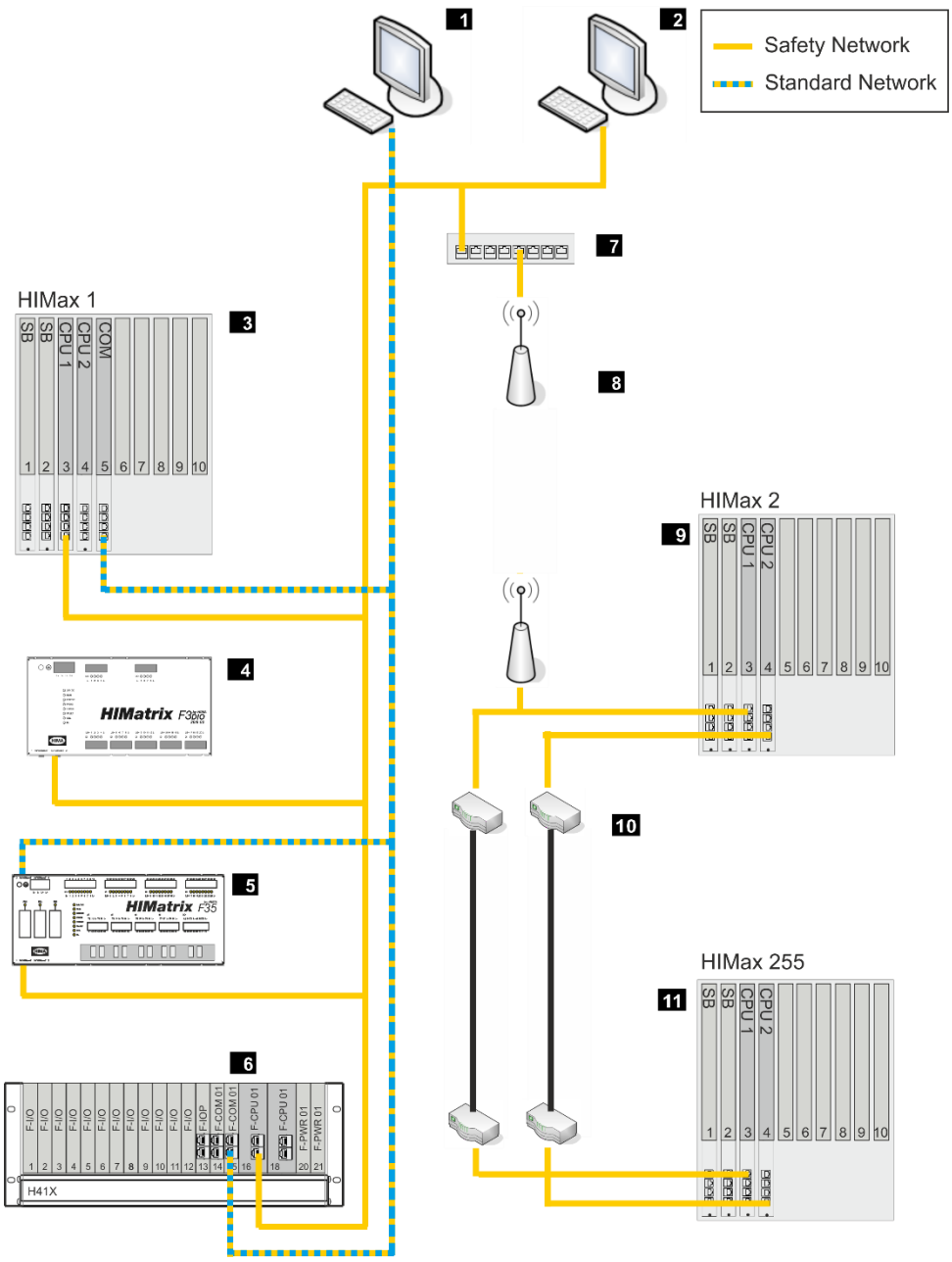
safe**ethernet** uses the abilities of standard Ethernet so that security and real-time capability are made possible. A special protocol mechanism ensures a deterministic behavior even if faults occur or new communication subscribers join the network. The system automatically integrates new components in the running system. All network components can be replaced during operation. Transmission times can be clearly defined using switches. If properly configured, Ethernet is thus real-time capable.

The possible transfer rate of up to 1 Gbit/s offers automation applications sufficient transmission capacity for safety-related data. Transmission media such as copper lines and fiber optic cables can be used.

safe**ethernet** data can be transmitted via the existing company-internal Ethernet network in addition to other data traffic on the Ethernet network. However, this could increase security risks.

i To reduce security risks, HIMA recommends setting up a safety network via the CPU modules and a separate standard network via the COM modules. The standard network is used to connect to non-safety components such as X-OPC Server, see Figure 4.

safe**ethernet** allows flexible system structures to be created with defined response times for decentralized automation. Depending on the requirements, the intelligence can be distributed to the network subscribers in a centralized or decentralized manner.



1 PC (X-OPC Server)
2 PC (PADT SILworX)
3 HIMax (address 1)
4 Remote I/O
5 Separating HIMatrix switch ports via VLAN
6 HIQuad X H41 X
7 Switch/router
8 Radio, satellite, WLAN
9 HIMax (address 2)
10 Fiber optic cable
11 HIMax (address 255)

Figure 4: Flexible System Structure with safeethernet

i A faulty network structure can cause a part of or the entire HIMA system to shut down.
The generally accepted regulations for developing Ethernet networks must be observed. no network loop may occur Data packets may only reach a controller over a single path, see also Chapter 4.7.

4.2 User Requirements for safeethernet in a Noisy Network

The plant manufacturer and the operator must include the effects of the noisy network on the application in their safety analysis.

To ensure that safe**ethernet** achieves sufficient availability for the respective application, users must comply with the following requirements.

- Users must select a suitable transmission system for the safety-related process data communication and set the safe**ethernet** parameters in such a way that sufficient availability is achieved for the application. In their safety analysis, users must consider the dangers of an unintentional shutdown by safe**ethernet** , for example. In case of doubt, the degree of availability required has to be agreed with the responsible test authority.
- Users must ensure that their communication system adheres to the configured response time and that this is less than or equal to half the value of the receive timeout. If not, the worst case response time must be suitable for the safety-related function even if the double the value of the receive timeout is included in the worst case response time calculation.
- If users cannot always ensure that their communication system meets the configured response time, they must monitor this response time and the response time measured by the system (system variable of the connection). Only in rare exceptional cases may the measured response time be exceeded by more than half the value of the receive timeout. Alternatively, users can also include double the value of the receive timeout in the worst case response time calculation of the safety-related function.
- If users operate a safe**ethernet** connection in a noisy network, or if the configured response time is not or frequently not observed and/or a cleanroom profile is used, HIMA does not recommend using the cleanroom profile due to potentially reduced availability!
  If safe**ethernet** needs to be used under these conditions, the *Receive Timeout* must be set so that the worst case response time for the safety-related function is still suitable if double the value of the *Receive Timeout* were to be used for calculating the worst case response time.
  The factor *n* in *Response Time* ≤ *Receive Timeout* / *n*, where *n* > 4, can for instance be configured to increase the availability of the safe**ethernet** connection. The value of n depends on the availability actually required or necessary. The characteristics of the transmission system must be considered.

4.3 HIMA System Quantity Structure for safeethernet

HIMA systems HIMax and HIQuad X support the safeethernet protocol with the following properties.

Element	HIMax	HIQuad X	Description
System view			The pictures are examples of the respective system family. The figures depict a HIMax and a HIQuad X H51X.
Module/controller	For each HIMax 1…4 X-CPU 01 1…2 X-CPU 31	For each H41X/H51X: 1…2 F-CPU 01	safeethernet is run on the safety-related CPU module.
Ethernet interfaces	X-CPU 01: 1 GBit/s X-CPU 31:100 Mbit/s X-COM 01: 100 Mbit/s	F-CPU 01: 100 Mbit/s F-COM 01: 100 Mbit/s	The Ethernet interfaces in use can simultaneously be used for additional protocols.
Connections	255	128	safeethernet connections to other controllers and remote I/Os.
Connections between two controllers	1 prior to CPU OS V6 64 as of CPU OS V6	64	safeethernet connections
Redundant connections	255	128	2-channel operation Redundant safeethernet connections between HIMA controllers can be configured in the safeethernet Editor.
Process data volume for each connection	1100 bytes	1100 bytes	For each safeethernet connection.
n.a.: not applicable			

Table 35: safeethernet Protocol for HIMax und HIQuad X

HIMA's HIMatrix systems support the safeethernet protocol with the following properties.

Element	HIMatrix	Description
System view		The picture is an example of the respective system family. It shows an F30.
Module/controller	Integrated CPU module of the controller	safe**ethernet** is run on the safety-related CPU module.
Ethernet interfaces	100 Mbit/s	The Ethernet interfaces in use can simultaneously be used for additional protocols.
Connections	128 prior to CPU OS V12 255 as of CPU OS V12	safe**ethernet** connections to other controllers and remote I/Os.
Connections between two controllers	1 prior to CPU OS V10 64 as of CPU OS V10	safe**ethernet** connections
Redundant connections	128 prior to CPU OS V12 255 as of CPU OS V12	2-channel operation. Redundant safe**ethernet** connections between HIMA controllers can be configured in the safe**ethernet** Editor.
Process data volume for each connection	1100 bytes	For each safe**ethernet** connection.
n.a.: not applicable		

Table 36: safeethernet Protocol for HIMatrix

4.4 Configuring a Redundant safeethernet Connection

This example shows how to configure a redundant safe**ethernet** connection between two HIMA controllers.

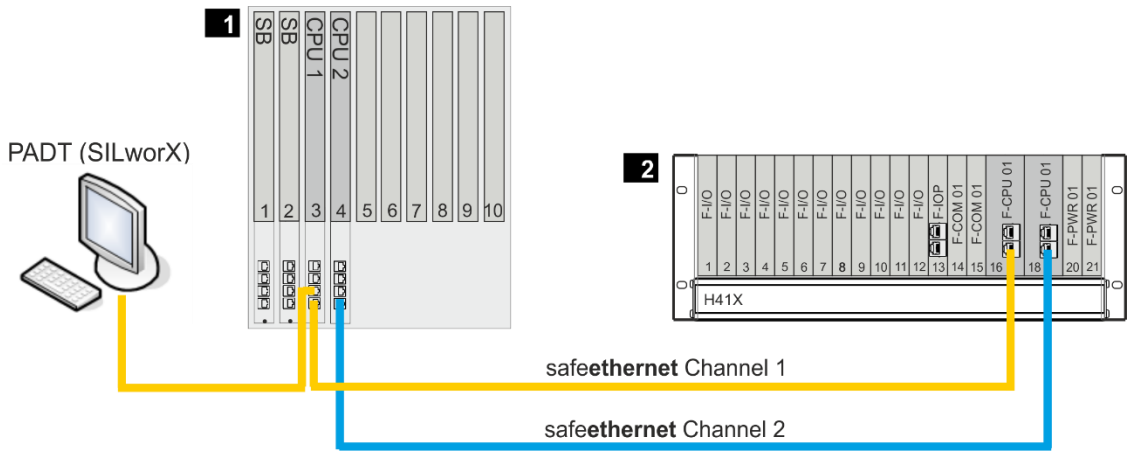


Figure 5: Structure for Configuring a Redundant Connection

i For redundant safe**ethernet** connections, HIMA recommends implementing the two transport paths (channel 1 and channel 2) via two Ethernet networks that are completely separated from one another. In doing so, the bandwidth and the delay on the respective transport paths must be nearly identical.

4.4.1 Establishing the safe**ethernet** Connection

In the safe**ethernet** Editor, create a safeethernet connection between Resource A and Resource B.

To open the safeethernet Editor of resource A

1. In the structure tree, open **Configuration**, **Resource**.
2. Right-click safe**ethernet** and select **Edit** from the context menu.
   ☑ *Resource B* is located in the Obj**e**ct Panel.

To create the safeethernet connection to resource B

1. In the Object Panel, click **Resource B** and drag it onto a free space within the workspace of the safe**ethernet** Editor.
   ☑ A dialog box appears to enter a name for the safe**ethernet** connection. This name must be unique.

i The reciprocal communication path is automatically added to resource B in the safe**ethernet** Editor.

To configure the safeethernet connection

1. Select **Ethernet Interfaces Channel 1** for resource A and resource B.
2. Select **Ethernet Interfaces Channel 2** for resource A and resource B.
3. Select the **Network Profile** (e.g., Fast&Noisy) for the safeethernet connection.
4. Calculate and enter the **Receive Timeout** and **Response Time** (see Chapter 4.8).

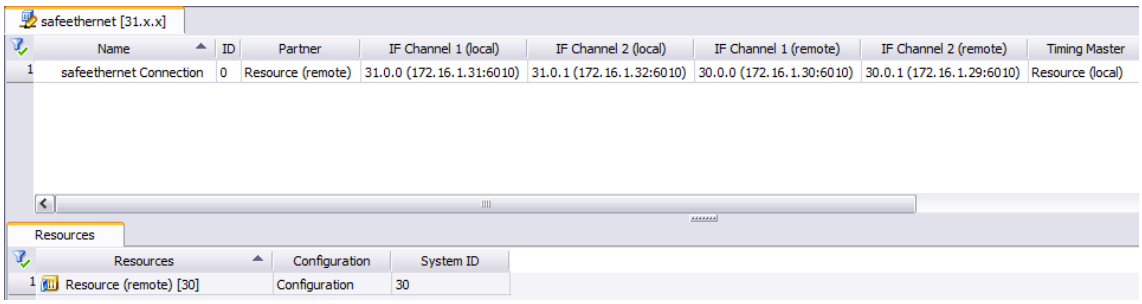


Figure 6: View in the safe**ethernet** Editor

4.4.2 Configuring within the safe**ethernet** Connection Editor

To connect process variables in the safe**ethernet** connection editor.

i Only global variables from the configuration context may be used, and not from the resource or project context!

To open the connection editor

1. Right-click the created safe**ethernet** connection and open the context menu.
2. Select **Edit** from the context menu to open the connection editor of the safe**ethernet** connection.
3. Select the **Resource A<->Resource B** tab.
4. In the Object Panel, select a Global Variable and drag it onto the **Resource A --> Resource B** area or onto the **Resource B --> Resource A** area depending on the selected transport direction.
5. Repeat this step for additional global variables.

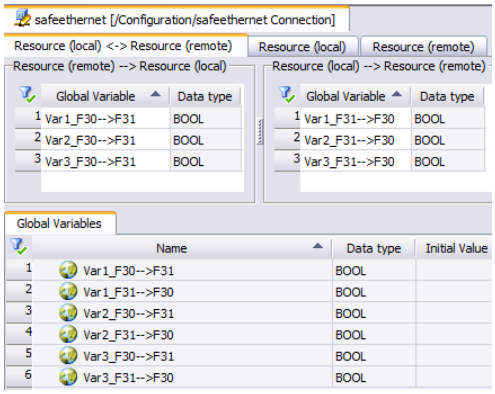


Figure 7: View in the safe**ethernet** Connection Editor

i Evaluate the system variables of the safe**ethernet** connection in the user program!
In the respective subtabs of Resource A and Resource B, global variables should at least be assigned to the system variables Connection State, Quality of Channel 1 and Quality of Channel 2 to evaluate these in the user program.

To verify the safeethernet connection

1. In the structure tree, select **Configuration, Resource**, safe**ethernet** .
2. Right-click and select **Verification** from the context menu.
3. Thoroughly verify the messages displayed in the logbook and correct potential errors.

i The configuration of the safe**ethernet** connection must be compiled with the user program of resource A and resource B and transferred to the controllers. The new configuration can only be used for communicating with the HIMA controller upon completion of this step.

4.4.3 Verifying safeethernet Communication

Reset the views in the Control Panel to zero with **Reset safeethernet Statistics**.

To verify that the redundant safe**ethernet** connection was established properly, disconnect and reconnect one redundant connection and then repeat this test for the other connection. During this test, there must be no faults in the safe**ethernet** communication. Also observe the values for Quality Channel 1 and Quality Channel 2 here.

i Additional causes for *Bad Messages and Resends*!

Verify the correct network design (e.g., wires, switches, PCs).
If the Ethernet network is not exclusively used for safe**ethernet** , also verify the network load (probable data collisions).

4.5 safeethernet Connection Overview

The safe**ethernet** connection overview for a resource lists all configured safe**ethernet** connections. The overview can also be used to create new safe**ethernet** connections.

To open the safe**ethernet** connection overview

1. In the structure tree, open **Configuration**, **Resource**.
2. Right-click safeethernet and select **Edit** from the context menu.

The safe**ethernet** connection overview displays the following safe**ethernet** protocol parameters:

Parameters	Description
Name	Name of the safe**ethernet** connection
ID	safe**ethernet** connection ID. Range of values: 0…63
Partner	Resource name of the link partner
IF Channel	Ethernet interfaces available on the (local) and (remote) resource, see also Chapter 3.3.
Timing Master	The timing master provides the value for *Receive Timeout*, *Resend Timeout* and the *Acknowledge Timeout* for this safe**ethernet** connection. The opposite controller is the timing slave, which adopts these values. If no timing master is selected, the controller with the smaller IP address determines these safe**ethernet** parameters.
Profile	Combination of matching safe**ethernet** parameters, see also Chapter 4.10.
Rsp t	*Response Time* is the time period expressed in milliseconds (ms) until the sender of the message receives acknowledgement from the recipient, see also Chapter 4.8.3. Default value: 500 ms
Receive Timeout	Monitoring time of controller 1 within which a valid response from controller 2 must be received, see also Chapter 4.8.2. Default value: 1000 ms

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Resend Timeout</td><td>Monitoring time expressed in milliseconds (ms) and set in controller 1 within which controller 2 must have acknowledged the receipt of a data packet; upon expiration of this period, the data packet is sent again, see also Chapter 4.8.5.</td></tr>
<tr><td>Acknowledgment Timeout</td><td>Time period expressed in milliseconds (ms) within which the CPU must acknowledge the receipt of a data packet, see also Chapter 4.8.6.</td></tr>
<tr><td>Prod Rate</td><td>The production rate is the minimum time interval between two data packets, see also Chapter 4.8.7.</td></tr>
<tr><td>Memory</td><td>Number of data packets that can be sent without acknowledgment, see also Chapter 4.8.8.</td></tr>
<tr><td>Behavior</td><td>Behavior of the input variables for this safeethernet connection if the connection is interrupted.
<table>
<tr><td>Use Initial Value</td><td>The initial data are used for the import variables.</td></tr>
<tr><td>Freeze Process Value Indefinitely</td><td>The import variables are frozen to the current value and used until a new connection is established.</td></tr>
<tr><td>Initial Value after [ms]</td><td>Input: Double-click the field and enter the time value in milliseconds.
The import variables are frozen to the current value and used until the configured timeout. Afterwards, the initial data are used for the input variables.
The timeout can be extended by up to a CPU cycle.</td></tr>
</table>
⚠ Caution
 
For safety-related functions implemented via safeethernet, Use Initial Value is the only setting which may be used.</td></tr>
<tr><td>Diag.Entry</td><td>The number of warnings that must occur in sequence within the Warning Period [ms] before the warnings are recorded in the diagnostics or communication fault statistic.</td></tr>
<tr><td>Prio A&E</td><td>The function is only activated for the connection to the X-OPC Server.
This defines the priority for events requested by the X-OPC Server from the controller.
Fragments with priority n and fragments with priority m are sent at a ratio of n to m times.</td></tr>
<tr><td>Prio Sync</td><td>The function is only activated for the connection to the X-OPC Server.
This defines the priority for state values requested by the X-OPC Server from the controller.
Fragments with priority n and fragments with priority m are sent at a ratio of n to m times.</td></tr>
<tr><td>Activate A&E</td><td>The function can only be used and changed for connections to the X-OPC Server.</td></tr>
<tr><td>Codegen</td><td>To operate safeethernet connections with communication partners with SILworX versions prior to V6, set the code generation version to Prior to V6.
V6 and higher: Reload of safeethernet connection is possible.
Prior to V6: Reload of safeethernet connection is not possible.
Default value: V6 and higher</td></tr>
</table>

Table 37: safe**ethernet** Protocol Parameters

Object Panel

The Object Panel contains all the project resources to which the current resource can be connected via safe**ethernet**.

i The archive function can be used for safe**ethernet** connections to resources outside the project (see Chapter 4.13).

4.6 Connection Editor of a safeethernet Connection

The safe**ethernet** Editor always refers to the local resource from which the safe**ethernet** Editor was started.

To open the safeethernet connection overview

1. In the structure tree, open **Configuration**, **Resource**.
2. Right-click safe**ethernet** and select **Edit** from the context menu.

To open the Connection Editor of a safeethernet Connection

1. Right-click the required safe**ethernet** connection to open the context menu.
2. Select **Edit**.
   ☑ The safe**ethernet** Editor includes the three tabs *Peer1<->Peer2, Peer1 and Peer2*.

4.6.1 The *Resource A<->Resource B* Tab

The *Resource A<->Resource B* tab is divided into two areas for the required transport direction: *Resource B-->Resource A* and *Resource A-->Resource B*.

Global Variables can be dragged onto these two areas from the Object Panel.

4.6.2 The *Resource B* Tab

The *Resource A* tab contains the tabs *System Variables* and *Fragment*
Definitions: *Resource B-->Resource A*, see Chapter 4.6.3.1 and Chapter 4.6.3.2.

4.6.3 The *Resource B* Tab

The *Resource B* tab contains the tabs *System Variables* and *Fragment*
Definitions: *Resource A-->Resource B*, see Chapter 4.6.3.1 and Chapter 4.6.3.2.

4.6.3.1 The System Variables Tab

The safeethernet connection can be controlled and evaluated by means of system variables.

<table>
<tr><th>Name</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.</td></tr>
<tr><td>Ack.Frame No.</td><td>UDINT</td><td>R</td><td>Receive counter (revolving).</td></tr>
<tr><td>Number of Faulty Messages</td><td>UDINT</td><td>R</td><td rowspan="2">Number of all faulty messages per channel (invalid CRC, invalid header, other faults).</td></tr>
<tr><td>Number of Faulty Messages for Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Number of Successful Connections</td><td>UDINT</td><td>R</td><td>Number of successful connections since statistics reset.</td></tr>
<tr><td>Number of Lost Messages</td><td>UDINT</td><td>R</td><td rowspan="2">Number of messages dropped out on one of the two transport paths since statistics reset.
The counter only continues to run until a channel completely fails.</td></tr>
<tr><td>Number of Lost Messages for Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Early Queue Usage</td><td>UDINT</td><td>R</td><td>Number of early messages since statistics reset. Early messages are stored in the Early Queue. See also Chapter 4.8.8.</td></tr>
<tr><td>Bad Messages</td><td>UDINT</td><td>R</td><td>Number of rejected messages since statistics reset.</td></tr>
<tr><td>Frame No.</td><td>UDINT</td><td>R</td><td>Send counter (revolving).</td></tr>
<tr><td>Channel State</td><td>USINT</td><td>R</td><td>Current state of Channel 1.
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>0</td><td>No message on the state of channel 1.</td></tr>
<tr><td>1</td><td>Channel 1 OK.</td></tr>
<tr><td>2</td><td>The last message was faulty, the current one is OK.</td></tr>
<tr><td>3</td><td>Error on Channel 1.</td></tr>
</table></td></tr>
<tr><td>Last Channel Latency</td><td>UDINT</td><td>R</td><td rowspan="9">Channel Latency specifies the delay between two redundant transport paths and the reception time of messages with identical SeqNo.
A statistic is kept specifying the average, minimum, maximum and last latency.
If the minimum value is greater that the maximum value, the statistics values are invalid.
The values of Last Channel Latency and Avg. Channel Latency are then 0.</td></tr>
<tr><td>Last Latency of Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Max. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Maximum Latency of Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Min. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Minimum Latency of Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Avg. Channel Latency</td><td>UDINT</td><td>R</td></tr>
<tr><td>Average Latency of Redundant Channel</td><td>UDINT</td><td>R</td></tr>
<tr><td>Monotony</td><td>UDINT</td><td>R</td><td>User data send counter (revolving).</td></tr>
<tr><td>Quality Channel 1</td><td>BYTE</td><td>R</td><td>Quality of the main transport path.
<table>
<tr><th>Bit no.</th><th>Bit = 0</th><th>Bit = 1</th></tr>
<tr><td>0</td><td>Transport path not enabled</td><td>Transport path enabled.</td></tr>
<tr><td>1</td><td>Transport path not used</td><td>Transport path actively used.</td></tr>
<tr><td>2</td><td>Transport path not connected</td><td>Transport path connected.</td></tr>
<tr><td>3</td><td>-</td><td>Transport path first provides message.</td></tr>
<tr><td>4 … 7</td><td>Reserved</td><td>Reserved.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Quality Channel 2</td><td>BYTE</td><td>R</td><td>Quality of the redundant transport path, see Quality of Channel 1 (main transport path).</td></tr>
<tr><td>Receive Timeout</td><td>UDINT</td><td>R</td><td>Time in milliseconds (ms) on controller1 within which a valid response must be received from controller2, see also Chapter 4.8.2.</td></tr>
<tr><td>Response Time</td><td>UDINT</td><td>R</td><td>Time in milliseconds (ms) until the acknowledgment of the last message is received by the sender.</td></tr>
<tr><td>Reset safeethernet Statistics</td><td>BYTE</td><td>W</td><td>In the user program, reset the statistical values for the communication connection (e.g., number of faulty messages, channel state, timestamp for the last fault on the red. channel [s], resends).
<table>
<tr><th>Value</th><th>Function</th></tr>
<tr><td>0</td><td>No reset.</td></tr>
<tr><td>1 … 255</td><td>Reset the safeethernet statistics.</td></tr>
</table></td></tr>
<tr><td>Signatur N</td><td>UDINT</td><td>R</td><td>Changing the safeethernetconfiguration results in a dual configuration.
Old signature of the safeethernet configuration.</td></tr>
<tr><td>Signatur N+1</td><td>UDINT</td><td>R</td><td>New signature of the safeethernetconfiguration.</td></tr>
<tr><td>Transmission Control for Channel 1</td><td>BYTE</td><td>W</td><td>Transmission control of channel 1.
<table>
<tr><th>Bit 0</th><th>Function</th></tr>
<tr><td>FALSE</td><td>Transport path enabled.</td></tr>
<tr><td>TRUE</td><td>Transport path locked.</td></tr>
</table>
<table>
<tr><th>Bit 1</th><th>Function</th></tr>
<tr><td>FALSE</td><td>Transport path enabled for tests.</td></tr>
<tr><td>TRUE</td><td>Transport path locked.</td></tr>
</table>
Bits 2...7 reserved.</td></tr>
<tr><td>Transmission Control for Channel 2</td><td>BYTE</td><td>W</td><td>Transmission control of channel 2, see Transmission Control for Channel 1.</td></tr>
<tr><td>Connection Control</td><td>WORD</td><td>W</td><td>Use this system variable to control the safeethernet connection from within the user program.
<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>AUTOCONNECT (0x0000)</td><td>Default value:
After a safeethernet communication loss, the controller attempts to re-establish the connection in the following CPU cycle.</td></tr>
<tr><td>Toggle Mode 0(0x0100) Toggle Mode 1(0x0101)</td><td>After a communication loss, the user program can change the toggle mode to re-establish the connection.
▪ TOGGLE MODE 0 (0x100) set: Set to TOGGLE MODE 1 (0x101) to re-establish the connection.
▪ TOGGLE MODE 1 (0x101) set: Set to TOGGLE MODE 0 (0x100) to re-establish the connection.</td></tr>
<tr><td>Disabled (0x8000)</td><td>safeethernet communication is disabled.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Name</th><th>Data type</th><th>R/W</th><th>Description</th></tr>
<tr><td>Connection State</td><td>UINT</td><td>R</td><td>The connection state evaluates the status of the communication between two controllers from within the user program.
<table>
<tr><th>Status/Value</th><th>Description</th></tr>
<tr><td>Closed (0)</td><td>The connection is closed and no attempt is made to open it.</td></tr>
<tr><td>Try_open (1)</td><td>An attempt is made to open the connection, but it is still closed. This state applies for both the active and the passive sides.</td></tr>
<tr><td>Connected (2)</td><td>The connection is established and functioning (active time monitoring and data exchange)</td></tr>
</table></td></tr>
<tr><td>Reload State</td><td>UINT</td><td>R</td><td>Reload state of this safeethernet connection, see also status of Reload in Chapter 4.11.1.
unknown 0x0000
up-to-date 0x0001
updated 0x0002
outdated 0x0003</td></tr>
<tr><td>Resends</td><td>UDINT</td><td>R</td><td>Number of resends since statistics reset [UDINT].</td></tr>
<tr><td>Timestamp of Last Fault on Red. Channel [ms]</td><td>UDINT</td><td>R</td><td>Millisecond fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp of Last Fault on Red. Channel [s]</td><td>UDINT</td><td>R</td><td>Second fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp of Last Error [ms]</td><td>UDINT</td><td>R</td><td>Millisecond fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp of Last Error [ms]</td><td>UDINT</td><td>R</td><td>Second fraction of the timestamp (current system time).</td></tr>
<tr><td>Redundant Channel State</td><td>USINT</td><td>R</td><td>Current state of channel 2.
It is the current state of channel 2 when a message with Seq. no. X is being received (Seq. no X-1).
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>0</td><td>No message on the state of channel 2.</td></tr>
<tr><td>1</td><td>Channel 2 OK.</td></tr>
<tr><td>2</td><td>The last message was faulty, the current one is OK.</td></tr>
<tr><td>3</td><td>Error on channel 2.</td></tr>
</table></td></tr>
</table>

Table 38: System Variables Tab in the safe**ethernet** Editor

4.6.3.2 The *Fragment Definitions* Tab

The *Fragment Definitions* tab contains the statuses and parameters of the fragments sent by the opposite controller.

The refresh rate of the received fragments from all connected controllers required for this controller (or X-OPC Server) can be set here. The priority setting is primarily intended for the X-OPC Server, which processes a large volume of data from various controllers.

<table>
<tr><th>Name</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.</td></tr>
<tr><td>Fragment Definition</td><td>-</td><td>-</td><td>The Priority column is used to define how often this fragment should be received compared to the other fragments.
A fragment in the HIMax, HIQuad X and HIMatrix is ≤ 1100 bytes.
Default setting: Priority 1.
Range of values: Priority 1 (highest) to 65535 (lowest).</td></tr>
<tr><td>Fragment Version State</td><td>UINT</td><td>R</td><td>Reload version state of this safeethernet fragment, see also the Reload status in Chapter 4.11.1.
unknown: 0x0000
up-to-date 0x0001
updated 0x0002
outdated 0x0003</td></tr>
<tr><td>Timestamp [ms]</td><td>UDINT</td><td>R</td><td>Millisecond fraction of the timestamp (current system time).</td></tr>
<tr><td>Timestamp [s]</td><td>UDINT</td><td>R</td><td>Second fraction of the timestamp (current system time).</td></tr>
<tr><td>Fragment State</td><td>UINT</td><td>R</td><td>
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>0</td><td>CLOSED: Connection is closed.</td></tr>
<tr><td>1</td><td>TRY_OPEN: An attempt is made to open the connection, but it is still closed.</td></tr>
<tr><td>2</td><td>CONNECTED: The connection exists and the current fragment data has been received (cf. timestamp). As long as no fragment data has been received, the fragment state is set to TRY_OPEN while the connection is being established.</td></tr>
</table>
The connection state of the safeethernet Editor is set to CONNECTED as soon as the connection is open. Unlike the Fragment state, no data needs to have been exchanged yet.
</td></tr>
</table>

Table 39: The Fragment Definitions Tab

4.7 Network Structures for safeethernet Connections

This chapter lists a number of combinations for safeethernet connections.

i To reduce security risks, HIMA recommends setting up a safety network via the CPU modules and a separate standard network via the COM modules. The standard network is used to connect to non-safety components such as X-OPC Server.

Logically, a safe**ethernet** connection is always a connection between two HIMA systems that can be configured as 1-channel or 2-channel.
The Ethernet interfaces available for a safe**ethernet** connection are always displayed related to the resource for which the safe**ethernet** Editor was opened.
All Ethernet interfaces available for a controller are shown in the drop-down menu for the respective **IF Channel**... parameter.

Element	Description
IF Channel 1 (local)	Ethernet interface of the resource for which the safe**ethernet** Editor has been opened.
IF Channel 2 (local)	
IF Channel 1 (remote)	Ethernet interface of the partner resource
IF Channel 2 (remote)	

Table 40: Available Ethernet Interfaces

i When designing the network structure and calculating the maximum latency, HIMA recommends consulting a network expert.
A faulty network structure can cause a part of or the entire HIMA system to shut down.
In accordance with the generally accepted regulations for developing Ethernet networks, no network loop may occur. Data packets may only reach a controller over a single path.

4.7.1 Mono safe**ethernet** Connection (Channel 1)

For a mono connection, configure the Ethernet interfaces *IF Channel 1 (local)* and *IF Channel 1 (remote)* within the connection. Remove any automatically entered *IF Channel 2.*

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	safeethernet Connection	0	Resource (remote)	31.0.0 (172.16.1.31:6010)	None	30.0.0 (172.16.1.30:6010)	None
2	safeethernet Connection_RIO	0	HIMatrix F3 DIO 20/8 02_1	31.0.0 (172.16.1.31:6010)		31.200.0 (172.16.1.200:6010)	

Figure 8: safe**ethernet** Overview of the Example in Figure 9

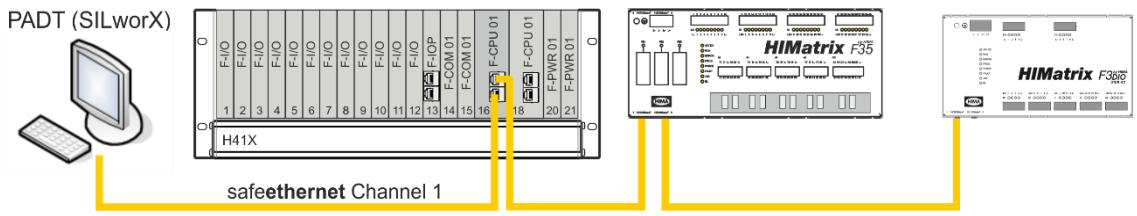


Figure 9: Mono safeethernet Connection (Channel 1)

All HIMA systems programmed with SILworX are suitable for mono safe**ethernet** connection.

4.7.2 Redundant safe**ethernet** Connection (Channel 1 and Channel 2)

Redundant safe**ethernet** transport paths between two HIMA controllers are possible.
For a redundant connection, the following Ethernet interfaces can be used:

- Ethernet interfaces *IF Channel 1 (local)* and *IF Channel 1 (remote)* for channel 1.
- Ethernet interfaces *IF Channel 2 (local)* and *IF Channel 2 (remote)* for channel 2.

i The redundant transport paths must be sufficiently homogeneous to ensure that the bandwidth and the delay on the two transport paths are nearly identical.
Once the offset of the received messages becomes too large or the messages arrive delayed by more than the response time, the diagnostic function for the transport path no longer operates as intended and considers these delays as a fault of the transport path.
To evaluate the transport path diagnostics, refer to the system variables *State of the Red. Channel* and *Channel State*.

4.7.2.1 Redundant safe**ethernet** Connection to Multiple Systems

A redundant connection to two separate logical and physical transmission paths (channel 1 and channel 2) can be established with HIMA controllers. To allow all three controllers to exchange safe**ethernet** data with one another, at least one safe**ethernet** connection each must be configured between them. In the safe**ethernet** overview, this looks similar to the one in the following figures.

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	HIMax <-> HIMatrix	0	HIMatrix	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)	35.0.0 (172.16.1.31:6010)	35.0.1 (172.16.1.32:6010)
2	HIMax <-> HIQuad X	0	HIQuad X	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)

Figure 10: HIMax Resource: safe**ethernet** Overview of the Example in Figure 12

	Name	ID	Partner	IF Channel 1 (local)	IF Channel 2 (local)	IF Channel 1 (remote)	IF Channel 2 (remote)
1	HIMax <-> HIQuad X	0	HIMax	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)	100.0.3 (172.16.1.100:6010)	100.0.4 (172.16.1.101:6010)
2	HIQuad X <-> HIMatrix	0	HIMatrix	41.1.16 (172.16.1.40:6010)	41.1.18 (172.16.1.41:6010)	35.0.0 (172.16.1.31:6010)	35.0.1 (172.16.1.32:6010)
3	HIQuad X <-> Remote IO	0	HIMatrix F3 DIO 20/8 02_1	41.1.16 (172.16.1.40:6010)		41.200.0 (172.16.1.200:6010)	

Figure 11: HIQuad X Resource: safe**ethernet** Overview of the Example in Figure 12

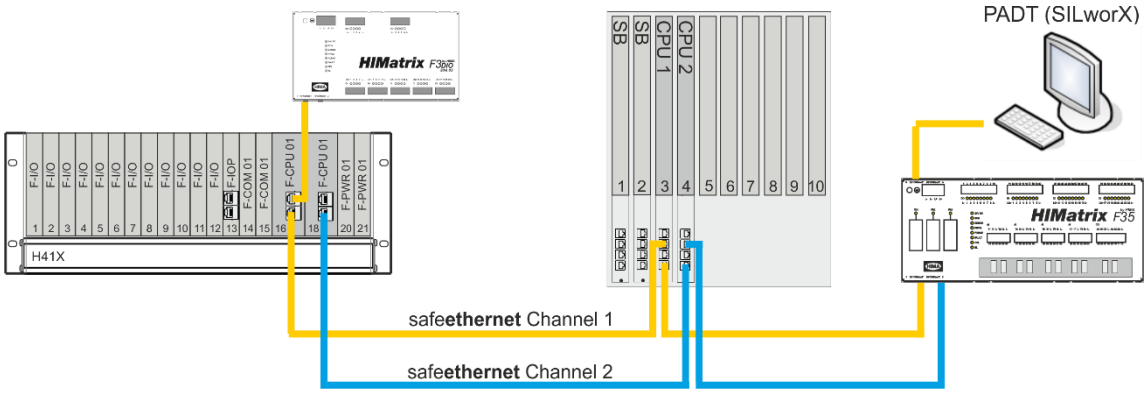


Figure 12: Parallel safe**ethernet** Redundancy

If HIMatrix controllers are used, the switch ports are separated from one another via VLAN, see Chapter 4.6.3.4. Remote I/Os are not suitable for parallel safe**ethernet** connection.

4.7.2.2 Redundancy via safe**ethernet** Ring

A redundant connection in accordance with IEC 62439-3 is also possible with a ring topology. In a ring network, data packet transmission is doubled, i.e., in both directions. Even if the transmission path is interrupted at any point in the safe**ethernet** ring, transmission is ensured.

The safe**ethernet** connection must be established via a ring switch in the ring topology. To this end, a suitable switch with ring management must be used.

In a safe**ethernet** ring, HIMax, HIQuad X and HIMatrix can be interconnected. These controllers only use one IP address each for safe**ethernet** communication.

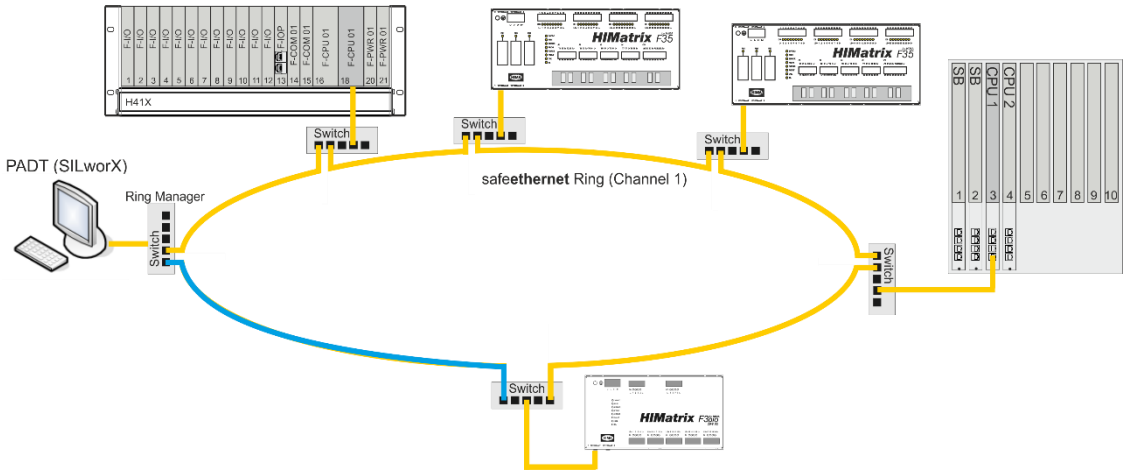


Figure 13: safe**ethernet** Ring Topology

i Contact HIMA technical support for recommended switches and media converters!

4.8 safeethernet Parameters

Safety-related communication is configured in the safe**ethernet** Editor. The parameters described in this chapter must be set.

For determining the *Receive Timeout* and *Response Time* safe**ethernet** parameters, the following condition applies:

The communication time slice must be sufficiently high to allow all the safe**ethernet** connections to be processed within one CPU cycle, see Chapter 7.1.

4.8.1 Calculating a Suitable Watchdog Time (Max. Cycle Time)

A conservative calculation of the watchdog time for the system in use (HIMax, HIMatrix or HIQuad X) is described in the safety manual for the respective controller.

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

In the following cases, contact HIMA technical support:

- If the prerequisites for the strategy described in the safety manual for determining the watchdog time cannot be complied with.
- If the result is not satisfying.

HIMA systems allow settings that ensure an even better performance. In-depth knowledge in several areas is required to identify these settings.

4.8.2 Receive Timeout

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

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

For safety-related functions implemented via safe**ethernet** , *Use Initial Value* is the only setting which may be used.

Since *Receive Timeout* is a safety-relevant component of the worst case response time TR (see Chapter 4.9.1 et seqq.), its value must be determined as described below and entered in the safe**ethernet** Editor.

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

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

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

i The availability of the safe**ethernet** communication can be increased by incrementing the *Receive Timeout* value (e.g., by doubling it), provided that the configured time is still sufficient to perform the safety-related function (worst case response time).

The plant manufacturer and the operator are responsible for ensuring that the safe**ethernet** connection complies at least with the following condition: Receive Timeout ≥ 2*Response Time.

4.8.3 Response Time

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

When configuring parameters using a safe**ethernet** profile, the Response Time expected to result from the physical circumstances of the transmission path must be set.

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

Response Time ≤ Receive Timeout / n

n = 2, 3, 4, 5, 6, 7, 8 …

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

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

[2.5*Max. Cycle Time + 2*Delay] ≤ **Min. Response Time** ≤ [Receive Timeout / 2]

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

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

i It must be ensured that the transport path complies with the configured *Response Time*!

If this cannot always be ensured, a corresponding safe**ethernet** connection system variable for monitoring the *Response Time* is available. If the configured *Response Time* is frequently exceeded, HIMA urgently recommends increasing the its value.

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

The plant manufacturer and the operator are responsible for ensuring that the safeethernet connection complies at least with the following condition: *Receive Timeout* ≥ *2*Response Time*.

4.8.4 Sync/Async

Sync	Function is not currently supported.
Async	This is the default setting. If Async is set, data is received by the safe**ethernet** protocol instance during the CPU input phase and are sent during the CPU output phase in accordance with the sending rules.

4.8.5 Resend Timeout

Resend Timeout cannot be set manually, but it is calculated based on the profile and *Response Time*.

Monitoring time expressed in milliseconds (ms) and set in controller 1, within which controller 2 must have acknowledged the receipt of a data packet; upon expiration of this period, the data packet is sent again.

Automatic calculation in accordance with the following rule:
Resend Timeout ≤ Receive Timeout

If the *Resend Timeout* set in the communication partners differ, the active protocol partner (with the lowest system ID) determines the *Resend Timeout* for the protocol connection.

4.8.6 Acknowledge Timeout

Acknowledge Timeout cannot be set manually, but it is calculated based on the profile and Response Time.

Acknowledge Timeout is the time period within which the CPU must acknowledge the receipt of a data packet.

In a rapid network, *Acknowledge Timeout* is zero, i.e., the receipt of a data packet is acknowledged immediately. In a slow network (e.g., a telephone modem line), *Acknowledge Timeout* is greater than zero. In this case, the system attempts to transmit the acknowledgment message together with the process data to reduce the network load by avoiding addressing and security blocks.

Automatic calculation in accordance with the following rules:

- **Acknowledge Timeout must be ≤ Receive Timeout.**
- **Acknowledge Timeout must be ≤ Resend Timeout if Production Rate > Resend Timeout.**

4.8.7 Production Rate

Production Rate cannot be set manually, but it is calculated based on the profile and *Response Time*.

Minimum time interval in milliseconds (ms) between two data packets.

The *Production Rate* is used to limit the volume of data packets and prevent a (slow) communication channel from being overloaded. This ensures a uniform load of the transmission medium and prevents the receiver from receiving obsolete data.

Automatic calculation in accordance with the following rules:

- **Production Rate ≤ Receive Timeout**
- **Production Rate ≤ Resend Timeout, if Acknowledge Timeout > Resend Timeout.**

i A zero production rate means that data packets are transferred in every user program cycle.

4.8.8 Queue

Queue cannot be set manually, but it is calculated based on the profile and *Response Time*.

Queue is the number of data packets that can be sent with no need to wait for their acknowledgement. The value depends on the network's transfer capacity and potential network delays.

All safeethernet connections share the available message queue space in the CPU.

4.9 Worst Case Response Time for safeethernet

In the examples from Chapter 4.9.3 on, the formulas for calculating the worst case response time only apply for a connection to HIMatrix controllers if the parameter Safety Time = 2 * Watchdog Time is set. These formulas always apply to HIMaxand HIQuad X controllers.

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

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

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

Table 41: safe**ethernet** Parameter Description and Conditions

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

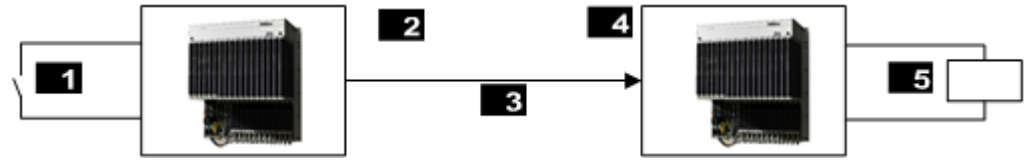
- The signals transmitted over safe**ethernet** must be processed in the corresponding controllers within one CPU cycle.
- The response times of the sensors and the actuators must also be added up.

The calculations also apply to signals in the opposite direction.

i HIMA systems allow settings that ensure an even better performance. In-depth knowledge in several areas is required to identify these settings.

4.9.1 Worst Case Response Time of 2 HIMax 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 HIMax controller 1
3 Safety-related protocol
4 HIMax controller 2
5 Output

Figure 14: Response Time with Interconnection of 2 HIMax Controllers

$T_R = t_1 + t_2 + t_3$

T_R: Worst case response time.

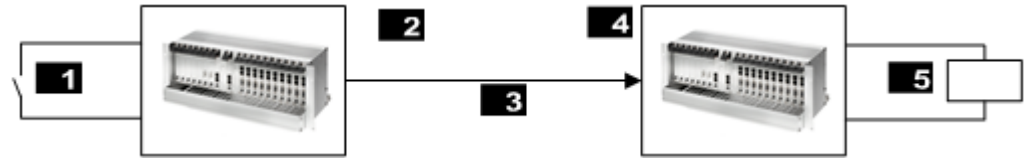
t_1: Safety time of HIMax controller 1.

t_2: Receive timeout.

t_3: Safety time of HIMax controller 2.

4.9.2 Worst Case Response Time of 2 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 15: Response Time with Interconnection of 2 HIQuad X Controllers

$T_R = t_1 + t_2 + t_3$

T_R: Worst case response time.

t_1: Safety time of HIQuad X controller 1.

t_2: Receive timeout.

t_3: Safety time of HIQuad X controller 2.

4.9.3 Worst Case Response Time of 1 HIMax Connected to 1 HIMatrix Controller

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

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

Figure 16: Response Time for a HIMax Connected to a HIMatrix Controller

$T_R = t_1 + t_2 + t_3$

T_R: Worst case response time.

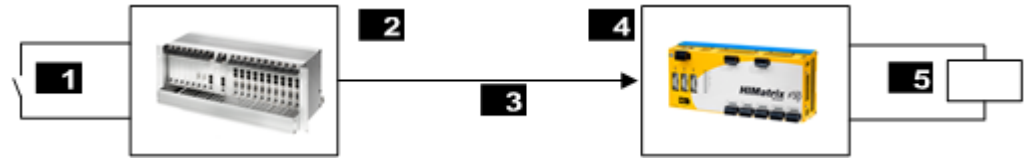
t_1: Safety time of the HIMax controller.

t_2: Receive timeout.

t_3: 2 * watchdog time of the HIMatrix controller.

4.9.4 Worst Case Response Time of 1 HIQuad X Connected to 1 HIMatrix Controller

The worst case response time TR 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 the HIMatrix controller. It is calculated as follows:



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

Figure 17: Response Time for a HIQuad X Connected to a HIMatrix Controller

$T_R = t_1 + t_2 + t_3$

T_R: Worst case response time.

t_1: Safety time of the HIQuad X controller.

t_2: Receive timeout.

t_3: 2 * watchdog time of the HIMatrix controller.

4.9.5 Worst Case Response Time of 1 HIMax Connected to 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 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 HIMax controller
4 Remote I/O 2
5 Output

Figure 18: Response Time with 2 Remote I/Os and 1 HIMax Controller

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

T_R: Worst case response time.

t_1: 2 * watchdog rime of remote I/O 1.

t_2: Receive timeout1

t_3: 2 * watchdog time of the HIMax controller.

t_4: Receive timeout2

t_5: 2 * watchdog time of 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.

4.9.6 Worst Case Response Time of 1 HIMatrix Connected to 2 HIMax Controllers

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

1 Input
2 HIMax controller 1
3 HIMatrix controller
4 HIMax controller 2
5 Output

Figure 19: Response Time with 2 HIMax Controllers and 1 HIMatrix Controller

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

T_R: Worst case response time.
t_1: Safety time of HIMax controller 1.
t_2: Receive timeout1
t_3: 2 * watchdog time of the HIMatrix controller.
t_4: Receive timeout2
t_5: Safety time of HIMax controller 2.

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

4.9.7 Worst Case Response Time of 2 HIMatrix Controllers

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

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

Figure 20: Response Time with Interconnection of 2 HIMatrix Controllers

$$T_R = t_1 + t_2 + t_3$$

T_R: Worst case response time.
t_1: 2 * watchdog time of the HIMatrix controller 1.
t_2: Receive timeout.
t_3: 2 * watchdog time of the HIMatrix controller 2.

4.9.8 Worst Case Response Time of 1 HIMatrix Controller connected to 2 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 of the second HIMatrix controller or remote I/O (out). It is calculated as follows:

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

Figure 21: Response Time with Remote I/Os

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

T_R: Worst case response time.
t_1: 2 * watchdog rime of remote I/O 1.
t_2: Receive timeout1.
t_3: 2 * watchdog time of the HIMatrix controller.
t_4: Receive timeout2.
t_5: 2 * watchdog time of remote I/O 2.

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

4.10 safe**ethernet Profile**

safe**ethernet** profiles are combinations of parameters compatible with one another that are automatically set when one of the safe**ethernet** profiles is selected.
When configuring, only the receive timeout and the expected response time parameters must be set individually.
A safe**ethernet** profile is used to optimize the data throughput in a network in light of the physical circumstances.

To ensure that the optimization is effective, the following conditions must be met:

- The communication time slice value must be sufficiently large to allow all the safe**ethernet** connections to be processed within one CPU cycle.
- Average CPU cycle time < response time.
- Average CPU cycle time < ProdRate or ProdRate = 0.

i Unsuitable combinations of CPU cycle, communication time slice, response time and production rate are not rejected during code generation and download/reload. However, these combinations can cause communication disturbances up to and including a failure of the safe**ethernet** communication.

In the Control Panels of the two controllers, verify the *Faulty Messages* and *Resends* values.

6 safe**ethernet** profiles are available. The safe**ethernet** profile most suitable for the transmission path can be selected from these.

For a safe**ethernet** connection with high availability, HIMA recommends using the *Fast&Noisy*, *Medium&Noisy* or *Slow&Noisy* profile.

Fast & Cleanroom	Only recommended for network free from interference.
Fast & Noisy	Recommended for high availability of the safe**ethernet** connection.
Medium & Cleanroom	Only recommended for network free from interference.
Medium & Noisy	Recommended for high availability of the safe**ethernet** connection.
Slow & Cleanroom	Only recommended for network free from interference.
Slow & Noisy	Recommended for high availability of the safe**ethernet** connection.
Fixed	Starting with V4, a modified calculation applies to all Cleanroom profiles. If a project created with a SILworX version prior to V4 should be converted, the configured profile must be set to Fixed to ensure that the CRC does not change.

4.10.1 Profile I (Fast&Cleanroom)

i For a safe**ethernet** connection with high availability, HIMA recommends using the *Fast&Noisy*, *Medium&Noisy* or *Slow&Noisy* profile.
The use of the Cleanroom profile is only recommended for networks free from interference, see Chapter 4.2.

Use

The *Fast&Cleanroom* profile is suitable for applications in ideal environments such as laboratories!

- For the fastest data throughput.
- For applications that require fast data transmission.
- For application that require a worst case response time as low as possible.

Network requirements:

- Fast: 100 Mbit technology (100Base Tx), 1 Gbit technology.
- Clean: Noise-free network.
  Data loss due to network overload, external influences or network manipulation must be prevented.
- LAN switches are necessary!

Communication path characteristics:

- Minimum delays.
- Expected Response Time ≤ Receive Timeout
  (otherwise ERROR during configuration).

4.10.2 Profile II (Fast & Noisy)

Use

The *Fast&Noisy* profile is the SILworX standard profile for communicating via safe**ethernet**.

- For fast data throughput.
- For applications that require fast data transmission.
- For applications that require a worst case response time as low as possible.

Network requirements:

- Fast: 100 Mbit technology (100Base Tx), 1 Gbit technology.
- Noisy: Interference within the network.
  Low probability of data packet loss. Time for ≥ 1 resend(s).
- LAN switches are necessary!

Communication path characteristics:

- Minimum delays.
- Expected Response Time ≤ Receive Timeout / 2
  (otherwise ERROR during configuration).

4.10.3 Profile III (Medium&Cleanroom)

i For a safe**ethernet** connection with high availability, HIMA recommends using the *Fast&Noisy*, *Medium&Noisy* or *Slow&Noisy* profile.
The use of the Cleanroom profile is only recommended for networks free from interference, see Chapter 4.2.

Use

The *Medium&Cleanroom* profile is only suitable for applications in a network free from interference and requiring a moderately fast data transmission rate.

- For medium data throughput.
- Suitable for VPN (virtual private networks) in which data is exchanged slowly, but without faults since intermediate safety devices (e.g., firewalls, encryption) are used.
- Suitable for applications in which the worst case response time is not a critical factor.

Network requirements

- Medium: 10 Mbit (10BASE-T), 100 Mbit (100BASE-Tx), 1 Gbit technology.
- LAN switches are necessary!
- Clean: Noise-free network.
  Data loss due to network overload, external influences or network manipulation must be prevented; time for ≥ 0 resends.

Communication path characteristics

- Moderate delays.
- Expected Response Time ≤ Receive Timeout (otherwise ERROR during configuration).

4.10.4 Profile IV (Medium&Noisy)

Use

The *Medium&Noisy* profile is suitable for applications that require moderate fast data transmission.

- For medium data throughput.
- For applications that require moderate fast data transmission.
- Suitable for applications in which the worst case response time is not a critical factor.

Network requirements

- Medium: 10 Mbit (10BASE-T), 100 Mbit (100BASE-Tx), 1 Gbit technology.
- LAN switches are necessary!
- Noisy: Interference within the network.
  Low probability of data packet loss. Time for ≥ 1 resend(s).

Communication path characteristics

- Moderate delays.
- Expected Response Time ≤ Receive Timeout / 2 (otherwise ERROR during configuration).

4.10.5 Profile V (Slow&Cleanroom)

i For a safe**ethernet** connection with high availability, HIMA recommends using the *Fast&Noisy*, *Medium&Noisy* or *Slow&Noisy* profile.
The use of the Cleanroom profile is only recommended for networks free from interference, see Chapter 4.2.

Use

The *Slow&Cleanroom* profile is suitable for applications in a network free from interference and requiring a slow data transmission rate.

- For slow data throughput.
- For applications that only require a slow data transmission rate to controllers (potentially located far away) or if the communication path conditions cannot be defined in advance.

Network requirements

- Slow: Data transmission via ISDN, dedicated line or radio relay.
- Clean: Network free from interference.
  Data loss due to network overload, external influences or network manipulation must be prevented; time for ≥ 0 resends.

Communication path characteristics

- Moderate delays.
- Expected Response Time = Receive Timeout (otherwise ERROR during configuration)

4.10.6 Profile VI (Slow&Noisy)

Use

The *Slow&Noisy* profile is suitable for applications that only require a slow data transmission rate to the controllers (potentially located far away).

- For slow data throughput.
- Generally for applications and data transfer via bad telephone lines or disturbed radio relays.

Network requirements

- Slow: Data transmission via telephone, satellite, radio etc.
- Noisy: Interference within the network.
  Low probability of data packet loss. Time for ≥ 1 resend(s).

Communication path characteristics

- Moderate to significant delays.
- Expected Response Time ≤ Receive Timeout / 2 (otherwise ERROR during configuration).

4.11 Control Panel (safe**ethernet**)

The Control Panel can be used to verify the safe**ethernet** connection settings. It also displays details about the current status of the safe**ethernet** connection (e.g., cycle time, bus state, etc.).

To open Control Panel for monitoring the safeethernet connection

1. In the structure tree, select Resource.
2. Select Online from the resource context menu.
3. In the **System Log-in** window, enter the access data to open the Control Panel for the resource.
4. In the structure tree associated with the Control Panel, select safe**ethernet** .

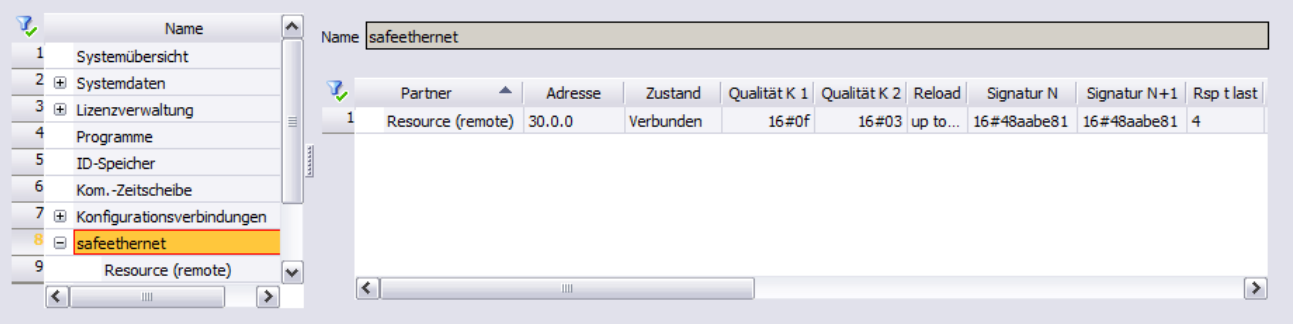


Figure 22: Control Panel for safeethernet Connection Overview

To reset the statistical data of the safeethernet connection

This context menu function is used to reset the statistical data (e.g., min./max. cycle time etc.) to zero.

1. Select safeethernet connection in the structure tree.
2. In the context menu of the safeethernet connection, select Reset safe**ethernet** Statistics.

4.11.1 View Box (safe**ethernet** Connection)

The view box displays the following values of the selected safe**ethernet** connection.

Element	Description
Partner	Resource name of the communication partner
Address	System ID
State	State of the safe**ethernet** connection. (See also Chapter 4.6).
Quality Ch 1	Quality of transport path, Channel 1. (See also Chapter 4.6).
Quality Ch 2	Quality of transport path, Channel 2. (See also Chapter 4.6).

Element	Description
Reload	safeethernet reload status unknown: State of the loaded partner signatures is unknown: - There is no connection. - The partner has an old operating system without the safe**ethernet** reload function. updated: The current code has been loaded into this controller; it still has to be loaded into the partner. outdated: The current code has been loaded into the partner; it still has to be loaded into this controller. up-to-date: Both partners have an identical N+1 signature.
Signature N	Changing the safe**ethernet** configuration results in a dual configuration. Old signature of the safe**ethernet** configuration.
Signature N+1	New signature of the safe**ethernet** configuration.
Rsp t last	Actual response time as minimum, maximum, last and average value. See also Chapter 4.8.3.
Rsp t avg	
Rsp t min	
Rsp t max	
Error	Bad Messages Number of rejected messages since statistics reset.
Rsnd	Number of resends since statistics reset.
Succeeded	Number of successful connections since statistics reset.
Early	Early Queue Usage Number of early messages since statistics reset. Early messages are stored in the Early Queue.
Frame	Frame No. Revolving send counter.
Ack Frame	Ack.Frame No. Revolving receive counter.
Monotony	Revolving user data send counter
Receive Timeout	Receive Timeout [ms] (See also Chapter 4.8.2)
Resend Timeout	Resend timeout [ms] (See also Chapter 4.8.5)
Acknowledgment Timeout	Acknowledge Timeout [ms] (See also Chapter 4.8.6)
Conn Ctrl	Connection Control
Ctrl Ch 1	Transmission Control for Channel 1 (See also Chapter 4.6).
Ctrl Ch 2	Transmission Control for Channel 2 (See also Chapter 4.6).
Protocol	0-1: Protocol version for ELOP II Factory resources. 2: Protocol version for SILworX resources.

Table 42: View Box of the safe**ethernet** Connection

4.12 safeethernet Reload

Thanks to this feature, changes performed to a safe**ethernet** configuration can be loaded during operation by performing a reload to the controller while the safeethernet connection continues to run with no interruptions.

4.12.1 Requirements

safe**ethernet** reload is possible for HIMax, HIMatrix and HIQuad X. The following system requirements apply to all controllers participating in safe**ethernet** the connection:

- HIMax as of CPU OS V6 and COM OS V6.
- HIQuad X ab CPU BS V10 und COM BS V10.
- HIMatrix as of CPU OS V10 and COM OS V15.

The above-mentioned COM OS versions or higher are required to ensure that safe**ethernet** connections are properly routed via the COM module, see Chapter 4.12.7.

In the properties of the safe**ethernet** connection, set the *Codegen* parameter to V6 and higher.

i If a redundant module is available, the operating systems of HIMax modules can be updated during operation. This ensures that the conversion to safe**ethernet** reload is performed without interruptions, even in HIMax plants using previous operating systems.

4.12.2 Technical Concept

The safe**ethernet** signature is a CRC code used to uniquely identify the safe**ethernet** configuration. The safe**ethernet** signature is created during the code generation and is part of the loaded configuration.

safe**ethernet** communication between 2 communication partners can only occur if both partners have the same safe**ethernet** configuration with identical signature.

To use reload to perform changes to a safe**ethernet** connection, the controller must be provided with 2 safe**ethernet** configurations and corresponding signatures (N and N+1). This is supported for SILworX as of V6.

In the two controllers, configuration I1 is connected to a safe**ethernet** signature

After changing the connection and reload for controller 1, configurations I1 and I2 are available. The previous safe**ethernet** configuration I1 with signature N is still active in Controller1.

Changing the safe**ethernet** configuration results in a dual configuration (in the example: I1+I2). The safe**ethernet** reload state of Controller1 is `updated` and the version state of Controller2 is `outdated`, which signalizes that a reload must be performed in Controller2.

1) safe**ethernet** version state, see Chapter 4.12.5

Upon completion of the reload process for controller 2, the new safe**ethernet** configuration I2 is active with signature N+1. The dual configuration (I1+I2) is now available for both controllers and should be deleted as recommended by performing an additional reload, see Chapter 4.12.3.1.

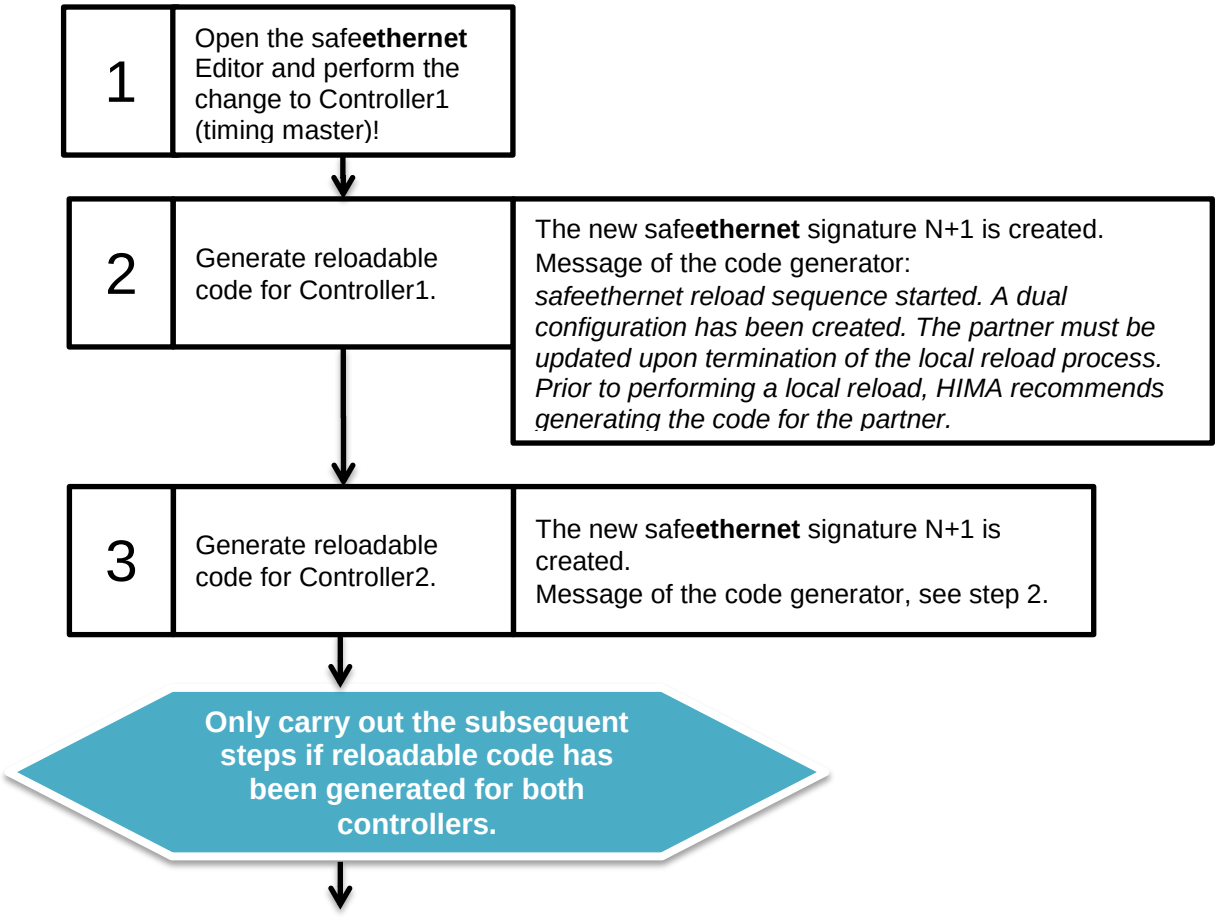
1) safe**ethernet** version state, see Chapter 4.12.5

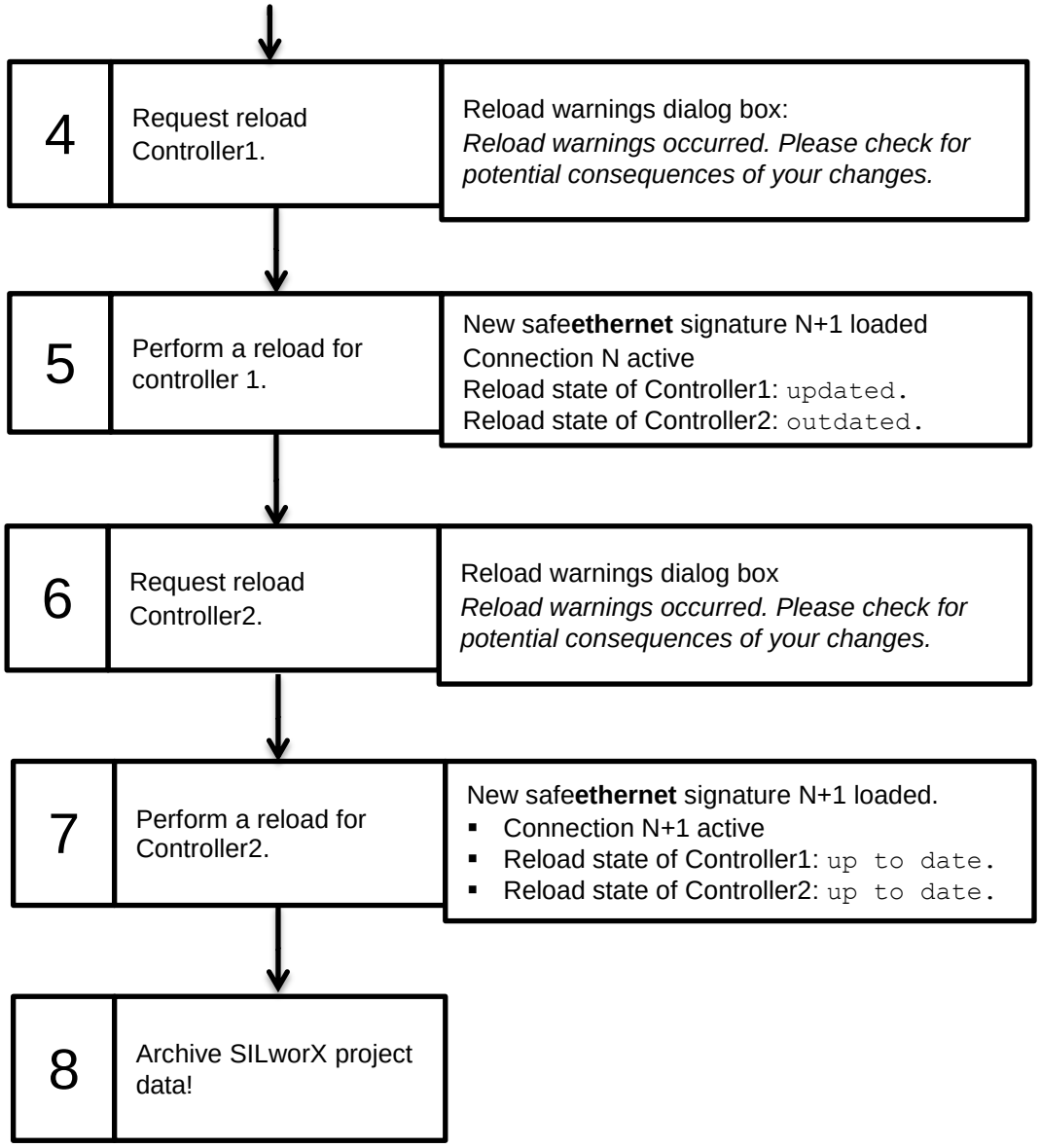
i With respect to reload, HIMA recommends always starting the process for the controller that is configured as Timing Master of the safeethernet connection. The new safeethernet connection becomes active after the reload procedure is complete for both controllers.

4.12.3 Procedure to Be Observed

safe**ethernet** connections are to be considered holistically, i.e., changes should always be performed on both partners and in direct succession to ensure the consistency of the safe**ethernet** .

The previous safe**ethernet** configuration is active up to step 5. The new safe**ethernet** configuration becomes active after a successful reload in step 5.




4
Request reload Controller1.
Reload warnings dialog box:
Reload warnings occurred. Please check for potential consequences of your changes.
5
Perform a reload for controller 1.
New safe**ethernet** signature N+1 loaded
Connection N active
Reload state of Controller1: updated.
Reload state of Controller2: outdated.
6
Request reload Controller2.
Reload warnings dialog box
Reload warnings occurred. Please check for potential consequences of your changes.
7
Perform a reload for Controller2.
New safe**ethernet** signature N+1 loaded.
Connection N+1 active
Reload state of Controller1: up to date.
Reload state of Controller2: up to date.
8
Archive SILworX project data!

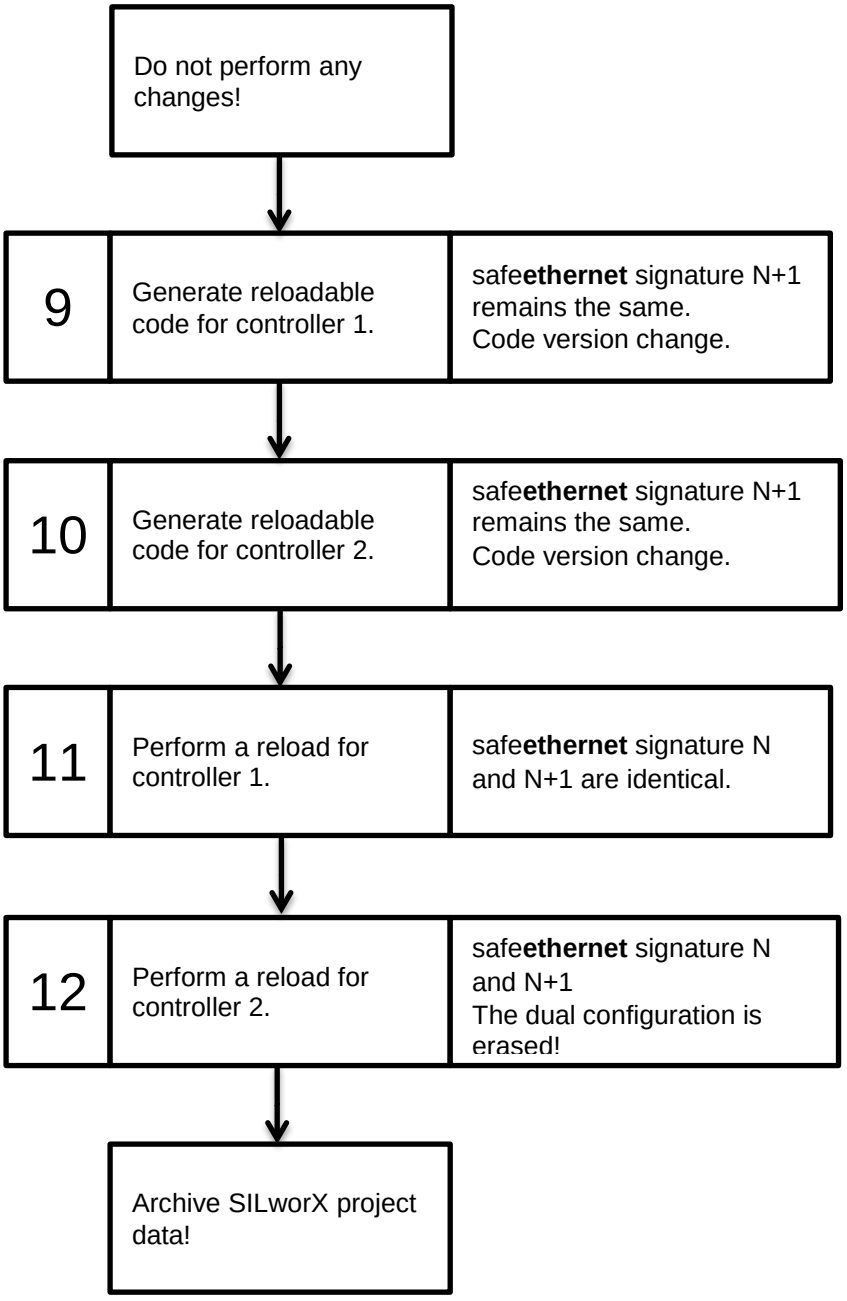
4.12.3.1 Align Signatures N and N+1

Changes to the safe**ethernet** configuration such as described in Chapter 4.12.3 result in a dual configuration. The controllers contain the following 2 configurations:

- The previous configuration with safe**ethernet** signature N through which safe**ethernet** communication is running, remains active until both controllers have been updated.
- The new configuration with safe**ethernet** signature N+1 through which safe**ethernet** communication is running, becomes active after both controllers have been updated.

i After completion of an additional code generation with no safe**ethernet** change, the dual configuration is deleted. This means that the same CRC code is set in the *Signature N* and *Signature N+1* system variables). HIMA recommends always erasing the dual configuration. This must be performed for both resources.

To erase a dual configuration, perform steps 9 through 12 as described below!



4.12.4 Integrated Protective Mechanisms

The protective mechanisms integrated in SILworX and in the controller's operating system ensure early detection of unintended interruption or resumption of a safe**ethernet** connection and generate a warning message.

4.12.4.1 Automatic Test during Code Generation

The following table contains the messages output during a code generation and connected to safe**ethernet** reload, informing the user about the current safe**ethernet** reload state.

Information in the code generator dialog	Description
Reload Warning *safeethernet reload sequence started. A dual configuration has been created. The partner must be updated upon termination of the local reload process. Prior to performing a local reload, HIMA recommends generating the code for the partner.*	**Procedure OK!** This information is provided after a change performed to the safe**ethernet** connection and the code generation! Follow the recommended procedure, see Chapter 4.12.2.
Reload Info *Dual configuration safeethernet reload for connection of "safeethernet V1" to "controller2" has been removed.*	**Procedure OK!** A reload has been performed after completion of a new code generation without any safeethernet change. The dual configuration has been erased, i.e., there is once again only one configuration with one safe**ethernet** signature, see Chapter 4.12.3.1.
The safeethernet connection of "safeethernet V1" to "controller2" could be interrupted. Please update this partner. No matching connection version could be found in the partner's download configuration.	**Caution!** Do not perform any reload to ensure that the connection will not be interrupted! Please contact HIMA technical support! With the partner controller, there is no longer a common configuration with identical signature so that no safe**ethernet** reload can be performed.

Table 43: Messages from the Code Generator

4.12.4.2 Automatic Test during the Controller's Reload

Warning messages are only issued before a safe**ethernet** reload if suitable CPU operating systems are loaded in the controllers.

- HIMax CPU OS as of V6.
- HIQuad X ab CPU BS V10.
- HIMatrix CPU OS as of V10.

Prior to performing a reload, the operating system checks the safe**ethernet** reload state to ensure that is suitable for a reload. If a controller detects that a reload could result in the interruption of the safe**ethernet** connection, it generates a corresponding warning message displayed in SILworX. In this scenario, reload can be aborted by the user. After an aborted reload, the controllers continue to operate with the last suitable safe**ethernet** configuration.

Information in the Dialog Box	Description
A reload is to be performed although a safeethernet connection reports the safeethernet reload state updated, partner's safeethernet address: x/x/x. The connection might be lost by activating the configuration. Check for potential consequences.	**Caution!** Do not perform a reload. Please contact HIMA technical support! If reload is performed anyway, the safe**ethernet** connection may be interrupted!
A reload is to be performed although a safeethernet connection reports the safeethernet reload state unknown (i.e., no connection exists to the partner), partner's safeethernet address: x/x/x. If a connection is established before the configuration has been activated, the configuration activation could cause the connection to be lost again. Check for potential consequences.	**Caution!** The unknown safe**ethernet** reload state is reported, if a safe**ethernet** connection is interrupted, see Chapter 4.12.5. Prior to performing a new reload, check the physical connection, e.g., if all the Ethernet cables are properly plugged in.

Table 44: Messages from the Operating System

4.12.5 safe**ethernet** Reload State

The reload state provides information on the current state of the safe**ethernet** connection and about whether suitable safe**ethernet** configurations are loaded or are to be loaded. The consistent procedure applied to safe**ethernet** reload is a requirement for ensuring that the reload status is properly displayed, see Chapter 4.12.3.

The following safe**ethernet** reload state is displayed:

unknown	State of the loaded partner signatures is unknown: ▪ There is no connection. ▪ The partner has an old operating system without the safe**ethernet** reload function.
updated	The current code has been loaded into this controller; it still has to be loaded into the partner.
outdated	The current code has been loaded into the partner; it still has to be loaded into this controller.
up-to-date	Both partners have an identical N+1 signature.

If no suitable configuration is available after a reload, a warning is issued informing the user that the reload can be aborted.

If, however, the reload process is continued in spite of the warning messages described in Chapter 4.12.4, a suitable configuration might no longer be present in the partner controller. The safe**ethernet** connection to the partner controller could be interrupted (CLOSED)!

The safe**ethernet** version state is called Reload in the SILworX Online View of the safeethernet connection. The same information is provided by the *Version State* system variable, which can be assigned a global variable and used as such in the user program.

4.12.6 Maximum Number of safe**ethernet** Connections during Reload

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

The maximum number of simultaneous safe**ethernet** connections during reload is as follows:

- HIMax = 300 (max. 255 safe**ethernet** connections + 45 (reload buffer)).
- HIMatrix = 277 (max. 255 safe**ethernet** connections + 22 (reload buffer)).
- HIQuad X = 150 (max. 128 safe**ethernet** connections + 22 (reload buffer)).

These limits are defined to restrict the maximum storage space required during a reload.

i If during the reload code generation, the maximum number of safe**ethernet** connections allowed for reload is exceeded, the reload code generation is aborted and an error message is issued.
For the maximum number of safe**ethernet** connections between two controllers refer to Chapter 4.3.

If multiple changes are required, these must be performed through multiple consecutive reloads.

4.12.7 safe**ethernet** Connection via the Communication Module

HIMA recommends setting the *Code Generation* parameter of the communication module to V6 and higher to prevent, as far as possible, a cold reload of the communication module. In doing so, the safeethernet connections routed through this communication module are not interrupted, even if changes are performed to variables or parameters, e.g., profiles.

For further details on the safe**ethernet** reload behavior in connection with the communication module and additional changes, refer to the following Chapter 4.12.8.

4.12.8 Changes to the safe**ethernet** Configuration

The following table provides an overview of the changes to the safe**ethernet** configuration and their effects on the safe**ethernet** reload.

Changes to	CPU	COM
To add or delete global variables for:		
safeethernet	•	•
X-OPC (DA)	•	•
X-OPC (events)	•	•
To change the number of views (X-OPC).	•	•
To add or delete a new safe**ethernet** connection.	•	•[1)]
safe**ethernet** parameters (e.g., *Timing Master*, *Receive Timeout*).	•	•
IP addresses (changed transport path).	•	•[1)]
safe**ethernet** parameter (*Profile*).	-	n. a.
safe**ethernet** parameter (*Behavior on Connection Loss*).	-	n. a.

- safe**ethernet** reload possible.
- safe**ethernet** reload not possible.

n.a.: not applicable

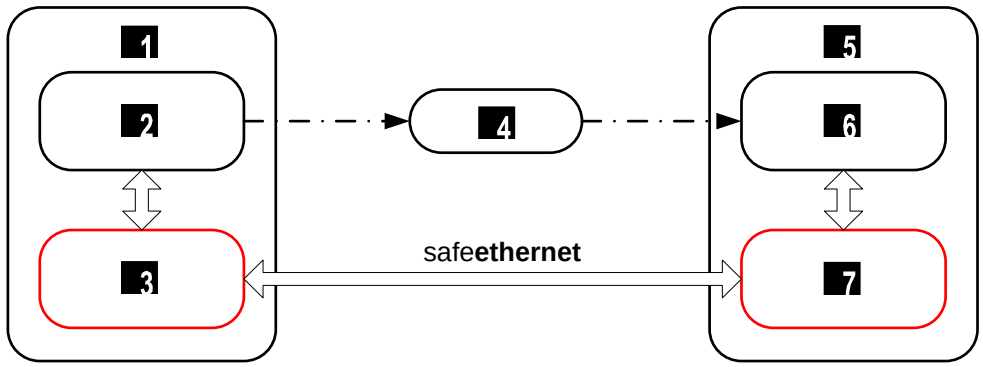
[1)] Only in connection with *Cold Reload*, i.e., with stopped communication module.

Table 45: safe**ethernet** Reload after Changes

4.13 Cross-Project Communication

Cross-project safety-related communication is used to connect resources from various projects.

The connection between the two projects is established via proxy resource. A proxy resource substitutes a resource from the other project.



1 Project A
2 Resource A
3 Proxy resource B
4 Configuration file
5 Project B
6 Resource B
7 Proxy resource A

Figure 23: safe**ethernet** Connection Between Resource A in Project A and Resource B in Project B

In project A, the safe**ethernet** connection is configured and the configuration file is created and archived.

In project B, the configuration file is restored. Proxy resource A is automatically created with the data of resource A from project A.

4.13.1 Configuration in SILworX

An example is given to illustrate the basic procedure. The names used for the projects, configurations and resources are only examples.

For clarity, configuration A and configuration B are created in both SILworX projects.

Project A

- Configuration A
  - Resource A
- Configuration B
  - Resource B (as proxy)
- Global Variables

Project B

- Configuration B
  - Resource B
- Configuration A
  - Resource A (as proxy)
- Global variables (Global variables can be created by restoring an archive or importing an Excel list.)

4.13.1.1 Creating Configuration B in Project A

Create a separate configuration B for proxy resource B in project A.

To create configuration B

1. Open project A in which configuration B should be created.
2. Right-click **Project A**, and then select **New**, **Configuration**.
   ☑ A new configuration (Configuration B) is created.

4.13.1.2 Creating Proxy Resource B in Project A

Proxy resource B serves as placeholder for a resource from an external project B and is used for configuring the process data exchange via safe**ethernet** .

To create Proxy Resource B

1. Right-click **Configuration B**, and select **New**, **Proxy Resource** SILworX.
   ☑ A new proxy resource (Proxy Resource B) is created.

To configure Proxy Resource B

1. Right-click Proxy Resource B, and select **Properties**.
2. Enter a unique name in the **Name** field.
   Use the name of resource B in project B for proxy resource B in project A.
3. Read the **System ID** from project B and enter it in proxy resource B.
4. Click **OK** to confirm.

To open the structure tree for Proxy Resource B

1. Right-click **Hardware** and select **Edit**.
2. Select the resource type used in project B:
   - **HIMatrix 03 proxy**
   - HIMatrix proxy
   - HIMax system proxy
   - H41X system proxy
   - H51X system proxy
3. Click **OK** to confirm. The Hardware Editor for proxy resource B appears.
4. For proxy HIMatrix 03, successively double-click the CPU and COM module to be used for establishing the redundant connection to proxy resource B.

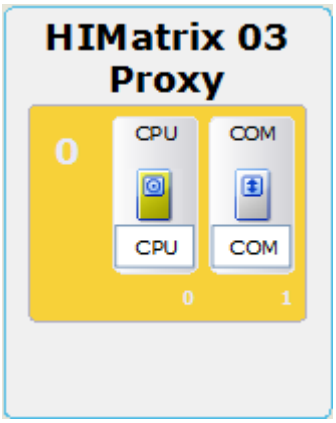


Figure 24: HIMatrix Proxy Resource

5. Enter the IP addresses and click **Save**.
6. Repeat these steps for every further proxy resource in project A.

4.13.1.3 Creating and Archiving Global Variables for safeethernet Connection

To create global variables for the safeethernet connection

1. Right-click **Project A**, and then select **New**, **Global Variables**.
   ☑ The Global Variables structure tree object is created at project level.
2. Right click **Global Variables**, and select **Edit** from the context menu to open the Variable Editor.
3. Right click a free space within the workspace of the Variable Editor and select **New Global Variable** from the context menu to create a new global variable.
4. Repeat these steps for each additional new global variable for the safe**ethernet** connection.
5. Additionally, create the global variables *Connection State*, *Quality Channel 1* (and possibly *Quality Channel 2* for redundant connections). Create each system variable twice, once from the perspective of resource A and once from the perspective of resource B.

To archive the global variables

TIP If at project level the *Global Variable* object already exists in project B, the SILworX function for importing or exporting contents as CSV can be used as an option. With the appropriate filter settings, the required global variables can be exported selectively, refer to the online help for more details.
Even with multiple proxy connections to various projects, export is more useful than archiving. In such a case, for each variable, enter a connection ID in the Additional Comment field.

1. In the structure tree, select **Project A**, **Global Variables**.
2. Select **Archive** from the context menu. The SILworX dialog box to archive an object appears.
3. In the dialog box, enter an archive name for the global variables object. The archive is saved with the ***.A3** file extension in the selected archive folder.
   ☑ The archived Global Variables object contains all the global variables created at project-level in project A.

4.13.1.4 Creating a Connection between Resource A and Proxy Resource B.

In the safe**ethernet** Editor, create a safe**ethernet** connection between resource A and proxy resource B.

To open the safeethernet Editor for Resource A

1. In the structure tree, select **Configuration A**, **Resource A**, safe**ethernet** .
2. Right-click safe**ethernet** , then select Edit.
   ☑ The new proxy resource B is created in the Object Panel.

To create the safeethernet connection to the proxy resource

1. Drag Proxy Resource B from the Object Panel onto a free space within the workspace of the safe**ethernet** Editor.
   Select an appropriate name for this connection, immediately.
2. Select proper Ethernet interfaces **IF Chx** of the resource and proxy resource.

4.13.1.5 Connecting Process Variables

Add the process variables in the editor of the safe**ethernet** connection.

To open the connection editor

The safe**ethernet** Editor of resource A is open.

1. Right-click the Proxy Resource B row and open the context menu.
2. Select Edit from the context menu to open the connection editor of the safe**ethernet** connection.
3. Select the Resource A<->Proxy Resource B tab.
4. In the Object Panel, select a **Global Variable** and drag it onto the **Resource A --> Resource B (Proxy)** area or onto the **Resource B (Proxy) --> Resource A** area depending on the selected transport direction.
5. Repeat this step for further variables.

4.13.1.6 Connecting System Variables

Connect the system variables Connection State, *Quality Channel 1* (and possibly *Quality Channel 2* for redundant connections) with global variables. For further information on the system variables, see Chapter 4.6.3.1.

To open the connection editor

The safe**ethernet** Editor of resource A is open.

1. Right-click the **Proxy Resource** row and open the context menu.
2. Select **Edit** from the context menu to open the connection editor of the safe**ethernet** connection.
3. Select the **System Variables** subtab in the **Resource A** tab.
4. In the Object Panel, select a suitable **Global Variable** for this system variable and drag it onto the **Global Variable** column.
5. Repeat this step for additional system variables.
6. Select the **System Variables** subtab in the **Resource B** tab.
7. In the Object Panel, select a suitable **Global Variable** for this system variable and drag it onto the **Global Variable** column.
8. Repeat this step for additional system variables.

4.13.1.7 Archiving the safe**ethernet** connection in Project A

The safeethernet connection configured in project A must be archived and then restored in project B.

To verify the safe**ethernet** connection

1. In the structure tree of **Project A**, select safe**ethernet** and open the context menu.
2. Select **Verification** from the context menu, and click **OK** to confirm.
3. Thoroughly verify the messages contained in the logbook and correct potential errors.

To archive the safeethernet connection

1. In the structure tree of **Project A**, select safe**ethernet** and open the context menu.
2. Select **Archive** from the context menu. The dialog box to archive an object appears.
3. In the dialog box, enter an archive name for the safeethernet object. The archive is saved with the ***.A3** file extension in the selected archive folder.
   ☑ All the safe**ethernet** connections contained in the safe**ethernet** object are now archived. safe**ethernet** connections can also be archived individually.
4. Close project A.

i The configuration of the safe**ethernet** connection must be recompiled with the user program of the resource and transferred to the controller. The new configuration can only be used for communicating with the controller upon completion of this step.

4.13.2 Configuration A in Project B

Create a separate Configuration A for proxy resource A in project B.

Project B is configured in SILworX like the first project. The resource from the first project is now the proxy resource.

4.13.2.1 Creating Proxy Resource A in Project B

Proxy resource A serves as placeholder for Resource A from an external project A and is used for exchanging process data via safeethernet.

To create a proxy resource

1. Open project B in which Proxy resource A should be created.
2. Right-click **Project B**, and then select **New**, **Configuration**.
   ☑ A new configuration (configuration A) is created.
3. Right-click **Configuration A**, and select **New**, **Proxy Resource** SILworX.
   ☑ A new proxy resource (proxy resource A) is created.

To configure a proxy resource

1. Right-click Proxy Resource A, and select **Properties**.
2. Enter a unique name in the **Name** field.
   Use the name of resource A in project A for proxy resource A in project B.
3. Read the **System ID** from project A and enter it in proxy resource A.
4. Click **OK** to confirm.

To open the structure tree for the proxy resource

1. Right-click **Hardware** and select **Edit**.
2. Select the resource type that is used in the first project:
   - H41X System proxy
   - H51X System proxy
   - HIMatrix 03 proxy
   - HIMatrix proxy
   - **HIMax system proxy**
3. Click **OK** to confirm. The Hardware Editor for the proxy resource appears.
4. Select **Generic Module** for HIMax system proxy and drag it to the base module on the proper slot, that is corresponding to the slot of the CPU / COM in the project A.

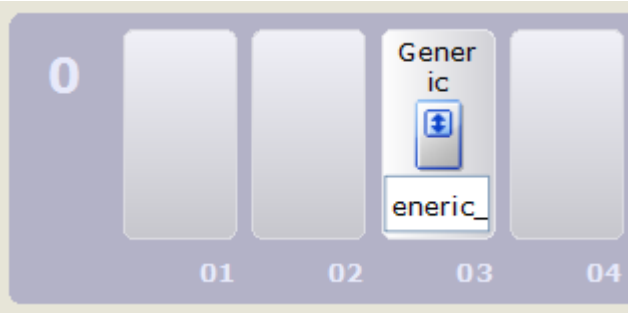


Figure 25: HIMax Proxy Resource

5. Double-click **Generic Module**, and enter the IP Address of the CPU and/or COM modules.
6. Click **Save**.
7. Repeat these steps for every further proxy resource in project B.

4.13.2.2 Creating Global Variables for safe**ethernet** Connection

The same global variables as in the first project must be created in project B.

TIP If at project level the Global Variable object already exists, the SILworX function for importing or exporting contents as CSV can be used as an option, see the online help.

To restore global variables in Project B

1. Right-click **Project**, and select **Restore** from the context menu.
   ☑ The SILworX dialog box to restore an object appears.
2. Open the archive folder and select the archived *Global Variables* object with the ***.A3** file extension that was previously created in project A.
   ☑ The restored global variables object contains all the global variables archived in project A.

4.13.2.3 Restoring the safe**ethernet** connection in Project B

To restore the safeethernet connection in Project B

1. Right-click **Project**, and select **Restore** from the context menu.
   ☑ The SILworX dialog box to restore an object appears.
2. Open the archive folder and select the archived safe**ethernet** object with the ***.A3** file extension that was previously created in project A.
   ☑ The restored safe**ethernet** object contains all the connections between resource A and proxy resource B in project B, including all assigned variables, process and system variables.

5 SNTP Protocol

The SNTP (Simple Network Time Protocol) is a simplified version of the NTP (Network Time Protocol).

The SNTP protocol is used by the SNTP server to synchronize the time of the SNTP clients via Ethernet.

HIMA systems can be configured and used as SNTP server and/or as SNTP client. The SNTP standard in accordance with RFC 2030 (SNTP V4) applies with the limitation that only the unicast mode is supported.

5.1 Equipment and System Requirements

Element	Description
Controller	HIMax HIQuad X HIMatrix
Activation	This function is activated by default in all HIMA systems.
Interface	Ethernet 10/100/1000BaseT

Table 46: Equipment and System Requirements for the SNTP Protocol

5.2 SNTP Client

To synchronize its time settings, the SNTP client only uses the SNTP server that is available and has the highest priority. If the priority is the same, the SNTP server that (randomly) first transmitted data to the SNTP client, is selected. This SNTP server is maintained until it is no longer available. Only then it is changed.

If the time difference is < 128 ms, the clock runs faster or slower by 0.5 ms per cycle until the time difference is compensated. If the time difference is ≥ 128 s, the clock is changed immediately.

For time synchronization, one SNTP client can be configured in each HIMA controller.

To create a new SNTP client

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**.
2. Right-click **Protocols**, then click **New**, **SNTP Client**.
   ☑ An SNTP server Info is added by default subordinate to the SNTP client.
3. Right-click the SNTP client, and click **Properties** and select the COM module.

The dialog box for the SNTP client contains the following parameters:

Element	Description
Type	SNTP client.
Name	Name for the SNTP client.
Module	Selection of the COM or processor module within which the protocol is processed.
Activate Max. µP Budget	Not taken into account by the operating system. Parameter was retained due to CRC and reload stability.
Max. µP Budget in [%]	Not taken into account by the operating system. Parameter was retained due to CRC and reload stability.
Description	Any unique description for the SNTP client.
Current SNTP version	The current SNTP version is displayed.

Element	Description
Reference stratum	The stratum of an SNTP client specifies the precision of its local time. The lowest the stratum, the more precise its local time. Zero means an unspecified or not available stratum (not valid). The SNTP server currently used by an SNTP client is the one that can be reached and has the highest priority. If the stratum of the current SNTP server is lower than the stratum of the SNTP client, the resource adopts the time of the current SNTP server. If the stratum of the current SNTP server is higher than the stratum of the SNTP client, the resource does not adopt the time of the current SNTP server. If the stratum of the current SNTP server is identical to the stratum of the SNTP client, two different cases result: ▪ If the SNTP client (resource) only operates as SNTP client, the resource adopts the time of the current SNTP server. ▪ If the SNTP client (resource) also operates as SNTP server, the resource adopts half the value of the time difference to the current SNTP server per SNTP client request (time adapts slowly). Range of values: 2…15 Default value: 15
Client Time Request Interval [s]	Time needed by the current SNTP server to perform time synchronization. The value set in the SNTP client for Client Time Request Interval must be greater than the timeout in the SNTP server. Range of values: 16…16384 s Default value: 16 s

Table 47: SNTP Client Properties

5.2.1 SNTP Server Info

The connection to the SNTP server (time server) is configured in the SNTP Server Info.

An SNTP server Info is subordinated to the SNTP client by default. A maximum of 4 SNTP Server Infos can be subordinated to an SNTP client.

i If several SNTP clients are configured in a HIMA system, only the (one) SNTP client whose active remote SNTP server has the highest priority may be used for time synchronization at any time.

To create a new SNTP Server Info

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**, **SNTP Client**.
2. Right-click **Protocols**, and then select **New**, **SNTP Server Info**.
   ☑ A new **SNTP Server Info** is created.

The dialog box for the SNTP Server Info contains the following parameters:

Element	Description
Type	SNTP Server Info
Name	Name for the SNTP server.
Description	Description for the SNTP server.
IP Address	IP address of the resource or PC in which the SNTP Server is configured. Default value: 0.0.0.0
SNTP Server Priority	Priority with which the SNTP client addresses this SNTP server. The SNTP servers configured for the SNTP client should have different priorities. Range of values: 0 (lowest priority) to 4294967295 (highest priority). Default value: 1
SNTP Server Timeout[s]	The timeout in the SNTP server must be set lower than the value for the *Time Request Interval* in the SNTP client. Range of values: 1…16384 s Default value: 1 s

Table 48: SNTP Server Info Properties

5.3 SNTP Server

The SNTP server on a HIMA system allows external systems to synchronize their date and time to the date and time of the HIMA system.

The SNTP server responds to SNTP requests when the system time is synchronized, otherwise SNTP requests are discarded.

The SNTP server of a HIMA system accepts the requests from an SNTP client (e.g., remote I/O) and sends its current time back to this SNTP client.

To create a new SNTP server

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**.
2. Right-click **Protocols**, and then select **New**, **SNTP Server**.
   ☑ A new SNTP server is created.
3. Right-click the SNTP server **Properties** and then select the **Module** used to connect the SNTP client.

The dialog box for the SNTP server contains the following parameters:

Element	Description
Type	SNTP Server
Name	Name of the SNTP server.
Module	Selection of the COM or processor module within which the protocol is processed.
Activate Max. µP Budget	Activated: Use the µP budget limit from the Max. µP Budget in [%] field. Deactivated: Do not use the µP budget limit for this protocol. Default value: Activated
Max. µP Budget in [%]	Maximum module's µP load that can be used for processing the protocol. Range of values: 1…100% Default value: 10%
Description	Description for the SNTP.
Current SNTP Version	The current SNTP version is displayed.
Stratum of Timeserver	The stratum of an SNTP server specifies the precision of its local time. The lowest the stratum, the more precise the local time. Zero means an unspecified or not available stratum (not valid). The value for the SNTP server stratum must be lower or equal to the stratum value of the requesting SNTP client. Otherwise, the SNTP client does not accept the SNTP server time. Range of values: 1…15 Default value: 14

Table 49: SNTP Server Properties

5.4 Configuration of Time Synchronization via SNTP

In the network structure shown, a HIMatrix is configured as SNTP server for time synchronization of the subordinate remote I/O. The HIMatrix is additionally configured as an SNTP client and gets the time synchronization from the network time server.

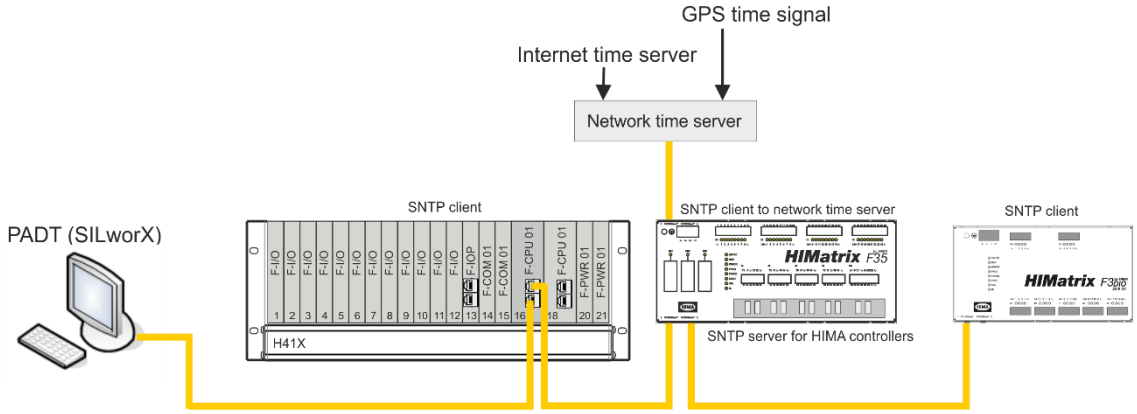


Figure 26: Time Synchronization of HIMA Systems via the SNTP Time Server

5.4.1 Creating an IP Connection to a Network Time Server

For time synchronization, one SNTP client can be configured in each resource.

To create a new SNTP client

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**.
2. Right-click **Protocols**, then click **New**, **SNTP Client**.
3. Right-click the SNTP client, click **Properties** and select the COM module connected with the PC.

   ☑ Standard reference stratum ‘15‘ can be retained if the COM module does not additionally function as an SNTP server.
   Rule: Value for the SNTP server stratum ≤ stratum value of the requesting SNTP client. Otherwise, the SNTP client does not accept the SNTP server time.

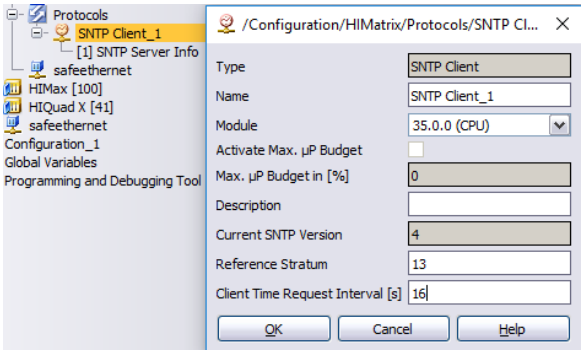


Figure 27: Configuring the SNTP Client for Time Synchronization

To configure the SNTP Server Info subordinate to the SNTP client

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**, **SNTP Client**.
2. Right-click **SNTP Server Info** and select **Properties** from the context menu.
3. In **Properties**, select the **IP Address** of the SNTP server (PC).

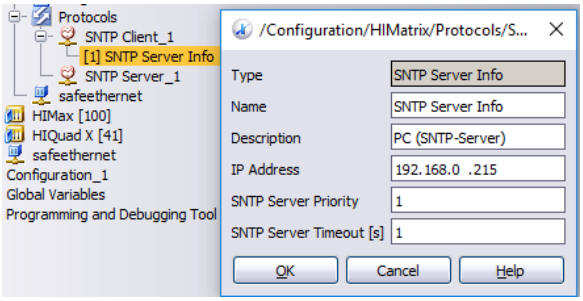


Figure 28: Configuring the IP Connection to the SNTP Server (PC)

5.4.2 SNTP Time Synchronization of a Remote I/O by a HIMA Resource

The remote I/O is synchronized via SNTP. To do so, an SNTP server must be created in the superordinate HIMA resource, whose time is synchronized via an Internet time server or a GPS clock.

To create an SNTP server for SNTP time synchronization

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**.
2. Right-click **Protocols**, and then select **New**, **SNTP Server**.
   ☑ A new SNTP server is created.
3. Right-click the SNTP server, click **Properties** and select the **Module** connected with the remote I/O. This has to be the identical module used for the safeethernet connection to the remote I/O. The stratum value must not exceed 14.

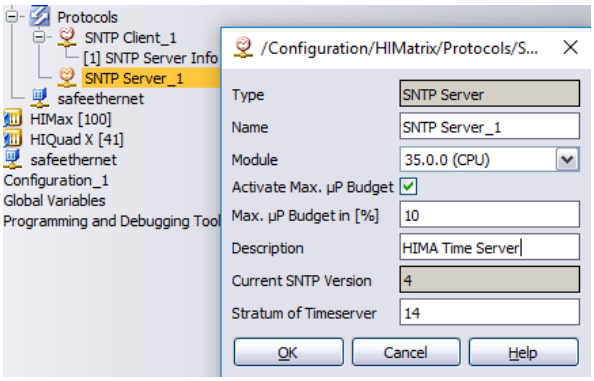


Figure 29: Creating an SNTP server for SNTP time synchronization

6 HART

The HART (Highway Addressable Remote Transducer) protocol allows digital fieldbus communication during which the HART signal is superimposed onto the (4…20 mA) analog current signal. The data rate of the HART protocol is 1200 bit/s. The HART signal is used to transfer measuring and device data of connected HART-capable sensors or actuators.

The X-HART 32 01 module establishes digital HART fieldbus communication between a maximum of 32 HART-capable field devices and the HIMax system.

The HART signal is used to transfer measuring and device data of connected HART-capable sensors or actuators. Within the system, the X-HART 32 01 module transmits the measuring and device data to the assigned X-COM 01 communication module. The X-COM 01 transfers the measuring and device data via the HART-IP protocol to an asset management system or a HART OPC Server.

i To reduce security risks, HIMA recommends preventing unauthorized changes to the HART field devices be implementing write-protection.

6.1 System Requirements

Equipment and system requirements for HART protocol:

Element	Description
Controller	HIMax with X-COM module and X-HART module.
X-CPU module	The Ethernet interfaces are not used for HART-IP. For setting the parameters on a per module basis: CPU operating system as of V5. For setting the parameters on a per channel basis: CPU operating system as of V11.
X-COM module	Ethernet 10/100BaseT are used for HART-IP. COM operating system as of V7.24.
X-HART 32 01	For setting the parameters on a per module basis: I/O operating system as of V5. For setting the parameters on a per channel basis: I/O operating system as of V7.48.
Analog module	Analog input or output module.
Activation	The HART-IP protocol is activated by default for HIMax systems.

Table 50: Equipment and System Requirements for the HART Protocol

6.1.1 HART Protocol Features

The HART hast the characteristics specified in the following table.

Properties	Description
Safety-related	No
Transfer rate	HART fieldbus communication: 1200 Bit/s. HART-IP via Ethernet: 100 Mbit/s full duplex.
Transport path	HART fieldbus communication 32-channel HART interface of the X-HART module. HART-IP via Ethernet Ethernet interfaces of the X-COM module. The Ethernet interfaces in use can simultaneously be employed for other protocols.
Max. number of X-HART modules	100 for each HIMax system. Based on dimensioning, refer to the system manual (HI 801 001 E).

Properties	Description
Max. number of I/O points	3200 for each HIMax system. Depending on the module type; in this case, for 100 analog modules with 32 inputs each.
Max. number of HART-IP protocol instances	1 for each X-COM module. 2 for each HIMax system (with 2 X-COM modules).
Max. number of HART-IP sessions via UDP	2 on each X-COM module.
Max. number of HART-IP sessions via TCP	2 on each X-COM module.

Table 51: HART Protocol Features

6.2 HART Communication for Safety-Related Applications

HART communication enables read and write access to the transmitters, including the option to change the transmitter configuration.

Since the HART-IP protocol was not developed in accordance with the requirements of IEC 61508, the data supplied via HART must not be used as a reliable source for safety-related functions.

However, the information provided via the HART protocol can be used within asset management systems, e.g., for diagnostics.

The safety-related analog values are processed in the HIMA safety-related controller and the HART data is processed in the asset management system (layers of protection in accordance with IEC 61511).

6.2.1 Safety Function

The safety function of HART communication via the HIMax system includes the following points:

- HART Deactivation: If the module is shut down, the HART channels are safely deactivated in accordance with SIL 3.
- HART Filtering: HART access to transmitters or sensors is locked in accordance with SIL 3.
- HART communication influences the analog metrological accuracy by 1 %. Further repercussions on the analog HIMax modules are excluded.
- HART parameter setting: The parameters of the X-HART module can be set on a per module basis for all 32 channels, or on a per channel basis for each individual channel.

⚠ WARNING

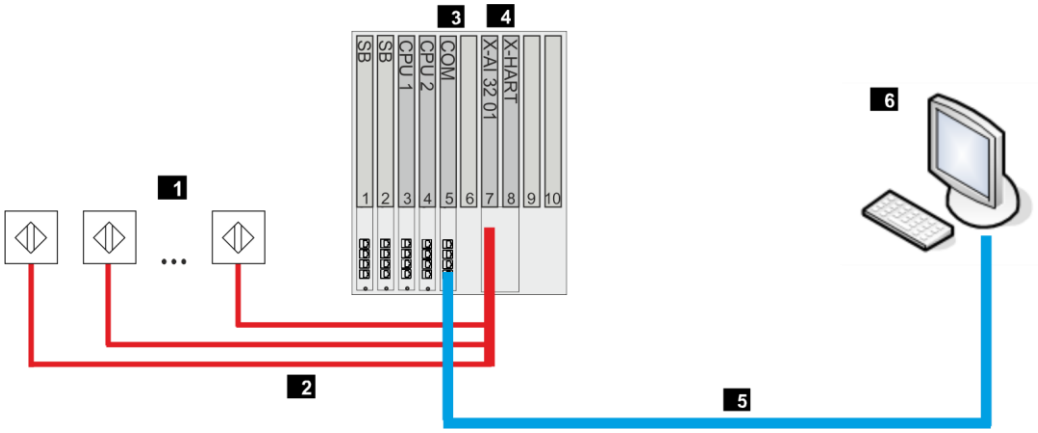
Manipulation of analog sensors and actuators!

If the HART filtering function is deactivated on the HART module, the corresponding analog sensor or actuator can be reprogrammed.

The operator is responsible for ensuring that the HART field devices used for the HART protocol are 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, see also Chapter 2.5.

6.3 Configuring a HART-IP Protocol Instance

This chapter provides an overview of the configuration of HART-IP instances and the interaction between HART field device, HIMax controller, engineering too and a HART OPC Server or FDT/DTM asset management system.



1 HART field device
2 HART via 4…20 mA
3 X-COM 01
4 X-HART 32 01 and analog I/O module
5 HART-IP (Ethernet)
6 HART OPC Server or FDT/DTM asset management system

Figure 30: Structure of the HART-IP Installation

6.3.1 HART OPC Server or FDT/DTM Asset Management System

A HART OPC Server or an FDT/DTM asset management system can be used to configure and monitor the HART field devices.

Supported asset management systems include:

- PACTWARE.
- FIELDCARE.
- Honeywell FDM.
- Yokogawa FieldMate.
- Other systems on request.

A suitable HART OPC Server can be obtained from the HART Foundation.

i The two device drivers *CommDTM* and *DeviceDTM* for the HIMax system can be obtained from HIMA.

6.3.2 HART Field Devices

The HART field devices must be connected to the analog input or output modules (e.g., X-AI 32 01, X-AO 16 01). If short-circuits or open-circuits occur, no HART communication is possible.

i HIMA recommends setting the polling address of all connected HART field devices to *zero*. The same sub-device address for each connected device is possible, since the HIMax system only provides one field device per HART channel (no multi-drop operation). The *search* for connected HART field devices starts with polling address *zero*. A device with an address of *zero* will be "found" fastest after a power-on.

6.3.3 Configuring the X-HART Module, X-COM Module and analog I/O Modules

The X-COM communication module and the assigned X-HART module form an I/O system in accordance with the HART specification.

The X-HART 32 01 module is a communication module with 32 channels. It is combined with an analog input or output module and connected through a connector board. The corresponding connector board occupies 2 slots for mono applications and 3 slots for redundant applications.

The HIMax modules are configured in the Hardware Editor of the SILworX programming tool.

To add the required modules in the Hardware Editor

1. In the structure tree, select **Configuration**, **Resource**, **Hardware**.
2. Right-click and select **Edit** from the context menu to open the Hardware Editor.
3. From the Object Panel, drag the modules **X-COM 01**, **X-AI 32 01** and **X-HART 32 01** to a suitable position on the base rack.

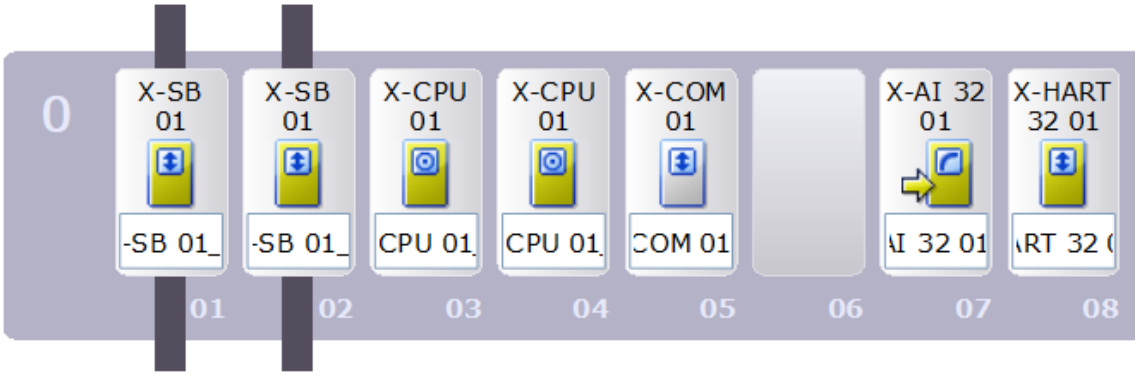


Figure 31: HART-IP Configuration in the SILworX Hardware Editor

6.3.3.1 X-AI 32 01 Analog Input Module

The X-AI 32 01 module is configured in the detail view of the Hardware Editor.

To open the detail view of the X-AI 32 01 module in the Hardware Editor

1. Right-click **X-AI 32 01** and select **Detail View** from the context menu.
   ☑ The detail view contains its own workspace, which sometimes includes additional tabs for configuring object parameters and analog inputs.

i For further information on how to configure the X-AI 32 01, refer to the corresponding manual (HI 801 021 E).

6.3.3.2 X-HART Module

The X-HART module is configured in the detail view of the Hardware Editor.

To open the detail view of the X-HART module in the Hardware Editor

1. Right-click **X-HART** and select **Detail View** from the context menu.
   ☑ The detail view contains its own workspace, which sometimes includes additional tabs for configuring object parameters.

Observe the following points when configuring the module:

- Configure the corresponding analog input or output module (e.g., X-AI 32 01).
- To diagnose the X-HART module and HART channels, the system parameters can be combined with global variables and evaluated within the user program.
- In case of analog output modules with redundant wiring, the Module Status parameter must be additionally taken into account, see the module-specific X-AO 16 01 manual (HI 801 111 E).

i For further information on how to configure the X-HART module, refer to the corresponding manual (HI 801 307 E).

6.3.3.3 Configuring the X-COM Module in the Detail View

The X-COM 01 module is configured in the detail view of the Hardware Editor.

To open the detail view of the X-COM 01 module in the Hardware Editor

1. Right-click **X-COM 01** and select **Detail View** from the context menu.
   ☑ The detail view contains its own workspace, which sometimes includes additional tabs for configuring object parameters.
2. Enter the **IP-Address** for connecting to the HART OPC Server or FDT/DTM asset management system.

i For further information on how to configure the X-COM 01, refer to the corresponding manual (HI 801 011 E).

6.3.4 Configuring the HART-IP Protocol Instance

The protocol and the required HIMax modules are configured in the SILworX programming tool.

To create a HART-IP protocol instance

1. In the structure tree, select **Configuration**, **Resource**, **Protocols**.
2. Select **New**, **HART-IP Protocol** from the context menu of protocols to add a new HART-IP protocol.
3. Right-click the HART protocol and select **Properties** of the **X-Com Module**.
   The default settings may be retained for the first configuration.

6.3.4.1 Properties

The Properties dialog box for the HART-IP protocol contains the following parameters:

Element	Description
Name	Name for the HART-IP protocol.
Module	Selection of the COM module within which the HART-IP protocol is processed.
Activate Max. µP Budget	Activated: Use the µP budget limit from the *Max. µP Budget in [%]* field. Deactivated: Do not use the µP budget limit for this protocol. Default value: Activated
Max. µP Budget in [%]	Maximum µP budget of the module that can be used for processing the protocols. Range of values: 1…100% Default value: 30%
Polling address	Polling address of X-COM Range of values: 0…63 Default value: 0
Use Standard HART TCP Port (5094)	Activated The TCP connection is enabled. Deactivated The TCP connection is disabled. Default value: Activated, TCP port 5094 is used.
Use Second HART TCP Port	Activated The TCP connection is enabled. Deactivated The TCP connection is disabled. Default value: Deactivated
Second HART TCP port	The second port number can be used as an alternative or in addition to the standard port. Range of values: 1…65535 Default value: 20004
Use Standard HART UDP Port (5094)	Activated The UDP connection is enabled. Deactivated The UDP connection is disabled. Default value: Activated, UDP port 5094 is used.
UseUse Second HART UDP Port	Activated The UDP connection is enabled. Deactivated The UDP connection is disabled. Default value: Deactivated
Second HART UDP port	The second port number can be used as an alternative or in addition to the standard port. Range of values: 1…65535 Default value: 20004

Table 52: HART-IP Protocol Properties

6.4 Online View of the X-COM Module

The settings for the HART protocol can be controlled and verified from within the online view of the X-COM module. Details about the current status of the field devices and X-COM module are displayed.

To open the online view of the Hardware Editor for the HART protocol:

1. Right-click the **Hardware** structure tree element and select **Online** from the context menu.
2. In the **System Login** window, enter the access data to open the online view for the hardware.
3. Double-click the **X-COM Module** and select the **HART Protocol** structure tree node.

6.4.1 View Box (HART Protocol)

The view box displays the following values of the selected HART protocol.

Element	Description
Name	Name for the HART-IP protocol.
Planned µP Budget [%]	Value displayed for the planned maximum µP budget of the X-COM module, which may be produced during the protocol's processing.
Current µP Budget [%]	Value displayed for the current µP budget of the X-COM module, which is being produced during the protocol's processing.
Polling Address	The polling address of X-COM is displayed. Range of values: 0…63
Unique COM Address	The 5-byte address of the X-COM (unique address) is displayed.
Standard HART TCP Port Number	The standard TCP port used for HART-IP is displayed online.
Second HART TCP Port Number	The TCP port additionally or alternatively used for HART-IP is displayed online.
Standard HART UDP Port Number	The standard UDP port used for HART-IP is displayed online.
Second HART UDP Port Number	The UDP port additionally or alternatively used for HART-IP is displayed online.
Number of HART Devices	The number of HART devices currently detected as connected is displayed. The X-COM 01, which is also a part of the HART configuration, is not included in this number.
Number of X-HART Modules	The number of X-HART 32 01 modules (I/O cards) detected and belonging to this X-COM 01 module is displayed.
Status Device Lock	It displays the device interlock status. The device interlock (interlock for the HART I/O subsystem) is triggered by the host through HART command 71. Range of values: See HCF_SPEC-183 (Common Tables) Table 25 Zero – The device is not locked Not equal to zero – Lock device status code Default value: 0
Device Lock through Host with IP	With the device interlock (device interlock status is not zero), this field displays the IP address of the host that triggered the interlock (i.e., which sent HART command 71). Range of values: IP address Default value: 0

Table 53: Online View of the HART Protocol

6.4.2 Online View of the Device List

To update the device list

1. In the structure tree, select **HART Protocol**, **Device List**.
2. Right-click and select **Update Device List**.

The **Device List** view box displays the following values.

Element	Description
Device Index	The device index is displayed online Range of values: 0…65535 (decimal, 2 bytes)
I/O Card Number	The I/O card number to which the device is connected is displayed online. Range of values: 0…249 (decimal, 1 byte) for connected devices. Value: 251 (None) for the X-COM itself.
Channel number	The channel number to which the device is connected is displayed online. Range of values: 1…31 (decimal, 1 byte) for connected devices, see Chapter 6.4.2.1. Range of values: 251 (None) for the X-COM itself.
Manufacturer ID	The ID of the device manufacturer is displayed online. Range of values: 0x00…0xFFFF (hexadecimal, 2 bytes)
Expanded Device Type Code	The expanded device type code of the device is displayed online. Range of values: 0x00…0xFFFF (hexadecimal 2 bytes)
Device ID	The ID of the device is displayed online. Range of values: 0x00 0x00 0x00…0xFF 0xFF 0xFF (hexadecimal 3 bytes)
HART Version	The HART version (Universal Command Revision Level) of the device is displayed online. Range of values 0…255 (decimal 1 byte)
Long Tag	The device long tag is displayed online. Range of values 32 characters (Latin-1)
Rack.Slot I/O Card	The I/O card slot (Rack.Slot) is displayed online. Format: Rack.Slot Range of values (Rack): 0…15 Range of values (Slot): 0…15
Telegram Counter STX	The telegram counter for the device's commands (Stx) is displayed online. Range of values 0…65535 (decimal 2 bytes revolving)
Telegram Counter ACK	The telegram counter for the device's acknowledgements (Ack) is displayed online. Range of values 0…65535 (decimal 2 bytes revolving)
Telegram Counter BACK	The telegram counter for the device's burst acknowledgements (Back) is displayed online. Range of values 0…65535 (decimal 2 bytes revolving)

Table 54: Online View of the Device List

6.4.2.1 HART Field Device Addressing

Channel number (X-HART 32 01 front plate)	Channel address (decimal)	Channel address (hexadecimal)
1…32	0…31	0x00…0x1f

Table 55: HART Field Device Addressing

The channel numbers displayed in the X-COM 01 online view correspond to the channel numbers specified on the front plate of the X-HART 32 01 module (channel count starting with 1).
If a connected HART field device is addressed, the following applies:
Channel address (channel number upon command 77) = channel number - 1.

Example:
Channel number = 15
The field device is addressed with channel address = 14 (0x0e).

7 General

This chapter describes parameters that are relevant for all communication protocols.

7.1 Maximum Communication Time Slice

The maximum communication time slice is the time period in milliseconds (ms) per CPU cycle assigned to the processor module for processing the communication tasks. Even if the protocol processing could not be completed within one communication time slice, the CPU still executes the safety-relevant monitoring for all protocols within one CPU cycle.

i If not all upcoming communication tasks can be processed within one CPU cycle, the whole communication data is transferred over multiple CPU cycles. The number of communication time slices is then greater than 1.

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

7.1.1 Determining the Maximum Duration of the Communication Time Slice

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

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

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

To determine the actual duration of the maximum communication time slice

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

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

7.2 Load Limitation

A computing time budget expressed in % (*µP budget*) can be defined for each communication protocol. It allows the available computing time to be distributed among the configured protocols. The sum of the computing time budgets configured for all communication protocols on a CPU or COM module may not exceed 100%.

The defined computing time budgets of the individual communication protocols are monitored. If a communication protocol has already achieved or exceeded its budget and no reserve computing time is available, the communication protocol cannot be processed.

If sufficient additional computing time is available, it is used to process the communication protocol that has already achieved or exceeded its budget. It can therefore happen that a communication protocol uses more computing time budget than has been allocated to it.

It is possible that more than 100% computing time budget is displayed online. This is not a fault; the computing time budget exceeding 100% indicates the additional computing time used.

i The additional computing time budget is not a guarantee for a certain communication protocol and can be revoked from the system at any time.

7.3 Configuring the Function Blocks

The fieldbus protocols and the corresponding function blocks operate on the COM module of the HIMA system. In the SILworX structure tree, these function blocks must therefore be created as child element of **Configuration**, **Resource**, **Protocols**.

To control the function blocks on the COM module, function blocks can be created in the SILworX user program (see Chapter 7.3.1). These can be used as standard function blocks.

Shared variables are used to connect the function blocks in the SILworX user program to the corresponding function blocks in the SILworX structure tree. These must have been previously created in the Global Variable Editor.

7.3.1 Purchasing Function Block Libraries

The function block libraries for PROFIBUS DP and TCP Send/Receive must be added to the project using the *Restore* function (context menu of the project).

The function block library is available from HIMA support upon request.

7.3.2 Configuring the Function Blocks in the User Program

Drag the required function blocks onto the user program. The inputs and outputs must be configured as described for the individual function block.

Upper part of the function block

The upper part of the function block corresponds to the user interface used by the user program to control the function block.

The variables used in the user program are connected at this level. The prefix A means Application.

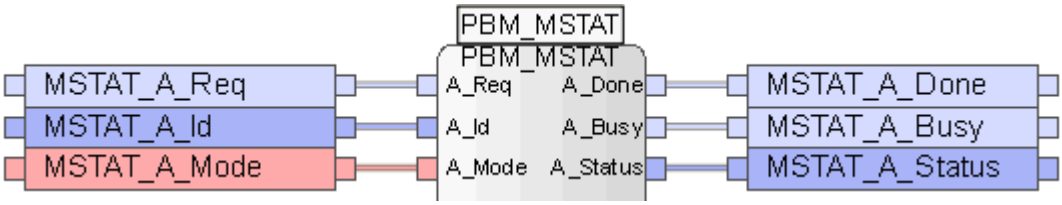


Figure 32: PNM_MSTST Function Block (Upper Part)

Lower part of the function block

The lower part of the function block represents the connection to the function block (in the SILworX structure tree).

The variables that must be connected to the function block located in SILworX structure tree are connected here. The prefix F means Field.

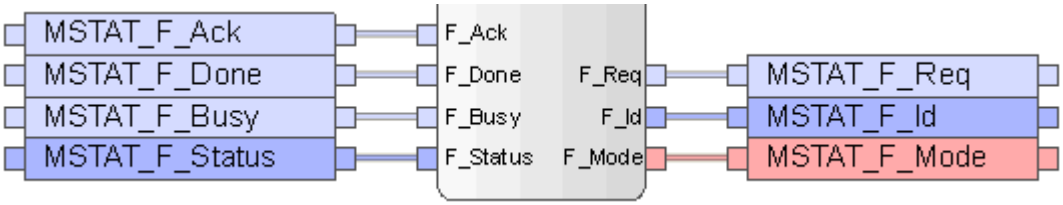


Figure 33: PNM_MSTST Function Block (Lower Part)

7.3.3 Configuring the Function Blocks in the SILworX Structure Tree

To create the function block in the SILworX structure tree

1. In the structure tree, open **Configuration**, **Resource**, **Protocols**, e.g., **PROFIBUS Master**.
2. Right-click **Function Blocks** and select **New**.
3. In the SILworX structure tree, select the suitable function block.

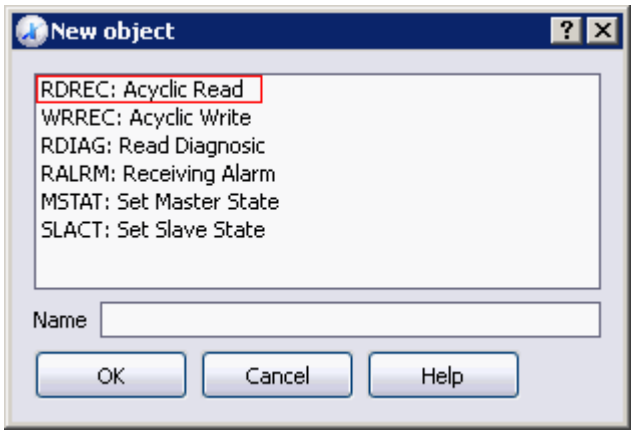


Figure 34: Selecting Function Blocks

The inputs of the function block (checkmark in the Input Variables column) must be connected to the same variables that are connected in the user program to the *F_Outputs* of the function block.

The outputs of the function block (no checkmark in the Input Variables column) must be connected to the same variables that are connected in the user program to the *F_Inputs* of the function block.

System Variables

F	Name	Data type	Input variable	Global Variable
1	ACK	BOOL	☑	MSTAT_F_Ack
2	BUSY	BOOL	☑	MSTAT_F_Busy
3	DONE	BOOL	☑	MSTAT_F_Done
4	M_ID	DWORD	☐	MSTAT_F_Id
5	MODE	INT	☐	MSTAT_F_Mode
6	REQ	BOOL	☐	MSTAT_F_Req
7	STATUS	DWORD	☑	MSTAT_F_Status

Figure 35: System Variables of the MSTAT Function Block

Appendix

Glossary

Term	Description
ARP	Address resolution protocol, network protocol for assigning the network addresses to hardware addresses.
Bit variable	Variable that is addressed bit by bit.
CENELEC	Comité Européen de Normalisation Électrotechnique (European Commitee for Electrotechnical Standardization).
COM	Communication module.
Connector board	Connector board for the HIMax module.
CPU	Processor module.
CRC	Cyclic redundancy check.
Data view	The global variables for output and output data are assigned to a data view to allow access to Modbus sources.
EN	European standard.
Export area	The export area is the process data volume that is written to by the system (a user program, hardware input or another protocol) and is read by the Modbus master.
FB	Fieldbus.
FBD	Function block diagrams.
ICMP	Internet control message protocol, network protocol for status or error messages.
IEC	International electrotechnical commission.
Import area	Process data volume that is written to by the Modbus master and can be used as input data for the system (in a user program, hardware output or another protocol).
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.
KE	Communication end point.
MAC address	Media access control address, hardware address of one network connection.
NSIP	Not safety-related protocol.
PADT	Programming and debugging tool (acc. to IEC 61131-3), PC with SILworX.
PE	Protective ground.
PELV	Protective extra low voltage.
PES	Programmable electronic system.
R	Read.
R/W	Read/Write.
Rack ID	Base rack identification (number).
Register variable	Variable that is addressed word by word.
SB	System bus.
SFF	Safe failure fraction, i.e., portion of faults that can be safely controlled.
SIF	Safety-instrumented function.
SIL	Safety integrity level (in accordance with IEC 61508).
SILworX	Programming tool for HIMax, HIQuad X und HIMatrix.
SIP	Safety-instrumented protocol.
SNTP	Simple network time protocol (RFC 1769).
SRS	System.Rack.Slot.
SW	Software.
TMO	Timeout.
W	Write.
WD	Watchdog.
WDT	Watchdog time.

Index of Figures

Index of Tables

Index

MANUAL
Communication
HI 801 101 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

westermo

www.westermo.com

Lynx L110-F2G & L210-F2G

Industrial Ethernet 10-Port Switch

WeOS

Table of Contents

1. General Information

1.1. Legal Information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind are made in relation to the accuracy and reliability or contents of this document, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Westermo reserves the right to revise this document or withdraw it at any time without prior notice.

Under no circumstances shall Westermo be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about Westermo can be found at www.westermo.com.

1.2. About This Guide

This guide is intended for installation engineers and users of the Westermo products.

It includes information on safety and regulations, a product description, installation instructions and technical specifications.

1.3. Software Tools

Related software tools are available at www.westermo.com/support/software-tools.

1.4. License and Copyright for Included FLOSS

This product includes software developed by third parties, including Free/Libre Open Source Software (FLOSS). The specific license terms and copyright associated with the software are included in each software package respectively. Please visit the product web page for more information.

Upon request, the applicable source code will be provided. A nominal fee may be charged to cover shipping and media. Please direct any source code request to your normal sales or support channel.

1.5. WeOS Management Guide

This product runs WeOS 4 (Westermo Operating System). Instructions for quick start, configuration, factory reset and use of USB port are found in the WeOS Management Guide at www.westermo.com.

2. Safety and Regulations

2.1. Warning Levels

Warning signs are provided to prevent personal injuries and/or damages to the product. The following levels are used:

Level of warning	Description	Consequence personal injury	Consequence material damage
 WARNING	Indicates a potentially hazardous situation	Possible death or major injury	Major damage to the product
 CAUTION	Indicates a potentially hazardous situation	Minor or moderate injury	Moderate damage to the product
 NOTICE	Provides information in order to avoid misuse of the product, confusion or misunderstanding	No personal injury	Minor damage to the product
 NOTE	Used for highlighting general, but important information	No personal injury	Minor damage to the product

Table 1. Warning levels

2.2. Safety Information

Before installation:

Read this manual completely and gather all information available on the product. Make sure it is fully understood. Check that your application does not exceed the safe operating specifications for the product.

WARNING - SAFETY DURING INSTALLATION

The product must be installed and operated by qualified service personnel and installed into an apparatus cabinet or similar, where access is restricted to service personnel only.

During installation, ensure a protective earthing conductor is first connected to the protective earthing terminal (only valid for metallic housings). Westermo recommends a cross-sectional area of at least 4 mm^2.

If the product does not have a protective earthing terminal, then the DIN-rail must be connected to protective earth. Upon removal of the product, ensure that the protective earthing conductor, or the connection to earth via the DIN-rail, is disconnected last.

WARNING - HAZARDOUS VOLTAGE

Do not open an energized product. Hazardous voltage may occur when connected to a power supply.

WARNING - PROTECTIVE FUSE

It must be possible to disconnect manually from the power supply. Ensure compliance to national installation regulations.

Replacing the internal fuse must only be performed by Westermo qualified personell.

WARNING - POWER SUPPLY CONNECTION

There are safety regulations on which power sources that shall be used in conjunction with the product. Refer to Interface Specifications.

WARNING - REDUCE THE RISK OF FIRE

To reduce the risk of fire, use only telecommunication line cords with a cable diameter of AWG 26 or larger. Regarding power cable dimensions, see Interface Specifications.

CAUTION - CLASS 1 LASER PRODUCT

Do not look directly into a fibre optical port or any connected fibre, although the product is designed to meet the Class 1 Laser regulations and complies with 21 CFR 1040.10 and 1040.11.

CAUTION - HANDLING OF SFP TRANSCEIVERS

SFP transceivers are supplied with plugs to avoid contamination inside the optical port. They are very sensitive to dust and dirt. If the fibre is disconnected from the product, the protective plugs on the transmitter/ receiver must be connected. The protective plugs must be kept on during transportation. The fibre optics cables must be handled the same way.

CAUTION - CORROSIVE GASES

If the product is placed in a corrosive environment, it is important that all unused connector sockets are protected with a suitable plug, in order to avoid corrosion attacks on the gold plated connector pins.

CAUTION - ELECTROSTATIC DISCHARGE (ESD)

Prevent electrostatic discharge damages to internal electronic parts by discharging your body to a grounding point (e.g. use a wrist strap).

CAUTION - HOT SURFACE

Be aware of that the surface of this product may become hot. When it is operated at high temperatures, the external surface may exceed Touch Temperature Limit according to the product's relevant electrical safety standard.

2.3. Care Recommendations

Follow the care recommendations below to maintain full operation of the product and to fulfill the warranty obligations:

- Do not drop, knock or shake the product. Rough handling above the specification may cause damage to internal circuit boards.
- Use a dry or slightly water-damp cloth to clean the product. Do not use harsh chemicals, cleaning solvents or strong detergents.
- Do not paint the product. Paint can clog the product and prevent proper operation.

If the product is used in a manner not according to specification, the protection provided by the equipment may be impaired.

If the product is not working properly, contact the place of purchase, nearest Westermo distributor office or Westermo technical support.

2.4. Product Disposal

This symbol means that the product shall not be treated as unsorted municipal waste when disposing of it. It needs to be handed over to an applicable collection point for recycling electrical and electronic equipment.

By ensuring the product is disposed of correctly, you will help to reduce hazardous substances and prevent potential negative consequences to both environment and human health, which could be caused by inappropriate disposal.

Figure 1. WEEE symbol for treatment of product disposal

2.5. Compliance Information

2.5.1. Agency Approvals and Standards Compliance

Type	Approval/Compliance
EMC	• EN/IEC 61000-6-1, Immunity residential environments • EN/IEC 61000-6-2, Immunity industrial environments • EN/IEC 61000-6-4, Emission industrial environments • EN 50121-4/IEC 62236-4, Railway signalling and telecommunications apparatus
Environmental	• NEMA TS 2, Traffic Controller Assemblies with NTCIP Requirements[a]
Safety	• UL 62368-1, Safety Communication Technology
Marine	• DNV GL rules for classification - Ships and offshore units[b]

[a]Valid for Lx10-F2G-12VDC

[b]Valid for Lx10-F2G

Table 2. Agency approvals and standards compliance

2.5.2. UL 62368-1 Notice

This product has been tested and found compliant to UL 62368-1, Safety for Communication Technology. In accordance with the definitions of the standard, this product shall be handled by instructed personnel. Energy source classifications are according to following:

Electrical energy source	Power port	ES1
	Serial port	ES1
	Ethernet port	ES1, TNV-1
	I/O port	ES1
Power source	Power port	PS3
Thermal energy source	Enclosure	TS1
Mechanical energy source	Enclosure	MS1
Radiation energy source	SFP	RS1

Table 3. UL 62368-1 notice

2.5.3. FCC Part 15.105 Class A Notice

This product has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the product is operated in a commercial environment.

This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the user manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful

interference in which case the user will be required to correct the interference at the users own expense.

2.5.4. AREMA

L110-F2G-12VDC has been tested according to AREMA Part 11.3.3, 11.5.1 and 11.5.2.

Port	Test	Remark
DC Power	3 x U_N, 80 ms	U_N (max)=24 VDC when powered from a vital signal battery

Table 4. AREMA Part 11.3.3 C.4. - Signal equipment surge withstand capability for DC input port

	Class C	Class D	Class E	Remarks
Temperature	X	X	X	
Relative humidity	X	X	X	
Vibration	X	X	X	
Mechanical shock	X	X	X	
Dielectric strength			X	Tested with 1.5 kVAC rms

Table 5. AREMA Part 11.5.1. - Environmental Class

	External	Internal
Enclosure port		
Radiated RF immunity Power Frequency Magnetic Field Pulse Magnetic Field	X X X	X X X
DC power port		
EFT/Burst Surge (1.2/50µs) Conducted RF	X - X	X X X
DI-, DO-port		
EFT/Burst Surge (1.2/50µs) Conducted RF	X - X	X X X
Ethernet ports		
EFT/Burst Surge (1.2/50µs) Conducted RF	X X X	X X X
Serial ports		
EFT/Burst Surge (1.2/50µs) Conducted RF	X X X	X X X

Table 6. AREMA Part 11.5.2. - Exposure Class

AREMA Part 11.3.3.E. - Equipment surge withstand documentation DC power port

1. Maximum normal circuit voltage when powered from a vital signal battery is 24 VDC
2. Surge protection clamping voltage is 58.1 VDC
3. Maximum energy handling capability is 2 J, 1 ms

2.5.5. Corrosive Environment

This product has been successfully tested in a corrosion test according to IEC 60068-2-60, method 3. This means that the product meets the requirements to be placed in an environment classified as ISA-S71.04 class G3.

CAUTION - CORROSIVE GASES

If the product is placed in a corrosive environment, it is important that all unused connector sockets are protected with a suitable plug, in order to avoid corrosion attacks on the gold plated connector pins.

2.5.6. Simplified Declaration of Conformity

Hereby, Westermo declares that this product is in compliance with applicable EU directives and UK legislations. The full declaration of conformity and other detailed information is available at www.westermo.com/support/product-support.

Figure 2. The European Conformity marking and the UK Conformity Assessment

3. Product Description

3.1. Product Description

The Lynx series consists of layer 2 or layer 3 industrial Ethernet switches, powered by WeOS, the Westermo network operating system. The Lynx switches are the most compact switches or device servers on the market, available with various ports depending on model, whereof two are 100 Mbit or Gbit SFP transceivers.

The Lynx series is designed for simple use in industrial applications, from the robust DIN rail clip solution to the configurable fault contact and the industrial level of dual power inputs.

Only industrial grade components are used which ensures a long service life. A wide operating temperature range of -40 to +74°C (-40 to +165°F) can be achieved with no moving parts or cooling holes in the case.

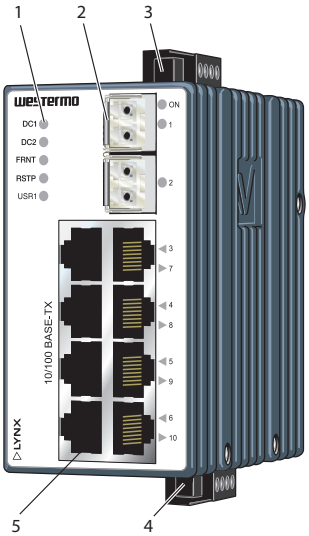
The Lynx series has been tested both by Westermo and external test institutes to meet many EMC, isolation, vibration and shock standards, all to the highest levels suitable for heavy industrial environments and rail trackside applications.

WeOS has been developed by Westermo to offer cross platform and future proof solutions. WeOS delivers unique functionality in legacy IP solutions, supporting Modbus Gateway, virtual COM, modem replacement or several options in dual TCP applications. For more WeOS functionality, please see the WeOS datasheet.

3.2. Available Models

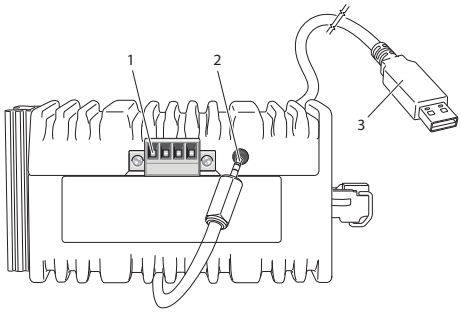
Art. no.	Model	100 Mbit TX ports	Gbit SFP ports	Serial ports	Software	Rated voltage
3643-0100	L110-F2G	8	2	-	L2	24-48 VDC
3643-0110	L110-F2G-12VDC	8	2	-	L2	12-48 VDC
3643-0105	L210-F2G	8	2	-	L3	24-48 VDC

3.3. Hardware Overview



No.	Description	No.	Description
1	LED indicators	2	SFP transceivers
3	Power connection	4	I/O connection
5	Ethernet connection TX		

Figure 3. Location of interface ports and LED indicators



No.	Description	No.	Description
1	I/O connection	2	Console port
3	Accessorie cable, art. no. 1211-2027		

Figure 4. Location of interface ports, bottom view

3.4. Connector Information

3.4.1. Ethernet Connection TX

Illustration	Pin no.	Signal	Direction	Description
	1	TD+	In/Out	Transmitted/Received data
	2	TD-	In/Out	Transmitted/Received data
	3	RD+	In/Out	Transmitted/Received data
	4	-	-	Not connected
	5	-	-	Not connected
	6	RD-	In/Out	Transmitted/Received data
	7	-	-	Not connected
	8	-	-	Not connected
	Shield			Connected to PE

Table 7. Ethernet connection TX

3.4.2. Power Input

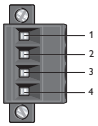
Illustration	Position	Product marking	Direction	Description
	1	+DC1	Input	Supply voltage
	2	+DC2	Input	Supply voltage
	3	-COM	Input	Common
	4	-COM	Input	Common

Table 8. Power input

The product supports redundant power connection. The positive inputs are +DC1 and +DC2, the negative input for both supplies are -COM. Connect the primary voltage (e.g. +24 VDC) to the +DC1 pin and return to one of the -COM pins on the power input.

3.4.3. I/O Connection

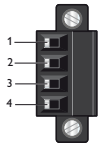
Illustration	Pin no.	Product marking	Direction	Description
	1	Status +	Output	Status relay contact (alarm)
	2	Status -	Output	Status relay contact (alarm)
	3	Digital in +	Input	Digital in +
	4	Digital in -	Input	Digital in -

Table 9. I/O connection

The Status output is a potential free, opto-isolated, normally closed, solit-state relay. This can be configured to monitor various alarm events within the unit, see *WeOS Management Guide*. An external load in series with an external voltage source is required for proper functionality. For voltage/current, see Interface Specifications.

The Digital in is an opto-isolated digital input, which can be used to monitor external events. For voltage/current, see Interface Specifications.

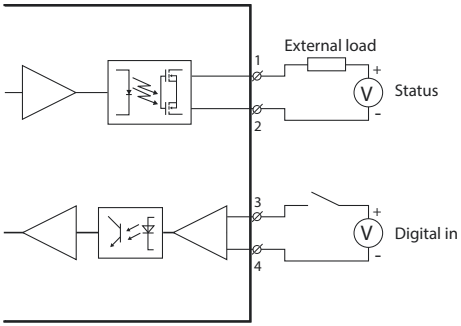


Figure 5. Digital in

3.4.4. Connection to the Console Port

The console port can be used to connect to the CLI (Command Line Interface).

1. Connect the serial diagnostic cable to the console port (use only Westermo cable 1211-2027).
2. Connect cable to your computer (USB port, if drivers are needed they can be downloaded from the Westermo web).
3. Use a terminal emulator and connect with correct speed and format (115200, 8N1) to the assigned port.

For more information about the CLI, see the WeOS Management guide.

Accessories	
Description	Art. no.
Westermo console cable	1211-2027
RJ45 to terminal block	1200-2490
RJ45 to DB9 cable	1211-2210

Table 10. Accessories table

3.5. LED Indicators

LED	Status	Description
ON	OFF	Product has no power
	GREEN	All OK, no alarm condition
	RED	Alarm condition, or until product has started up. (Alarm conditions are configurable, see *WeOS Management Guide*)
	BLINK	Location indicator ("Here I am!"). Activated when connected to WeConfig tool, or upon request from web or/and CLI. RED BLINK during boot indicates pending cable factory reset.
DC1	OFF	Product has no power
	GREEN	Voltage present on DC1
	RED	Power failure on +DC1
DC2	OFF	Product has no power
	GREEN	Voltage present on DC2
	RED	Power failure on +DC2
FRNT	OFF	FRNT disabled
	GREEN	FRNT OK
	RED	FRNT error
	BLINK	Product configured as FRNT focal point
RSTP	OFF	RSTP disabled
	GREEN	RSTP enabled
	BLINK	Product selected as RSTP/STP root switch
USR1	Configurable, see *WeOS Management Guide*	
1 to 10	OFF	No link
	GREEN	Link established
	GREEN FLASH	Data traffic indication
	YELLOW	Port alarm and no link. Or if FRNT or RSTP mode, port is blocked.

Table 11. LED indicators

3.6. SFP Transceivers

The product supports UL and IEC certified transceivers only. See Westermo's modular transceivers datasheets 100 Mbit and 1 Gbit for supported SFP transceivers, which can be downloaded from the product support pages at www.westermo.com/support/product-support.

Each SFP slot can hold one SFP transceiver. See "*Transceiver User Guide 6100-0000*" for transceiver handling instructions, which also can be downloaded from the product support pages at www.westermo.com/support/product-support.

In the event of contamination, the optical connectors in the SFP transceivers should only be cleaned by the use of forced nitrogen and some kind of cleaning stick. Recommended cleaning fluids are methyl-, ethyl-, isopropyl- or isobutyl alcohol, hexane or naphtha.

3.7. Supported Transceivers

Firmware prior to 4.4.0 accepts Westermo branded transceivers only. From 4.5.0 other transceivers are accepted with a notice and the product will no longer be UL approved. Temperature specifications are also depending on the used transceivers.

CAUTION - HANDLING OF SFP TRANSCEIVERS

SFP transceivers are supplied with plugs to avoid contamination inside the optical port. They are very sensitive to dust and dirt. If the fibre is disconnected from the product, the protective plugs on the transmitter/receiver must be connected. The protective plugs must be kept on during transportation. The fibre optics cables must be handled the same way.

3.8. Deviations

With copper transceiver 1100-0148, the specified operating temperature of the product is 0 to 50°C. FRNT reconfiguration times can not be guaranteed with copper transceivers.

3.9. Dimensions

Dimensions are stated in mm and are regardless of model.

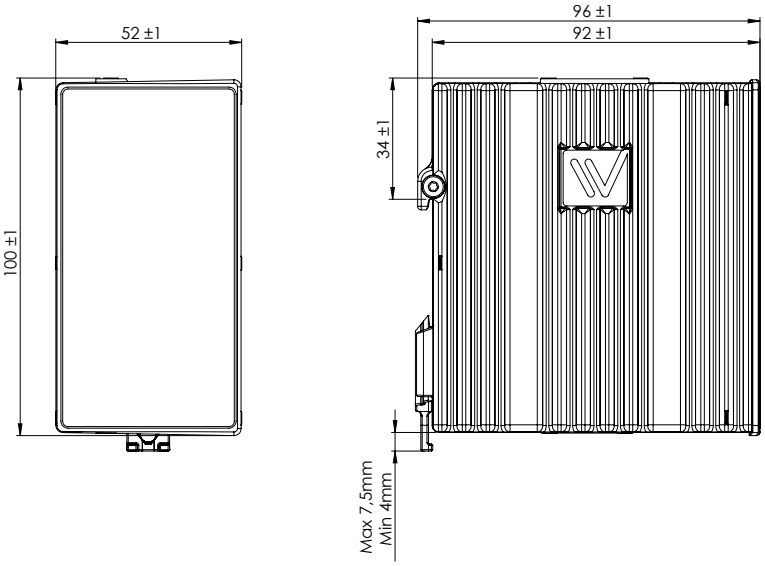


Figure 6. Dimensional drawing

4. Installation

4.1. Mounting

This product should be mounted on a 35 mm DIN-rail, which is horizontally mounted inside an apparatus cabinet or similar. It is recommended that the DIN-rail is connected to ground. Snap on the product to the DIN-rail according to the figure.

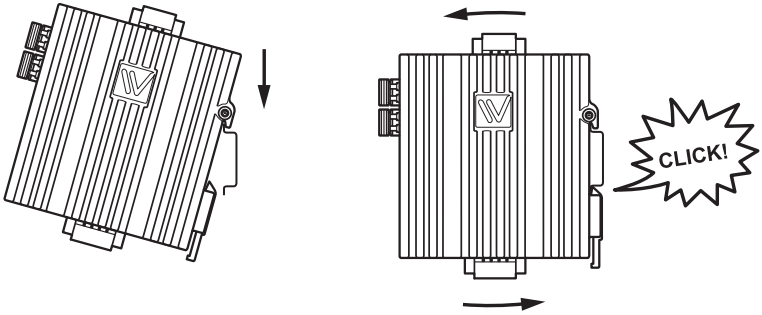


Figure 7. Mounting of product

4.2. Removal of Product

This product has an integrated DIN-clip. To remove the product, press down the support at the back with a screwdriver and lift it off the DIN-rail.

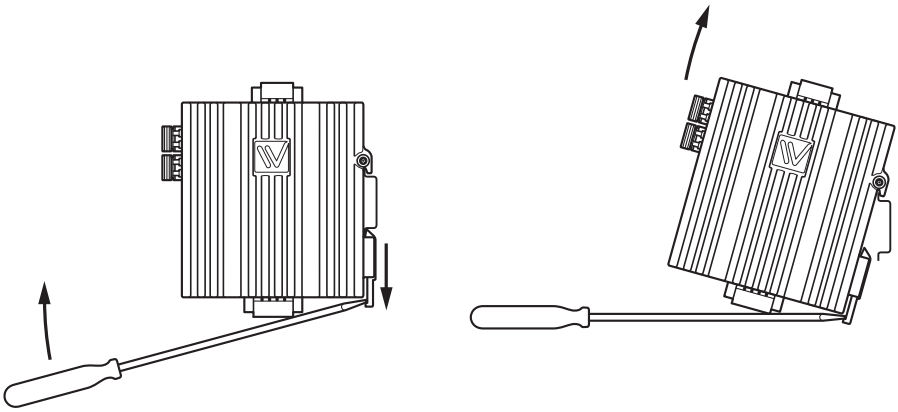


Figure 8. Removal of product

4.3. Cooling

This product uses convection cooling. Spacing is recommended for the use of the product in full operating temperature range and service life. To avoid obstructing the airflow around the product, use the following spacing rules.

Minimum spacing of 25 mm (1 inch) above/below and 10 mm (0.4 inches) left/right of the product is recommended.

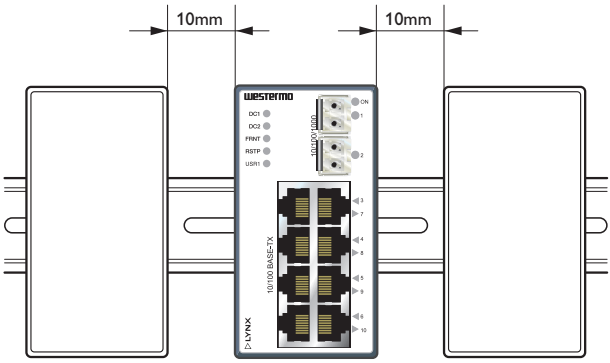


Figure 9. Miminum spacing of product

WARNING - REDUCE THE RISK OF FIRE
To reduce the risk of fire, use only telecommunication line cords with a cable diameter of AWG 26 or larger. Regarding power cable dimensions, see Interface Specifications.

4.4. Getting Started

This product runs the Westermo Operating System (WeOS) which provides several management tools that can be used for configuration of the unit.

- **WeConfig tool**
  This is a custom Westermo tool used for discovery of attached Westermo product.
- **Web**
  Configuration of the product using the web browser.
- **CLI**
  Configuration of the product via the Command Line Interface.
  Username: *admin*
  Password: *westermo*

If the computer is located in the same subnet as the switch you can easily use a web browser to configure the product. Within the web you can configure most of the available functions. If you are not sure about the subnet – consult your network administrator.

For advanced network settings and more diagnostic information, please use the CLI. Detailed documentation is available in the chapter *"The Command Line Management Tool"* in the *WeOS Management Guide*.

Factory default:
IP address: *192.168.2.200*
Netmask: *255.255.255.0*
Gateway: *disabled*

4.5. Configuration Via a Web Browser

The product can easily be configured via a web browser. Open the link http://192.168.2.200 in your web browser, and you will be prompted with a login screen, where the default settings are:

Username: *admin*
Password: *westermo*

Once logged in, use the extensive integrated help function describing all configuration options.

Two common task when configuring a new switch is to assign appropriate IP settings, and to change the password of the admin account. The password can be up to 64 characters long, and should consist of printable ASCII characters (ASCII 33-126); 'Space' is not a valid password character.

NOTE
Note! Version of WeConfig tool must be 10.3.0 or higher.

4.6. Factory Default

It is possible to set the product to factory default settings by using two straight standard Ethernet RJ-45 cables.

1. Power off the product and disconnect all Ethernet cables (copper and fibre).
2. Connect one Ethernet cable between Ethernet ports 3 and 10, and the other between Ethernet ports 6 and 7. The ports need to be connected directly by an Ethernet cable, i.e., not via a hub or switch. Use a straight cable – not a cross-over cable – when connecting the ports.
3. Power on the product.
4. Wait for the product to start up. Control that the ON LED is flashing red. The product is now ready to be either reset to factory default or to boot as normal.

To go ahead with factory reset:

NOTE
Do not power off the product while the factory reset process is in progress.

- Acknowledge that you wish to conduct the factory reset by unplugging the Ethernet cables. The ON LED will stop flashing. This initiates the factory reset process, and after approximately 1 minute the product will restart with factory default settings. When the product has booted up, the ON LED will show a green light, and is now ready to use.

To boot as normal:

- To skip the factory reset process, just wait for approximately 30 seconds (after the ON LED starts flashing RED) without unplugging the Ethernet cables. The product will conduct a normal boot with the existing settings.

5. Specifications

5.1. Interface Specifications

DC, Power port		
	Lx10-F2G:	Lx10-F2G-12VDC:
Rated voltage	24 - 48 VDC	12 - 48 VDC
Operating voltage	19 - 60 VDC	9.8 - 60 VDC
Rated current	240 mA at 24 VDC 120 mA at 48 VDC	420 mA at 12 VDC 220 mA at 24 VDC 115 mA at 48 VDC
Rated frequency	DC	
Inrush current, I^2t	22.7 mA^2s at 48 VDC	53 mA^2s at 12 VDC 20 mA^2s at 48 VDC
Startup current[a]	2 x rated current	
Polarity	Reverse polarity protected	
Redundant power input	Yes	
Isolation	All other ports	
Connector	Detachable screw terminal	
Conductor cross section	0.2-2.5 mm^2 (AWG 24-12)	
Stripping length cable	7 mm	
Tightening torque, terminal screw	0.5 - 0.6 Nm	
Terminal torque, screw flange	0.3 Nm	
Shielded cable	Not required	

[a]Recommended external supply current capability for proper startup

Ethernet TX	
Electrical specification	IEEE std 802.3
Data rate	10 Mbit/s, 100 Mbit/s, manual or auto
Duplex	Full or half, manual or auto
Circuit type	TNV-1
Transmission range	Up to 150 m with CAT5e cable or better
Isolation	All other ports
Connector	RJ-45, auto MDI/MDI-X
Cabling	Shielded CAT5e or better is recommended
Conductive chassis	Yes
Number of ports	8

Ethernet SFP pluggable connections (FX or TX)	
Electrical specification	IEEE std 802.3
Data rate	100 Mbit/s, 1000 Mbit/s, transceivers supported
Duplex	Full or Auto, depending on transceiver
Transmission range	Depending on transceiver
Connection	SFP slot holding fibre transceiver or copper transceiver
Number of ports	1 or 2

I/O connection, Relay output	
Maximum voltage/current	60 VDC/80 mA
Connect resistance	Maximum 30 Ω
Isolation	To all other ports
Connector	Detachable screw terminal
Conductor cross section	0.14 - 1.5 mm² (AWG 28-16)
Stripping length cable	7 mm
Tightening torque, terminal screw	0.22 - 0.25 Nm
Terminal torque, screw flange	0.3 Nm

I/O connection, Digital input	
Maximum voltage/load current	60 VDC/2mA
Isolation	To all other ports
Connector	Detachable screw terminal
Conductor cross section	0.14 - 1.5 mm² (AWG 28-16)
Stripping length cable	7 mm
Tightening torque, terminal screw	0.22 - 0.25 Nm
Terminal torque, screw flange	0.3 Nm
Voltage levels	Logic one: >12 VDC Logic zero: <1 VDC

Console port	
Electrical specification	TTL-level
Data rate	115.2 kbit/s
Circuit type	SELV
Data format	8 data bits, no parity, 1 stop bit, no flow control
Connection	2.5 mm jack, use only Westermo cable 1211-2027

5.2. Type Tests and Environmental Conditions

Environmental phenomena	Basic standard	Description	Test levels
ESD	EN 61000-4-2	Enclosure	Contact: ±6 kV Air: ±8 kV
Fast transients	EN 61000-4-4	Power port	± 2 kV, direct coupling
		Earth port	
		Ethernet ports	± 2 kV, capacitive coupling clamp
		I/O port	
Surge	EN 61000-4-5	Power port	L-E: ± 2 kV, 12 Ω, 9 µF, 1.2/50 µs L-E: ± 2 kV, 42 Ω, 0.5 µF, 1.2/50 µs L-L: ± 1 kV, 2 Ω, 18 µF, 1.2/50 µs L-L: ± 1 kV, 42 Ω, 0,5 µF, 1.2/50 µs
		Ethernet ports	L-E: ± 2 kV, 2 Ω, direct on shield, 1.2/50 µs
		I/O port	L-E, L-L: ± 1 kV, 12 Ω, 9 µF, 1.2/50 µs L-E, L-L: ±2 kV, 42 Ω, 0.5 µF, 1.2/50 µs
Power frequency magnetic field	EN 61000-4-8	Enclosure	300 A/m; 0, 16.7, 50, 60 Hz
Pulsed magnetic field	EN 61000-4-9	Enclosure	300 A/m
Radiated RF immunity	EN 61000-4-3	Enclosure	20 V/m at (80 - 2700) MHz 10 V/m at (2.7 - 6) GHz 1 kHz sine, 80% AM
Conducted RF immunity	EN 61000-4-6	Power port	10 V, 80% AM, 1 kHz; (0.15-80) MHz
		Signal ports	
		Earth port	
Radiated RF emission	CISPR 16-2-3 IEC 60945 ANSI C63,4	Enclosure	Class A (Industrial), 30 MHz to 6 GHz DNVGL-CG - Bridge and Deck Zone, 0.15 MHz to 2 GHz FCC Part 15 B, Class A, 6.5 GHz
Conducted RF emission	CISPR 16-2-1 IEC 60945 ANSI C63,4	Power port	Class B (Residential), 0.15 to 30 MHz DNVGL-CG - Bridge and Deck Zone, 10 kHz to 30 MHz
		Signal ports	
Compass safe distance	IEC 60945	Enclosure	Standard compass (5.4°/H deviation) = 15 cm Steering/standby steering /emergency compass (18°/H deviation) = 10 cm
Supply voltage surge	AREMA	Power port	3 x U_N, 80 ms (72 VDC)[a]
Power supply failure	DNVGL-CG-0339	Power port	U_N-100 %, 30 s

Environmental phenomena	Basic standard	Description	Test levels
Power supply variation	DNVGL-CG-0339	Power port	1.3 x U_N (62.4 VDC), 0.75 x U_N (18 VDC), 15 min
Immunity to conducted low frequency interference	DNVGL-CG-0339	Power port	3 Vrms, 0.05 to 10 kHz
Dielectric strength	UL 62368-1	Power port to all other ports	1.5 kVrms, 50 Hz, 1 min
		I/O port to all other ports	
	UL 62368-1 IEEE 802.3	Ethernet ports to all other ports	
Insulation resistance	DNVGL-CG-0339	Power port to all other ports	500 VDC, 60 s, > 3 GΩ

[a]Only valid for L110-F2G-12VDC

Table 12. EMC and electrical conditions

Environmental phenomena	Basic standard	Description	Test levels
Temperatures	EN 60068-2-1 EN 60068-2-2	Operational	Lx10-F2G-12VDC: -40 to +74°C (-40 to +165°F)[a] Lx10-F2G: -40 to +70°C (-40 to +158°F)
		Storage and transport	-50 to +85°C (-58 to +185°F)
Humidity	EN 60068-2-30	Operational	5-95% relative humidity
		Storage and transport	
Altitude		Operational	2000 m/70 kPa
Service life		Operational	10 years
MTBF	MIL-HDBK 217F		630,000 hours
Vibration	IEC 60068-2-6 (sine)	Operational	3 - 13.2 Hz: 1 mm 13.2 - 100 Hz 0.7 g 5.5 - 30 Hz: 1.5 g 30 - 50 Hz: 0.42 mm 50 - 500 Hz: 4.2 g[b]
Shock	IEC 60068-2-27	Operational	30 g, 11 ms 100 g, 6 ms[b]
Bump	IEC 60068-2-27	Operational	10 g, 11 ms
Enclosure	UL 62368-1	Zinc	Fire enclosure
Weight			0.7 kg
Degree of protection	EN 60529	Enclosure	IP40
Cooling			Convection

[a]Refer to "Safety and Regulations" chapter regarding touch temperature

[b]Might require Ethernet cables to be fastened close to the unit.

Table 13. Environmental and mechanical conditions

6. Revision Notes

Revision	Date	Change description
Rev. P	2021-04	2.5.1 Agency Approvals and Standards Compliance updated, 2.5.2 UL 62368-1 Notice new chapter, 2.5.6 Simplified Declaration of Conformity text and logo updated, 5.2 Type Tests and Environmental Conditions updated
Rev. O	2020-10	Westermo logo updated, illustrations updated from brown to blue, new information structure throughout the manual, 1.2 About This Guide - new chapter, 2 Safety and Regulations - entire chapter updated, 2.5.3 AREMA - new chapter, 3.1. Product Description updated, 3.2. Available Models - new chapter, 3.5 LED Indicators updated, 3.6 SFP Transceivers updated, 3.9 Dimensions - new chapter, 4.1 Mounting updated, 4.2 Removal of Product updated, 5.1 Interface Specifications updated

Westermo • Metallverksgatan 6, SE-721 30 Västerås, Sweden
Tel +46 16 42 80 00 Fax +46 16 42 80 01
E-mail: info@westermo.com
www.westermo.com

6643-2213 REV. P 2021 04 Westermo Network Technologies AB, Sweden