HIMatrix

Veiligheidsgerichte besturing

Veiligheidshandboek

voor

spoortoepassingen

(Safety Manual for Railway Applications)

HIMA Paul Hildebrandt GmbH

Industrie-automatisering

Alle technische gegevens en aanwijzingen in dit handboek werden met de meest grote zorgvuldigheid uitgewerkt en onder toepassing van probate maatregelen ter controle samengesteld. Richt u zich bij vragen alstublieft direct aan HIMA. Voor suggesties, bv welke informaties nog in het handboek zouden moeten worden opgenomen, is HIMA dankbaar.

Technische veranderingen voorbehouden. Voorts behoudt zich HIMA voor aanpassingen van het schriftelijke materiaal zonder voorafgaande aankondiging uit te voeren.

Verdere informaties zijn in de documentatie op de HIMA DVD en op onze website onder `http://www.hima.de` en `http://www.hima.com` te vinden.

Contact

HIMA adres:

HIMA Paul Hildebrandt GmbH

Postbus 1261

68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-mail: info@hima.com

Originele document	Beschrijving
HI 800 436 D, Rev. 2.00 (1334)	Nederlandse vertaling van het Duitse originele document

Inhoudsopgave

1 Introductie

Dit handboek omvat informaties voor het reglementair gebruik van de veiligheidsgerichte HIMatrix automatiseringstoestellen.

Voorwaarde voor installatie, ingebruikneming en voor de veiligheid bij werking en reparatie van de HIMatrix automatiseringssystemen zijn:

- Kennis van voorschriften.
- technisch foutvrije uitvoering van de in dit handboek onthouden veiligheidsinstructies door gekwalificeerd personeel.

In de volgende gevallen kunnen door storingen of belemmeringen van veiligheidsfuncties zwaar lichamelijk letsel, materiële schade of milieuschade optreden, waarvoor de HIMA geen aansprakelijkheid kan aanvaarden:

- Bij niet gekwalificeerde operaties in de toestellen.
- Bij uitschakelen of omzeilen (bypass) van veiligheidsfuncties.
- Bij veronachtzaming van instructies uit dit handboek.

HIMA ontwikkelt, produceert en controleert HIMatrix automatiseringssystemen onder inachtneming van de desbetreffende veiligheidsnormen. Het gebruik van de toestellen is slechts toegestaan, wanneer aan alle volgende voorwaarden is beantwoordt:

- Alleen de in de beschrijvingen beoogde inzetgevallen.
- Alleen de gespecificeerde omgevingscondities.
- Alleen in verbinding met toegelaten vreemde toestellen.

Om redenen van de overzichtelijkheid omvat dit handboek niet alle details van alle uitvoeringen van de HIMatrix automatiseringstoestellen. Verdere details zijn aan de desbetreffende handboeken te ontlenen.

1.1 Opbouw en gebruik van de documentatie

Dit veiligheidshandboek omvat de volgende onderwerpen:

- Reglemtaire toepassing
- Veiligheidsconcept
- Centrale functies
- Ingangen
- Uitgangen
- Software
- Veiligheidstechnische aspecten voor het gebruikersprogramma
- Configuratie van de communicatie
- Aanhangsel:
  - Glossarium
  - Registers/Index

i Compacte besturingen en Remote I/Os worden als *toestel*, insteekkaarten van een modulaire besturing als *component* betekent.

In SILworX worden componenten als *module* betekent.

De volgende HIMatrix toestellen hebben verdere functies:

- F60 CPU 03
- F35 03
- F31 03
- F30 03
- F10 PCI 03

Deze toestellen worden in dit document onder de benaming **F*03** samengevat. De verdere functies van deze toestellen tegenover de standaard-toesteleln zijn de volgende:

- Verhoogde performance
- Registratie van voorvallen mogelijk
- Multitasking mogelijk
- Reload mogelijk
- Twee IP-adressen

Het handboek onderscheidt de volgende varianten van het HIMatrix systeem:

Programmeerwerktuig	Hardware	Processor-besturingssysteem	Communicatie-besturingssysteem
SILworX	F*03	Vanaf CPU BS V8	Vanaf COM BS V13
SILworX	Standaard	Vanaf CPU BS V7	Vanaf COM BS V12
ELOP II Factory	Standaard	Tot CPU BS V6.x	Tot COM BS V11.x

Tabel 1: Varianten van het HIMatrix systeem

De varianten worden in het handboek onderscheiden door:

- Aparte subhoofdstukken
- Tabellen, met onderscheiding van de versies

i **Met ELOP II Factory vervaardigde projecten kunnen in SILworX niet worden bewerkt en omgekeerd!**

1.2 Geldigheid en actualiteit

De meest recente versie van dit veiligheidshandboek die door het hoogste revisienummer is gekenmerkt, is telkens van toepassing. De recente versie is aan de website *www.hima.com* of aan de actuele HIMA DVD te ontlenen.

Voor de toepassing van vroegere versies van HIMatrix, ELOP II Factory en SILworX dienen de desbetreffend vroegere revisies van dit handboek in acht te worden genomen.

1.3 Doelgroep

Dit document richt zich aan planners, projecteuren en programmeurs van automatiseringsinstallaties alsook aan personen die tot ingebruikneming, bedrijf en onderhoud van de toestellen, componenten en systemen zijn gerechtigd. Speciale kennis op het gebied van de veiligheidsgerichte automatiseringssystemen wordt verondersteld.

1.4 Weergaveconventies

Voor een betere leesbaarheid en ter verduidelijking zijn in dit document de volgende schrijfwijzen van toepassing:

Vet	Accentuering van belangrijke tekstdelen. Benamingen van schakelvlakken, menupunten en registers in het programmeerwerktuig die kunnen worden aangeklikt
Cursief	Parameters en systeemvariabelen
`Courier`	Woordelijke invoeren van gebruikers
RUN	Benamingen van bedrijfstoestanden in kapitalen
Hoofdst. 1.2.3	Verwijzingen zijn hyperlinks, ook wanneer ze niet bijzonder zijn gekenmerkt. Wordt de cursor hierop geplaatst, verandert hij van vorm. Bij een klik springt het document naar de desbetreffende plaats.

Veiligheids- en gebruikaanwijzingen zijn bijzonder gekenmerkt.

1.4.1 Veiligheidsinstructies

De veiligheidsinstructies in het document zijn als volgt beschreven weergregeven.
Om een zo gering als mogelijk risico te waarborgen, moeten ze in ieder geval wordne opgevolgd. De inhoudelijke opbouw is

- Signaalwoord: waarschuwing, vorzichtig, instructie
- Soort en bron van het risico
- Gevolgen bij veronachtzaming
- Voorkomen van het risico

⚠ SIGNAALWOORD

Soort en bron van het risico!
Gevolgen bij veronachtzaming
Voorkomen van het risico

De betekeni van de signaalwoorden is

- Waarschuwing: Bij veronachtzaming dreigt zwaar lichamelijk letsel tot dood
- Voorzichtig: Bij veronachtzaming dreigt licht lichamelijk letsel
- Instructie: Bij veronachtzaming dreigt materiële schade

INSTRUCTIE

Soort en bron van de schade!
Voorkomen van het risico

1.4.2 Gebruiksaanwijzingen

Extra informaties zijn volgens het volgende voorbeeld opgebouwd:

i Hier staat de tekst van de extra informatie.

Nuttige tipps en tricks verschijnen in de vorm:

TIP Hier staat de tekst van de tip.

2 Aanwijzingen met betrekking tot de inzet

De veiligheidsinformaties, instructies en aanwijzingen in dit document in ieder geval lezen. Het product alleen onder inachtneming van alle richtlijnen en veiligheidsrichtlijnen inzetten.

2.1 Reglemtaire toepassing

Dit hoofdstuk beschrijft de voorwaarden voor de inzet van HIMatrix systemen.

2.1.1 Toepassingsbereik

De veiligheidsgerichte besturingen HIMatrix kunnen tot het veiligheids-integriteitslevel SIL 4 volgens EN 50126, EN 50128 en EN 50129 worden ingezet.

De HIMatrix systemen zijn voor proces-besturingen, veiligheidssystemen, branderinstallaties en machinebesturingen gecertificeerd.

Bij het gebruik van de veiligheidsgerichte communicatie tussen verschillende toestellen dient in acht te worden genomen, dat de totale reactietijd van het systeem niet de tijd van de storingstolerantie te boven gaat. De in het hoofdstuk 9 vermelde berekeningsbeginsels dienen te worden toegepast.

Aan de communicatie-interfaces mogen alleen toestellen worden aangesloten die een veilige elektrische scheiding waarborgen.

2.1.1.1 Ruststroomprincipe

De automatiseringstoestellen zijn voor het ruststroomprincipe geconstrueerd.

Een systeem, dat volgens het ruststroomprincipe werkt, vereist geen energie om zijn veiligheidsfunctie uit te voeren (*deenergize to trip*).

Als veilige toestand in geval van storing wordt hiermee bij ingangs- en uitgangssignalen de spanning- of stroomvrije toestand ingenomen.

2.1.1.2 Werkstroomprincipe

De HIMatrix besturingen kunnen ook in het werkstroom-toepassingen worden ingezet.

Een systeem, dat volgens het werkstroomprincipe werkt, vereist energie, bv elektrische of pneumatische energie, om zijn veiligheidsfunctie uit te voeren (*energize to trip*).

Bij het concept van de besturing zijn de vereisten uit de toepassingsnormen in acht te nemen, bv kan een draaddiagnose van de ingangen en uitgangen of een terugmelding van de geactiveerde veiligheidsfunctie noodzakelijk zijn.

2.1.2 Onreglementaire inzet

De transmissie van de veiligheidsrelevanten gegevens via openbare netten (bv internet) is met extra maatregelen ter verhoging van de veiligheid (bv VPN-tunnel, Firewall, etc.) toegestaan.

Met de veldbusinterfaces is geen veiligheidsgerichte communicatie mogelijk.

2.2 Testvoorwaarden

De HIMatrix systemen werden onder inachtneming van de vereisten van de volgende normen voor EMV-, klimaat- en milieuvereisten getest:

Norm	Inhoud
IEC/EN 61131-2: 2007	Programmable controllers, Part 2: Equipment requirements and tests
IEC/EN 61000-6-2: 2005	EMC Generic standard, Part 6-2 Immunity for industrial environments
IEC/EN 61000-6-4: 2006	Electromagnetic compatibility (EMC) Generic emission standard, industrial environments

Tabel 2: Normen voor EMV-, klimaat- en milieuvereisten

Voor de inzet van de veiligheidsgerichte besturingssystemen HIMatrix zijn de onderstaand vermelde algemene voorwaarden op te volgen:

Soort conditie	Inhoud van de voorwaarde
Veiligheidsklasse	Veiligheidsklasse III volgens IEC/EN 61131-2
Verontreiniging	Verontreinigingsgraad II volgens IEC/EN 61131-2
Opstelhoogte	< 2000 m
Behuizing	Standaard: IP20 Indien de desbetreffende applicatienormen (bv EN 60204, EN ISO 13849-1) het verlangen, moet het toestel in een behuizing van het verlangde veiligheidssoort (bv IP54) worden ingebouwd.

Tabel 3: Algemene voorwaarden

2.2.1 Klimatische voorwaarden

De belangrijste controles en grenswaarden voor klimatische voorwaarden zijn in de onderstaande tabel vermeldt:

IEC/EN 61131-2	Klimaatkeuringen
	Bedrijfstemperatuur: 0...+60 °C (testgrenzen: -10...+70 °C)
	Opslagtemperatuur: -40...+85 °C
	Droge warmte en koelheid, bestendigheidskeuringen: +70 °C / -25 °C, 96 h, stroomvoorziening niet aangesloten
	Temperatuurwissel, bestendigheids- en ongevoeligheidskeuring: -40 °C / +70 °C en 0 °C / +55 °C, stroomvoorziening niet aangesloten
	Cycli met vochtige warmte, bestendigheidskeuringen: +25 °C / +55 °C, 95 % relatieve vochtigheid, stroomvoorziening niet aangesloten

Tabel 4: Klimatische voorwaarden

Bij overschrijden van de temperatuurgrenzen, zie hoofdstuk 3.3.4.

2.2.2 Mechanische voorwaarden

De belangrijste controles en grenswaarden voor mechanische voorwaarden zijn in de onderstaande tabel vermeldt:

IEC/EN 61131-2	Mechanische keuringen
	Ongevoeligheidskeuring tegen vibraties: 5...9 Hz / 3,5 mm 9...150 Hz, 1 g, kandidat in werking, 10 cycli per as
	Ongevoeligheidskeuring tegen shocks: 15 g, 11 ms, kandidaad in werking, 3 shocks per as (18 shocks)

Tabel 5: Mechanische keuringen

2.2.3 EMV-voorwaarden

Voor veiligheidsgerelateerde systemen worden verhoogde niveaus bij de storingsbeïnvloeding verlangt. HIMatrix systemen beantwoorden aan deze vereisten volgens IEC 62061 en IEC 61326-3-1. Zie kolom *Criterium FS* (Functionele veiligheid).

IEC/EN 61131-2	Controles van de storingsvastheid	Criterium FS
IEC/EN 61000-4-2	ESD-keuring: 6 kV contact-, 8 kV luchtontlading	6 kV, 8 kV
IEC/EN 61000-4-3	RFI-keuring (10 V/m): 80 MHz...2 GHz, 80 % AM RFI-keuring (3 V/m): 2 GHz...3 GHz, 80 % AM: RFI-keuring (20 V/m): 80 MHz...1 GHz, 80 % AM	- - 20 V/m
IEC/EN 61000-4-4	Burst-keuring: Voedingsspanning: 2 kV en 4 kV Signaalleidingen: 2 kV	 4 kV 2 kV
IEC/EN 61000-4-12	Keuring met gedempte vibraties: 2,5 kV L-, L+ / PE 1 kV L+ / L-	 - -
IEC/EN 61000-4-6	Hoogfrequentie, asymmetrisch: 10 V, 150 kHz...80 MHz, AM 20 V, ISM-frequenties, 80 % AM	 10 V -
IEC/EN 61000-4-3	900 MHz-impulsen	-
IEC/EN 61000-4-5	Stootspanning: Voedingsspanning: 2 kV CM, 1 kV DM Signaalleidingen: 2 kV CM, 1 kV DM bij AC E/A	 2 kV /1 kV 2 kV

Tabel 6: Keuringen van de storingsvastheid

IEC/EN 61000-6-4	Keuringen van de storingsuitzending
EN 55011 Klasse A	Storingsuitzending: gestraald, draadgerelateerd

Tabel 7: Keuringen van de storingsuitzending

2.2.4 Voedingsspanning

De belangrijste controles en grenswaarden voor de voedingsspanning zijn in de onderstaande tabel vermeldt:

IEC/EN 61131-2	Controle van de eigenschappen van de gelijkstroomvoorziening
	De voedingsspanning moet aan de volgende normen beantwoorden: IEC/EN 61131-2: SELV (Safety Extra Low Voltage) of PELV (Protective Extra Low Voltage)
	De afzekering van de HIMatrix systemen moet volgens de gegevens in dit handboek geschieden.
	Keuring van het spanningbereik: 24 VDC, -20...+25 % (19,2...30,0 V)
	Keuring op ongevoeligheid tegen korttijdonderbreking van de externe stroomverzorging: DC, PS 2: 10 ms
	Polariteitsomkeer van de voedingsspanning Aanwijzing in het desbetreffende hoofdstuk van het systeemhandboek of in het datablad van de stroomverzorging.

Tabel 8: Controle van de eigenschappen van de gelijkstroomverzorging

2.2.5 ESD-veiligheidsmaatregelen

Slechts personeel, dat kennis over ESD-veiligheidsmaatregelen bezit, mag veranderingen of uitbreidingen van het systeem of het vervangen van een component uitvoeren.

INSTRUCTIE

Elektrostatische ontladingen kunnen de in de HIMatrix systemen ingebouwde elektronische componenten beschadigen!

- **Voor de werkzaamheden een antistatisch beveiligde werkplaats gebruiken en een aardband dragen.**
- **Componenten - bij niet-gebruik het toestel elektrostatisch beschermd bewaren, bv in de verpakking.**

2.3 Extra testvoorwaarden voor spoortoepassingen

De volgende tabel toont de HIMatrix varianten voor spoortoepassingen:

Compacte besturingen
F30 014
F30 034
F35 014
F35 034
Remote I/Os
F1 DI 16 014
F2 DO 4 01 [1)]
F2 DO 8 014
F2 DO 16 014
F2 DO 16 02 [1)]
F3 AIO 8/4 014
F3 DIO 8/8 014
F3 DIO 16/8 014
F3 DIO 20/8 023
F3 DIO 20/8 024
Modulair systeem F60
PS 014
CPU 034
AI 8 014
CIO 2/4 014
DI 24 014
DI 32 014
DIO 24/16 014
MI 24 014
GEH 014
[1)] Alleen voor het temperatuurbereik 0…+60 °C toegelaten

Tabel 9: Beschikbare HIMatrix varianten voor spoortoepassingen

De HIMatrix varianten voor spoortoepassingen werden onder inachtneming van de vereisten van de volgende normen voor EMV-, klimaat- en milieuvereisten getest.

2.3.1 Klimatische voorwaarden

De HIMatrix varianten voor spoortoepassingen zijn voor een temperatuurbereik van -25…+70 °C geconstrueerd. De volgende klimatische voorwaarden werden in acht genomen:

Norm	Temperatuurklasse
EN 50155	T1 en T2 [1)]
EN 50125-1	T1, T2 [1)] en T3
EN 50125-3	T1, T2 [1)] en TX [1)]
[1)] T2 en TX bij inzet van een verwarming voor de opwarming op minimaal -25 °C	

Tabel 10: Klimatische vooraarden bij HIMatrix varianten voor spoortoepassingen

2.3.1.1 Derating van de digitale uitgangen

Bij een omgevingstemperatuur groter 60 °C moet de belasting van de digitale uitgangen worden gereduceerd (derating). De uitgangen kunnen in dit geval met telkens maximaal 0,5 A worden belast, zie handboeken van de toestellen.

2.3.2 Mechanische voorwaarden

De belangrijste controles en grenswaarden voor mechanische voorwaarden zijn in de onderstaande tabel vermeldt:

EN 50125-3	Mechanische keuringen
	Trillingscontrole: 2,3 m/s^2 tussen 5...2000 Hz, kandidaad in werking
	Ongevoeligheidskeuring tegen shocks: 20 m/s^2, 11 ms, kandidaad in werking

Tabel 11: Mechanische voorwaarden voor de inzet in de signaaltechniek

De in Tabel 9 vermelde toestellen en componenten werden volgens de EN 50155 mechanisch gekeurd en zijn voor de inzet op spoorvoertuigen geschikt. De keuring vond volgens EN 61373, categorie 1, klasse B plaats.

2.3.3 EMV-voorwaarden

De belangrijste controles en grenswaarden voor EMV-voorwaarden zijn in de onderstaande tabel vermeldt:

EN 50121-4	Controles van de storingsvastheid
ESD-controle	6 kV contact-, 8 kV luchtontlading
EM-veld	80 MHz…1 GHz: 10 V/m 80 MHz…3 GHz: 10 V/m 800…960 MHz: 20 V/m
Burst-keuring	Voedingsspanning: 2 kV I/O-leidingen: 2 kV Aardaansluiting: 1 kV
Surge [1)]	Voedingsspanning: 2 kV CM 1 kV DM
Instroming	Voedingsspanning: 10 V I/O-leidingen: 10 V Aardaansluiting: 10 V
Magneetveld met netfrequentie	16 2/3 Hz, 50 Hz, 60 Hz: 100 A/m DC 300 A/m
Magneetveld, pulserend	300 A/m
[1)] Bij HIMatrix compactsystemenm is de externe filter H 7013 in ieder geval noodzakelijk. Er kunnen ook overspanningsafleiders van andere fabrikanten worden toegepast, wanneer de gegevens op de lijst met de technische inlichtingen gelijkwaardig of beter zijn.	

Tabel 12: EMV-voorwaarden voor de inzet in de signaaltechniek

EN 50121-3-2	Controles van de storingsvastheid
ESD-controle	6 kV contact-, 8 kV luchtontlading
EM-veld	80 MHz…1 GHz: 20 V/m 1400…2100 MHz: 10 V/m 2100…2500 MHz: 5 V/m
Burst-keuring	Voedingsspanning: 2 kV I/O-leidingen: 2 kV
Surge [1)]	Voedingsspanning: 2 kV CM 1 kV DM
Instroming	Voedingsspanning: 10 V I/O-leidingen: 10 V
[1)] Bij HIMatrix compactsystemenm is de externe filter H 7013 in ieder geval noodzakelijk. Er kunnen ook overspanningsafleiders van andere fabrikanten worden toegepast, wanneer de gegevens op de lijst met de technische inlichtingen gelijkwaardig of beter zijn.	

Tabel 13: EMV-voorwaarden voor spoorvoertuigen

De in Tabel 9 vermelde toestellen en componenten werden volgens de EMV vereisten van de EN 50121-4 en EN 50121-3-2 positief getest.

2.3.4 Bemoeilijkte voorwaarden

De Remote I/O F3 DIO 20/8 023 voldoet aan verhoogde vereisten met betrekking tot zoute nevel volgens IEC 60068-2-11 (5 % voor een duur van 96 uren).

De geschiktheid werd door middel van keuring aangetoond.

2.4 Taken van de fabrikant van machine en installatie alsook van de exploitant

De fabrikanten van machine en installatie alsook de exploitant zijn ervoor verantwoordelijk, dat de veilige toepassing van de HIMatrix systemen in de automatiseringsinstallaties en in totale installaties is gewaarborgd.

De correcte programmering van de HIMatrix systemen moet door de fabrikanten van de machines en installaties voldoende worden gevalideerd.

2.5 Verdere systeemdocumentaties

Voor de projectering van de HIMatrix systemen staan bovendien nog de volgende documentaties ter beschikking:

Naam	Toepasbaar	Inhoud	Document-nr.
HIMatrix Safety Manual	Alle versies	Veiligheidsfuncties van het HIMatrix systeem	HI 800 023 E
HIMatrix System Manual Compact Systems	Alle versies	Beschrijvingen van de compactsystemen met technische gegevens	HI 800 640 NL
HIMatrix System Manual Modular Systems	Alle versies	Beschrijving van het modulaire systeem F60 met technische gegevens	HI 800 191 E
Certified test report [1)]	Alle versies	Testbeginsels, veiligheidsvereisten, resultaten	
Communication Manual (configuration performed with SILworX)	Vanaf CPU BS V7	Beschrijving van de communicatieprotocollen, ComUserTask en de projectering hiervan in SILworX	HI 801 101 E
HIMatrix PROFIBUS-DP Master/Slave Manual	Tot CPU BS V6.x	Beschrijving van het PROFIBUS-protocol en diens projectering in ELOP II Factory	HI 800 009 E
HIMatrix Modbus Master/Slave Manual	Tot CPU BS V6.x	Beschrijving van het Modbus-protocol en diens projectering in ELOP II Factory	HI 800 003 E
HIMatrix TCP S/R Manual	Tot CPU BS V6.x	Beschrijving van het TCP°S/R-protocol en diens projectering in ELOP II Factory	HI 800 117 E
HIMatrix ComUserTask (CUT) Manual	Tot CPU BS V6.x	Beschrijving van de ComUserTask en de projectering hiervan in SILworX	HI 800 329 E
SILworX Online Help	Vanaf CPU BS V7	SILworX bediening	-
ELOP II Factory Online Help	Tot CPU BS V6.x	ELOP II Factory bediening, Ethernet IP-protocol, INTERBUS-protocol	-
SILworX First Steps Manual	Vanaf CPU BS V7	Introductie in SILworX (aan het voorbeeld van HIMax)	HI 801 103 E
ELOP II Factory First Steps Manual	Tot CPU BS V6.x	Introductie in ELOP II Factory	HI 800 006 E
[1)] Levering alleen samen met een HIMatrix systeem			

Tabel 14: Aanvullend geldige handboeken

Details omtrent de toestellen en componenten in de desbetreffende handboeken.

De actuele handboeken bevinden zich op de HIMA website www.hima.com. Aan de hand van de revisie-index in de voetregel kan de actualiteit van eventueel voorhanden handboeken met de internetuitgave worden vergeleken.

3 Veiligheidconcept voor de inzet van de PES

Dit hoofdstuk bevat zich met belangrijke algemene vragen omtrent de functionele veiligheid van HIMatrix systemen.

- Veiligheid en beschikbaarheid
- Voor veiligheid belangrijke tijden
- Veiligheidsvoorschriften

3.1 Veiligheid en beschikbaarheid

De automatiseringstoestellen zijn voor het ruststroomprincipe geconstrueerd: de periferie en de werking van de besturing beschouwen de energievrije toestand als veilige toestand.

Als veilige toestand in geval van storing wordt hiermee bij ingangs- en uitgangssignalen de spanning- of stroomvrije toestand ingenomen.

Van de HIMatrix systemen gaan geen directe risico´s uit.

⚠ WAARSCHUWING

Lichamelijk letsel door verkeerd aangesloten of verkeerd geprogrammeerde veiligheidsgerichte automatiseringssystemen!

Aansluitingen voor de ingebruikname controleren en gehele installatie testen!

3.1.1 THR-berekeningen

Voor de HIMatrix systemen werd volgens EN 50129 de THR-berekening uitgevoerd.

EN 50129 legt een THR van 10^{-9}…10^{-8} per uur (SIL 4) vast.

De veiligheidsfuncties, bestaande uit een veiligheidsgerelateerde loop (ingang, verwerkingsunit, uitgang en communicatie tussen HIMatrix systemen) beantwoorden in alle combinaties aan de boven beschreven vereisten. Aan deze vereisten worden door de besturingen van de Remote I/Os en de componenten voldaan.

3.1.2 Zelftest en storingdiagnose

Het besturingssysteem van de besturingen voert bij de start en in het draaiende bedrijf omvangrijke zelftests uit. Getest worden hierbij met name:

- De processoren
- De geheugenbereiken (RAM, niet-vluchtige geheugens)
- De watchdog
- De afzonderlijke I/O-kanalen

Constateren deze tests storingen, schakelt het besturingssysteem het defecte toestel, de defecte component of het defecte I/O-kanaal uit.

Bij een systeem zonder redundantie betekent dit, dat deelfuncties of de gehele PES kunnen worden uitgeschakeld.

Alle HIMatrix toestellen en componenten beschikken telkens over eigen LEDs ter weergave van de ontdekte storingen. Hiermee is in geval van storing een snelle storingdiagnose voor een als foutief gemeld toestel of de externe schakeling mogelijk.

Aanvullend kan het gebruikersprogramma verschillende systeemvariabelen of systeemsignalen evalueren die de toestand van de toestellen en componenten tonen.

Een omvangrijke diagnostische opname van het systeemgedrag en herkende storingen worden in het diagnosegeheugen van de besturingen gedeponeerd. De opname kan ook ook na een systeemstoring via de PADT worden uitgelezen.

Details over de evaluatie van de diagnosemeldingen zie ook systeemhandboekes (System Manual Compact Systems HI 800 640 NL of System Manual Modular Systems HI 800 191 E), hoofdstuk *Diagnosis*.

Bij een zeer klein gedeelte van de component-defecten die de veiligheid niet beïnvloeden, vervaardigt het HIMatrix systeem geen diagnosyeinformaties.

3.1.3 PADT

Met de PADT vervaardigt de gebruiker het programma en configureert de besturing. Het veiligheidsconcept van de PADT ondersteunt de gebruiker bij de correkte uitvoering van de besturingstaak. Het PADT voert talrijke maatregelen ter controle van de ingevoerde informaties uit.

Het PADT is een personalcomputer, waarop het programmeerwerktuig is geïnstalleerd.

Voor het HIMatrix systeem zijn twee programmeerwerktuigen voorhanden, afhankelijk van de versie van het besturingssysteem op de besturing:

- met een CPU BS vanaf versie 7 is SILworX te gebruiken.
- met een CPU BS tot versie 6.x is ELOP II Factory te gebruiken.

3.1.4 Opbouw van veiligheidssystemen volgens het werkstroomprincipe

Veiligheidssystemen die volgens het werkstroomprincipe (*energize to trip*) werken, hebben de volgende functies:

1. De veilige toestand van een toestel is de energievrije toestand. Deze toestand wordt bijvoorbeeld bij een storing in het toestel ingenomen.
2. Op verzoek kan de besturing de veiligheidsfunctie door inschakelen van een actuator activeren.

3.1.4.1 Onderscheiden van uitgevallen componenten

Het veiligheidssysteem herkent door de automatisch verlopende diagnose, dat toestellen defect zijn.

3.1.4.2 Veiligheidsfunctie in het werkstroomprincipe

De uitvoering van de veiligheidsfuncties bestaat daarin, dat het veiligheidssysteem één of meerdere actuatoren ingeschakeld (*energize*), zo dat de veilige toestand wordt behaald.

Door de gebruiker is het volgende te plannen:

- Kortsluiten- en draadbreuk-controle bij ingangs-/uitgangstoestellen.
  Deze dienen te worden geparametreerd.
- De functie van actuatoren kan via een standterugmelding worden gecontroleerd.

3.2 Voor de veiligheid belangrijke tijden

Deze zijn:

- Tolerantietijd storingen
- Veiligheidstijd
- Reactietijd
- Watchdog-tijd

3.2.1 Tolerantietijd storingen

De tolerantietijd storingen (FTZ, zie DIN VDE 0801, aanhangsel A1 2.5.3) is een eigenschap van het proces en beschrijft de periode, waarin het proces door gebrekkige signalen kan worden toegepast, zonder dat een veiligheidskritische toestand wordt behaald.

3.2.2 Veiligheidstijd

De veiligheidstijd is de tijd, waarin de besturing in de RUN-toestand na optreden van een interne storing moet reageren.

Vanuit de proceszijde gezien, is de veiligheidstijd de maximale tijd, waarin het veiligheidssysteem bij een verandering van ingangssignalen aan de uitgangen moet reageren (reactietijd).

Versie van het besturingssysteem	Veiligheidstijd in het bereik
Vanaf CPU BS V7	20...22 500 ms
Tot CPU BS V6.x	20...50 000 ms

Tabel 15: Waardebereik van de veiligheidstijd

3.2.3 Veiligheidstijd van het gebruikersprogramma

De veiligheidstijd van het gebruikersprogramma laat zich niet direct instellen. HIMatrix berekent de veiligheidstijd van een gebruikersprogramma uit de parameters *Max. safetytime* van de ressource en *Maximum Number of Cycles*. Met betrekking tot de details zie 8.2.9.

3.2.4 Reactietijd

De maximale reactietijd van cyclisch werkende HIMatrix besturingen is de dubbele cyclustijd van deze systemen, wanneer niet door parametrering of de logica van het gebruikersprogramma een vertraging plaatsvindt.

De cyclustijd van een besturing bestaat uit de volgende belangrijke delen:

- Lezen van de ingangen
- Verwerken van het gebruikersprogramma of de gebruikersprogramma´s
- Schrijven van de uitgangen
- Procesdatacommunicatie
- Uitvoeren van testroutinen

Bij F*03-toestellen resp. componenten kan de cyclus van een gebruikersprogramma meerdere cycli van het procesoorsysteem omvatten. Voor zulke gebruikersprogramma´s is de reactietijd desbetreffend verhoogd, zie beneden.

Aanvullend zijn bij worst case-beschouwing van het gehele systeem de schakeltijden van de ingangen en uitgangen in acht te nemen.

De reactietijd $t_{Response}$ zet zich samen uit:

$t_{Response} = t_{Input} + t_{IN\ communication} + 2*t_{WDT} + t_{Out\text{-}communication} + t_{Output}$

t_{Input}	Schakel-/omzettingtijd van de ingang
$t_{IN\ communication}$	Bij Remote I/O: transmissietijd tussen ingang in Remote I/O en besturing
t_{WDT}	Deze is afhandelijk van het soort toestel: ▪ bij standaard-toestellen/componeten is ze de watchdog-tijd van de ressource ▪ bij F*03-toestellen/componenten is ze de watchdog-tijd van het gebruikersprogramma en kan een meervoudige van de watchdog-tijd van het processorsysteem bedragen
$t_{Out\ communication}$	Bij Remote I/O: transmissietijd tussen besturing en uitgang in Remote I/O
t_{Output}	Schakel-/omzettingstijd van de uitgang

3.2.5 Watchdog-tijd van het processorsysteem

De watchdog-tijd wordt in het menu voor de instelling van de eigenschappen van de PES voorgegeven. Ze is de maximaal toegestane duur van een RUN-cyclus (cyclustijd). Overschrijdt de cyclustijd de voorgegeven watchdog-tijd, schakelt het systeem uit. Vervolgens start het systeem opnieuw, indien autostart werd geparametreerd. Indien autostart niet werd geparametreerd, gaat het systeem in de toestand STOP/VALID CONFIGURATION.

De watchdog-tijd van het processorsysteem mag ingesteld worden op:
≤ 1/2 * veiligheidstijd van de PES.

Versie van het besturingssysteem	HIMatrix	Waardebereik watchdog-tijd	Standaardwaarden besturingen	Standaardwaarde Remote I/Os
Vanaf CPU BS V8	F*03	4…5000 ms	200 ms	100 ms
Vanaf CPU BS V7	Standaard	8...5000 ms	200 ms	100 ms
Tot CPU BS V6.x	Standaard	2...5000 ms	50 ms	10 ms

Tabel 16: Waardebereik van de watchdog-tijd

i Voor de te besturen installatie zijn veiligheidstijd en watchdog-tijd te bepalen.

3.2.6 Watchdog-tijd van het gebruikersprogramma bij F*03.

Leder gebruikersprogramma heeft een eigen watchdog-tijd.

De watchdog-tijd van het gebruikersprogramma laat zich niet direct instellen. HIMatrixs F*03 toestellen/componenten berekenen de watchdog-tijd van een gebruikersprogramma uit de parameters *Max. Watchdog Time* van de ressource en *Maximum Numer of Cycles*.

Er dient erop gelet te worden, dat de berekende watchdog-tijd hooguit zo groot is dan de reactietijd die voor het door het gebruikersprogramma bewerkte gedeelte van het proces is verlangt.

3.3 Veiligheidsvoorschriften

Voor de inzet van de veiligheidsgerichte componenten van het systeem HIMatrix zijn de volgende veiligheidsvoorschriften van toepassing:

3.3.1 Hardware-projectering

Personen die de HIMatrix hardware projecteren, moeten rekening houden met de volgende veiligheidsvoorschriften.

3.3.1.1 Productonafhankelijke voorschriften

- Voor het veiligheidsgericht bedrijf mag slechts hiervoor toegelaten storingzekere hardware en software worden toegepast. De toegelaten hardware en softwrae is in de *Version List of Devices and Firmware of HIMatrix Systems of HIMA Paul Hildebrandt GmbH* vermeld. De telkens actuele versiestanden zijn aan de samen met de testisntantie gevoerde versielijst te ontlenen. De actuele versielijst bevindt zich op de HIMA website www.hima.com.
- De gespecificeerde gebruiksomstandigheden (zie hoofstuk 2.2 en 2.3) met betrekking tot EMV, mechanische, chemische, klimatische invloeden moeten worden opgevolgd.
- Niet storingveilige, maar terugwerkingsvrije hardware en software mag voor de verwerking van niet veiligheidsrelevante signalen worden toegepast, niet echter voor de bewerking van veiligheidstechnische taken.
- Bij alle extern aan het systeem aangesloten veiligheidsstroomcircuits dient het ruststroomprincipe te worden nageleefd.

3.3.1.2 Productafhankelijke voorschriften

- Aan het systeem mogen slechs toestellen worden aangesloten die een veilige scheiding van het net vertonen.
- De veilige elektrische scheiding van de stroomverzorging dient in de 24 V-verzorging van het systeem te geschieden. Er mogen slechts nettransformatoren in uitvoeringen worden toegepast die waarborgen, dat besturing en Remote I/Os met laagspanning 24 V worden geëxploiteerd.
- Om de veiligheidsmaatregelen met betrekking op elektrische veiligheid en aarding op te volgen, moet de fabrikant van de bepaalde applicatie geschikte scheidingsmaatregelen tussen binnen- en buiteninstallatie in overeenstemming met EN 50122 voorzien. De HIMatrix systemen moeten hierdoor tegen invloeden van onderdelen van de buiteninstallatie in het bovenleiding- en stroomafnemerbereik en tegen spoorterugstromen worden gezekerd. Er dienen voor het spoorbereik toegelasten energieverzorgingsvoorzieningen te worden toegepast.

3.3.2 Programmering

Personen die gebruikersprogramma´s vervaardigen, moeten rekening houden met de volgende veiligheidsvoorschriften.

3.3.2.1 Productonafhankelijke voorschriften

- In veiligheidsrelevante toepassingen dient op de correcte parametrering van de veiligheidsrelevanten systeemgrootten te worden gelet. Mogelijke parametreringen zijn in het veiligheidshandboek beschreven, zie hoofdstuk 7.4.
- Met name dient de vastlegging van systeemconfiguratie, maximale cyclustijd en veiligheidsheid in acht te worden genomen, zie hoofdstuk 3.2.

3.3.2.2 Productafhankelijke voorschriften - vanaf CPU BS V7

Voorschriften voor het gebruik van het programmeerwerktuig:

- Voor de programmering dient **SILworX** te worden toegepast.
- Na vervaardiging van de applicatie dient door een dubbel compileren en vergelijking van de configuratie-CRCs te worden gewaarborgd, dat het compileren correct heeft plaatsgevonden.
- De correcte omzetting van de specificatie van de applicatie dient te worden gevalideerd en geverifieerd. Er dient een volledige controle van de logica door beproeving plaats te vinden.

- De storingsreactie van het systeem bij storingen in de storingveilige ingang- en uitgangcomponenten moet volgens de installatiespecifieke veiligheidstechnische gegevens door het gebruikersprogramma worden vastgelegd.
- Het programmeerwerktuig SILworX heeft een functie die na een verandering van het gebruikersprogramma of de systeemconfiguratie slechts de veranderingen weergeeft. Een analyse van de veranderingen (change impact analysis IA) heeft de noodzakelijke testomvang te definieren. Deze IA heeft de te verwachten veranderingen op basis van de uitgevoerde modificaties, de uitgave van de vergelijkingsfunctie van SILworX en vereiste regressietests in acht te nemen.

3.3.2.3 Productafhankelijke voorschriften - tot CPU BS V6.x

Voorschriften voor het gebruik van het programmeerwerktuig:

- Voor de programmering dient **ELOP II Factory** te worden toegepast.
- Na vervaardiging van de applicatie dient door een handmatig dubbel compileren en vergelijking van de configuratie-CRCs te worden gewaarborgd, dat het compileren correct heeft plaatsgevonden.
- De correcte omzetting van de specificatie van de applicatie dient te worden gevalideerd en geverifieerd. Er dient een volledige controle van de logica door beproeving plaats te vinden.
- De storingsreactie van het systeem bij storingen in de storingveilige ingang- en uitgangcomponenten moet volgens de installatiespecifieke veiligheidstechnische gegevens door het gebruikersprogramma worden vastgelegd.

3.3.3 Communicatie

- Bij het gebruik van de veiligheidsgerichte communicatie tussen verschillende toestellen dient in acht te worden genomen, dat de totale reactietijd van het systeem niet de tijd van de storingstolerantie te boven gaat. De in het hoofdstuk 9.2 vermelde berekeningsbeginsels dienen te worden toegepast.
- De datatransmissie moet via gesloten transmissiesystemen (categorie 1) volgens EN 50159 plaatsvinden.
- De toepassing van open transmissiesystemen (categorie 2 en categorie 3) volgens EN 50159 is mogelijk, wanneer extra maatregelen voor het waarborgen van de veiligheid van het transmissiekanaal werden genomen (bv door firewalls of versleuteling).
- De seriële interfaces zijn in dit uitbouwniveau uitsluitend voor niet veiligheidsgerichte doeleinden toepasbaar.
- Aan alle communicatie-interfaces mogen alleen toestellen worden aangesloten die een veilige elektrische scheiding waarborgen.

3.3.4 Voorschriften voor spoortoepassingen

- Voor spoortoepassingen dienen de relevante normen te worden toegepast.
- De digitale uitgangen bezitten een kortsluitingscontrole. Maargelen bij het reageren van de controle moeten door het gebruikersprogramma plaatsvinden.
- De temperatuurtoestand (bedrijfstemperatuur) van de HIMatrix systemen moet door het gebruikersprogrammw worden geëvalueerd. Veiligheidsgerichte maatregelen moeten eveneens door het gebruikersprogramma plaatsvinden. Voor verdere informaties zie systeemhandboeken (System Manual Compact Systems HI 800 640 NL en System Manual Modular Systems HI 800 191 E), hoofdstuk *Monitoring the Temperature State*.
- Storingsmeldingen moeten door het gebruikersprogramma worden geëvalueerd. Storingen worden door statusbits doorgegeven en staan zodoende het gebruikersprogramma ter beschikking. Aanvullend worden storingen in het diagnosegeheugen van de besturing geregistreerd en kunnen met het toegepaste programmeringswerktuig worden uitgelezen. Voor verdere informaties zie systeemhandboeken (System Manual Compact Systems HI 800 640 NL en System Manual Modular System HI 800 191 E), hoofdstuk *Diagnosis*.
- Een aardsluitingherkenning dient extern te worden geconfigureerd.

4 Centrale functies

Bij de toestellen van het type F1.., F2.., F3.. handelt het zich om compactsystemen die niet gemodificeerd worden.

Bij de besturingen van het type F60 handelt het zich om modulaire systemen, waarbij binnen een besturing met nettransformator- en procesmodule maximaal zes I/O-componenten kunnen worden ingezet.

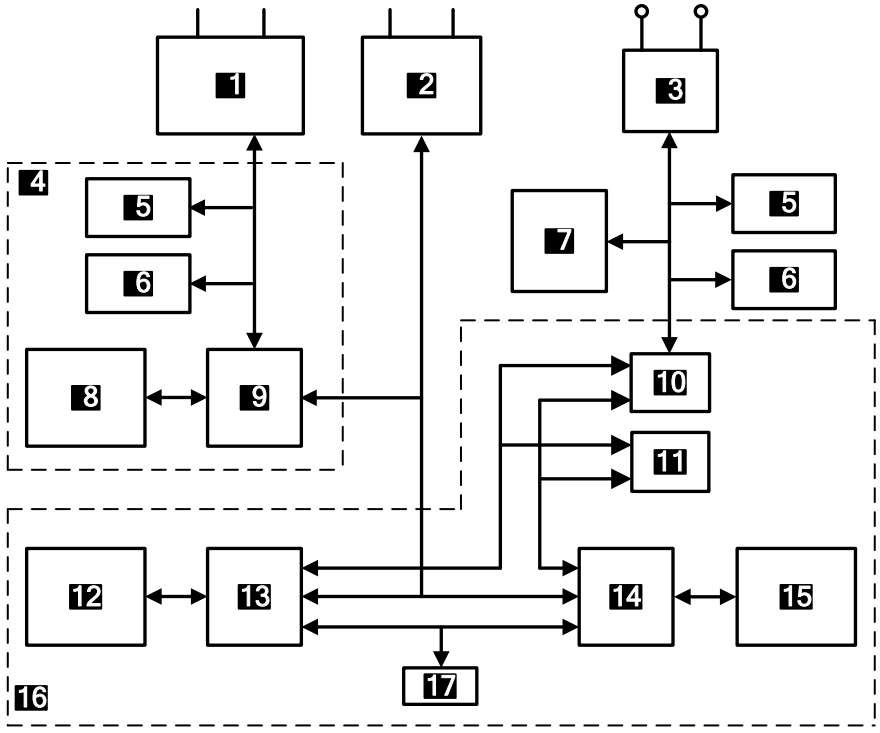
4.1 Nettransformatoren

De verzorging van de HIMatrix systemen moet uit nettransformatoren geschieden die de besturingen en de Remote I/Os met laagspanning 24 V verzorgen.

De reglementaire werking van de besturing wordt met opvolgen van de toegelasten spanninggrenzen gewaarborgd.

4.2 Functiebeschrijving van het centraal deel

De CPU is de centrale module van de besturing. Ze bestaat uit de volgende functieblokken:



1 Veldbus interfaces
2 Ethernet-interfaces
3 I/O-bus-module
4 Communicatiesysteem
5 nvSRAM
6 Flash
7 V_{CC} en temperatuurcontrole
8 SDRAM van het communicatiesysteem
9 Processor van het communicatiesysteem
10 Vergelijker
11 Watchdog
12 SDRAM 1 van het processorsysteem
13 Processor 1 van het processorsysteem
14 Processor 2 van het processorsysteem
15 SDRAM 2 van het processorsysteem
16 Veiligheidsgericht processorsysteem
17 Real time clock

Afbeelding 1: Weergave van de functieblokken aan het voorbeeld van de CPU 03 van de F60

Eigenschappen van het processorsysteem

- Twee pulssynchrone microprocessoren (processor 1 en processor 2)
- Iedere microprocessor heeft een eigen SDRAM-geheugen
- Testbare hardware-vergelijker voor alle externe toegangen van beide microprocessoren
- In geval van storing wordt de watchdog in de veilige toestand gezet
- Flash EPROMs, het programmageheugen voor besturingssystemen en gebruikersprogramma, geschikt voor min. 100 000 opslagcycli
- Datageheugen in nvSRAM
- Goldcap ter buffering van datum/tijd
- Communicatieprocessor voor veldbus- en Ethernet-aansluitingen
- Interface voor de data-uitwisseling tussen toestellen, besturingen F60 en de PADT, gebaseerd op Ethernet
- Optioneel/optionele interface(s) voor de data-uitwisseling per veldbus
- Doorgeven van de systeemtoestanden door LEDs
- I/O-bus-logica ter verbinding met de I/O-componenten
- Veilige watchdog (WD)
- Nettransformatorcontrole, testbaar (1,8 VDC / 3,3 VDC)
- Temperatuurcontrole

4.3 Zelftests

De zelftestvoorziening herkennen afzonderlijke storingen die tot een veiligheidskritische bedrijfstoestand kunnen leiden en activeren binnen de veiligheidstijd van de besturing gedefineerde storingsreacties, die de defecte onderdelen in de veilige toestand brengen.

Onderstaand worden de belangrijkste zelftestroutinen van het veiligheidsgericht processorsysteem trefwoordachtig uiteengezet:

4.3.1 Microprocessor-test

Gekeurd worden:

- alle toegepaste orders en adresseringssoorten,
- de beschrijfbaarheid van de flags en de door haar veroorzaakte orders,
- de beschrijfvbaarheid en het overspreken van de registers.

4.3.2 Test van de geheugenbereiken

Het besturingssysteem, het gebruikersprogramma, de constanten en parameters alsook de variabele gegevens zijn in geheugenbereiken van beide processoren opgeslagen en worden door een hardware-vergelijker gecontroleerd.

4.3.3 Opgeslagen geheugenbereiken

Besturingssysteem, gebruikersprogramma en parameterbereik zijn in telkens een geheugen gedeponeerd. Ze worden door een schrijfbeveiliging en een CRC-test gezekerd.

4.3.4 RAM-test

Een schrijf- en leestest controleert de veranderbare RAM-bereiken vooral op stuck-at en overspreken.

4.3.5 Watchdog-test

Het watchdog-signaal schakelt zich uit, wanneer het niet in het vastgelegd tijdvenster door beide CPUs wordt getriggerd; evenzo, wanneer de test van de hardware-vergelijker mislukt. Door een verdere test wordt de uitschakelbaarheid van het watchdog-signaal gecontroleerd.

4.3.6 Test van de I/O-bus binnen de besturing

De verbinding tussen CPU en de bijbehorende ingangen en uitgangen (I/O-componenten) wordt gecontroleerd.

4.3.7 Reacties op storingen in het processorsysteem

Een hardware-vergelijker binnen de processormodule vergelijkt permanent, of de gegevens van het microprocessorsysteem 1 identiek met de gegevens van het microprocessorsysteem 2 zijn. Is dit niet het geval of zijn de testroutinen in het centraal bereik negatief, gaat de besturing automatisch in ERROR STOP en het watchdog-signaal wordt uigeschakeld. Dit betekent, dat geen ingangssignalen meer worden verwerkt en de uitgangen in de energievrije, uitgeschakelde toestand overgaan.

Bij de eerste zulke storing start de besturing opnieuw (reboot). Treedt binnen een minuut na de herstart een verdere interne storing op, gaat de besturing in de toestand STOP/INVALID CONFIGURATION en blijft in deze toestand.

4.4 Storingdiagnose

Alle componenten van de F60 beschikken telkens over een eigen LED voor de weergave bij storingen van de component of de externe schakeling. Hiermee is in geval van storing een snelle storingdiagnose voor een als foutief gemeld toestel of de externe schakeling mogelijk.

Bij de compactsystemen F1.., F2.., F3.. zijn deze storingsweergaven tot één verzamel-storingsmelding samengevat.

Aanvullend kan in het gebruikersprogramma een evaluatie van verschillende systeemsignalen van de ingangen en uitgangen of de besturing plaatsvinden.

Een storingindicatie vindt alleen plaats, wanneer de storing de communicatie met het processorsysteem niet belemmerd, d.w.z. een evaluatie via het processorsysteem nog mogelijk maakt.

De logica in het gebruikersprogramma kan de storingcodes van alle ingangs- en uitgangssignalen en de systeemsignalen evalueren.

Eine umfangreEen omvangrijke diagnostische opname van het systeemgedrag en herkende storingen worden in het diagnosegeheugen van de processor en het communcatiesysteem gedeponeerd. De opname kan ook ook na een systeemstoring via de PADT worden uitgelezen.

Details over de evaluatie van de diagnosemelding zie ook systeemhandboeken (System Manual Compact Systems HI 800 640 NL en System Manual Modulares System F60 HI 800 191 E), hoofdstuk *Diagnosis*.

5 Ingangen

Overzicht van de ingangen van het HIMatrix systeem:

Toestel	Type	Aantal	veiligheids-gericht	terugwerkingsvrij	elektrisch gescheiden
Compactsystemen					
F20	Digitaal	8	•	•	– [1]
F30	Digitaal	20	•	•	– [1]
F35	Digitaal	24	•	•	– [1]
	Teller 24 bit	2	•	•	– [1]
	Analoog	8	•	•	– [1]
F1 DI 16 01	Digitaal	16	•	•	– [1]
F3 DIO 8/8 01	Digitaal	8	•	•	– [1]
F3 DIO 16/8 01	Digitaal	16	•	•	– [1]
F3 AIO 8/4 01	Analoog	8	•	•	– [1]
F3 DIO 20/8 02	Digitaal	20	•	•	– [1]
Modulair systeem F60					
DIO 24/16 01	Digitaal	24	•	•	•
DI 32 01 (met Line Control configureerbaar)	Digitaal	32	•	•	•
DI 24 01 (110 V)	Digitaal	24	•	•	•
CIO 2/4 01	Teller 24 bit	2	•	•	•
AI 8 01	Analoog	8	•	•	•
MI 24 01	Analoog of digitaal	24	•	•	•

[1] Referentiepotentiaal L-

Tabel 17: Overzicht van de ingangen

5.1 Algemene informaties

Het is mogelijk, veiligheidsgerichte ingangen zowel voor veiligheidsgerichte als ook voor niet-veiligheidsgerichte signalen te gebruiken.

De besturingen leveren status- en storingsinformaties op de volgende manieren:

- Door diagnose-LEDs van de toestellen en componenten.
- Door systeemsignalen resp. systeemvariabelen die het gebruikersprogramma kan evalueren.
- Door aantekeningen in het diagnosegeheugen die PADT kan uitlezen.

Veiligheidsgerichte ingangscomponenten voeren gedurende het bedrijf automatisch een hoogwaardige, cyclische zelftest uit. Deze testroutingen zijn TÜV-gekeurd en controleren de veilige werking van de desbetreffende component.

Bij een zeer klein gedeelte van de component-defecten die de veiligheid niet beïnvloeden, wordt geen diagnose-informatie vervaardigd.

5.2 Veiligheid van sensoren, encoders en transmitters

In een veiligheidsgerichte toepassing moeten zowel de besturing als ook de hieraan aangesloten sensoren, encoders en transmitters aan de veiligheidsvereisten (SIL) beantwoorden.

Aan de ingangen van de besturing kunnen de veiligheidsgerichte sensoren, encoders en transmitters met de vereiste SIL worden aangesloten. Staan geen sensoren, encoders en transmitters met de specifieke SIL ter beschikking, kunnen ze ook zonder SIL worden aangesloten. In het applicatieprogramma moet dan echter een koppeling en controle van de signalen worden geprogrammeerd.

Aanwijzingen voor het bereiken van de noodzakelijke SIL kunnen bijvoorbeeld uit IEC 61511-1, paragraaf 11.4 worden ontleend.

5.3 Veiligheidsgerichte digitale ingangen

De beschreven eigenschappen zijn zowel voor de digitale ingangskanalen van de componenten van de F60 als ook voor de digitale ingangskanalen van alle compactsystemen van toepassine, wanneer geen specifieke aanwijzingen plaatsvinden.

5.3.1 Algemene informaties

De digitale ingangen worden eenmaal in iedere cyclus gelezen en intern opgeslagen; ze worden cyclisch op een veilige werking getest.

Ingangssignalen die korter dan de tijd tussen twee aftastingen (dus korter dan voor een cyclustijd) aanstaan, worden eventueel niet geregistreerd.

5.3.2 Testroutinen

De testroutinen controleren, of de ingangskanalen in staat zijn, onafhankelijk van de aanstaande ingangssignalen beide signaalniveaus (low en high) door te schakelen. Deze functietest wordt bij ieder lezen van de ingangssignalen uitgevoerd.

5.3.3 Reactie in geval van storing

Constateren de testroutinen voor digitale ingangen een storing, activeert een compactsysteem de LED *ERROR,* een F60 component de LED *ERR*.

5.3.3.1 CPU BS vanaf V7

Een gebruikersprogramma verwerkt de initiale waarde van de globale variabelen.

Het is niet noodzakelijk, dat het gebruikersprogramma de storingcode verwerkt.

De gebruikmaking van de storingcode biedt aanvullende mogelijkheden in het gebruikersprogramma de externe schakeling te controleren en storingreacties te programmeren.

De systeemvariabele die de storingcode omvat, heet *->Error Code [Byte].* Ze is toegankelijk in het register **...Channels** in het detailaanzicht van de component of van het toesteldeel, in de regel met het kanaalnummer.

5.3.3.2 CPU BS tot V6.x

Het gebruikersprogramma verwerkt voor het defecte kanaal in overeenstemming met het ruststroomprincipe een low-niveau.

Het gebruikersprogramma moet aanvullend tot de signaalwaarde van het kanaal de desbetreffende storingcode in acht nemen.

De gebruikmaking van de storingcode biedt aanvullende mogelijkheden in het gebruikersprogramma de externe schakeling te controleren en storingreacties te programmeren.

Het systeemsignaal dat de storingcode omvat, heet *DI[xx].Error Code*, waarbij *xx* voor het kanaalnummer staat. Het is toegankelijk in het venster *Signal Connections...* van de bouwgroep of het toesteldeel.

5.3.4 Surge op digitale ingangen

Veroorzaakt door de korte cyclustijd van de HIMatrix systemen kunnen digitale ingangen een surge-impuls volgens EN 61000-4-5 als tijdelijk high-niveau inlezen.

De volgende maatregelen voorkomen storingsfuncties in omgevingen, waarin surges kunnen optreden:

1. Installatie van afgeschermde ingangsleidingen
2. Storingsuittasting in het gebruikersprogramma programmeren. Een signaal moet ten minste twee cycli aanstaan, alvorens het wordt geëvalueerd.

i Van de boven vermelde maatregelen kan afstand worden genomen, wanneer door de invulling van de installatie surges in het systeem kunnen worden uitgesloten.

Tot de invulling behoren met name veiligheidsmaatregelen aangaande overspanning, blikseminslag, aarding en installatiebedrading op basis van de gegevens van de fabrikant en de relevante normen.

5.3.5 Parametreerbare digitale ingangen

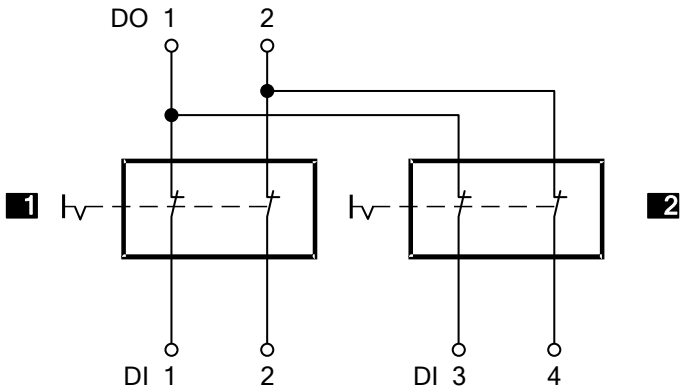
De digitale ingangen van de besturing F35 en de component MI 24 01 werken volgens het principe van analoge ingangen die echter door parametrering van schakeldrempels een digitale waarde leveren.

Voor parametreerbare digitale ingangen gelden de voor analoge ingangen genoemde testroutinen en veiligheidsfuncties zoals in hoofdstuk 5.4.1 vermeld.

5.3.6 Line Control

Line Control is een kortsluitings- en draadbreuk-herkenning bijvoorbeeld van NOOD-UIT-toestellen die bij HIMatrix systemen met digitale ingangen (niet met parametreerbare digitale ingangen) kan worden geconfigureerd.

Hiervoor de digitale uitgangen DO van het systeem met de digitale ingangen DI van hetzelfde systeem op de volgende manier verbonden (voorbeeld):

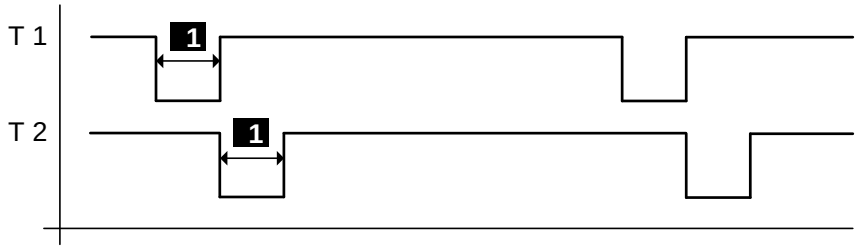


1 NOOD-UIT 1
2 NOOD-UIT 2

NOOD-UIT-schakelaars volgens de normen EN 60947-5-1 en EN 60947-5-5

Afbeelding 2: Line Control

De besturing pulst de digitale uitgangen, om kortsluiting en draadbreruk van de leidingen naar de digitale ingangen te herkennen. Hiervoor in SILworX de systeemvariabele *Value [BOOL] ->* en in ELOP II Factory het systeemsignaal *DO[01].Value* parametreren. De variabelen voor de pulsuitgaven moeten bij kanaal 1 beginnen en direct naast elkaar liggen (zie systeemvariabelen in de handboeken).



1 Configureerbaar 5...2000 µs

Afbeelding 3: Pulssignalen T1, T2

Line Control kan volgende storingen constateren:

- Dwarssluiting tussen twee parallele leidingen,
- verruiling van twee leidingen (bv DO 2 naar DI 3),
- aardsluiting van één van de leidingen (alleen bij geaarde referentiepool),
- draadbreuk of openen van de contacten, d.w.z. ook bij het bedienen van een van de boven getoonde NOOD-UIT-schakelaars knippert de LED FAULT, en de storingcode wordt gegenereerd.

Treedt een zulke storing op, vinden de volgende reacties plaats:

- De lichtdiode *FAULT* op de frontplaat van de besturing of de component knippert.
- De ingangen worden op low-niveau gezet.
- Een (evalueerbare) storingcode wordt gegenereerd.

5.4 Veiligheidsgerichte analoge ingangen (F35, F3 AIO 8/4 01 en F60)

De analoge ingangskanalen converteren de gemeten ingangsstromen in een INTEGER-waarde. De waarden staan het gebruikersprogramma in variabelen ter beschikking, die bij de volgende systeembariabelen/systeemsignalen zijn ingedeeld:

Versie van het besturingssysteem	Waarde
Vanaf CPU BS V7	Systeemvariable -> *Value [INT]*
Tot CPU BS V6.x	Systeemsignaal *AI[xx].Value* (xx = kanalnummer).

Tabel 18: Waarde veiligheidsgerichte analoge ingangen

De veiligheidstechnische exactheid is de gegarandeerde exactheid van de analoge ingang zonder storingreactie van het toestel of de component. Deze waarde is bij de parametering van veiligheidsfuncties in acht te nemen.

De waardebereiken van de ingangen zijn afhankelijk van het toestel of de component:

- Besturing F35:

Ingangs-kanalen	Meet-methode	Stroom, spanning	Waardebereik in de toepassing		Veiligheidstechni-sche exactheid
			FS1000 [1]	FS2000 [1]	
8	unipolair	0…+10 V	0…1000	0…2000	2 %
8	unipolair	0…20 mA	0…500 [2] 0…1000 [3]	0…1000 [2] 0…2000 [3]	2 %

[1] instelbaar via typekeuze in de PADT

[2] met externe shunt-adapter 250 Ω, Onderdeelnummer: 98 2220059

[3] met externe shunt-adapter 500 Ω, Onderdeelnummer: 98 2220067

Tabel 19: Analoge ingangen van de besturing F35

- Remote I/O F3 AIO 8/4 01:

Ingangs-kanalen	Meet-methode	Stroom, spanning	Waardebereik in de toepassing	Veiligheidstechni-sche exactheid
8	unipolair	0…+10 V	0…2000	2 %
8	unipolair	0/4…20 mA	0…1000 [1] 0…2000 [2]	2 %

[1] met externe shunt-adapter 250 Ω, Onderdeelnummer: 98 2220059

[2] met externe shunt-adapter 500 Ω, Onderdeelnummer: 98 2220067

Tabel 20: Analoge ingangen van de Remote I/O F3 AIO 8/4 01

- Besturing F60:

Ingangs-kanalen	Meet-methode	Stroom, spanning	Waardebereik in de toepassing		Veiligheidstechnische exactheid
			FS1000 [1]	FS2000 [1]	
AI 8 01					
8	unipolair	-10…+10 V	-1000…1000	-2000…2000	1 %
8	unipolair	0…20 mA	0…1000 [3]	0…2000 [3]	1 %
8	unipolair	0…20 mA	0…500 [2]	0…1000 [2]	4 %
4	bipolair	-10…+10 V	-1000…1000	-2000…2000	1 %
MI 24 01					
	unipolair	0…20 mA	0…2000 [4]		1 %

[1] instelbaar via typekeuze in de PADT(F60)

[2] met externe meet-shunt 250 Ω, Onderdeelnummer: 00 0710251

[3] met externe meet-shung 500 Ω, Onderdeelnummer: 00 0603501 (exactheid 0,05 %, P 1 W)

[4] interne meet-shunts

Tabel 21: Analoge ingangen van de besturing F60

De component AI 8 01 van de F60 kan in het gebruikersprogramma op acht unipolaire of vier bipolaire functies worden geconfigureerd. Het mengen van de functies op een component is echter niet toegestaan.

De analoge ingangen van de besturing F35, de Remote I/O F3 AIO 8/4 01 en de component AI 8 01 werken met spanningsmeting. Met de analoge ingangen van de F35 en de F3°AIO°8/4°01 kunnen digitale uitgangen van het eigen systeem (F35) of van andere HIMatrix besturingen op draadbreuk worden gecontroleerd. Nadere details omvatten de handboeken van de desbetreffende HIMatrix besturingen.

Bij draadbreuk (er vind geen draadcontrole door het systeem plaats) worden aan de hoogohm ingangen willekeurige ingangssignalen verwerkt. De uit deze zwevende ingangsspanning resulterende waarde is niet zeker; bij spanningingangen moeten de kanalen met een weerstand van 10 kΩ worden afgesloten. De interne weerstand van de bron dient hierbij in acht te worden genomen.

Voor een stroommeting wordt de ingang van de shunt parallel geschakeld; de weerstand van 10 kΩ is dan niet noodzakelijk.

De ingangen van de component MI 24 01 zijn op grond van de interne meet-shunts stroomingangen en kunnen niet als spanningsingangen worden toegepast.

Bij niet gebruikte ingangskanalen moet de meetingang met het referentiepotentiaal worden verbonden. Negatieve invloeden op andere kanalan in geval van een draadbreuk (zwevende spanningswaarden) worden zodoende voorkomen.

Versie van het besturingssysteem	Handelwijze
Vanaf CPU BS V7	Het is voldoende, bij niet gebruikte ingangen geen globale variabele in te delen.
Tot CPU BS V6.x	Voor de niet gebruikte ingang in ELOP II hardware management het desbetreffende signaal *AI[0x].Used* auf den Standardwert *FALSE* resp. *0* zetten. Hiermee wordt het kanaal binnen het gebruikersprogramma uitgeregeld, d.w.z. er zijn geen signaalmeldingen meer beschikbaar.

Tabel 22: Configuratie van niet gebruikte ingangen

5.4.1 Testroutinen

De analoge waarden worden parallel via twee multiplexer en twee analoog/digitaal-omzetters met 12-bit resolutie verwerkt en de resultaten worden met elkaar vergeleken. Aanvullend worden via voorhanden digitaal/analoog-omzetters testwaarden opgeschakeld, weer in digitale waarden teruggevormd en met de voorgegeven waarde vergeleken.

5.4.2 Reactie in geval van storing

Treedt kanaalstoringen in de analoge ingangen op, activeert een compactsystem de LED *FAULT*, een F60 component de LED *ERR*.

5.4.2.1 CPU BS vanaf V7

De storingcode van het defecte kanaal wordt op een waarde > 0 gezet. Indien het zich om een storing voor de gehele component handelt, wordt de storingcode voor de component op een waarde > 0 gezet. Het gebruikersprogramma verwerkt de geparametreerde initiale waarde.

Is de waarde 0 mA in het toegestaan meetbereik onthouden, moet het gebruikersprogramma aanvullend tot de analoge waarde de storingcode evalueren.

De gebruikmaking van de storingcode biedt aanvullende mogelijkheden in het gebruikersprogramma de externe schakeling te controleren en storingreacties te programmeren.

De systeemvariabele die de storingcode omvat, heet *->Error Code [Byte].* Ze is toegankelijk in het register **...Channels** in het detailaanzicht van de component of van het toesteldeel, in de regel met het kanaalnummer.

5.4.2.2 CPU BS tot V6.x

De storingcode van het defecte kanaal wordt op een waarde > 0 gezet. Indien het zich om een storing voor de gehele component handelt, wordt de storingcode voor de component op een waarde > 0 gezet. Het gebruikersprogramma verwerkt de geparametreerde initiale waarde.

Het gebruikersprogramma moet aanvullend tot de analoge waarde de storingcode evalueren. Bij een waarde > 0 moet een veiligheidsgerichte reactie geprojecteerd zijn.

De gebruikmaking van de storingcode biedt aanvullende mogelijkheden in het gebruikersprogramma de externe schakeling te controleren en storingreacties te programmeren.

Het systeemsignaal dat de storingcode omvat, heet *Error Code AI[xx]*, storingcode, waarbij *xx* voor het kanaalnummer staat.Het is toegankelijk in het venster *Signal Connections...* van de component of het toesteldeel.

5.5 Veiligheidsgerichte tellers (F35 en F60)

De vermelde punten zijn zowel voor de teller-component van de F60 als ook voor de teller van de F35 van toepassing, voorzover geen specifieke benaming plaatsvindt.

5.5.1 Algemene informaties

Een tellerkanaal is voor het bedrijf als snelle voorwaarts-/achterwaartsteller met 24-bit resolutie of als decoder in de Gray-code parametreerbaar.

Bij het gebruik als snelle voorwaarts-/achterwaartsteller zijn als signalen de impulsingang en de telrichtingsingang in de toepassing noodzakelijk. Een reset vindt slechts in de gebruikersprogramma plaats.

De encoder-resolutie 4- of 8-bit geldt voor de teller-component CIO 2/4 01 van F60; bij de F35 heeft de encoder 3- of 6-bit resolutie. Een reset is mogelijk.

De verbinding van twee onafhankelijke 4-bit ingangen tot een 8-bit-ingang (voorbeeld voor F60) geschiedt uitsluitend per gebruikersprogramma. Een schakelmogelijkheid voor dit doeleinde is niet gepland.

De encoder-functie controleert de verandering van de bitpatronen aan de ingangskanalen. De bitpatronen aan de ingangen worden direct aan het gebruikersprogramma overhandigd. De weergave in PADt geschiedt in vorm van een met de bitpatroon overeenstemmende decimale cijfer (*Counter[0x].Value*).

Al naar applicatie kan dit getal dat aan het Gray-code-bitpatroon beantwoordt, bv in de bijbehorende decimale waarde worden omgevormd.

5.5.2 Reactie in geval van storing

Constateren de testroutingen in het tellerdeel van het toestel of van de component een storing, zetten een statusbit voor de evaluatie in het gebruikersprogramma. Aanvullend kan het gebruikersprogramma ook de desbetreffende storingcode in acht nemen.

Een compactsysteem activeert de *ERROR*, een F60 component de LED *ERR*.

De gebruikmaking van de storingcode biedt aanvullende mogelijkheden in het gebruikersprogramma de externe schakeling te controleren en storingreacties te programmeren.

Versie	Toegang tot de storingcode	Naam van de storingcode
Vanaf CPU BS V7	In het register ...*Channels* in het detailaanzicht van de component of het toesteldeel	->Storingcode [Byte] in de regel met het kanalnummer
Tot CPU BS V6.x	In het venster *Signal Connections....* van de component of het toesteldeel	Teller[*xx*].Storingcode, *xx* = kanalnummer

Tabel 23: Storingcodes bij telleringangen

5.6 Checklijst voor veiligheidsgerichte ingangen

Deze checklijst is een advies voor de projectering, programmering en ingebruikneming van veiligheidsgerichte ingangen. Ze is als planningdocument inzetbaar, dient echter gelijktijdig ook als bewijs voor een zorgvuldig uitgevoerde planning.

Voor iedere afzonderlijke van de in het systeem toegepaste veiligheidsgerichte ingangskanalen is in het kader van de projectering resp. ingebruikneming een eigen checklijst ter controle van de in acht te nemen vereisten in te vullen. Alleen dan kan worden gewaarborgd, dat de vereisten volledig en overzichtelijk zijn geregistreerd. De checklijst is ook een documentatie over de verbinding tussen externe bedrading en gebruikersprogramma.

De checklijst HIMatrix_Checklist_Inputs.doc staat als document in het formaat van Microsoft© Word© ter beschikking. Het ZIP.-bestand HIMatrix_Checklists.zip omvat alle checklijsten en kan van de HIMA website www.hima.com worden gedownload.

6 Uitgangen

Overzicht van de uitgangen van het HIMatrix systeem:

Toestel	Type	Aantal	veiligheids-gericht	elektrisch gescheiden
Compactsystemen				
F20	Digitaal	8	•	–[1)]
	Puls	4	-	–[1)]
F30 (configureerbaar voor Line Control)	Digitaal	8	•	–[1)]
F35	Digitaal	8	-	–[1)]
F1 DI 16 01	Puls	4	•	–[1)]
F2 DO 4 01	Digitaal	4	•	–[1)]
F2 DO 8 01	Digitaal	8	•	
F2 DO 16 01	Digitaal	16	•	–[1)]
F2 DO 16 02	Relais	16	•	
F3 DIO 8/8 01	Digitaal 1-polig	8	•	–[1)]
	Digitaal 2-polig	2		
F3 DIO 16/8 01	Digitaal 1-polig	16	•	–[1)]
	Digitaal 2-polig	8		
F3 AIO 8/4 01	Analoog	4	-	–[1)]
F3 DIO 20/8 02 (configureerbaar voor Line Control)	Digitaal	8	•	–[1)]
Modulair systeem F60				
DIO 24/16 01 (configureerbaar voor Line Control)	Digitaal	16	•	•
DO 8 01 (110V)	Relais	8	•	•
CIO 2/4 01	Digitaal	4	•	•
AO 8 01	Analoog	8	•	•
[1)] Referentiepotentiaal L-				

Tabel 24: Overzicht van de uitgangen

6.1 Algemene informaties

De besturing beschrijft de veiligheidsgerichte uitgangen een keer in iedere cyclus, leest de uitgangssignalen terug en vergelijkt ze met de voorgegeven uitgangsgegevens.

Bij de uitgangen is de waarde *0* of het geopende relaiscontact de veilige toestand.

In veiligheidsgerichte uitgangskanalen zijn drie testbare schakelaars in serie geïntegreerd. Zodoende is de veiligheidstechnisch vereiste, onafhankelijke tweede uitschakelweg uit de uitgangscomponent geïntegreerd. Deze geïntegreerde veiligheidsuitschakeling schakelt in geval van storing alle kanalen van de defecte uitgangscomponent veilig uit (energievrije toestand).

Bovendien is ook het watchdog-signaal van de CPU de tweede mogelijkheid van de veiligheidsuitschakeling: een wegval van het watchdog-signaal zorgt voor het directe innemen van de veilige toestand.

Deze functie is alleen werkzaam voor alle digitale uitgangen en relaisuitgangen van de besturingen.

De gebruikmaking van de desbetreffende storingcode biedt aanvullende mogelijkheden, storingsreacties in het gebruikersprogramma te configureren.

6.2 Veiligheid van actuatoren

In een veiligheidsgerichte toepassing moeten zowel de besturing als ook de hieraan aangesloten actuatoren aan de veiligheidsvereisten en de specifieke SIL beantwoorden.

6.3 Veiligheidsgerichte digitale uitgangen

De vermelde punten gelden zowel voor de digitale uitgangskanalen van de componenten van de F60 als ook voor de digitale uitgangskanalen van de compacttoestellen. Hiervan uitgezonderd zijn in beide gevallen de relaiscomponenten, tenzij deze specifiek worden genoemd.

6.3.1 Testroutinen voor digitale uitgangen

De toestellen en componenten worden automatisch gedurende het bedrijf getest.
De belangrijkste testfuncties zijn:

- Teruglezen van het uitgangssignaal van de schakelversterker. De schakeldrempel voor een teruggelezen low-niveau is 2 V. De ingezetten dioden voorkomen een terugvoeden van signalen,
- controle van de geïntegreerde dubbele veiligheidsuitschakeling,
- Een uitschakeltest de uitgangen geschiedt als achtergrondtest voor telkens max 200 µs. De minimumafstand tussen twee tests bedraagt ≥ 20 s.

De bedrijfsspanning van het gehele systeem wordt gecontroleerd, alle uitgangen worden bij een onderspanning van < 13 V afgeregeld.

6.3.2 Reactie in geval van storing

Constateert het toestel een foutief signaal, zet ze de betrokken uitgang van het toestel of de component via de veiligheidsschakelaars in de veilige (energievrije) toestand. Bij een modulestoring worden alle uitgangen van het toestel of de component uitgeschakeld.
Een toestel toont beide storingen aanvullend met de LED *ERROR*, een F60 component met de LED *ERR*.

6.3.3 Gedrag bij externe kortsluiting of overbelasting

Bij een kortsluiting van de uitgang naar L- of bij overbelasting blijft de testbaarheid van het toestel of de component bewaard. Een uitschakeling via de veiligheidsuitschakeling is niet noodzakelijk.

De besturing controleert de gehele stroomopname van het toestel of de component en zet bij overschrijden de drempen van alle uitgangskanalen in de veilige toestand.

De uitgangen worden in deze toestand cyclisch in een afstand van weinige seconden gecontrolerd, of de overbelasting nog voorhanden is. Bij normale toestand worden de uitgangen weer bijgeschakeld.

6.3.4 Line Control

De besturing kan veiligheidsgerichte digitale uitgangen pulsen en samen met veiligheidsgerichte digitale ingangen van hetzelfde systeem (niet echter met parametreerbare digitale ingangen) voor een kortsluiting- en draadbreuk-herkenning toepassen, zie hoofdstuk 5.3.6.

INSTRUCTIE

Storingen van de aangesloten actuatoren mogelijk!

Pulsuitgangen mogen niet als veiligheidsgerichte uitgangen worden toegepast, bv ter aansturing van veiligheidsgerichte actuatoren!

Relaisuitgangen kunnen niet als pulsuitgangen worden toegepast.

6.4 Veiligheidsgerichte 2-polige digitale uitgangen

De hier beschreven eigenschappen relateren naar 2-polige digitale uitgangen van de Remote I/Os F3 DIO 8/8 01 en F3 DIO 16/8 01.

De toestellen testen zich automatisch gedurende het bedrijf. De belangrijkste testfuncties zijn:

- Teruglezen van het uitgangssignaal van de schakelversterker. De ingezetten dioden voorkomen een terugvoeden van signalen.
- Controle van de geïntegreerde (dubbele) veiligheidsuitschakeling
- Een uitschakeltest de uitgangen geschiedt als achtergrondtest voor telkens max 200 µs. De minimumafstand tussen twee tests bedraagt ≥ 20 s.
- Draaddiagnose bij 2-poligem aansluiting
  F3 DIO 16/8 01:
  - Kortsluiting tegen L+, L-
  - Kortsluiting tussen 2-polige aansluitingen
  - Draadbreuk in één van de beide 2-polige aansluitingen

  F3 DIO 8/8 01:
  - Kortsluiting tegen L+, L-

Het systeem controleert zijn bedrijfsspanning en regelt alle uitgangen bij een onderspanning < 13 V af.

Bij een 2-polige aansluiting dienen de volgende instructies in acht te worden genomen:

i Een abusievelijk inschakelen van een aan de uitgang aangesloten relais of actuator mogelijk!

Bij toepassingen in de machineveiligheid zijn bij herkennen van een kortsluiting de uitgangen DO+, DO- uit te schakelen.

i Kunnen de boven vermelde vereisten niet worden vervuld, dient er rekening te worden gehouden met het volgende geval:

Bij een kortsluiting van DO- naar L- kan een relais aantrekken of een overige actuator in een andere schakeltoestand worden verzet.

Reden: gedurende de voor de draaddiagnose lopende controletijd ligt een 24-V-spanningsniveau (DO+ uitgang) aan de verbruiker (relais, schakelende actuator) aan, zo dat deze voldoende elektrische energie zou kunnen opnemen, om in een andere toestand te schakelen.

De controletijd dient zo te worden geparametreerd, dat een actuator door de testpuls voor de draaddiagnose niet kan worden geactiveerd.

i Storing van de draadbreuk-herkenning mogelijk!

Bij 2-polige aansluiting mag geen DI-ingang met een DO-uitgang zijn verbonden. Dit zou het opsporen van een draadbreuk voorkomen.

6.4.1 Reactie in geval van storing

DO- uitgangen

Bij constateren van een foutief signaal zet het toestel de betrokken uitgang in de veilige, energievrije toestand. Een storing van het toestel leidt tot uitschakelen van alle uitgangen. Beide storingssoorten toont het toestel bovendien met de LED *ERROR* aan.

DO+ uitgangen

Bij constateren van een foutief signaal zet het toestel de betrokken uitgang in de veilige, energievrije toestand. Een storing van het toestel leidt tot uitschakelen van alle uitgangen. Beide storingssoorten toont het toestel bovendien met de LED *ERROR* aan.

6.4.2 Gedrag bij externe kortsluiting of overbelasting

Bij een kortsluiting van de uitgang naar L-, L+ of bij overbelasting blijft de testbaarheid van het toestel bewaard. Een uitschakeling via de veiligheidsuitschakeling is niet noodzakelijk.

De gehele stroomopname van het toestel wordt gecontroleerd. Bij overschrijden van de drempel zet het toestel alle kanalen in de veilige toestand.

Het toestel controleert in deze toestand cyclisch in een afstand van weinige seconden, of de overbelasting van de uitgangen nog voorhanden is. Bij normale toestand schakelt het toestel de uitgangen weer bij.

6.5 Relaisuitgangen

De relaisuitgangen stemmen overeen met functioneel digitale uitgangen, bieden echter galvanische scheiding en hogere proefspanning.

6.5.1 Testroutinen voor relaisuitgangen

Het toestel of de component test zijn uitgangen automatisch gedurende het bedrijf.
De belangrijkste testfuncties zijn:

- Teruglezen van de uitgangssignalen van de schakelversterker voor de relais,
- controle van het schakelen van de relais met gedwongen gevoerde contacten,
- Controle van de geïntegreerde dubbele veiligheidsuitschakeling.

Het systeem controleert zijn bedrijfsspanning en regelt alle uitgangen bij een onderspanning < 13 V af.

Bij de component DO 8 01 en de Remote I/Os F2 DO 8 01 en F2 DO 16 02 zijn de uitgangen met drie veiligheidsrelais uitgerust:

- twee relais met gedwongen gevoerde contacten
- een standaardrelais

Hiermee zijn de uitgangen voor veiligheidsuitschakelingen toepasbaar.

6.5.2 Reactie in geval van storing

Bij constateren van een foutief signaal zet het toestel of de betrokken component de betrokken uitgang via de veiligheidsschakelaar in de veilige, energievrije toestand. Bij een modulestoring schakelt het alle uitgangen uit. Beiude storingen toont een compactsysteem aanvullend met de LED *ERROR*, een F60 component met de LED *ERR*.

6.6 Veiligheidsgerichte analoge uitgangen (F60)

De component AO 8 01 heeft een eigen veiligheidsgericht 1oo2 A/D-microprocessorsysteem met veilige communicatie. Het beschrijft de analoge uitgangen een keer per cyclus en slaat de waarden intern op. De component test haar functie zelf.

DIP-schakelaars op de veiligheidsgerichte analoge uitgangscompoenten kunnen de uitgangen op spanning- of stroomuitgang instellen. Hierbij dient te worden gewaarborgd, dat hun instelling met het gebruik in het systeem en de parametrering in het gebruikersprogramma overeenstemmen. Een veronachtzaming leidt tot een foutief gedrag van de component.

INSTRUCTIE

Foutieve functie van de component

Voor het inzetten van de component in het systeem controleren:

- **DIP-schakelaarinstellingen van de component.**
- **Parametrering van de component in het gebruikersprogramma.**

Al naar keuze van het type toestel (...FS1000, ...FS2000) bij de configuratie, dienen in de logica verschillende waarden voor de uitgangssignalen in acht te worden genomen, om identieke uitgangswaarden te verkrijgen, zie AO 8 01 handboek (AO 8 01 Manual HI 800 1975 E), hoofdstuk *Signals and Error Codes of the Outputs*.

Telkens twee analoge uitgangen zijn galvanisch met elkaar verbonden:

- uitgang 1 en 2.
- uitgang 3 en 4.
- uitgang 5 en 6.
- uitgang 7 en 8.

De analoge uitgangscircuits verkrijgen stroom- of spanningcontrole, teruglees- en testkanalan ook voor parallele uitgangscircuits, alsook twee extra veiligheidsschakelaars voor de veilige uitschakeling van de uitgangsstroomcircuits in geval van storing. Hierdoor wordt de veilige toestand (stroomuitgang: 0 mA, spanninguitgang: 0 V) bereikt.

6.6.1 Testroutinen

De component wordt automatisch gedurende het bedrijf getest. De belangrijkste testfuncties zijn:

- Dubbel teruglezen van het uitgangssignaal.
- Test op overspreken tussen de uitgangen.
- Controle van de geïntegreerde veiligheidsuitschakeling.

6.6.2 Reactie in geval van storing

Eenmaal per cyclus leest de component de uitgangssignalen terug en vergelijkt ze met de intern opgeslagen uitgangssignalen. Constateert de component een discrepantie, schakelt ze de foutieve uitgangskanaal via de beide veiligheidsschakelaars uit en meldt de modulestoring via de LED *ERR*.

Met de gebruikmaking van de desbetreffende storingcode existeren aanvullende mogelijkheden, storingsreacties in het gebruikersprogramma te configureren.

Voor de worst case-reactietijd van de analoge uitgangen is bij de dubbele watchdog-tijd ($2 * WDZ_{CPU}$) nog de dubbele watchdog-tijd van de AO-CPU ($2 * WDZ_{AO\text{-}\mu C}$) op te tellen.

De worst case-reactietijd is in het handboek vermeld.

6.7 Analoge uitgangen met veiligheidsgericht uitschakeling (F3 AIO 8/4 01)

De Remote I/O beschrijft de analoge uitgangen een keer per cyclus en slaat de waarden intern op.

De uitgangen zijn nicht veiligheidsgericht, ze kunnen echter samen veilig worden uitgeschakeld.

Voor het bereiken van SIL 4 moeten de uitgangswaarden via veiligheidsgerichte analoge ingangen worden teruggelezen en in het gebruikersprogramma worden geëvalueerd.
Daar moeten ook reacties op foutieve uitgangswaarden worden vastgelegd.

6.7.1 Testroutinen

De Remote I/O test de beide veiligheidsschakelaars voor het uitschakelen van alle vier uitgangen automatisch gedurende het bedrijf.

6.7.2 Reactie in geval van storing

Bij een interne storing van de Remote I/O worden alle vier uitgangskanalen gelijktijdig via de beide veiligheidsschakelaars uitgeschakeld en de modulestoring via de LED *FAULT* op de frontplaat gemeld.

Met de gebruikmaking van de desbetreffende storingcode bestaan aanvullende mogelijkheden, storingsreacties in het gebruikersprogramma te configureren.

6.8 Checklijst voor veiligheidsgerichte uitgangen

Deze checklijst is een advies voor de projectering, programmering en ingebruikneming van veiligheidsgerichte uitgangen. Ze is als planningdocument inzetbaar, dient echter gelijktijdig ook als bewijs voor een zorgvuldig uitgevoerde planning.

Voor iedere afzonderlijke van de in het systeem toegepaste veiligheidsgerichte uitgangskanalen is in het kader van de projectering resp. ingebruikneming een eigen checklijst ter controle van de in acht te nemen vereisten in te vullen. Alleen dan kan worden gewaarborgd, dat de vereisten volledig en overzichtelijk zijn geregistreerd. Hiermee kan ook een documentatie over de verbinding tussen externe bedrading en gebruikersprogramma plaatsvinden.

De checklijst *HIMatrix_Checklist_Outputs.doc* staat als document in het formaat van Microsoft© Word© ter beschikking. Het ZIP.-bestand *HIMatrix_Checklists.zip* omvat alle checklijsten en kan van de HIMA website www.hima.com worden gedownload.

7 Software voor HIMatrix systemen

De software voor de veiligheidsgerichte automatiseringstoestellen van de HIMatrix systemen deelt zich in de volgende blokken in:

- besturingssysteem,
- gebruikersprogramma,
- programmeerwerktuig volgens IEC 61131-3.

Het besturingssysteem wordt in het centraal gedeelte (CPU) van de besturing geladen en is in de telkens geldige, door de TÜV gekeurde vorm voor veiligheidsgerichte toepassingen in te zetten.

Het programmeerwerktuig dient ter vervaardiging van het gebruikersprogramma dat de installatiespecifieke functies omvat, de het automatiseringstoestel dient uit te voeren.
De parametrering en bediening van functies van het besturingssysteem geschiedt eveneens via het programmeerwerktuig.

De codegenerator van het programmeerwerktuig zet het gebruikersprogramma in de machinecode om. Het programmeerwerktuig zet deze machinecode via een Ethernet-interface in de flash-EPROMs van het automatiseringstoestel over.

7.1 Veiligheidstechnische aspecten voor het besturingssysteem

Ieder toegelaten besturingssysteem is door zijn benaming gekenmerkt. Voor een betere onderscheiding zijn de revisie en de CRC-signatuur vermeldt. De telkens geldige, door de TÜV voor veiligheidsgerichte automatiseringstoestellen toegelaten versies van het besturingssysteem en de bijbehorende signaturen (CRCs) zijn aan de revisiecontrole onderworpen en worden in een lijst gedocumenteerd die HIMA gemeenschappelijk met de TÜV vervaardigt.

Een uitlezen van de draaiende versie van het besturingssysteem is alleen met het programmeerwerktuig mogelijk. Een controle door de gebruiker is noodzakelijk, zie hoofdstuk 7.6.

7.2 Werkwijze en functies van het besturingssysteem

Het besturingssysteem werkt het gebruikersprogramma cyclisch af. Hierbij worden in sterk vereenvoudigde vorm de volgende functies uitgevoerd:

- Lezen van de ingangsgegevens,
- Verwerken van de logicafuncties die volgens IEC 61131-3 werden geprogrammeerd,
- Schrijven van de uitgangsgegevens.

Hier komen de volgende belangrijke functies bij:

- Omvangrijke zelftests,
- Tests van de I/O-componenten gedurende het bedrijf,
- Datatransmissie,
- Diagnose.

7.3 Veiligheidstechnische aspecten voor de programmering

7.3.1 Veiligheidsconcept van het programmeerwerktuig

Het veiligheidsconcept van de programmeerwerktuigen ELOP II Factory en SILworX:

- Bij de installatie van het programmeerwerktuig zekert een CRC-testsom de integriteit van het programmapakket op de weg van de fabrikant naar de gebruiker.
- Het programmewerktuig voert plausibiliteitskeuringen uit, om storingen bij de invoer te reduceren.
- Dubbele compilatie met aansluitende vergelijking van de vervaardigde CRC-testsommen waarborgt, dat vervalsingen van de toepassing door temporaire storingen van de toegepaste PCs worden herkend.
- Het programmeerwerktuig en de in dit veiligheidshandboek vastgelegde maatregelen maken het voldoende onwaarschijnlijk, dat een semantisch en syntactisch correcte code wordt vervaardigt die nog niet herkende systematische storingen uit het proces van de code-vervaardiging onthoudt.

Functietest van de besturing

1. Controle van de correcte omzetting van de besturingstaak aan de hand van de gegevens en signaalstromen.
2. Volledige functiecontrole van de logica door beproeving (zie controle van de configuratie en het gebruikersprogramma).

De besturing en het gebruikersprogramma zijn voldoende gecontroleerd.

Vanaf CPU BS V7

De veilige revisievergelijker van SILworX kan de veranderingen tegenover voorafgaande versies opsporen en weergeven.

Na een verandering van het gebruikersprogramma zijn slechts die programmadelen te testen die van de verandering getroffen.

Tot CPU BS V6.x

Na een verandering van het gebruikersprogramma is dit door een complete functietest te controleren.

7.3.2 Controle van de configuratie van het gebruikersprogramma

Om het vervaardigde gebruikersprogramma op naleving van de specifieke veiligheidsfunctie te controleren, dienen geschikte testgevallen te worden vervaardigt, die de specificatie afdekken.

In de regel is de onafhankelijke test van iedere loop (bestaand uit ingang, de uit gebruikerszicht belangrijke koppelingen, en uitgang) voldoende.

Ook voor de numerieke evaluatie van formules zijn geschikte testgevallen te genereren. Zinvol zijn equivalentieklassetests, dit zijn tests binnen gedefinieerde waardbereiken, aan de grenzen of in ongeoorloofde waardebereiken. De testgevallen moeten zo worden gekozen, dat de correctheid van de berekening wordt aangetoond. Het vereist aantal van testgevallen is afhankelijk van de toegepaste formule en moet kritische waardeparen omvatten.

HIMA adviseert, een actieve simulatie met bronnen uit te voeren. Hiermee is een correcte bedrading van de sensoren en actuatoren van het systeem aantoonbaar, ook voor via Remote I/Os aangesloten sensoren en actuatoren. Alleen zo is het mogelijk, de systeemconfiguratie te controleren.

Deze handelwijze betreft de eerste vervaardiging van een gebruikersprogramma alsook diens veranderingen.

7.3.3 Archiveren van een project

HIMA adviseert, na ieder laden van het programma in de besturing, het programma te archiveren.

Het archiveren van een project verschilt principieel tussen de werktuigen ELOP II Factory en SILworX.

Archiveren van een project CPU BS V7

SILworX legt een project in een projectbestand aan. Dit is geschikt, bv op een geheugenmedium, te zekeren.

Vervaardiging van een projectarchief tot CPU BS V6.x

ELOP II Factory legt een project in een subregisterstructuur aan. Ter archivering kan ELOP II Factory de inhoud van deze structuur in een archiefbestand, het projectarchief, opslaan. Dit projectarchief is geschikt, bv op een geheugenmedium, te zekeren.

Vervaardiging van een project-archief

1. Printen van het gebruikersprogramme ter vergelijking van de logica met de voorgegeven richtlijnen.
2. Overzetten van het gebruikersprogramma ter vervaardiging van de configuratie-CRC van de CPU.
3. Noteren van de versie van de configuratie-CRC van de CPU. Hiervoor wordt in het hardware-managment de besturing gekozen, en in het contextmenu **Configuratie-informaties** worden de versies weergegeven. Tot het bepalen van een versie behoren:
   - rootcpu.config toont de veiligheidsgerichte configuratie van de CPU, de configuratie-CRC van de CPU.
   - rootcom.config toont de niet-veiligheidsgerichte configuratie van de COM.
   - root.config toont de gehele configuratie inclusieve de Remote I/Os (CPU + COM).
4. Archief van het project op opslagmedium vervaardigen en van namen van de gebruikersprogrammas, configuratie-CRCs van de CPUs en datum voorzien.
   Dit advies vervangt niet de interne documentatievereisten van de gebruiker.

Het projectarchief is vervaardigd.

7.3.4 Mogelijkheid ter programma- en configuratie-identificatie

De gebruikersprogramma´s worden duidelijk aan de configuratie-CRCs van het project geïdentificeerd. Dit laat zich met de configuratie-CRC van het geladen project vergelijken.

Projectbestanden - vanaf CPU BS V7

Om te waarborgen, dat het gezekerde projectbestand onveranderd is, de onthouden ressource compileren en de configuratie-CRC met de CRC van de geladen configuratie vergelijken.
Dit kan met SILworX worden aangetoond.

Archieven - tot CPU BS V6.x

De benaming van een archief dient de configuratie-CRCs van de root.config te omvatten.

Om te waarborgen, dat het toegepaste archief onveranderd is, de ressource na het herstel van het project uit het archief compileren en de configuratie-CRC van de root.config met de CRC van de geladen configuratie vergelijken die met ELOP II Factory kan worden weergegeven.

Ter controle opent men in het control panel de ressource van het menu
Ressource → Consistentie controleren.

i Bij de eerste ingebruikname of een verandering van het gebruikersprogramma van een veiligheidsgerichte besturing dient een volledige functietest te worden uitgevoerd.

Een project-archief is te vervaardigen.

7.4 Parameters van de ressource

⚠ WAARSCHUWING

Lichamelijk letsel door foutieve configuratie mogelijk!

Noch het programmerwerktuig noch de besturing kunnen enkele projectspecifiek vastgelegde parameters controleren. Vandaar is het in ieder geval noodzakelijk deze parameters correct in het programmeerwerktuig te registreren en de plaatsgevonden aantekening te controleren.

Deze parameters zijn:

- **System ID**
- **Rack ID, zie het systeemhandboeken (HI 800 640 NL en HI 800 191 E).**
- **Safety Time**
- **Watchdog Time**
- **Allow Online Settings (tot SILworX V5: Main Enable)**
- **Autostart**
- **Start Allowed**
- **Load Allowed**
- **Reload Allowed**
- **Global Forcing Allowed**

De onderstaand vermelde parameters worden in het programmeerwerktuig voor de toegestane handelingen in het veiligheidsgericht bedrijf van het automatiseringstoestel vastgelegd en als veiligheidsgerichte parameters gekenmerkt.

De gedurende het veiligheidsgericht bedrijf mogelijke vastleggingen zijn niet stijf aan een bepaalde vereistenklasse gebonden, maar zijn voor iedere inzet van de besturing met de bevoegde keuringsinstantie af te stemmen.

7.4.1 Parameters vanaf CPU BS V7

Vanaf CPU BS V7 is er een verdeling in systeemparameters van de ressource en systeemparameters van de hardware.

Systeemparameters van de ressource

Deze parameters leggen de verhouding van de besturing gedurende het bedrijf vast en worden in SILworX ingesteld, in het diagloogvenster **Properties** van de ressource.

Parameters / Schakelaars	Beschrijving	Standaard-waarde	Instelling voor veilig bedrijf
Name	Naam van de ressource		Willekeurig
System ID [SRS]	Systeem-ID van de ressource 1...65 535 Het is noodzakelijk, de systeem-ID een andere waarde dan de standaardwaarde toe te delen, anders is het project niet tot afloop bekwaam!	60 000	Eenduidige waarde binnen het netwerk van de besturingen. Dat zijn alle besturingen die potentieel met elkaar zijn verbonden.
Safety Time [ms]	Veiligheidstijd in milliseconden 20...22 500 ms	600 ms/ 400 ms[1)]	applicatie-specifiek
Watchdog Time [ms]	Watchdog-tijd in milliseconden 8...5000 ms voor standaardtoestellen/-componenten 4…5000 ms voor F*03-toestellen-/componentengroepen	200 ms/ 100 ms[1)]	applicatie-specifiek

Parameters / Schakelaars	Beschrijving	Standaard-waarde	Instelling voor veilig bedrijf
Target Cycle Time [ms]	Gewenste of maximale cyclustijd, zie *Target Cycle Time Mode*, 0...7500 ms. De norm-cyclustijd mag hooguit zo groot zijn dan de *Watchdog Time* – minimale watchdog-tijd, anders wijst de PES ze af. Is de standaardwaarde 0 ms ingesteld, wordt de norm-cyclustijd niet in acht genomen.	0 ms	applicatie-specifiek
Target Cycle Time Mode	Toepassing van de *Target Cycle Time [ms]* zie Tabel 26. Bij F*03-toestellen/componenten zijn alle waarden toepasbaar, bij standaard-toestellen/componenten alleen *vast*!	Fixed-tolerant	applicatie-specifiek
Multitasking Mode	Alleen toepasbaar bij F*03-toestellen/componenten! Mode 1 De lengte van een cyclus van de CPU richt zich naar de vereiste uitvoeringsduur van alle gebruikersprogramma´s. Mode 2 Processor stelt van gebruikersprogramma´s met lage prioriteit niet benodigde uitvoeringstijd aan de gebruikersprogramma´s met hoge prioriteit ter beschikking. Bedrijfssoort voor hoge beschikbaarheid. Mode 3 Processor wacht niet benodigde uitvoeringstijd van gebruikersprogramma´s af en verlengt zo de cyclus.	Mode 1	applicatie-specifiek
Max.Com. Time Slice ASYNC [ms]	Maximumwaarde in ms van de tijdschijf die binnen de cyclus van de ressource voor communicatie wordt toegepast, zie communicatiehandboek (Communication Manual HI 801 101 ED), 2...5000 ms	60 ms	applicatie-specifiek
Max. Duration of Configuration Connections [ms]	Alleen toepasbaar bij F*03-toestellen/componenten! Definieert, hoe veel tijd binnen een CPU-cyclus voor de procesdatacommunicatie ter beschikking staat, 2...3500 ms	6 ms	applicatie-specifiek
Maximum System Bus Latency [µs]	Voor HIMatrix besturingen niet toepasbaar!	0 µs	-
Allow Online Settings	ON: Alle onder OFF genoemde schakelaars/parameters zijn online met de PADT veranderbaar. OFF: Deze parameters zijn **niet** online veranderbaar: ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Load Allowed* ▪ *Reload Allowed* ▪ *Start Allowed* Deze parameters zijn online veranderbaar, wanneer *Reload Allowed* ON is: ▪ *Resource Watchdog Time* ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* Ze zijn niet online veranderbaar, wanneer *Reload Allowed* OFF is. i Alleen bij gestopte PES is het mogelijk, *Allow Online Settings* op ON te zetten!	ON	OFF geadviseerd

Parameters / Schakelaars	Beschrijving	Standaard-waarde	Instelling voor veilig bedrijf
Autostart	ON: Wordt het processorsysteem aan de voedingspanning aangesloten, start het gebruikersprogramma automatisch OFF: geen automatische start na bijschakelen van de voedingspanning.	OFF	applicatie-specifiek
Start Allowed	ON: Koude start of warme start door PADT in de toestand RUN of STOP toegestaan. OFF: Geen start toegestaan	ON	applicatie-specifiek
Load Allowed	ON: Download van de configuratie toegestaan OFF: Download van de configuratie niet toegestaan	ON	applicatie-specifiek
Reload Allowed	Alleen toepasbaar bij F*03-toestellen/componenten! ON: Reload van de configuratie toegestaan. OFF: Reload van de configuratie niet toegestaan. Een draaiende reload-proces wordt bij het omschakelen op OFF niet gestopt	ON	
Global Forcing Allowed	ON: Globaal forcen voor deze ressource toegestaan OFF: Globaal forcen voor deze ressource niet toegestaan	ON	applicatie-specifiek
Global Force Timeout Reaction	Legt vast, hoe zich de ressource bij de afloop van de globale force-timeout gedraagt: ▪ Stop Forcing ▪ Stop the Resource	Stop Forcing	applicatie-specifiek
Minimum Configuration Version	Met deze instelling is het mogelijk, een code te genereren die in overeenstemming met de projectvereisten met oude of nieuwe versies van het CPU-besturingssysteem compatibel is. SILworX V2: Codegenereren vindt bij SILworX V2 plaats. Met deze instelling wordt de inzet van de code op standaard-toestellen en -componenten met het CPU-besturingssysteem V 7 ondersteunt. SILworX V3: Voor HIMatrix besturingen niet toepasbaar! SILworX V4: De gegenereerde code is compatibel met het CPU-besturingssysteem V8. SILworX V5: Stemt overeen met *SILworX V4*. Met deze instelling is de compatibiliteit met latere versies gewaarborgd. Deze parameter wordt bij projecten die uit een voorafgaande versie werden geconverteerd, op de daar gekozen instelling gezet.	SILworX V5 bij nieuwe projecten	applicatie-specifiek
safeethernet-CRC	SILworX V.2.36.0: De vervaardiging van de CRC voor safe**ethernet** geschiedt zoals in SILworX V.2.36.0. Deze instelling is noodzakelijk voor de datauitwisseling met ressourcen die met SILworX V.2.36 of vroeger zijn gepland. Actuele versie: De vervaardiging van de CRC voor safe**ethernet** geschiedt met het actuele algoritme.	Actuele versie	applicatie-specifiek

[1] Eerste waarde geldt voor besturingen, tweede waarde voor Remote I/Os.

Tabel 25: Systeemparameters van de ressource vanaf CPU BS V7

De volgende tabel beschrijft de werking van de normcyclustijd-modus.

Target Cycle Time Mode	Werking op gebruikersprogramma´s	Werking op reload van processormodulen
Fixed	De PEs volgt de norm-cyclustijd op en verlengt de cyclus, indien nodig. Indien de afwerkingstijd van de gebruikersprogramma´s de normcyclustijd overschrijdt, wordt de cyclus verlengd.	Reload wordt alleen uitgevoerd, indien de norm-cyclustijd voldoende is.
Fixed-tolerant	Zoals bij *Fixed*.	Hooguit iedere vierde cyclus wordt verlengd, om reload uit te voeren.
Dynamic-tolerant	Zoals bij *Dynamic*.	Hooguit iedere vierde cyclus wordt verlengd, om reload uit te voeren.
Dynamic	HIMatrix houdt naar mogelijkheid de norm-cyclustijd aan en voert de cyclus in zo kort als mogelijke tijd uit.	Reload wordt alleen uitgevoerd, indien de norm-cyclustijd voldoende is.

Tabel 26: Werking van de normcyclustijd-modus

Aanwijzing met betrekking tot de parameter *Minimum Configuration Version*:

- Bij een nieuw aangelegd project wordt telkens de meest actuele *Minimum Configuration Version* gekozen. Of deze instelling bij de toegepaste hardware past, moet worden gecontroleerd, bv vereisen HIMatrix standaard-toestellen de waarde *SILworX V2* voor de *Minimum Configuration Version*.
- Bij een project dat door een vroegere SILworX versie werd geconverteerd, blijft de in de voorafgaande versie ingestelde waarde voor de *Minimum Configuration Version* bewaard. Hierdoor is gewaarborgd, dat de codegeneratie dezelfde configuratie-CRC vervaardigt dan in de voorafgaande versie en de gegenereerde configuratie compatibel met het besturingssysteem in de hardware blijft.

  Bij geconverteerde projecten dient vandaar de *Minimum Configuration Version* niet te worden gewijzigd.
- SILworX vervaardigt automatisch een hogere configuratieversie dan de ingestelde *Minimum Configuration Version*, wanneer in het project capaciteiten worden benut, die alleen een hogere configuratieversie ter beschikking stelt. Dit toont SILworX in het resultaat van de codegeneratie. De hardware verwerpt het laden van een hogere configuratieversie dan tot haar besturingssysteem passend.

  Als remedie kan de confrontatie van de door de versievergelijker gelevderde informaties met de het overzicht over de modulegegevens dienen.
- Is voor een ressource een *Minimum Configuration Version* van *SILworX V4* of hoger ingesteld, moet in ieder gebruikersprogramma (zie beneden) de parameter *Code Generation Compatibilty* op *SILworX V4* worden ingesteld.

Systeemvariabelen van de hardware vanaf CPU BS V7

Deze variabelen dienen ertoe, het gedrag van de besturing in het draaiend bedrijf bij bepaalde toestanden te veranderen. Deze variabelen zijn instelbaar in de Hardware Editor van SILworX, in het detailaanzicht van de hardware.

Parameters / Schakelaars	Functie	Standaard-instelling	Instelling voor veilig bedrijf
Force Deactivation	Dient voor het verhinderen en direct uitschakelen van het forcen	FALSE	applicatie-specifiek
Spare 0...Spare 16	Geen functie	-	-
Emergency Stop 1... Emergency Stop 4	Nooduitschakelaar voor het uitschakelen van de besturing in door het gebruikersprogramma ontdekte storingsgevallen	FALSE	applicatie-specifiek
Relaiscontact 1... Relaiscontact 4	Alleen toepasbaar bij F*03! Stuurt de desbetreffende relaiscontacten aan, indien voorhanden.	FALSE	applicatie-specifiek
Read-only in RUN	Na het starten van de besturing is geen bedienhandeling (stop, start, download) via SILworX meer mogelijk, uitzonderingen: forcen en reload	FALSE	applicatie-specifiek
Reload Deactivation	Alleen toepasbaar bij F*03! Voorkomt een laden van de besturing door middel van reload.	FALSE	applicatie-specifiek
User-LED 1... User LED 2	Alleen toepasbaar voor speciale besturingen! Stuurt de desbetreffende LED aan, indien voorhanden.	FALSE	-

Tabel 27: Systeemvariabelen van de hardware vanaf CPU BS V7

Deze systeemvariabelen laten zich bij globale variabelen indelen, diens waarde door een fysieke ingang of de logica van het gebruikersprogramma wordt gewijzigd.

Voorbeeld. aan een digitale ingang is een sleutelschakelaar aangesloten. De digitale ingang is bij een globale variabele ingedeeld die de systeemvariabelen *Read-only in Run* is toegewezen. Dan kan de bezitter van een sleutel met de sleutelschakelaar de bedienhandelingen *Stop*, *Start*, en *Download* toelaten of blokkeren.

7.4.2 Systemparameters tot CPU BS V6.x

Schakelaar	Functie	Standaard -waarde	Instelling voor veilig bedrijf
Main Enable	De volgende schakelaars/parameters kunnen in het bedrijf (= RUN) met de PADT worden veranderd.	ON	OFF [1)]
Autostart	Automatisch starten na Power ON van de besturing.	OFF	ON / OFF [2)]
Start/Restart Allowed	Koude start, warme start of hete start door PADT in de toestand RUN of STOP.	ON	OFF [1)]
Load Allowed	Laadvrijgave voor een gebruikersprogramma.	ON	ON
Test Mode Allowed	Testmodus voor het gebruikersprogramma toegestaan of verboden. Bij de testmodus wordt de afwerking van het programma bevroren resp. gestopt. De uitgangen blijven aangestuurd en de afwerking van het programma kan in enkel-cyclus-stappen worden uitgevoerd.	OFF	OFF
Changing the variables in the OLT allowed	Waarden van variabelen laten zich in de online-test (OLT)-velden van de logica weergeven en veranderen.	OFF	OFF [3)]
Forcing Allowed	Invoer en activering van waarden voor variabelen/signalen van de PES zijn toegestaan, onafhankelijk van de actuele waarde van het proces- of logicasignaal.	OFF	Door keuringsinstantie vastgelegd
Stop at Force Timeout	Stop van de CPU na overschrijden van de force-tijd.	ON	Door keuringsinstantie vastgelegd

[1)] In het RUN-bedrijf is alleen de wissel op de waarde OFF mogelijk.

[2)] Instelling ON of OFF is applicatiespecifiek.

[3)] In het RUN-bedrijf is alleen de wissel naar ON mogelijk.

Tabel 28: Parameters van de ressource tot CPU BS V6.x

7.5 Bescherming tegen manipulaties

De gebruiker moet samen met de bevoegde keuringsinstantie defineren, welke maatregelen ter bescherming tegen manipulatie worden toegepast.

In de PES en in het programmeerwerktuig zijn beschermingsmechanismen geïntegreerd die abusievelijke of niet ingewilligde veranderingen aan het veiligheidssysteem voorkomen:

- Een verandering van het gebruikersprogramma of de configuratie leidt tot een nieuwe CRC. Deze veranderingen kunnen alleen met een download naar de besturing worden overgebracht (de besturing is hierbij in de STOP).
- De bedienmogelijkheden zijn afhankelijk van het inloggen van de gebruiker bij het PES.
- Het programmeerwerktuig benodigt voor de verbinding naar de PES bij het inloggen van de gebruiker een codewoord.
- De verbinding tussen PADT en PEs is gedurende hete RUN-bedrijf niet noodzakelijk en kan worden onderbroken.

De vereisten van de veiligheids- en toepassingsnormen met betrekking tot de bescherming tegen manipulaties dienen in acht te worden genomen. De autoristatie van medewerkers en de vereiste veiligheidsmaatregelen zijn aan de verantwoordelijkheid van de exploitant onderworpen.

INSTRUCTIE

Slechts bevoegd personeel mag op de HIMatrix besturing toegrijpen!

Ter bescherming tegen onbevoegde veranderingen aan de besturing de volgende maatregelen nemen:

- **Standaardinstellingen voor gebruikernaam en codewoord veranderen.**
- **Iedere gebruiker moet zijn codewoord geheim houden.**
- **De PADt na afsluiting van de ingebruikneming van de besturing scheiden en alleen dan opnieuw verbinden, als veranderingen noodzakelijk zijn.**

De toegang tot de gegevens van de PES is alleen mogelijk, wanneer de toegepaste PADT over het programmeerwerktuig en het gebruikersproject in de actueel draaiende versie (archief-onderhoud!) beschikt.

De verbinding tussen PADT en PES is alleen voor de download van het gebruikersprograma of het uitlezen van variabelen /signalen noodzakelijk. Gedurende het normaal bedrijf is de PADT niet noodzakelijk. Een scheiding van PADT en PES in de normale bedrijfsfase beschermt tegen ongeoorloofd toegrijpen.

7.6 Checklijst voor de vervaardiging van een gebruikersprogramma

Deze checklijst is een advies voor de gebruiker voor de inachtneming van de veiligheidstechnische aspecten bij de programmering voor en na het laden van het nieuwe of gewijzigde programma.

De checklijst *HIMatrix_Checklist_Program.doc* staat als document in het formaat van Microsoft© Word© ter beschikking. Het ZIP.-bestand *HIMatrix_Checklists.zip* omvat alle checklijsten en kan van de HIMA website www.hima.com worden gedownload.

8 Veiligheidstechnische aspecten voor het gebruikersprogramma

Algemene afloop van de programmering van de HIMatrix automatiseringstoestellen voor veiligheidstechnische toepassingen:

- Specificatie van de besturingsfunctie.
- Schrijven van het gebruikersprogramma.
- Compileren van het gebruikersprogramma met de C-code-generator.
- Tweemalig overzetten van het gebruikersprogramma, beide resultaten (CRC) moeten worden vergeleken.
- Het programma is storingvrij vervaardigd en loopbekwaam.
- Verificatie en validatie.

Afsluitend kan de PES het veilige bedrijf opnemen.

8.1 Frame voor de veiligheidsgerichte inzet

(voorschriften en regels, verklaringen bij de veiligheidsvoorschriften hoofdstuk 3.3)

Het gebruikersprogramma met het toegestaan programmeerwerktuig invoeren:

- SILworX voor CPU BS met een versie vanaf V7.
- ELOP II Factory voor CPU BS met een versie tot V6.x.

De vrijgegeven besturingssystemen voor personalcomputers zijn aan de vrijgavemededelingen van het programmeerwerktuig te ontlenen.

Het programmeerwerktuig omvat in principe:

- Invoer (Function Block Editor), bewaking en documentatie.
- Variablen met symbolische naam en datatype (BOOL, UINT enz.).
- Indeling van de besturingen van het systeem HIMatrix.
- Codegenerator (overzetten van het gebruikersprogramma in de machinecode).
- Hardware-configuratie.
- Configuratie van de communicatie.

8.1.1 Basis van de programmering

De sturingstaak moet in vorm van een specificatie of een takenschrift voorliggen.
Deze documentatie is de grondslag voor de controle van de correcte omzetting in het gebruikersprogramma. De manier van weergave van de specificatie richt zich naar de taakstelling. Dit kan zijn:

- Combinatorische logica
  - Cause/effect diagram
  - Logica van de verbinding met functies en functiebouwstenen
  - Functieblokken met gespecificeerde eigenschappen
- Sequentiebesturingen (afloop-besturingen)
  - Verbale beschrijving van de stappen met voortschakelvoorwaarden en de te regelen externe componenten.
  - Afloopschema´s.
  - Matrix- of tabelvorm van de voortschakelvoorwaarden en de te regelen externe componenten.
  - Definitie van de randvoorwaarden, bv bedrijfssoorten, NOOD-UIT enz.

Het I/O-concept van de installatie moet de analyse van de veldcircuits, d.w.z. het soort externe componenten, omvatten:

- Externe componenten (veldtoestellen)
  - Ingangssignaal in het normaal bedrijf (ruststroomprincipe bij digitale veldtoestellen)
  - Ingangssignaal in geval van storing
  - Vastlegging van veiligheidstechnisch vereiste redundanties (1oo2, 2oo3)
  - Diskrepantiecontrole en reactie
  - Positie en aansturing in het normaal bedrijf
  - Veilige reactie/positie bij uitschakeling of energiewegval

Doelen bij de programmering van het gebruikersprogramma:

- eenvoudig te begrijpen
- eenvoudig na te voelen
- eenvoudig te veranderen
- eenvoudig te testen

8.1.2 Functies van het gebruikersprogramma

De programmering is aan geen beperking door de hardware onderworpen. De functies van het gebruikersprogramma zijn vrij te programmeren.

- Binnen de logica worden uitsluitend elementen volgens IEC 61131-3 met hun desbetreffende functievoorwaarden toegepast.
- De fysieke ingangen en uitgangen werken principieel in het ruststroomprincipe, d.w.z. hun veilige toestand is *0*. Dit is bij de programmering in acht te nemen.
- Het gebruikersprogramma omtvat nuttige logische en/of aritmetische functies zonder inachtneming van het ruststroomprincipe van de fysieke ingangen en uitgangen.
- De logica dient overzichtelijk te zijn geconcipieerd en verstaanbaar voor een eenvoudig zoeken van storingen te zijn gedocumenteerd. Dit omvat het gebruik van functiediagrammen.
- Willekeurige negeringen zijn toegestaan.
- Storingsignalen van ingangen en uitgangen of uit logica-bouwstenen zijn te evalueren.

Belangrijk is het kapselen van functies in zelf vervaardigde functiebouwstenen en functies uit standaardfuncties. Hierdoor kan een programma in modulen (functies, functiebouwstenen) duidelijk worden gestructureerd. Iedere module kan op zich worden beschouwd, en door het samenschakelen van de modulen tot een grotere module of tot een programma komt een klare, complexe functie voort.

8.1.3 Signaal en variabelendeclaratie

Een variabele is een plaatshouder voor een waarde binnen de programmalogica. Via de variabelennaam wordt de geheugenplaats met de opgeslagen waarde symbolisch geadresseerd. Een variabele wordt in de variabelendeclaratie van het programma of een functiebouwsteen vervaardigd.

Versie	Aantal tekens voor variabelennaam
Vanaf CPU BS V7	31
Tot CPU BS V6.x	256

Tabel 29: Lengte van de variabelennamen

De toepassing van symbolische namen in plaats van het fysieke adres heeft twee belangrijke voordelen:

- In het gebruikersprogramma kunnen de installatiebenamingen van ingangen en uitgangen worden toegepast.
- Veranderingen van de indeling van signalen bij de ingangs- en uitgangskanalen hebben geen invloed op het gebruikersprogramma.

Vanaf CPU BS V7 zijn er geen signalen meer, alleen nog maar variabelen.

Variabelen zonder door de gebruiker gedefinieerde initiale waarden hebben na een koude start de standaard initiale waarde 0 resp. FALSE.

Variabele, diens bron ongeldig is, bv door hardware-storing bij fysieke ingang, nemen de geconfigureerde initale waarde aan.

Signalen - tot CPU BS V6.x

Een signaal dient als indeling tussen verschillende bereiken van de gehele besturing.
Het signaal wordt in de signaaleditor aangelegd en stemt het globaal niveau van een VAR_EXTERNAL van het programma overeen, in zover de relatie tot stand werd gebracht.

i Signalen als bedoeld in dit handboek zijn vooral niet optische, akoestische of lichttechnische weergaven van het spoorbedrijf.

8.1.4 Aanvaarding door goedkeuringsinstanties

HIMA adviseert, bij de projectering van een goedkeuringsplichtige installatie zo vroeg als mogelijk de goedkeuringsinstanties te verwittigen.

8.2 Handelwijzen

Dit hoofdstuk beschrijft typische handelwijzen bij de ontwikkeling van gebruikersprogramma´s voor veiligheidsgerichte HIMatrix besturingen.

8.2.1 Indeling van variabelen bij ingangen en uitgangen

De vereiste testroutingen voor veiligheidsgerichte I/O-toestellen, I/O-componenten of I/O-kanalen worden door het besturingssysteem automatisch uitgevoerd.

De indeling van de in het gebruikersprogramma toegepaste variabelen verschilt tussen ELOP II Factory en SILworX.

Vanaf CPU BS V7

Variable bij een I/O-kanaal indelen

1. Een globale variabele met geschikte type definiëren.
2. Bij de definitie van een geschikte initiale waarde vermelden.
3. De globale variabele de kanaalwaarde van het I/O-kanaal indelen.
4. In het gebruikersprogramma de storingcode *-> Error Code [Byte]* evalueren en een veiligheidsgerichte reactie programmeren.

De globale variabele is een ingangs-/uitgangskanaal toegewezen.

Tot CPU BS V6.x

Dient de waarde van een variabele bij een I/O-kanaal te worden ingedeeld, dient op de volgende manier te werk te worden gegaan:

Signaal bij een I/A-kanaal indelen

1. In de signaaleditor van het hardware-management een signaal definiëren.
2. Signaal per drag&drop in de variabelendeclaratie van het programma trekken.
   ☑ VAR_EXTERNAL wordt automatisch vervaardigd.
3. Signaal per drag&drop in de kanaallijst van de I/O-component trekken.
4. In het gebruikersprogramma de storingcode evalueren en een veiligheidsgerichte reactie programmeren.

Het signaal is bij een I/O-kanaal toegewezen.

De naam van het systeemsignaal voor de storingcode is afhankelijk van het type I/O-kanaal.

8.2.2 Af- en opensluiten van de besturing

Locking van de besturing betekent het vergrendelen van functies en operatiemogelijkheden van de gebruiker gedurende het bedrijf. Een manipulatie van het gebruikersprogramma wordt hiermee voorkomen. De omvang van de ontgrendelingen is in afhankelijkheid van de veiligheidsvereisten aan de inzet van de PES te zien, kan echter ook in afspraak met de voor de installatiekeuring bevoegde keuringsinstantie plaatsvinden.

Unlolocking van debesturing betekent het verwijderen van actieve vergrendelingen, bijvoorbeeld voor het uitvoeren van maatregelen aan de besturing.

i Het open- en afsluiten is alleen bij besturingen en bij de Remote I/O F3 DIO 20/8 01 mogelijk, niet bij andere Remote I/Os!

Vanaf CPU BS V7

Voor het ontgrendelen dienen drie systeemvariabelen:

Variabele	Functie
Read only in Run	ON: Start, Stop en Download van de besturing zijn geblokkeerd. OFF: Start, Stop en Download van de besturing zijn mogelijk.
Reload Deactivation	ON: Reload is geblokkeerd. OFF: Reload is mogelijk.
Force Deactivation	ON: Forcen wordt uitgeschakeld. OFF: Forcen is mogelijk.

Tabel 30: Systeemvariabele voor het af- en opensluiten van de PES

Zijn alle drie systeemvariabelen ON, is geen toegrijpen op de besturing meer mogelijk.
In dit geval kan de besturing alleen door herstart weer in de toestand STOP/VALID CONFIGURATION worden gezet. Dan is een nieuw laden van een gebruikersprogramma mogelijk.

Voorbeeld voor het gebruik van deze systeemvariabele:

Besturing afsluitbaar maken

1. Globale variabele van het type BOOL definiëren, initiale waarde op OFF zetten.
2. Globale variabele bij de drie systeemvariabelen *Read only in Run*, *Reload Deactivation* en *Force Deactivation* indelen.
3. Globale variabele bij de kanaalwaarde van een digitale ingang indelen.
4. Sleutelschakelaar aan de digitale ingang aansluiten.
5. Programma compileren, op de bestuirng laden en starten.

De bezitter van een passende sleutel kan de besturing af- en opensluiten. Bij een storing in het desbetreffende ingangstoestel of de ingangscomponent, is de besturing open gesloten.

Tot CPU BS V6.x

Lock: Voor het afsluiten van de PES dient de volgende manier van handelen te worden opgevolgd:

Afsluiten van de besturing

1. De volgende waarden voor het compileren bij de besturing instellen (zie ook hoofdstuk 8.2.3):

Main Enable	open	ON
Forcing Allowed	open	OFF (al naar toepassing)
Test Mode Allowed	open	OFF
Start/Restart Allowed	open	ON
Load Allowed	open	ON
Autostart	open	ON / OFF
Stop at Force Timeout	open	ON (al naar toepassing)

2. Na het laden en starten in de besturing online de volgende schakelaars in deze volgorde veranderen:

Start/Restart Allowed	open	OFF
Load Allowed	open	OFF
Main Enable	open	OFF

i Alleen in afspraak met de keuringsinstanatie kunnen de volgende schakelaars op andere waarden worden gezet:

Forcing Allowed	open	ON
Stop at Force Timeout	open	ON / OFF
Start/Restart Allowed	open	ON
Autostart	open	ON

De besturing is afgesloten.

Unlock: Voorwaarde voor het opensluiten (hoofdvrijgave op ON) is de STOP-toestand van de besturing. Een activeren van de hoofdvrijgave bij een draaiende besturing (in de RUN-toestand) is niet mogelijk; echter kan de hoofdvrijgave in de RUN-toestand worden gedeactiveerd.

Om een nieuwe start na een initialisatie van de CPU (na spanningwegval) mogelijk te maken, dient bij het opensluiten van de PES als volgt te werk te worden gegaan:

Opensluiten van de besturing

1. Hoofdvrijgave op ON zetten
2. Start/herstart op ON zetten.
3. Starten van het gebruikersprogramma.

De besturing is open gesloten.

8.2.3 Code-vervaardiging

Na de volledige invoer van het gebruikersprogramma en de I/O-indeling van besturing de code vervaardigen. Hierbij vormt de codegenerator de configuratie-CRC. Deze is een signatuur over de gehele configuratie van CPU, ingangen, uitgangen en communicatie en wordt als hex-code in 32-bit-formaat uitgegeven. De signatuur omvat alle configureerbare of veranderbare elementen zoals logica, variabele en schakelaarinstellingen.

Vanaf CPU BS V7

Door het dubbele compileren met vergelijking van de testsommen laten zich mogelijke vervalsingen van het gebruikersprogramma opsporen die door sporadische storingen in de hardware of in het besturingssysteem van de toegepaste PC worden veroorzaakt.

Dubbel compileren met vergelijking van de testsommen is een verkiesbare optie bij de codegeneratie.

Tot CPU BS V6.x

Om invloeden van de niet veilige PC uit te sluiten, code dubbel vervaardigen.
De configuratie-CRC moet bij beide doorlopingen identiek zijn.

Code voor veiligheidsgericht bedrijf vervaardigen

1. Codegenerator starten, om code met configuratie-CRC te vervaardigen.
   ☑ Afloopbekwame code 1 met CRC1.
2. Codegenerator opnieuw starten, om code met configuratie-CRC te vervaardigen.
   ☑ Afloopbekwame code 2 met CRC 2.
3. CRC 1 met CRC 2 vergelijken.
   ☑ Beide zijn identiek.

De vervaardigde code is voor het veiligheidsgericht bedrijf bruikbaar, ook ter certificatie door keuringsinstanties.

8.2.4 Laden en starten van het gebruikersprogramma

Het laadproces (download) van een PEs van het HIMatrix systeem kan alleen plaatsvinden, wanneer tevoren STOP werd gezet.

Hardwareversie	Aantal gebruikersprogramma´s per besturing
Standaard	1
F*03	1...32

Tabel 31: Aantal gebruikersprogramma´s in een PES

Het volledige laden van een gebruikersprogramma wordt gecontroleerd. Vervolgens kan het gebruikersprogramma worden gestart, d.w.z. het cyclische afwerken van de routine begint.

i HIMA adviseert, na ieder laden van een gebruikersprogramma in de besturing de projectgegevens te zekeren, bv op een wisselgeheugenmedium.

Hiermee dient te worden gewaarborgd, dat de ter configuratie op de besturing passende projectgegevens verder beschikbaar zijn, ook wanneer de PADT wegvalt.

HIMA adviseert een regelmatige back-up, ook onafhankelijk van het laden van het programma.

8.2.5 Reload - bij F*03

Werden veranderingen aan gebruikersprogramma´s uitgevoerd, kunnen deze in het draaiende bedrijf op de PES worden overgebracht. De firmware controleert en activeert het veranderde gebruikersprogramma, dat dan de besturingstaak overneemt.

Bij het reload van stapkettingen dient op het volgende te worden gelet:

De reload-informatie voor stapketting houdt geen rekening met de actuele status van de ketting. Vandaar is het mogelijk, door reload van een desbetreffende verandering van de stapketting deze in een ongedefinieerd toestand te verzetten. De verantwoordelijkheid hiervoor draagt de gebruiker.

Voorbeelden:

- Wissen van de actieve stap. Hierna heeft geen stap van de stapketting de toestand *active.*
- Herbenaming van de initiale stap gedurende een andere stap actief is.
  Dit leidt tot een stapketting met twee actieve stappen!

Bij de reload van actions dient op het volgende te worden gelet:

Reload laadt actions met hun complete gegevens. De consequenties hieruit dienen voor de reload zorgvuldig te worden overgedacht.

Voorbeelden:

- Verwijderen van een timer-bepalingsteken door de reload leidt ertoe, dat de timer meteen is afgelopen. Daardoor kan de uitgang *Q* in afhankelijkheid van de overige indeling op TRUE gaan.
- Verwijderen van het bepalingsteken bij hechtende elementen (bv bepalingsteken *S*), die gezet waren, leidt ertoe, dat de elementen gezet blijven.
- Verwijderen van een bepalingsteken *P0*, dat TRUE was gezet, activeert de trigger.

8.2.6 Forcen

Forcen betekent het vervangen van de actuele waarde van een variabele door een force-waarde. Een variabele kan haar actuele waarde door een fysieke ingang, door de communicatie of door een logische koppeling verkrijgen. Wordt de variabele geforct, is haar waarde niet meer van het proces afhankelijk, maar wordt door de gebruiker voorgegeven.

⚠ WAARSCHUWING

Storing van het veiligheidsgericht bedrijf door geforcte waarden mogelijk!

- **Geforcte waarden kunnen tot verkeerde uitgangswaarden leiden.**
- **Forcen verlengt de cyclustijd. Hierdoor kan de watchdog-tijd worden overschreden.**

Forcen is alleen na ruggespraak met de voor de afname van de installatie bevoegde keuringsinstanatie toegestaan.

Gedurende het forcen moet de verantwoordelijke de veiligheidstechnisch toerijkende bewakking van het proces door andere technische en organisatorische maatregelen waarborgen. HIMA adviseert, het forcen tijdelijk te beperken.

Nadere informaties met betrekking tot het forcen in de systeemhandboeken (System Manual Compact Systems HI 800 640 NL en System Manual Modular Systems HI 800 191 E).

8.2.7 Online-verandering van systeemparameters - vanaf CPU BS V7

Het is mogelijk, sommige systeemparameters/schakelaars online in de besturing te veranderen. Een toepassingsgeval is de tijdelijke verhoging van de watchdog-tijd, om een reload te kunnen uitvoeren.

Parameters die online kunnen worden veranderd:

Parameters	Hardware	Versie van het besturingssysteem
System ID	Alle	Alle
Safety time	Alle	Alle
Resource Watchdog Time	Alle	Alle
Target Cycle Time	Alle	Vanaf CPU BS V8
Target Cycle Time Mode	F*03	Vanaf CPU BS V8
Allow Online Settings	Alle	Vanaf CPU BS V8
Main Enable	Standaard	Voor CPU BS V8
Autostart	Alle	Alle
Start Allowed	Alle	Alle
Load Allowed	Alle	Alle
Reload Allowed	F*03	Vanaf CPU BS V8
Global Forcing Allowed	Alle	Alle
Global Force Timeout Reaction	Alle	Alle

Tabel 32: Online veranderbare parameters

Voor het zetten van de parameters door een online-commondo dient te worden bedacht, of deze parameterverandering tot een veiligheidskritische toestand kan leiden. Indien nodig, zijn organisatorische en/of technische maatregelen te nemen, om een schadegeval te voorkomen.

Allow Online Settings of *Main Enable* staat het veranderen van de overige parameters toe. *Allow Online Settings* of *Main Enable* kan alleen in de toestand STOP op TRUE worden gezet. gesetzt werden.

De waarden van de veiligheidstijd en de watchdog-tijd zijn door de van de toepassing vereiste veiligheidstijd resp. de feitelijke cyclustijd te controleren. Deze waarden kunnen van de PES niet worden geverifieerd!

Bij F*03-toestellen/componenten zijn veranderingen aan systeemparameters gedurende het bedrijf ook door reload mogelijk.

8.2.8 Programma-documentatie voor veiligheidsgerichte toepassingen

Het programmawerktuig maakt het automatisch printen van de documentatie van en project mogelijk. De belangrijkste documentatiesoorten zijn:

- Interfacedeclaratie
- Signaallijst
- Logica
- Beschrijving van de bestandstypes
- Configuratie voor systeem, componenten en systeemparameters
- Configuratie van het netwerk
- Signaal-verwijzingenlijst
- Codegenerator-informaties

De documentatie is onderdeel van de functiegoedkeuring van een voor goedkeuring plichtige installatie door een keuringsinstantie (bv TÜV). De goedkeuring relateert alleen naar de gebruikersfunctie, nicht echter op de veiligheidsgerichte componenten en automatiseringstoestellen van het systeem HIMatrix die al gekeurd zijn.

8.2.9 Multitasking - bij F*03

Multitasking kenmerkt het vermogen van de HIMatrix F*03 systemen, tot en met 32 gebruikersprogramma´s binnen het processorsysteem af te werken.

De afzonderlijke gebruikersprogramma´s laten zich onafhankelijk van elkaar starten, stoppen, laden - ook door reload - en wissen.

De cyclus van een gebruikersprogramma kan meerde cycli van de processor duren. Dit is door parameters van de ressource en het gebruikersprogramma regelbaar. Uit deze parameters berekent SILworX de watchdoch-tijd van het gebruikersprogramma:
watchdog-tijd$_{gebruikersprogramma}$ = *Watchdog-tijd*$_{processormodule}$ * *Maxiamaal aantal cycli!*

De afzonderlijke gebruikersprogramma´s verlopen principieel terugwerkingsvrij van elkaar af. Een wederzijdse beïnvloeding is echter mogelijk door:

- Toepassing van dezelfde globale variabelen in meerdere toepassingsprogramma´s.
- Onvoorspelbaar lange looptijden bij afzonderlijke gebruikersprogramma´s, indien geen parametrreerbare limitaite door *Max Duration for Each Cycle* plaatsvindt.
- De verdeling van de gebruikersprogramma-cycli op meerde processormodule-cycli beïnvloedt de reactietijd van het gebruikersprogramma en de door het beschreven variabelen sterk!
- Een gebruikersprogramma evalueert globale variabelen die een ander gebruikersprogramma heeft beschreven, om tot zo vele cycli van het processorsysteem later uit, zoals de systeemparameter *Maximum Number of CPU Cycles* voor het programma is ingesteld.
  In het meest ongunstige geval is de volgende afloop denkbaar:
  - Programma A schrijft globale variabele die programma B benodigd.
  - Programma A beëindigt zijn cyclus binnen die cyclus van het processorsysteem, waarin programma B zijn cyclus begint.
  - Dan kan programma B pas bij begin van zijn volgende cyclus de door A geschreven waarden lezen.
  - De zojuist begonnen cyclus van B kan *Maximum Number of CPU Cycles* cyclustijd duren. B verkrijgt de door A geschreven waarden pas op dit tijdpunt.
  - Tot een reactie vn B op deze waarden plaatsvindt, kunnen verdere *Maximum Numer of CPU Cycles* cycli van het processorsysteem verstrijken!

INSTRUCTIE

Wederzijdse beïnvloeding van gebruikersprogramma´s mogelijk!

Toepassing van dezelfde globale variabelen in meerdere toepassingsprogramma´s kan tot wederzijdse beïnvloeding van gebruikersprogramma´s met verschillende gevolgen leiden.

- **Toepassing van globale variabelen in meerdere gebruikersprogramma´s zorgvuldig plannen.**
- **Verwijzingen in SILworX gebruiken, om het gebruik van globale gegevens te controleren. Globale gegevens mogen alleen aan een plaats met waarden worden beschreven, of in een gebruikersprogramma van veiligheidsgerichte ingangen of door veiligheidsgerichte communicatieprotocollen!**

Het ligt binnen de verantwoordelijkheid van de gebruiker, storingen van het bedrijf door wederzijdse beïnvloeding van gebruikersprogramma´s uit te sluiten!

Details met betrekking tot multitasking zie systeemhandboeken (System Manual Compact Systems HI 800 640 NL of System Manual Modular System F60 HI 800 191 E).

8.2.10 Aanvaarding door goedkeuringsinstanties

Er wordt adviseert, bij de projectering van een goedkeuringsplichtige installatie zo vroeg als mogelijk de goedkeuringsinstanties te verwittigen.

De goedkeuring relateert alleen naar de gebruikersfunctie, nicht echter op de veiligheidsgerichte modulen en toestellen van het systeem HIMatrix die al gekeurd zijn.

9 Configuratie van de communicatie

Behalve de fysieke ingangs- en uitgangsvariabelen kunnen variabelen ook via een dataverbinmding met andere systemen worden uitgewisseld. Hiervoor worden de variabalen van de desbetreffende ressource in de protocoleditor van het programmeerwerktuig gedeclareert.

Deze gegevensuitwisseling kan zowel lezend als ook schrijvend zijn.

9.1 Standaardprotocollen

Een reeks van communicatieprotokollen staat alleen een niet veiligheidsgericht overdracht van gegevens toe. Deze kunnen voor niet veiligheidsgerichte delen van een automatiseringstaak worden toegepast.

⚠ VOORZICHTIG

Lichamelijk letsel door gebruik van onveilige importgegevens!

Uit niet veilige bronnen geïmporteerde gegevens niet voor de veiligheidsfuncties van het gebruikersprogramma toepassen!

De volgende standaardprotocollen staan al naar uitvoering van de besturing ter beschikking:

- SNTP
- Send/Receive TCP
- Modbus (Master/Slave)
- PROFIBUS-DP (Master/Slave)
- PROFINET en PROFIsafe (vanaf CPU BS V7)

Alle standaardprotocollen zijn terugwerkingsvrij op het veilige processorsysteem.

9.2 Veiligheidsgericht protocol (safe**ethernet)**

Voor de veiligheidsgerichte gegevensuitwisseling tussen veiligheidsgerichte componenten dient safe**ethernet** te worden toegepast.

Als systeemcomponen van de HIMatrix ist safe**ethernet** tot SIL 4 gecertificeerd.

De controle van de veiligheidsgerichte communcatie is in de safe**ethernet**-editor / peer-to-peer-editor te parametreren.

Voor de berekening van de safe**ethernet** parameters *Receive Timeout* en *Response Time* is de volgende voorwaarde van toepassing:
de communicatie-tijdschijf moet voldoende groot zijn, om in een CPU-cyclus alle safe**ethernet** verbindingen af te werken.

Voor de veiligheidsgerichte functies die via safe**ethernet** worden gerealiseerd, mag alleen de instelling *Use Initial Data* worden gebruikt.

INSTRUCTIE

Ongewilde overgang in de veilige toestand mogelijk!

***ReceiveTMO* is een veiligheidsgerichte parameter!**

De waarde van een signaal moet langer dan *ReceiveTMO* aanstaan of via loop-back worden gecontroleerd, indien iedere waarde dient te worden overgebracht.

9.2.1 Receive Timeout

Receive Timeout is de controletijd in milliseconden (ms), binnen die een correct antweoord van de communicatiepartner moet worden ontvangen.

Komt binnen de *Receive Timeout* geen correct antwoord van de communicatiepartner binnen, wordt de veiligheidsgerichte communicatie gesloten. De input variabelen van deze safe**ethernet** vervinding gedragen zich volgens de ingestelde parameter *Freeze-Data on Lost Connection [ms]*.

Voor de veiligheidsgerichte functies die via safe**ethernet** worden gerealiseerd, mag alleen de instelling *Use Initial Data* worden gebruikt.

Omdat de *Receive Timeout* veiligheidsrelevant en onderdeel van de worst case reaction time T_R (maximale reactietijd, zie hoofdstuk 9.2.3vlg.) is, moet de *Receive Timeout* als volgt worden berekend en in de safe**ethernet** editor worden geregistreerd.

Receive Timeout ≥ 4*Delay + 5*max. cyclustijd

Voorwaarde: de communicatie-tijdschijf moet voldoende groot zijn, om in een CPU-cyclus alle safe**ethernet** verbindingen af te werken.

Delay:	Vertraging op het transmissietraject, bv door switch, satelliet
max. cyclustijd:	maximale cyclustijd van de beide besturingen

i Een gewenste storingstolerantie van de communicatie kan via een verhoging van de *Receive Timeout* worden bereikt, wanneer dit voor het toepassingsproces tijdelijk is toegestaan.

INSTRUCTIE

De maximaal toestane waarde voor *Receive Timeout* is afhankelijk van he toepassingsproces en wordt in de safe**ethernet-editor samen met de maximaal te verwachten response time en het profiel ingesteld.**

9.2.2 Response Time

De *Response Time* is de tijd in milliseconden (ms) die voorbijgaat, tot de afzender van een bericht de ontvangstbevestiging van de ontvanger verkrijgt.

Voor de parametrering onder toepassing van een safe**ethernet** profiel moet een door fysieke omstandigheden van het transmissietraject verwachte *Response Time* worden voorgegeven.

De voorgegeven *Response Time* heeft invloed op de configuratie van alle parameters van de safe**ethernet** verbinding die als volgt zijn te berekenen:

Response Time ≤ Receive Timeout / n

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

De verhouding van de *Receive Timeout* en de *Response Time* beïnvloedt het vermogen tot storingstolerantie, bv bij pakketverliezen (herhaling van verloren gegane datapakketten) of vertragingen op de transmissieweg.

In een netwerk, waarin het tot pakketverliezen kan komen, moet aan de volgende voorwaarde zijn voldaan:

min. Response Time ≤ Receive Timeout / 2 ≥ 2*Delay + 2,5*max. cyclustijd

Werd aan deze voorwaarde voldaan, kan het verlies van ten minste een datapakket worden opgevangen, zonder dat de safe**ethernet** verbinding / peer-to-peer-verbinding wordt onderbroken.

i Werd aan deze voorwaarde niet voldaan, kan de beschikbaarheid van een safe**ethernet** verbinding alleen in een collisie- en storingvrij netwerk worden gegarandeerd. Dit betekent echter geen veiligheidsprobleem voor de processormodule!

i Er moet worden gewaarborgd, dat het communicatiesysteem de geparametreerde response-time naleeft!

Voor gevallen, waarin dit niet altijd kan worden gegarandeerd, staat ter controle van de response-time een desbetreffende systeemvariabele van de verbinding ter beschikking. Komt het niet alleen in zelden afzonderlijke gevallen tot een overschrijden van de gemeten response-time over de halve Receive Timeout, moet de geparametreerde respone time worden verhoogd.

De receive-timeout is de nieuw te parametreren response time aan te passen.

INSTRUCTIE

In de volgende voorbeelden gelden de formules voor de berekening van de maximale reactietijd in geval met een verbinding met HIMatrix besturingen alleen dan, wanneer op deze de

veiligheidstijd = 2 * watchdog-tijd

is ingesteld.

9.2.3 Maximale cyclustijd van de HIMatrix besturing

Ter bepaling van de maximale cyclustijd voor een HIMatrix besturing adviseert HIMA de volgende manier van handelen:

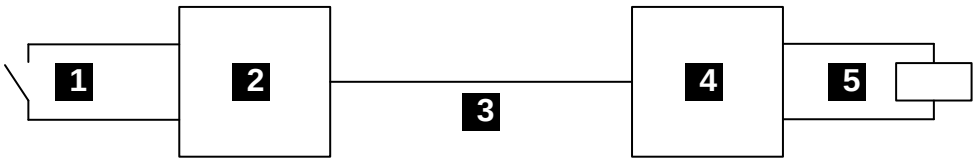
Maximale cyclustijd van de HIMatrix besturing bepalen

1. Systeem onder volle last xploiteren. Hierbij moeten alle communicatieverbindingen in werking zijn, zowel via safe**ethernet** als ook via standaardprotocollen. De cyclustijd in het Control Panel vaker aflezen en de maximale cyclustijd noteren.
2. Stap 1 voor de communicatiepartner (tweede HIMatrix besturing) herhalen.
3. De grotere van de beide berekende maximale cyclustijden is de gezochte maximale cyclustijd.

De maximale cyclustijd is berekend en vindt ingang in de volgende berekeningen.

9.2.4 Berekening van de maximale reactietijd

De maximale reactietijd T_R (*Worst Case*) van de wissel van een veldcomponent van de besturing 1 (in) tot aan de reactie van de uitgang (out) van de besturing 2 kan als volgt worden berekend:



1 Ingang
2 Besturing 1
3 Veiligheidsgericht protocol
4 Besturing 2
5 Uitgang

Afbeelding 4: Reactietijd bij verbinding van twee HIMatrix besturingen

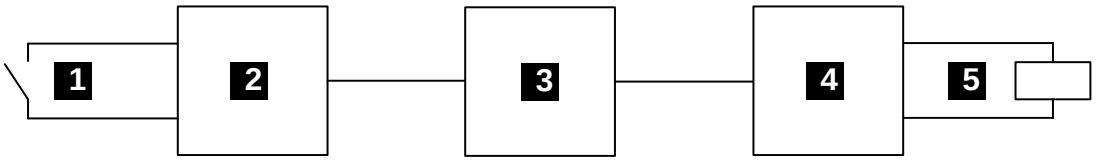
$$\mathbf{T_R = t_1 + t_2 + t_3}$$

T_R	Worst Case Reaction Time
t_1	2 ∗ Watchdog-tijd van de besturing 1
t_2	Receive Timeout
t_3	2 ∗ Watchdog-tijd van de besturing 2

De maximale reactietijd is afhankelijk van het proces en met de keurende instantie af te stemmen.

9.2.5 Berekening van de max. reactietijd met twee Remote I/Os

De maximale reactietijd T_R van de wissel van een veldcomponent (In) van de eerste Remote I/O tot aan de reactie van de uitgang (Out) de tweede Remote I/O kan als volgt worden berekend:



1 Ingang
2 Remote I/O 1
3 Besturing
4 Remote I/O 2
5 Uitgang

Afbeelding 5: Reactietijd met Remote I/Os

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

T_R	Worst Case Reaction Time
t_1	2 ∗ Watchdog-tijd van de Remote I/O 1
t_2	Receive $Timeout_1$
t_3	2 ∗ Watchdog-tijd van de besturing
t_4	Receive $Timeout_2$
t_5	2 ∗ Watchdog-tijd van de Remote I/O 2

Opmerking: de tijden zijn ook dan geldig, wanneer in plaats van een Remote I/O van een besturing wordt ingezet.

9.2.6 Begrippen

Receive Timeout	Controletijd in besturing 1, waarin een geldige antwoord van besturing 2 moet worden ontvangen. Na afloop van de tijd wordt de veiligheidsgerichte communicatie gesloten.
Receive $Timeout_1$	Remote I/O 1 → Besturing
Receive $Timeout_2$	Besturing → Remote I/O 2
Watchdog-tijd	Maximaal toegestane duur van de RUN-cyclus van een PES
Worst Case	Maximale reactietijd voor de overdracht van de verandering van het signaal van een fysieke ingang (in) van een besturing 1 tot aan de verandering van de fysieke uitgang (out) van een besturing 2.

De gegevensoverdracht geschiedt met een veiligheidsgerichte protocol.

9.2.7 Gunning van de safe**ethernet**-adressen

Bij de gunning van de netwerkadressen (IP-adressen) voor safe**ethernet** op de volgende punten letten:

- De adressen moeten duidelijk in het toegepaste net zijn.
- Bij het verbinden van het safe**ethernet** met een andere net (bedrijfsinterne LAN, enz.), erop letten, dat geen storingen kunnen optreden. Mogelijke storingsbronnen zijn bv:
  - het daar ontstaande gegevensverkeer.
  - Koppeling met verdere netten (bv internet).

In zulke gevallen geschikte maatregelen nemen, bv inzet van Ethernet-switches, Firewall, om de storingen tegen te werken.

i De exploitant heeft ervoor te zorgen, dat de voor de safe**ethernet** communicatie / peer-to-peer-communicatie toegepaste Ethernet voldoende tegen manipulaties (bv door crackers) zijn beschermd.

Soort en omvang van de maatregelen zijn met de keurende instantie af te stemmen.

Aanhangsel

Glossarium

Begrip	Beschrijving
ARP	Address Resolution Protocol: netwerkprotocol voor de indeling van netwerkadressen bij hardware-adressen
AI	Analog Input, analoge ingang
AO	Analog Output, analoge uitgang
COM	Communicatiemodule
CRC	Cyclic Redundancy Check, testsom
DI	Digital Input, digitale ingang
DO	Digital Output, digitale uitgang
ELOP II Factory	Programmeerwerktuig voor HIMatrix systemen
EMV	Elektromagnetische verdraagzaamheid
EN	Europese normen
ESD	ElectroStatic Discharge, elektrostatische ontlading
FB	Veldbus
FBS	Functiebouwsteentaal
FTZ	Tolerantietijd storingen
ICMP	Internet Control Message Protocol: netwerkprotocol voor status- en storingsmeldingen
IEC	Internationale normen voor de elektrotechniek
MAC-adres	Hardware-adres van een netwerkaansluiting (Media Access Control)
PADT	Programming and Debugging Tool (volgens IEC 61131-3), PC met SILworX of ELOP II Factory
PE	Protective Earth: aarding
PELV	Protective Extra Low Voltage: functiekleinspanning met veilige scheiding
PES	Programmeerbaar elektronisch systeem
R	Read: Systeemvariabele/signaal levert waarde, bv aan gebruikersprogramma
Rack-ID	Identificatie van een basisdrager (nummer)
terugwerkingsvrij	Er zijn twee ingangsschakelingen aan dezelfde bron (bv transmitter) aangesloten. Dan wordt een ingangsschakeling *terugwerkingsvrij* genoemd, wanneer ze de signalen van de andere ingangsschakeling niet vervalst.
R/W	Read/Write (kolomoverschrift voor soort van systeemvariabele/signaal)
SELV	Safety Extra Low Voltage: beschermingskleinspanning
SFF	Safe Failure Fraction, aandeel van de veilig te beheersen storingen
SIL	Safety Integrity Level (volgens IEC 61508)
SILworX	Programmeerwerktuig voor HIMatrix systemen
SNTP	Simple Network Time Protocol (RFC 1769)
S.R.S	System.Rack.Slot adressering van een module
SW	Software
TMO	Timeout
W	Write: Systemvariablee/signaal wordt met waarde verzorgd, bv door het gebruikersprogramma
w_{SS}	Piek-Piek-waarde van de gehele wisselspanningscomponenten
Watchdog (WD)	Tijdcontrole voor modulen of programma´s. Bij overschrijden van de watchdog-tijd gaat de module of het programma in de storingsstop.
WDZ	Watchdog-tijd

Lijst met afbeeldingen

Lijst met tabellen

Index

HIMA Paul Hildebrandt GmbH
Postbus 1261
68777 Brühl
Tel.: +49 6202 709-0
Fax: +49 6202 709-107
E-mail: info@hima.com Internet: www.hima.com

(1447)