

Wichtiger Hinweis

Alle in diesem Handbuch genannten HIMA-Produkte sind mit dem HIMA-Warenzeichen geschützt. Dies gilt gegebenenfalls, soweit nicht anders vermerkt, auch für andere genannte Hersteller und deren Produkte.

Technische Änderungen vorbehalten.

Alle technischen Angaben und Hinweise in diesem Handbuch wurden mit größter Sorgfalt erarbeitet und unter Einschaltung wirksamer Kontrollmaßnahmen zusammengestellt. Trotzdem sind Fehler nicht ganz auszuschließen. HIMA weist darauf hin, daß weder eine Garantie noch eine juristische Verantwortung oder irgend eine Haftung übernommen werden können für die Folgen, die auf fehlerhafte Angaben zurückgehen. Für die Mitteilung eventueller Fehler ist HIMA dankbar.

Kontakt

HIMA-Adresse:

© HIMA Paul Hildebrandt GmbH + Co KG
Postfach 1261
D - 68777 Brühl
Telefon +49 06202 709-0
Fax +49 06202 709-107
E-Mail Info@hima.com
Internet <http://www.hima.de>

Revisions- index	Änderungen	Art der Änderung	
		technisch	redaktionell
1.00	Neues Layout des Dokuments, Generelle Überarbeitung	X	X

Inhaltsverzeichnis

1	Einleitung.	7
1.1	Gültigkeit und Aktualität.	7
1.2	Darstellungskonventionen.	7
1.2.1	Sicherheitshinweise.	8
1.2.2	Gebrauchshinweise.	8
1.3	Zielgruppe.	8
1.4	Restgefahren.	8
2	Bestimmungsgemäßer Einsatz.	9
2.1	Anwendungsgebiet.	9
2.1.1	Anwendung im Ruhestromprinzip.	9
2.1.2	Anwendung im Arbeitsstromprinzip.	9
2.1.3	Explosionsschutz.	9
2.1.4	Einsatz in Brandmelderzentralen.	9
2.2	Nichtbestimmungsgemäßer Einsatz.	10
2.3	Einsatzbedingungen.	10
2.3.1	Umgebungsbedingungen und technische Daten.	10
2.3.2	Klimatische Bedingungen.	11
2.3.3	Mechanische Bedingungen.	11
2.3.4	EMV-Bedingungen.	12
2.3.5	Spannungsversorgung.	12
2.3.6	ESD-Schutzmaßnahmen.	13
2.4	Qualifikation des Personals.	13
2.5	Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers.	13
3	Sicherheitsphilosophie und Auflagen.	15
3.1	Zertifizierung.	15
3.2	Sicherheit und Verfügbarkeit.	16
3.2.1	Sicherheit.	16
3.2.2	Übersicht.	16
3.3	Sicherheitszeiten.	17
3.4	Wiederholungsprüfung.	18
3.4.1	Durchführung der Wiederholungsprüfung.	18
3.4.2	Häufigkeit der Wiederholungsprüfungen.	18
3.5	Sicherheitsauflagen.	19
3.5.1	Hardware-Projektierung: produktunabhängige Auflagen.	19
3.5.2	Hardware-Projektierung: produktabhängige Auflagen.	19
3.5.3	Programmierung: produktunabhängige Auflagen.	19
3.5.4	Programmierung: produktabhängige Auflagen.	19
3.5.5	Kommunikation: produktabhängige Auflagen.	20
3.5.6	Sonderbetriebsarten: produktunabhängige Auflagen.	20
4	Zentralbaugruppen.	21
4.1	Zentralbaugruppen und Bausätze für die Systeme H41q und H41qc.	21
4.2	Zentralbaugruppen und Bausätze für das System H51q.	21
4.3	Weitere zentrale Baugruppen für die Systeme H41q, H41qc und H51q.	22
4.4	Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsgerichteten Zentralbaugruppen.	23
4.4.1	Netzgeräte.	23
4.4.2	Funktionale Beschreibung der sicherheitsgerichteten Zentralbaugruppen F 8652 X / F 8650 X.	23
4.5	Prinzipielle Arbeitsweise von sicherheitsgerichteten Zentralbaugruppen.	24
4.5.1	Selbsttestroutinen.	24
4.5.2	Reaktion auf festgestellte Fehler bei Zentralbaugruppen.	25
4.5.3	Diagnoseanzeige.	25

4.6	Reaktion auf festgestellte Fehler im E/A-Bus-Bereich.	26
4.7	Hinweis zum Austausch von Zentralbaugruppen.	26
5	Eingangsbaugruppen.	27
5.1	Gesamtübersicht der Eingangsbaugruppen für die Systeme H41q, H41qc und H51q.	27
5.2	Sicherheit und Verfügbarkeit von sicherheitsgerichteten Eingangsbaugruppen.	27
5.2.1	Sicherheit von Sensoren, Gebern, Transmittern.	28
5.3	Sicherheitsgerichtete digitale Eingangsbaugruppen F 3236, F 3237, F 3238, F 3240 und F 3248.	28
5.3.1	Testroutinen.	28
5.3.2	Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Eingangsbaugruppen.	29
5.4	Sicherheitsgerichtete Zählerbaugruppe F 5220.	29
5.4.1	Testroutinen.	29
5.5	Sicherheitsgerichtete analoge Eingangsbaugruppen F 6213, F 6214 und F 6217.	30
5.5.1	Testroutinen.	30
5.5.2	Reaktionen auf festgestellte Fehler bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6213, F 6214.	30
5.5.3	Reaktionen auf festgestellte Fehler bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6217.	31
5.6	Sicherheitsgerichtete analoge eigensichere Thermoelement-Eingangsbaugruppe F 6220.	31
5.6.1	Testroutinen.	31
5.6.2	Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten Thermoele- mentbaugruppe F 6220.	32
5.6.3	Projektierungshinweise.	32
5.7	Sicherheitsgerichtete analoge eigensichere Eingangsbaugruppe F 6221.	32
5.7.1	Testroutinen.	32
5.7.2	Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten analogen Eingangsbaugruppe F 6221.	33
5.7.3	Weitere Projektierungshinweise.	33
5.8	Hinweis zum Wechseln von Eingangsbaugruppen.	33
6	Ausgangsbaugruppen.	35
6.1	Gesamtübersicht der Ausgangsbaugruppen für die Systeme H41q, H41qc und H51q.	35
6.2	Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsgerichteten Ausgangsbaugruppen.	35
6.2.1	Sicherheitsgerichtete digitale Ausgangsbaugruppen.	36
6.2.2	Sicherheitsgerichtete analoge Ausgangsbaugruppen.	36
6.3	Prinzipielle Arbeitsweise von sicherheitsgerichteten Ausgangsbaugruppen.	37
6.4	Sicherheitsgerichtete digitale Ausgangsbaugruppen F 3330, F 3331, F 3333, F 3334, F3335, F 3348, F3349.	37
6.4.1	Testroutinen.	37
6.4.2	Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Ausgangsbaugruppen.	37
6.5	Sicherheitsgerichtete digitale Relaisbaugruppe F 3430.	38
6.5.1	Testroutinen.	38
6.5.2	Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Relaisbaugruppen.	38
6.5.3	Hinweis zur Projektierung mit F 3430.	38

6.6	Sicherheitsgerichtete analoge Ausgangsbaugruppe F 6705.	38
6.6.1	Testroutinen.	38
6.6.2	Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten analogen Ausgangsbaugruppe.	38
6.7	Hinweis zum Wechseln von Ausgangsbaugruppen.	39
6.8	Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicher- heitsgerichteten Ausgangsbaugruppen.	39
7	Software.	41
7.1	Sicherheitstechnische Aspekte für das Betriebssystem.	41
7.1.1	Kennzeichnung, aktuelle freigegebene Version für sicherheitstechnische Anwendungen (CRC-Signatur).	41
7.1.2	Arbeitsweise und Funktionen des Betriebssystems.	41
7.2	Sicherheitstechnische Aspekte des Anwenderprogramms.	42
7.2.1	Vorgaben und Regeln für den Einsatz in sicherheitstechnischen Anwendungen (Auflagen aus Baumustergutachten etc.).	42
7.2.1.1	Basis der Programmierung.	42
7.2.2	Sicherheitstechnische Aspekte für die Programmierung mit ELOP II.	43
7.2.2.1	Anwendung des Sicherheitswerkzeugs von ELOP II bei der Programmierstellung.	44
7.2.2.2	Anwendung des Sicherheitswerkzeugs von ELOP II bei der Programmänderung.	44
7.2.3	Verwendung von Variablen und PLT-Namen.	46
7.2.3.1	Zuordnung von PLT-Namen zu Variablennamen.	47
7.2.3.2	Arten von Variablen.	48
7.2.3.3	Digitale Ein- und Ausgänge für boolesche Variablen.	48
7.2.3.4	Analoge E/A-Baugruppen.	48
7.2.3.5	Importierte oder exportierte Variablen.	48
7.2.4	Signaturen des Anwenderprogramms.	49
7.2.4.1	Codeversionsnummer.	49
7.2.4.2	Runversionsnummer.	49
7.2.4.3	Datenversionsnummer.	49
7.2.4.4	Bereichsversionsnummer.	50
7.2.5	Verwendung von Standardfunktionsbausteinen für sicherheitstechnische Anwen- dungen.	50
7.2.5.1	Standardfunktionsbausteine unabhängig von der E/A-Ebene.	50
7.2.5.2	Standardfunktionsbausteine abhängig von der E/A-Ebene.	51
7.2.6	Parametrierung des Automatisierungsgeräts.	51
7.2.6.1	Sicherheitsparameter.	51
7.2.6.2	Verhalten bei Fehlern in sicherheitsgerichteten Ausgangskanälen.	53
7.2.7	Identifizierung des Programms.	53
7.2.8	Überprüfung des erstellten Applikationsprogramms auf Einhaltung der spezifi- schen Sicherheitsfunktion.	53
7.3	Checkliste: Maßnahmen zur Erstellung eines Anwenderprogramms.	54
7.4	Reload (Reloadbarer Code).	54
7.4.1	Systeme mit einer Zentralbaugruppe.	54
7.4.2	Systeme mit redundanten Zentralbaugruppen.	55
7.4.3	Einschränkungen beim Reload.	55
7.5	Offline-Test.	56
7.6	Forcen.	56
7.7	Schutz vor Manipulationen.	57
7.8	Funktionen des Anwenderprogramms.	57
7.8.1	Gruppenabschaltung.	57
7.8.2	Softwarebausteine für einzelne sicherheitsgerichtete E/A-Baugruppen.	58
7.8.3	Redundante E/A-Baugruppen.	58

7.8.3.1	Redundante, nicht sicherheitsgerichtete Sensoren.	58
7.8.4	Analoge redundante Sensoren.	60
7.8.5	Eingangsbaugruppen mit 2oo3-Verschaltung.	61
7.9	Programmdokumentation für sicherheitsgerichtete Anwendungen.	61
7.10	Sicherheitstechnische Aspekte für die Kommunikation (sicherheitsgerichtete Datenübertragung).	62
7.10.1	Sicherheitsgerichtete Kommunikation.	62
7.10.2	Zeitliche Anforderungen.	62
7.10.3	Hinweise für die Erstellung des Anwenderprogramms.	63
8	Einsatz für Brandmelderzentralen entsprechend DIN EN 54-2 und NFPA 72.	65

Anhang

1	Standard-Software-Bausteine für den Zentralbereich.	67
1.1	Baustein HK-AGM-3.	67
1.2	Baustein HK-COM-3.	67
1.3	Baustein HK-MMT-3.	67
1.4	Baustein H8-UHR-3.	67
2	Standard-Software-Bausteine für den E/A-Bereich.	68
2.1	Baustein H8-STA-3.	68
2.1.1	Baustein-Eingänge.	68
2.1.2	Baustein-Ausgänge.	68
2.2	Baustein HA-LIN-3.	69
2.3	Baustein HA-PID-3.	69
2.3.1	Bausteineingänge.	70
2.3.2	Bausteinausgänge.	70
2.4	Baustein HA-PMU-3.	70
2.5	Baustein HA-RTE-3.	70
2.5.1	Eingänge.	71
2.5.2	Ausgänge.	71
2.6	Baustein HB-BLD-3.	71
2.6.1	Eingänge.	72
2.6.2	Ausgänge.	72
2.7	Baustein HB-BLD-4.	72
2.7.1	Eingänge.	73
2.7.2	Ausgänge.	73
2.8	Baustein HB-RTE-3.	74
2.8.1	Eingänge.	74
2.8.2	Ausgänge.	75
2.9	Baustein HF-AIX-3.	76
2.10	Baustein HF-CNT-3.	77
2.11	Baustein HF-CNT-4.	78
2.12	Baustein HF-TMP-3.	79
2.13	Baustein HK-LGP-3.	80
2.14	Baustein HZ-DOS-3.	80
2.15	Baustein HZ-FAN-3.	81
2.15.1	Eingänge.	81
2.15.2	Ausgänge.	81

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Handbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der sicherheitsgerichteten HIMA Automatisierungsgeräte H41q und H51q.

Voraussetzung für die gefahrlose Installation, Inbetriebnahme und für die Sicherheit bei Betrieb und Instandhaltung der H41q/H51q Automatisierungsgeräte sind:

- Kenntnis von Vorschriften.
- technisch einwandfreie Umsetzung der in diesem Handbuch enthaltenen Sicherheitshinweise durch qualifiziertes Personal.

In folgenden Fällen können durch Störungen oder Beeinträchtigungen von Sicherheitsfunktionen schwere Personen-, Sach- oder Umweltschäden eintreten, für die HIMA keine Haftung übernehmen kann:

- Bei nicht qualifizierten Eingriffen in die Geräte.
- Bei Abschalten oder Umgehen (Bypass) von Sicherheitsfunktionen.
- Bei Nichtbeachtung von Hinweisen dieses Handbuchs.

HIMA entwickelt, fertigt und prüft H41q/H51q Automatisierungsgeräte unter Beachtung der einschlägigen Sicherheitsnormen. Die Verwendung der Geräte ist nur zulässig, wenn alle folgenden Voraussetzungen erfüllt sind:

- die in den Beschreibungen vorgesehenen Einsatzfälle
- die spezifizierten Umgebungsbedingungen
- nur zugelassene Fremdgeräte angeschlossen

Aus Gründen der Übersichtlichkeit enthält dieses Handbuch nicht sämtliche Details aller Ausführungen der H41q/H51q Automatisierungsgeräte.

1.1 Gültigkeit und Aktualität

Es gilt jeweils die neueste Ausgabe des Sicherheitshandbuchs auch für ältere Versionen des Betriebssystems. Besonderheiten einzelner Versionen sind im Text erwähnt.

Die neueste Ausgabe steht auf der Webseite www.hima.de zur Verfügung.

Umfassende Änderungen des Handbuchs sind durch einen neuen Revisionsstand gekennzeichnet, weniger umfangreiche durch einen neuen Ausgabestand. Der Revisionsstand steht auf der Vorderseite hinter der Dokumentennummer, der Ausgabestand auf der Rückseite.

1.2 Darstellungskonventionen

Zur besseren Lesbarkeit und zur Verdeutlichung gelten in diesem Dokument folgende Schreibweisen:

Fett	Hervorhebung wichtiger Textteile. Bezeichnungen von Schaltflächen, Menüpunkten und Registern im Programmierwerkzeug, auf die Sie klicken können
<i>Kursiv</i>	Parameter und Systemvariablen
<code>Courier</code>	Wörtliche Benutzereingaben
RUN	Bezeichnungen von Betriebszuständen in Großbuchstaben
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Wenn Sie den Mauszeiger darauf positionieren, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.2.1 Sicherheitshinweise

Die Sicherheitshinweise im Dokument sind wie folgend beschrieben dargestellt.

Um ein möglichst geringes Risiko zu gewährleisten, sind sie unbedingt zu befolgen. Der inhaltliche Aufbau ist

- Signalwort: Gefahr, Warnung, Vorsicht, Hinweis
- Art und Quelle der Gefahr
- Folgen der Gefahr
- Vermeidung der Gefahr

SIGNALWORT



**Signalwort! Art und Quelle der Gefahr.
Folgen der Gefahr
Vermeidung der Gefahr**

Die Bedeutung der Signalworte ist

- Gefahr: Bei Missachtung folgt schwere Körperverletzung bis Tod
- Warnung: Bei Missachtung droht schwere Körperverletzung bis Tod
- Vorsicht: Bei Missachtung droht leichte Körperverletzung
- Hinweis: Bei Missachtung droht Sachschaden

HINWEIS



**Hinweis! Art und Quelle des Schadens.
Vermeidung des Schadens**

1.2.2 Gebrauchshinweise

Zusatzinformationen sind nach folgendem Beispiel aufgebaut:

i

An dieser Stelle steht der Text der Zusatzinformation.

Nützliche Tipps und Tricks erscheinen in der Form:

TIPP

An dieser Stelle steht der Text des Tipps.

1.3 Zielgruppe

Dieses Handbuch wendet sich an Planer, Projektoren und Programmierer von Automatisierungsanlagen. Vorausgesetzt werden spezielle Kenntnisse auf dem Gebiet der sicherheitsgerichteten Automatisierungstechnik.

1.4 Restgefahren

Von einem H41q/H51q-Gerät selbst geht keine Gefahr aus.

Restgefahren können ausgehen von:

- Fehlern in der Projektierung
- Fehlern im Anwenderprogramm
- Fehlern in der Verdrahtung

2 Bestimmungsgemäßer Einsatz

2.1 Anwendungsgebiet

Die sicherheitsgerichteten Automatisierungsgeräte H41q, H41qc und H51q sind einsetzbar bis zum Sicherheits-Integritätslevel SIL 3 (IEC 61508) bzw. zur Sicherheitskategorie Kat 4/PI e (ISO 13849-1).

Alle Ein-/Ausgangsbaugruppen können sowohl bei redundanter als auch bei einkanaliger Ausführung der Zentralbaugruppen eingesetzt werden.

Bei der Verwendung der sicherheitsgerichteten Kommunikation zwischen verschiedenen Geräten muss beachtet werden, dass die Gesamtreaktionszeit des Systems nicht die Fehlertoleranzzeit überschreitet. Die im Sicherheitshandbuch HI 800 012 D aufgeführten Berechnungsgrundlagen sind anzuwenden

An die Kommunikationsschnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

Die H41q/H51q-Systeme sind für Prozess-Steuerungen, Schutzsysteme, Brenneranlagen und Maschinensteuerungen zertifiziert.

2.1.1 Anwendung im Ruhestromprinzip

Die Automatisierungsgeräte sind für das Ruhestromprinzip konzipiert.

Ein System, das nach dem Ruhestromprinzip funktioniert, benötigt keine Energie, um seine Sicherheitsfunktion auszuführen (**deenergize to trip**).

Als sicherer Zustand im Fehlerfall wird damit bei Eingangs- und Ausgangssignalen der spannungs- oder stromlose Zustand eingenommen.

2.1.2 Anwendung im Arbeitsstromprinzip

Die H41q/H51q-Steuerungen können auch in Arbeitsstrom-Anwendungen eingesetzt werden.

Ein System, das nach dem Arbeitsstromprinzip funktioniert, benötigt Energie, z. B. elektrische oder pneumatische Energie, um seine Sicherheitsfunktion auszuführen (**energize to trip**).

Dafür wurden die H41q/H51q-Steuerungen nach EN54 und NFPA72 für den Einsatz in Brandmeldeanlagen und Feuerlöschsystemen geprüft und zertifiziert. In diesen Systemen ist es gefordert, dass auf Anforderung der aktive Zustand zur Beherrschung der Gefahr angenommen wird.

2.1.3 Explosionsschutz



Die sicherheitsgerichteten Automatisierungsgeräte H41q, H41qc und H51q sind geeignet zum Einbau in die Zone 2. Die entsprechenden Konformitätserklärungen sind in den Datenblättern enthalten.

Die nachfolgend aufgeführten Einsatzbedingungen sind zu beachten!

2.1.4 Einsatz in Brandmelderzentralen

Alle H41q/H51q-Systeme mit analogen Eingängen können für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 eingesetzt werden.

Die nachfolgend aufgeführten Einsatzbedingungen sind zu beachten!

2.2 Nichtbestimmungsgemäßer Einsatz

Die Übertragung der sicherheitsrelevanten Daten über öffentliche Netze (z. B. Internet) ist ohne Zusatzmaßnahmen zur Erhöhung der Sicherheit (z. B. VPN-Tunnel, Firewall, etc.) nicht zulässig.

Mit den Feldbusschnittstellen ist ohne sicherheitsgerichtete Feldbusprotokolle keine sicherheitsgerichtete Kommunikation möglich.

2.3 Einsatzbedingungen

2.3.1 Umgebungsbedingungen und technische Daten

Für den Einsatz der sicherheitsgerichteten Steuerungssysteme H41q/H51q sind die nachfolgenden allgemeinen Bedingungen einzuhalten:

Art der Bedingung	Inhalt der Bedingung
Schutzklasse	Schutzklasse II nach IEC/EN 61131-2
Betriebstemperatur	Betriebstemperatur: 0...+60 °C
Lagertemperatur	Lagertemperatur: -40...+80 °C (mit Batterie: nur -30 °C...+75 °C)
Verschmutzung	Verschmutzungsgrad II
Aufstellhöhe	< 2000 m
Gehäuse	Standard: IP 20 Falls es die zutreffenden Applikationsnormen (z. B. EN 60204, EN 954-1) fordern, muss das Gerät in ein Gehäuse der geforderten Schutzart (z.B. IP 54) eingebaut werden.
Eingangsspannung Netzteil	24 V DC

Tabelle 1: Umgebungsbedingungen

Diverse Abweichungen sind dem entsprechenden Datenblatt zu entnehmen.

Die sicherheitsgerichteten Steuerungssysteme H41q, H41qc und H51q wurden für die Einhaltung der Anforderungen der folgenden Normen für EMV, Klima und Umweltauforderungen entwickelt.

Norm	Inhalt
IEC/EN 61131-2: 2006	Speicherprogrammierbare Steuerungen, Teil 2 Betriebsmittelanforderungen und Prüfungen
IEC/EN 61000-6-2: 2005	EMV Fachgrundnorm, Teil 6-2 Störfestigkeit Industriebereich
IEC/EN 61000-6-4: 2006	Elektromagnetische Verträglichkeit (EMV) Fachgrundnorm Störaussendung, Industriebereich

Tabelle 2: Normen

2.3.2 Klimatische Bedingungen

Die wichtigsten Prüfungen und Grenzwerte für klimatische Bedingungen sind in nachstehender Tabelle aufgelistet.

IEC/EN 61131-2	Klimaprüfungen
	Betriebstemperatur: 0...+60 °C (Prüfgrenzen: -10...+70 °C)
	Lagertemperatur: -40...+80 °C (mit Batterie: nur -30 °C)
	Trockene Wärme und Kälte; Beständigkeitsprüfungen: +70 °C / -25 °C, 96 h Stromversorgung nicht angeschlossen
	Temperaturwechsel; Beständigkeits- und Unempfindlichkeitsprüfungen: -25 °C / +70 °C und 0 °C / +55 °C Stromversorgung nicht angeschlossen
	Zyklen mit feuchter Wärme; Beständigkeitsprüfungen: +25 °C / +55°C, 95% relative Feuchte Stromversorgung nicht angeschlossen

Tabelle 3: Klimatische Bedingungen

2.3.3 Mechanische Bedingungen

Die wichtigsten Prüfungen und Grenzwerte für mechanische Bedingungen sind in nachstehender Tabelle aufgelistet:

IEC/EN 61131-2	Mechanische Prüfungen
	Unempfindlichkeitsprüfung gegen Schwingungen: 5...9 Hz / 3,5 mm 9... 150 Hz / 1 g, Prüfling in Betrieb, 10 Zyklen pro Achse
	Unempfindlichkeitsprüfung gegen Schocks: 15 g, 11 ms, Prüfling in Betrieb, 3 Schocks pro Achse (18 Schocks)

Tabelle 4: Mechanische Prüfungen

2.3.4 EMV-Bedingungen

Die wichtigsten Prüfungen und Grenzwerte für EMV-Bedingungen sind in nachstehender Tabelle aufgelistet.

IEC/EN 61131-2	Prüfungen der Störfestigkeit
IEC/EN 61000-4-2	ESD-Prüfung: 6 kV Kontakt-, 8 kV Luftentladung (EN 230, EN 50130)
IEC/EN 61000-4-3	RFI-Prüfung (10 V/m): 80 MHz...2 GHz, 80% AM
IEC/EN 61000-4-4	Burst-Prüfung: 2 kV auf Versorgungs-, 1 kV auf Signalleitungen, 2 kV auf AC-Leitungen

Tabelle 5: Prüfungen der Störfestigkeit

IEC/EN 61000-6-2	Prüfungen der Störfestigkeit
IEC/EN 61000-4-6	Hochfrequenz, asymmetrisch 10 V, 150 kHz...100 MHz, AM
IEC/EN 61000-4-3	434 MHz-, 900 MHz-Impulse, 20 V/m
IEC/EN 61000-4-5	Stossspannung: 2 kV, 1 kV auf Versorgungsleitung

Tabelle 6: Prüfungen der Störfestigkeit

IEC/EN 61000-6-4	Prüfungen der Störaussendung
EN 50011 Klasse A	Störaussendung: gestrahlt, leitungsgebunden

Tabelle 7: Prüfungen der Störaussendung

Alle Baugruppen der Systeme H41q und H51q erfüllen die Anforderungen der EMV-Richtlinie der Europäischen Union und haben das CE-Zeichen.

Bei Störbeeinflussung über die angegebenen Grenzen hinaus reagieren die Systeme sicherheitsgerichtet.

2.3.5 Spannungsversorgung

Die wichtigsten Prüfungen und Grenzwerte für die Spannungsversorgungsbedingungen sind in nachstehender Tabelle aufgelistet.

IEC/EN 61131-2:	Nachprüfung der Eigenschaften der Gleichstromversorgung
	Das Netzgerät muss alternativ die folgenden Normen erfüllen: IEC 61131-2 oder SELV (Safety Extra Low Voltage, EN 60950) oder PELV (Protective Extra Low Voltage, EN 60742)
	Die Absicherung der Systeme H41q, H41qc und H51q muss gemäß den Angaben in den Datenblättern erfolgen.
	Prüfung des Spannungsbereichs: 24 V DC, -20 %...+25 % (19,2...30,0 V DC)
	Prüfung auf Unempfindlichkeit gegen Kurzzeitunterbrechung der externen Stromversorgung: DC, PS 2: 10 ms
	Polaritätsumkehr der Versorgungsspannung: siehe Hinweis im entsprechenden Kapitel des Katalogs oder im Datenblatt der Netzgerätebaugruppe
	Pufferbatterie, Beständigkeitsprüfung: Prüfung B, 1000 h, Lithium-Batterie als Pufferbatterie

Tabelle 8: Nachprüfung der Eigenschaften der Gleichstromversorgung

2.3.6 ESD-Schutzmaßnahmen

Nur Personal, das Kenntnisse über ESD-Schutzmaßnahmen besitzt, darf Änderungen oder Erweiterungen des Systems oder den Austausch eines Moduls durchführen.



Elektrostatische Entladungen können die in den Systemen eingebauten elektronischen Bauelemente beschädigen.

- Zur elektrostatischen Entladung ein geerdetes Objekt berühren.
- Für die Arbeiten einen antistatisch gesicherten Arbeitsplatz benutzen und ein Erdungsband tragen.
- Das Gerät bei Nichtbenutzung elektrostatisch geschützt aufbewahren, z.B. in der Verpackung.

Änderungen oder Erweiterungen an der Verdrahtung des Systems nur durch Personal, das Kenntnis von ESD-Schutzmaßnahmen besitzt.

2.4 Qualifikation des Personals

Jedes Fachpersonal (Planung, Montage, Inbetriebnahme) muss über die Risiken und deren mögliche Folgen unterrichtet sein, die im Falle einer Manipulation von einem sicherheitsgerichteten Automatisierungssystem ausgehen können.

Planer und Projektierer müssen zusätzlich Kenntnisse in Auswahl und Einsatz elektrischer und elektronischer Sicherheitssysteme in Anlagen der Automatisierungstechnik haben, um z. B. die Folgen eines falschen Anschlusses oder einer falschen Programmierung zu vermeiden.

Der Anlagenbetreiber ist für die Qualifikation und Sicherheitseinweisung des Bedien- und Wartungspersonals verantwortlich.

Änderungen oder Erweiterungen an der Verdrahtung des Systems darf nur durch Personal durchgeführt werden, das Kenntnis von Steuer- und Regeltechnik, Elektrotechnik, Elektronik, Einsatz von PES und ESD-Schutzmaßnahmen besitzt.

2.5 Aufgaben der Maschinen- und Anlagenhersteller sowie des Betreibers

Die Maschinen- und Anlagenhersteller sowie der Betreiber sind dafür verantwortlich, dass die sichere Anwendung der H41q/H51q-Systeme in Automatisierungsanlagen und in Gesamtanlagen gewährleistet ist.

Die korrekte Programmierung der H41q/H51q-Systeme ist durch die Maschinen- und Anlagenhersteller ausreichend zu validieren.

3 Sicherheitsphilosophie und Auflagen

3.1 Zertifizierung

Die sicherheitsgerichteten Automatisierungsgeräte (PES = Programmierbares Elektronisches System) der Systemfamilien H41q, H41qc und H51q sind wie folgt zertifiziert:



TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am grauen Stein
D - 51105 Köln

Zertifikat und Prüfbericht Nr. 968/EZ 129.16/10

Sicherheitsgerichtete Automatisierungsgeräte
H41q-MS, H41q-HS, H41q-HRS
H41qc-MS, H41qc-HS, H41qc-HRS
H51q-MS, H51q-HS, H51q-HRS

Die sicherheitsgerichteten Automatisierungsgeräte der Systemfamilien H41q, H41qc und H51q sind nach den im folgenden aufgelisteten wichtigen Normen für die funktionale Sicherheit geprüft und zertifiziert:

IEC 61508: Teile 1-7: 1998-2000	bis SIL 3
IEC 61511: Teile 1-3: 2004	bis SIL 3
EN/ISO 13849-1: 2008	Kategorie 4, Performance Level e
EN 50156-1: 2004	
EN 12067-2: 2004, EN 298: 2003, EN 230: 2005	
NFPA 85: 2007, NFPA 86: 2007	
EN 61131-2: 2007	
EN 61000-6-2: 2005, EN 61000-6-4: 2007	
EN 54-2:1997, A1: 2006, NFPA 72: 2010	
EN 50130-4: 1998 + A1: 1998 + A2: 2003 + Corr. 2003	

Das Kapitel 2.3 enthält eine detaillierte Aufstellung aller durchgeführten Umwelt- und EMV-Prüfungen.

3.2 Sicherheit und Verfügbarkeit

Bereits als Monosysteme sind die Systemfamilien H41q, H41qc und H51q auf Grund der 1oo2D Mikroprozessorstruktur auf einer Zentralbaugruppe bis zu SIL 3 ausgelegt.

Je nach geforderter Verfügbarkeit lassen sich die HIMA-Automatisierungssysteme im Zentral- und E/A-Bereich mit redundanten Baugruppen bestücken. Redundante Baugruppen erhöhen die Verfügbarkeit, da im Defektfall einer Baugruppe diese automatisch außer Betrieb genommen wird und die redundante Baugruppe den Betrieb ohne Unterbrechung aufrechterhält.

3.2.1 Sicherheit

Für die sicherheitsbezogenen Systeme H41q, H41qc und H51q wurden gemäß IEC 61508 die PFD- (Probability of Failure on Demand) und PFH- (Probability of Failure per Hour) Berechnungen durchgeführt.

IEC 61508-1 legt für SIL 3 fest:

- eine PFD von $10^{-4} \dots 10^{-3}$
- eine PFH von $10^{-8} \dots 10^{-7}$ pro Stunde

Für die Steuerung werden 15% des Grenzwertes aus der Norm für PFD und PFH angenommen. Damit ergeben sich als Grenzwerte für den Anteil der Steuerung:

- PFD = $1,5 * 10^{-4}$
- PFH = $1,5 * 10^{-8}$ pro Stunde

Das Intervall für die Wiederholungsprüfung für die sicherheitsbezogenen Systeme H41q, H41qc und H51q wird auf 10 Jahre ¹⁾ festgelegt.

Die Sicherheitsfunktionen, bestehend aus einem sicherheitsbezogenen Loop (einem Eingang, Verarbeitungseinheit und einem Ausgang) erfüllen in allen Kombinationen die Anforderungen.

Weitere Informationen sind auf Anfrage erhältlich.

3.2.2 Übersicht

Die folgende Tabelle enthält eine Übersicht zu Systembezeichnungen, Sicherheit, Verfügbarkeit und Systemkonfigurationen

Systembezeichnung	H41qc-MS H41q-MS H51q-MS	H41qc-HS H41q-HS H51q-HS	H41qc-HRS H41q-HRS H51q-HRS
SIL / Kategorie	SIL 3 / Kat 4	SIL 3 / Kat 4	SIL 3 / Kat 4
Verfügbarkeit	normal	hoch	sehr hoch
Konfiguration			
Zentralbaugruppe	mono	redundant	redundant
E/A-Baugruppen	mono ¹⁾	mono ¹⁾	redundant
E/A-Bus	mono	mono	redundant ²⁾

¹⁾ Einzelne E/A-Baugruppen sind zur Erhöhung der Verfügbarkeit auch redundant oder in einer 2oo3-Auswahlschaltung (z. B. siehe Kapitel 7.8.5) einsetzbar

²⁾ HIMA empfiehlt, bei einem redundanten E/A-Bus nicht nur die E/A-Baugruppen, sondern auch die Peripherie (Sensoren und Aktoren in der Anlage) nach Möglichkeit redundant einzusetzen. Diese Elemente haben im Allgemeinen höhere Ausfallraten als die Baugruppen des PES.

Tabelle 9: Systembezeichnungen, Sicherheit, Verfügbarkeit und Systemkonfigurationen

¹⁾ Einschränkungen bei der Relaisbaugruppe F 3430, siehe Kapitel 6.5

Zur Erhöhung der Verfügbarkeit durch redundante Baugruppen sind drei Punkte wesentlich:

- Fehlerhafte Baugruppen müssen erkannt und abgeschaltet werden, damit sie nicht das System blockieren.
- Der Betreiber muss im Fehlerfall eine Meldung erhalten für den Austausch von Baugruppen.
- Nach Austausch einer Baugruppe muss diese automatisch in Betrieb gehen.

Diese Forderungen erfüllen die HIMA-Automatisierungssysteme in den entsprechenden Konfigurationen.

Für die Programmierung der Geräte wird ein PADT (Programmiergerät, PC) mit dem Programmierwerkzeug

ELOP II

nach IEC 61131-3 verwendet. Es bietet Unterstützung bei der Erstellung sicherheitsgerichteter Programme und der Bedienung der Automatisierungsgeräte.

3.3 Sicherheitszeiten

Einzelfehler, die zu einem gefährlichen Betriebszustand führen können, werden durch die Selbsttesteinrichtungen innerhalb der Fehlertoleranzzeit (min. 1 s) erkannt. Die Fehlertoleranzzeit wird als Sicherheitszeit im Menü für die Einstellung der Eigenschaften der Ressource vorgegeben.

Fehlertoleranzzeit

Prozestechnische Größe, die häufig in Anwenderrichtlinien als Sicherheitszeit bezeichnet wird.

Sicherheitszeit (im PES)

Größe, abhängig von Systemfähigkeit

Ausfälle, die sich nur in Kombination mit zusätzlichen Fehlern sicherheitskritisch auswirken können, werden durch Hintergrundtests innerhalb der Mehrfahlerintrittszeit (MEZ) erkannt. Die Mehrfahlerintrittszeit wird mit der Parametrierung der Sicherheitszeit festgelegt und ist im Betriebssystem als das 3600-fache davon definiert.

Bei den Tests werden unterschieden:

- *Tests innerhalb der Sicherheitszeit*
Sie werden innerhalb der Sicherheitszeit durchgeführt (Vordergrundtests),
Reaktionszeit: sofort, spätestens innerhalb der Sicherheitszeit.
- *Tests innerhalb der Mehrfahlerintrittszeit*
Sie werden innerhalb der Mehrfahlerintrittszeit durchgeführt und sind in viele Zyklen aufgeteilt (Hintergrundtest),
Reaktionszeit: bei Erkennen sofort, spätestens innerhalb der Mehrfahlerintrittszeit.

Beispiel für die Reaktionszeit: Maximal die zweifache Zykluszeit. Wird für den Prozess eine Fehlertoleranzzeit (Sicherheitszeit) von 1s gefordert, darf die Zykluszeit nicht länger als 500 ms sein.

Fehlerreaktionszeit

Die Fehlerreaktionszeit eines Automatisierungsgeräts entspricht der Sicherheitszeit ($\geq 1s$), die bei den Eigenschaften der Ressource definiert wird. Dabei ist zu beachten, dass die Zykluszeit nicht größer als die Hälfte der Sicherheitszeit wird, da auf Fehler in den Eingabebaugruppen innerhalb von max. 2 Zyklen reagiert wird. Die Zykluszeit wird von der Sicherheitszeit beeinflusst, die den Zeitraum festlegt, in dem alle Vordergrundtests durchgeführt werden.

Eine kurze Sicherheitszeit erhöht die Zykluszeit und umgekehrt. Bei langen Sicherheitszeiten werden einige Tests auf mehrere Zyklen verteilt.

Beispiel 1: Sicherheitszeit = 1 s

Zykluszeit für Anwenderprogramm = 450 ms

Zeitbedarf für Tests = 100 ms

innerhalb der Sicherheitszeit sind 2 Zyklen möglich

$100 \text{ ms} / 2 = 50 \text{ ms}$ / Zyklus Zeitbedarf für Tests

Gesamt-Zykluszeit = **500 ms**

Beispiel 2: Sicherheitszeit = 2 s

Zykluszeit für Anwenderprogramm = 450 ms

Zeitbedarf für Tests = 100 ms

innerhalb der Sicherheitszeit sind 4 Zyklen möglich

$100 \text{ ms} / 4 = 25 \text{ ms}$ / Zyklus Zeitbedarf für Tests

Gesamt-Zykluszeit = **475 ms**

i

Bei Ausgaben des Betriebssystems vor (07.14) ist der Wert 255 s für die Sicherheitszeit nicht erlaubt!

Nur der Wertebereich 1 bis 254 s ist zulässig!

3.4 Wiederholungsprüfung

Die Wiederholungsprüfungen erkennen verdeckte gefährliche Fehler, die sonst ggfs. die sichere Funktion der Anlage beeinträchtigen würden.

HIMA Sicherheitssysteme sind **in Intervallen von 10 Jahren**¹⁾ einer Wiederholungsprüfung zu unterziehen. Durch eine Analyse der realisierten Sicherheitskreise mittels eines Berechnungswerkzeugs kann das Intervall häufig verlängert werden.

Bei Relaisbaugruppen muss die Wiederholungsprüfung für die Relais in für die Anlage festgelegten Intervallen erfolgen.

3.4.1 Durchführung der Wiederholungsprüfung

Die Durchführung der Wiederholungsprüfung hängt von folgenden Punkten ab:

- Beschaffenheit der Anlage (EUC = equipment under control)
- Gefährdungspotential der Anlage
- für den Betrieb der Anlage anzuwendende und von der zuständigen Prüfstelle als Grundlage für die Genehmigung benutzte Normen

Nach den Normen IEC 61508 1-7, IEC 61511 1-3 und VDI/VDE 2180 Blatt 1 bis 4 hat bei sicherheitsgerichteten Systemen der Betreiber für eine Wiederholungsprüfung zu sorgen.

3.4.2 Häufigkeit der Wiederholungsprüfungen

Das HIMA-PES kann einer Wiederholungsprüfung unterzogen werden, indem der gesamte Sicherheitskreis überprüft wird.

In der Praxis wird für die Eingangs- und Ausgangs-Feldgeräte ein kürzeres Intervall für die Wiederholungsprüfung (z. B. alle 6 oder 12 Monate) gefordert als für die HIMA-Steuerung.

¹⁾ Ausnahme: die Baugruppe F 3430 ist für SIL 3 in Intervallen von 5 Jahren zu prüfen

Wenn der Anwender den kompletten Sicherheitskreis wegen des Feldgeräts prüft, dann ist die HIMA-Steuerung in diesen Test automatisch eingeschlossen. Es sind dann keine zusätzlichen Wiederholungsprüfungen für die HIMA-Steuerung erforderlich.

Falls die Wiederholungsprüfung der Feldgeräte die HIMA-Steuerung nicht mit einbezieht, dann muss diese mindestens einmal in 10 Jahren überprüft werden. Dies kann erreicht werden, indem die HIMA-Steuerung neu gestartet wird.

Zusätzliche Anforderungen für die Wiederholungsprüfung bestimmter Baugruppen sind im Datenblatt der jeweiligen Baugruppe beschrieben.

3.5 Sicherheitsauflagen

Für den Einsatz der sicherheitsgerichteten Steuerungen der Systeme H41q, H41qc und H51q gelten folgende Sicherheitsauflagen.

i

Für den sicheren Betrieb einer Anlage entsprechend den dafür gültigen Anwendungsnormen ist der **Betreiber** verantwortlich.

3.5.1 Hardware-Projektierung: produktunabhängige Auflagen

- Für den sicherheitsgerichteten Betrieb dürfen nur hierfür zugelassene fehlersichere Hardware-Baugruppen und Software-Komponenten verwendet werden. Die zugelassenen Hardware-Baugruppen und Software-Komponenten sind aufgeführt in der
Liste zur Verfolgung der Versionsfreigaben der Baugruppen und der Firmware der Firma HIMA Paul Hildebrandt GmbH + Co KG.
Die Zertifikatsnummer ist der letzten gültigen Freigabedokument zu entnehmen. Die jeweils aktuellen Versionsstände sind der gemeinsam mit der Prüfstelle geführten Versionsliste zu entnehmen.
- Die spezifizierten Einsatzbedingungen (siehe Kapitel 2.3) bezüglich EMV, mechanische, klimatische Einflüsse müssen eingehalten werden.
- Nicht fehlersichere, jedoch rückwirkungsfreie Hardware-Baugruppen und Software-Komponenten dürfen für die Verarbeitung nicht sicherheitsrelevanter Signale eingesetzt werden, nicht jedoch für die Bearbeitung sicherheitstechnischer Aufgaben.
- Bei allen extern an das System angeschlossenen Sicherheitsstromkreisen ist das Ruhestromprinzip einzuhalten.

3.5.2 Hardware-Projektierung: produktabhängige Auflagen

- An das System dürfen nur Geräte angeschlossen werden, die eine sichere Trennung zum Netz aufweisen.
- Die sichere elektrische Trennung der Stromversorgung muss in der 24 V Versorgung des Systems erfolgen. Es dürfen nur Netzteile in den Ausführungen PELV oder SELV eingesetzt werden.

3.5.3 Programmierung: produktunabhängige Auflagen

- In sicherheitsrelevanten Anwendungen ist auf eine korrekte Parametrierung der die Sicherheit beeinflussenden Systemgrößen zu achten. Mögliche Parametrierungen sind in den folgenden Kapiteln beschrieben. Insbesondere ist die Festlegung von Systemkonfiguration, maximaler Zykluszeit und Sicherheitszeit zu beachten.

3.5.4 Programmierung: produktabhängige Auflagen

- Die Fehlerreaktion des Systems bei Fehlern in den fehlersicheren Ein- und Ausgangsbaugruppen muss gemäß den anlagenspezifischen sicherheitstechnischen Gegebenheiten durch das Anwenderprogramm festgelegt werden.

- Bei Verwendung des Programmierwerkzeugs ELOP II, ab Rev. 3.5, kann die Verifizierung des erstellten Programms gemäß den Vorgaben dieses Sicherheitshandbuchs vereinfacht werden.
- Eine ausreichende Validierung des Programms muss jedoch erfolgen.
- Funktionsprüfungen/Verifikationen nach Änderung der Applikation können auf die geänderten Programmteile beschränkt werden.
- Die in Kapitel 7 beschriebene Vorgehensweise bei Programmerstellung und Änderung ist einzuhalten.

3.5.5 Kommunikation: produktabhängige Auflagen

- Bei der Verwendung der sicherheitsgerichteten Kommunikation zwischen verschiedenen Geräten ist zu beachten, dass die Gesamtreaktionszeit des Systems nicht die Fehlertoleranzzeit überschreitet. Die aufgeführten Berechnungsgrundlagen sind anzuwenden.
- Eine Übertragung der sicherheitsrelevanten Daten über öffentliche Netze (z. B. Internet) ist nur zulässig mit zusätzlichen Sicherheitsmaßnahmen, z. B. VPN-Tunnel.
- Falls die Übertragung der Daten über firmen-/fabrikinterne Netze erfolgt, muss durch administrative oder technische Maßnahmen dafür Sorge getragen werden, dass ausreichender Schutz vor Manipulation gegeben ist (z. B. Abschottung des sicherheitsrelevanten Teils des Netzes von anderen Netzen mit einer Firewall).
- An die Kommunikationsschnittstellen dürfen nur Geräte angeschlossen werden, die eine sichere elektrische Trennung gewährleisten.

3.5.6 Sonderbetriebsarten: produktunabhängige Auflagen

- Reload in Sicherheitsanwendungen ist nur nach Rücksprache mit der für die Anlagenabnahme zuständigen Prüfstelle und mit Hilfe des zertifizierten Werkzeugs ELOP II zulässig.
- Während des gesamten Reload muss der für den Reload Verantwortliche die sicherheitstechnisch ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen sicherstellen.
- Vor jedem Reload sind die Versionsänderungen gegenüber dem noch laufenden Anwenderprogramm mit Hilfe des C-Codevergleichers von ELOP II zu ermitteln.
- Beim Reload eines Mono-PES darf die Zeitdauer für die gesamte Änderung zuzüglich der doppelten Zykluszeit, die Fehlertoleranzzeit des Prozesses nicht überschreiten.
- Für den Einsatz von „Maintenance Override“ ist die jeweils aktuelle Version des Dokuments *Wartungseingriffe, Maintenance Override* auf der Webseite www.tuvasi.com des TÜV Rheinland zu beachten.
- Mit ELOP II ist ein statischer Offline-Test der Logik möglich. Die Offline-Simulation ist keiner sicherheitstechnischen Prüfung unterzogen worden. Die Simulation kann daher keine Funktionsprüfung der Anlage ersetzen.
- Erforderlichenfalls muss der Betreiber in Absprache mit der für die Applikation zuständigen Abnahmestelle administrative Maßnahmen für den Zugangsschutz zur Steuerung festlegen.

4 Zentralbaugruppen

Die erforderlichen zentralen Komponenten für die verschiedenen Ausführungen der HIMA-Automatisierungsgeräte sind in Bausätzen zusammengefasst. Der jeweilige Bausatz eines funktionsfähigen Zentralgerätes besteht aus:

- Zentralbaugruppenträger
- Zentralbaugruppen
- Netzgeräten
- Zubehör

Der genaue Umfang sowie die Verschaltung der Versorgungsspannung und die Anschaltung der E/A-Ebene kann den Datenblättern im Katalog *Programmierbare Systeme, Systemfamilien H41q/H51q*, HI 800 262, entnommen werden.

4.1 Zentralbaugruppen und Bausätze für die Systeme H41q und H41qc

Baugruppe/ Bausatz	Bezeichnung	sicherheits- gerichtet	rückwirkungs- frei
F 8652 X	Zentralbaugruppe, Doppelprozessor 1oo2	•	•
F 8653 X	Zentralbaugruppe		•
B 4231	Bausatz Zentralgerät H41q-MS	•	•
B 4233-1	Bausatz Zentralgerät H41q-HS	•	•
B 4233-2	Bausatz Zentralgerät H41q-HRS	•	•
B 4235	Bausatz Zentralgerät H41qc-MS	•	•
B 4237-1	Bausatz Zentralgerät H41qc-HS	•	•
B 4237-2	Bausatz Zentralgerät H41qc-HRS	•	•

Tabelle 10: Zentralbaugruppen und Bausätze für die Systeme H41q und H41qc

4.2 Zentralbaugruppen und Bausätze für das System H51q

Baugruppe/ Bausatz	Bezeichnung	sicherheits- gerichtet	rückwirkungs- frei
F 8650 X	Zentralbaugruppe, Doppelprozessor 1oo2	•	•
F 8651 X	Zentralbaugruppe		•
B 5231	Bausatz Zentralgerät H51q-MS	•	•
B 5233-1	Bausatz Zentralgerät H51q-HS	•	•
B 5233-2	Bausatz Zentralgerät H51q-HRS	•	•
B 9302	E/A-Baugruppenträger	•	•

Tabelle 11: Zentralbaugruppen und Bausätze für das System H51q

4.3 Weitere zentrale Baugruppen für die Systeme H41q, H41qc und H51q

Baugruppe/ Bausatz	Bezeichnung	sicherheits- gerichtet	rückwirkungs- frei
Stromverteilerbaugruppen			
F 7132	4fach Stromverteiler		•
F 7133	4fach Stromverteiler mit Sicherungsüberwachung		•
Zusatzbaugruppen			
F 7126	Stromversorgungsbaugruppe		•
F 7130A	Stromversorgungsbaugruppe		•
F 7131	Netzgeräteüberwachung mit Pufferbatterien für H51q		•
F 8621A	Coprozessorbaugruppe für H51q		•
F 8627 F 8627X	Kommunikationsbaugruppe für Ethernet		•
F 8628 F 8628X	Kommunikationsbaugruppe für Profibus DP (Slave)		•
Busverbindungen			
F 7553	E/A-Busverbindungsbaugruppe für H51q		•
Busanschlussmodule z. Aufbau von HIPRO			
H 7505	Schnittstellenumsetzer RS 485, V.24/20 mA 2-Draht/4-Draht (HIPRO)		•
H7506	Busanschlussklemme zum Aufbau von 2-Draht-Bussen		•

Tabelle 12: Weitere zentrale Baugruppen für die Systeme H41q, H41qc und H51q

4.4 Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsgerichteten Zentralbaugruppen

Für die System-Belegung der Zentral- und Netzgerätebaugruppen sowie Buskomponenten in den Baugruppenträgern der Systemfamilien H41q/H51q gelten nachfolgende Anforderungen:

Systeme H41q, H41qc	System H51q
<p>Im Systembaugruppenträger H41q sind einsetzbar:</p> <ul style="list-style-type: none"> • zwei Zentralbaugruppen • 12 E/A - Baugruppen • zwei Stromversorgungsbaugruppen • drei Sicherungsbaugruppen <p>Im Systembaugruppenträger H41qc sind einsetzbar:</p> <ul style="list-style-type: none"> • zwei Zentralbaugruppen • zwei Kommunikationsbaugruppen • 13 E/A - Baugruppen • zwei Stromversorgungsbaugruppen <p>Absicherung der Ein-/Ausgänge über Automaten</p>	<p>Im Zentralbaugruppenträger sind einsteckbar:</p> <ul style="list-style-type: none"> • zwei Zentralbaugruppen • pro Zentralbaugruppe drei Coprozessorbaugruppen F 8621/A oder fünf Kommunikationsbaugruppen F 8625, F 8626, F 8627, F 8628 <p>Die Grundkomponenten für E/A-Baugruppenträger sind in Bausätzen zusammengefasst.</p>

Tabelle 13: Sicherheit und Verfügbarkeit, Unterschiede H41q, H41qc und H51q

4.4.1 Netzgeräte

In sicherheitstechnischen Anwendungen ist immer ein Netzgerät 24 V = / 5 V = mehr einzusetzen als vom Stromverbrauch her nötig wäre. Dies gilt für den Zentralbaugruppenträger und für die Zusatzstromversorgung. Die Netzgeräte sind über Dioden entkoppelt und werden von den Zentralgeräten überwacht.

4.4.2 Funktionale Beschreibung der sicherheitsgerichteten Zentralbaugruppen F 8652 X / F 8650 X

Jede Zentralbaugruppe vom Typ F 8652 X oder F 8650 X besteht aus folgenden Funktionsblöcken:

- zwei takt synchrone Mikroprozessoren
- jeder Mikroprozessor hat einen eigenen Speicher
- die Speicher des einen Prozessors enthalten das Programm und die Daten in nicht invertierter Form, die Speicher des anderen Prozessors enthalten dagegen das Programm und die Daten in invertierter Form
- testbarer Hardware-Vergleicher für alle externen Zugriffe beider Mikroprozessoren
- im Fehlerfall wird der Watchdog in den sicheren Zustand gesetzt und der Prozessorstatus gemeldet
- Flash-EPROMs der Programmspeicher für Betriebssystem und Anwenderprogramm geeignet für min. 100.000 Speicherzyklen
- Datenspeicher in SRAM (statisches RAM)
- Multiplexer zum Anschluss von E/A-Bus, Dual Port RAM (DPR) und redundanter Zentralbaugruppe
- Pufferung der SRAMs über Batterien auf der Zentralbaugruppe
- 2 Schnittstellen RS 485 mit galvanischer Trennung, Übertragungsraten: max. 57600 bps; Einstellung auf 9600 bps und 57600 bps per Schalter oder Einstellung (auch anderer Übertragungsraten) per Software, wobei Softwarewerte vorrangig sind
- Diagnoseanzeige und 2 LEDs für Informationen des Systems, E/A-Bereichs und des Anwenderprogramms

- Dual-ported RAM für schnellen, wechselseitigen Speicherzugriff zur zweiten Zentralbaugruppe
- batteriegepufferte Hardware-Uhr
- E/A-Bus-Logik zur Verbindung mit den E/A-Baugruppen
- Sicherer Watchdog
- Netzgeräteüberwachung, testbar (5 V Systemspannung)
- Batterieüberwachung

4.5 Prinzipielle Arbeitsweise von sicherheitsgerichteten Zentralbaugruppen

Sicherheitsgerichtete Zentralbaugruppen bestehen aus zwei Mikroprozessoren mit je einem RAM, die gleichzeitig dieselben Programme, Betriebssystem und Anwenderprogramm, abarbeiten. Ein Vergleicher vergleicht ständig die Daten auf den Bussen zwischen den Mikroprozessoren und ihren Speichern.

Das Betriebssystem enthält Selbsttestroutinen, die immer wieder durchlaufen werden. Der Watchdog überwacht den Programmablauf.

4.5.1 Selbsttestroutinen

In der Tabelle 14 sind die Selbsttestroutinen der sicherheitsgerichteten Zentralbaugruppen F 8650 X und F 8652X und der Ankopplung an die E/A-Ebene erläutert:

Test	Beschreibung
CPU-Test	Geprüft werden: <ul style="list-style-type: none"> • Befehls- und Adressierungsarten • Beschreibbarkeit der Flags und die durch Flags bedingten Befehle • Beschreibbarkeit und das Übersprechen der Register • Rechenwerk (ALU)
Test der Speicherbereiche	Das Betriebssystem, das Anwenderprogramm, die Konstanten und Parameter sowie die variablen Daten sind in jeder Zentralbaugruppe direkt und invers gespeichert und werden von einem Hardwarevergleicher auf Antivalenz geprüft.
Feste Speicherbereiche	Betriebssystem, Anwenderprogramm und Parameterbereich sind in je einem Flash-EPROM gespeichert und werden durch einen CRC-Test gesichert.
RAM-Test	Die RAM-Bereiche werden mit einem Schreib-/ Lesetest insbesondere auf Übersprechen geprüft.
Watchdog-Test	Das Watchdog-Signal wird abgeschaltet, wenn es nicht in einem festgelegten Zeitraum von beiden CPUs mit antivalenten Bitmustern getriggert wird oder wenn der Hardwarevergleicher zwischen den beiden Speichern (direkt und invers) einen Unterschied feststellt. Durch einen weiteren Test wird die Abschaltbarkeit des Watchdog-Signals geprüft

Tabelle 14: Selbsttestroutinen

Test	Beschreibung
Test der Verbindung zur E/A-Ebene innerhalb der Zentralbaugruppe	Bei redundanten Zentralbaugruppen in Systemen H41q-HS / H41qc-HS / H51q-HS mit einkanaligem E/A-Bus ist die gegenseitige Verriegelung des E/A-Zugriffs der Zentralbaugruppen gesichert. Die dazu dienende Verriegelungsschaltung wird durch Selbsttests geprüft. Bei zweikanaliger E/A-Ebene - HR- oder HRS-System - wird die E/A-Zugriffsberechtigung zurückgelesen und geprüft. Bei einkanaliger E/A-Ebene - M- oder MS-System (einkanalige E/A-Baugruppen und einkanalige CPU) - wird die E/A-Zugriffsberechtigung zurückgelesen und geprüft.
Test der Verbindungsbaugruppe innerhalb der E/A-Baugruppenträger	Die Adressierung wird zyklisch nach jeder Bearbeitung einer sicherheitsgerichteten E/A-Baugruppe getestet. Die Adressen aller vereinbarten E/A-Baugruppenpositionen werden zurückgelesen und geprüft. Bei der Baugruppe F 7553 werden die Sicherheitsschalter getestet.

Tabelle 14: Selbsttestroutinen

4.5.2 Reaktion auf festgestellte Fehler bei Zentralbaugruppen

Die Testroutinen erkennen Fehler und schalten die defekte Zentralbaugruppe ab. Gleichzeitig wird über die Diagnoseanzeige der Fehler angezeigt und in der Systemdiagnose eingetragen.

Bei einer Zentralbaugruppe - MS-System - bedeutet dies eine Gesamtabstaltung des Automatisierungsgeräts.

Bei redundanten Zentralbaugruppen - HS- und HRS-Systeme - wird die defekte Zentralbaugruppe abgeschaltet. Die zweite Zentralbaugruppe führt den Betrieb unterbrechungsfrei weiter.

Wird bei redundanten Systemen die defekte Zentralbaugruppe gegen eine funktionsfähige mit gleichem Anwenderprogramm und Betriebssystem ausgetauscht, erhält die neue Zentralbaugruppe die aktuellen Daten von der laufenden Zentralbaugruppe, und das System geht wieder in den redundanten Betrieb.

Unter bestimmten Voraussetzungen (u.a. gleiche Betriebssystemversion, mindestens V7.0-8 (05.21) wird auch das Anwenderprogramm selbst von der noch laufenden Zentralbaugruppe in die neue, „leere“ Zentralbaugruppe geladen (*self-education*). Zu Einzelheiten siehe das Kapitel *Self-Education* im Betriebssystem-Handbuch HI 800 104 D.

4.5.3 Diagnoseanzeige

Die Diagnoseanzeige ist Bestandteil der Zentralbaugruppe. Sie besteht aus folgenden Teilen:

- einer 4stelligen alphanumerischen Anzeige für Texte und Werte
- einer LED *CPU* zur Anzeige von Zentralbaugruppenfehlern
- einer LED *IO* zur allgemeinen Fehleranzeige sicherheitsgerichteter E/A-Baugruppen.

Außerdem sind ein Quittierungstaster (ACK) und zwei Taster zum Abrufen weiterer Systeminformationen vorhanden.

Bei Fehlern in der Zentralbaugruppe leuchtet die LED *CPU*. Die 4stellige Anzeige zeigt STOP an. Es ist möglich, durch eine Bedienaktion den Fehlercode anzuzeigen. Eine Liste der Fehlercodes befindet sich im Handbuch *Funktionen des Betriebssystems* HI 800 104 D.

Bei Fehlern von sicherheitsgerichteten Baugruppen in der E/A-Ebene leuchtet die LED *IO*. Die 4stellige Anzeige zeigt die Baugruppenposition und evtl. den gestörten Kanal an.

Das Diagnosesystem stellt alle Fehlercodes für eine Visualisierung auf einem Prozess-Leitsystem bereit. Das Diagnosesystem pflegt eine Fehlerhistorie. Diese ist auf dem PADT anzeigbar und unterstützt die Erkennung von Problemen in der Anlage.

4.6 Reaktion auf festgestellte Fehler im E/A-Bus-Bereich

Bei Fehlern im E/A-Bus-Bereich zwischen Zentralbaugruppe und Verbindungsbaugruppen werden alle von diesem Fehler betroffenen E/A-Baugruppenträger abgeschaltet.

Tritt ein Fehler im E/A-Bus-Bereich nur innerhalb des E/A-Baugruppenträgers auf, schaltet die Verbindungsbaugruppe die Ausgangsbaugruppen in dem betroffenen E/A-Baugruppenträger ab.

4.7 Hinweis zum Austausch von Zentralbaugruppen

Der Austausch defekter Baugruppen sowohl im Zentralbereich als auch im E/A-Bereich kann während des Betriebs vorgenommen werden, ohne dass das Automatisierungsgerät abgeschaltet werden muss.

i

Betriebsunterbrechung möglich!
Ein Austausch von defekten Zentralbaugruppen wird dringend empfohlen.

Im Fehlerfall oder im Wartungsfall sind beim Austausch folgende Arbeitsschritte einzuhalten:

- Zentralbaugruppen für nicht redundante Automatisierungsgeräte mit integrierter Pufferbatterie müssen ohne Anwenderprogramm gelagert werden, wenn dieses Programm Variablen mit Haftverhalten (Retain-Variable) enthält. Diese werden beim Hochfahren des Systems nicht auf den Initialwert gesetzt.
- Zentralbaugruppen für redundante Automatisierungsgeräte mit integrierter Pufferbatterie können mit Anwenderprogramm gelagert werden, auch wenn dieses Programm Variablen mit Haftverhalten (Retain-Variable) enthält. Diese werden beim Hochfahren von der laufenden Zentralbaugruppe übernommen.

Die Diagnoseanzeige der Zentralbaugruppe signalisiert die entladene interne Batterie der Zentralbaugruppe mit dem Text *BATI*.

Eine Empfehlung zum Batteriewechsel auf den Baugruppen ist dem Datenblatt zu entnehmen.

i

Bei Ausfall der Batterie und gleichzeitigem Spannungsausfall verlieren die RETAIN-Variablen ihre gespeicherten Werte. Das System initialisiert in diesem Fall die Werte beim Hochfahren.

5 Eingangsbaugruppen

5.1 Gesamtübersicht der Eingangsbaugruppen für die Systeme H41q, H41qc und H51q

Baugruppe		sicherheitsgerichtet	rückwirkungsfrei	(Ex)i	dazugehöriger SW-Baustein
digitale Eingangsbaugruppen					
F 3221	16fach Eingangsbaugruppe		•		
F 3222	8fach Eingangsbaugruppe		•		
F 3223	4fach Eingangsbaugruppe		•	•	
F 3224A	4fach Eingangsbaugruppe		•	•	
F 3236	16fach Eingangsbaugruppe	•	•		
F 3237	8fach Eingangsbaugruppe	•	•		HB-RTE-3
F 3238	8fach Eingangsbaugruppe	•	•	•	HB-RTE-3
F 3240	8fach Eingangsbaugruppe	•	•		
F 3248	16fach Eingangsbaugruppe	•	•		
F 5220	2fach Zählerbaugruppe	•	•		HF-CNT-3, -4
analoge Eingangsbaugruppen					
F 6213	4fach Analogeingangsbaugruppe	•	•		HA-RTE-3
F 6214	4fach Analogeingangsbaugruppe	•	•		HA-RTE-3
F 6215	8fach Analogeingangsbaugruppe		•		
F 6217	8fach Analogeingangsbaugruppe	•	•		
F 6220	8fach Thermoelementbaugruppe	•	•	•	HF-TMP-3
F 6221	8fach Analogeingangsbaugruppe	•	•	•	HF-AIX-3

Tabelle 15: Eingangsbaugruppen für die Systeme H41q, H41qc und H51q

5.2 Sicherheit und Verfügbarkeit von sicherheitsgerichteten Eingangsbaugruppen

Einige Typen der analogen und digitalen Eingangsbaugruppen haben wegen ihrer erhöhten Komplexität ein eigenes 1oo2 Mikroprozessorsystem, das sicherheitsgerichtete Tests während des Betriebs automatisch durchführt und die sicheren Daten für die sichere Verarbeitungseinheit bereitstellt.

Die sicherheitsgerichteten Eingangsbaugruppen ermöglichen eine Diagnoseanzeige und somit eine Fehlererkennung und Fehlerlokalisierung.

i

In sicherheitstechnischen Systemen ist es möglich, sowohl sicherheitsgerichtete als auch rückwirkungsfreie Eingangsbaugruppen in Mischbestückung einzusetzen.

Sicherheitsgerichtete Eingangsbaugruppen werden in den Systemen H41q, H41qc und H51q während des Betriebes automatisch einem hochwertigen, zyklischen Selbsttest unterzogen. Die Eingangs-Baugruppen enthalten Schaltungsteile, die einen Test der Eingangs-Baugruppen-Funktion über spezielle im Betriebssystem integrierte Testroutinen ermöglichen. Diese Testroutinen sind TÜV geprüft und stellen die korrekte Funktion der

jeweiligen Baugruppe sicher. Bei jedem erkannten Fehler werden Fehlermeldungen erzeugt. Erkannte Fehler führen automatisch eine sicherheitsgerichtete Reaktion des Systems herbei. Die Fehlermeldungen sind eine Diagnoseinformation für den Betreiber. Bei der Planung und Realisierung der Anlage kann somit flexibel ein Diagnose-System erstellt werden.

Zur Erhöhung der Verfügbarkeit können die sicherheitsgerichteten Eingangsbaugruppen auch redundant eingesetzt werden.

Der Einsatz redundanter Eingangsbaugruppen beeinträchtigt die Sicherheit des Systems nicht.

Sicherheitsgerichtete Eingangsbaugruppen können sowohl für sicherheitsgerichtete als auch für nicht sicherheitsgerichtete Signale benutzt werden.

Für die zulässigen Steckplätze für Eingangsbaugruppen in den Systembaugruppenträgern und den E/A-Baugruppenträgern für die Systeme H41q, H41qc und H51q sind folgende Vereinbarungen zu beachten:

System H41q, H41qc	System H51q
Die Eingangsbaugruppen werden in den Systembaugruppenträger gefügt. Es stehen Bausätze mit 12 Steckplätzen (H41q) oder 13 Steckplätzen (H41qc) für E/A-Baugruppen zur Verfügung.	Die Eingangsbaugruppen werden in E/A-Baugruppenträgern (EABTs) mit jeweils 16 Steckplätzen für E/A-Baugruppen gefügt. Die erforderlichen Grundkomponenten für EABTs sind in Bausätzen zusammengefasst.

Tabelle 16: Zulässige Steckplätze

5.2.1 Sicherheit von Sensoren, Gebern, Transmittern

Sicherheitsgerichtete Signale sind nur gegeben, wenn die externen Sensoren, Geber oder Transmitter einen Sicherheitsnachweis haben. Haben sie keinen Sicherheitsnachweis, kann die Sicherheit von externen Sensoren, Gebern oder Transmittern auch durch eine besondere Verschaltung erreicht werden, siehe Handbuch *Funktionen des Betriebssystems* HI 800 104 D.

In diesem Fall sind mehrere Sensoren in einer 1oo2-, 2oo3- oder NooM-Schaltung zu verschalten. (Anmerkung: 1oo2 heißt „1 out of 2“, also 1 von 2.)

Die Sicherheit und Verfügbarkeit der Sensorik kann durch die Verschaltung der Sensoren erhöht werden. Realisierungsmöglichkeiten für verschiedene Sensorverschaltungen unter Sicherheits- und Verfügbarkeitsaspekten sind im Kapitel 7.8 ausführlich dargestellt. Das Anwendungsprogramm ist entsprechend auszulegen.

Auf Basis der IEC 61508 werden durch die Festlegung von Offline-Proof-Test-Intervallen entsprechende sicherheitstechnische Nachweise ermöglicht. Die Festlegungen im Detail sind hierzu anwendungsspezifisch zu definieren.

5.3 Sicherheitsgerichtete digitale Eingangsbaugruppen F 3236, F 3237, F 3238, F 3240 und F 3248

5.3.1 Testroutinen

Die Online-Testroutinen prüfen, ob die Eingangskanäle in der Lage sind, unabhängig von den anstehenden Eingangssignalen beide Signalpegel (Low- und High-Pegel) durchzuschalten. Dieser Funktionstest wird bei jedem Lesen der Eingangssignale durchgeführt. Bei jedem Fehler in der Eingangsbaugruppe wird im Anwenderprogramm der Low-Pegel (sicherer Zustand) verarbeitet.

Die Baugruppen für Initiatoren und für Kontaktgeber mit Leitungsüberwachung testen zusätzlich die Leitung bis zum Geber. An diese Baugruppen kann ein sicherheitsgerichteter Initiator angeschlossen werden. Durch die Selbsttests werden alle Anforderungen an die Erkennung der Schwellen der sicherheitsgerichteten Initiatoren erfüllt.

Die Überwachung des Geberstromes eines Kontaktgebers erfordert die Beschaltung mit zwei Widerständen gemäß Datenblatt.

5.3.2 Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Eingangsbaugruppen

Fehlerart	Systemreaktion	Bemerkung
Baugruppendefekt (Eingangsbaugruppe)	Weitergabe von FALSE ans Anwenderprogramm für alle Kanäle	Dadurch wird nach dem Ruhestromprinzip die sichere Funktion des Systems gewährleistet.
Leitungsbruch im Geberkreis	Einlesen von FALSE im betreffenden Kanal	Bei Baugruppen mit Leitungsüberwachung wird Leitungsfehler signalisiert. Bei sicherheitsgerichteten Eingängen ist dieses Signal mit dem Softwarebaustein HB-RTE-3 (siehe Anhang) auszuwerten, damit eine sichere Systemreaktion möglich ist.
Leitungsschluss im Geberkreis	Einlesen von TRUE im betreffenden Kanal	Bei Baugruppen mit Leitungsüberwachung wird Leitungsfehler signalisiert. Bei sicherheitsgerichteten Eingängen ist dieses Signal mit dem Softwarebaustein HB-RTE-3 (siehe Anhang) auszuwerten, damit eine sichere Systemreaktion möglich ist.
Allgemein	Die Diagnoseanzeige zeigt die Position der defekten Baugruppen an. Bei der Baugruppe F 3238, die zwei Steckplätze im Baugruppenträger belegt, wird die Position des rechten Steckplatzes angezeigt. Bei Verwendung von Eingangsbaugruppen mit Überwachung auf Drahtbruch und Kurzschluss des Geberkreises zeigt die Diagnoseanzeige neben der Baugruppenposition auch den fehlerhaften Kanal der Baugruppe an.	

Tabelle 17: Fehlerreaktion bei sicherheitsgerichteten digitalen Eingangsbaugruppen

5.4 Sicherheitsgerichtete Zählerbaugruppe F 5220

Die zweikanalige Zählerbaugruppe hat ein eigenes Doppelprozessorsystem mit einem sicherheitsgerichteten Ausgang pro Kanal. Sie ist zur Impulzzählung, Frequenzmessung oder Drehzahlmessung über eine einstellbare Torzeit sowie zur Drehrichtungsüberwachung einsetzbar.



Bei Änderungen der Torzeit steht der korrekte Messwert erst nach drei Torzeiten am Ausgang zur Verfügung!

5.4.1 Testroutinen

Die Baugruppe hat ein eigenes 1oo2-Mikroprozessorsystem, das sicherheitsgerichtete Online-Tests automatisch durchführt und die sicheren Daten für die sichere Signalverarbeitung am Softwarebaustein HF-CNT-3 / 4 bereitstellt.

5.4.2 Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten Zählerbaugruppe F 5220

Fehlerart	Systemreaktion im Fehlerfall	Bemerkung
Baugruppenfehler	Abschalten der sicherheitsgerichteten Ausgänge.	Im Fehlerfall Reaktion nur in sicherer Richtung.
Kanalfehler	Abschalten des zugeordneten sicherheitsgerichteten Ausgangs.	Im Fehlerfall Reaktion nur in sicherer Richtung.
Leitungsbruch oder Leitungsschluss im Initiatorkreis bzw. weitere Fehler.	Abschalten des zugeordneten sicherheitsgerichteten Ausgangs.	Nach Fehlerbehebung Reset-Signal am Eingang des Bausteins HF-CNT-3 / 4 nötig.

Tabelle 18: Fehlerreaktion bei der sicherheitsgerichteten Zählerbaugruppe F 5220

5.5 Sicherheitsgerichtete analoge Eingangsbaugruppen F 6213, F 6214 und F 6217

Bei Redundanz von sicherheitsgerichteten analogen Eingangsbaugruppen wird bei funktionsfähigen Baugruppen der Mittelwert verarbeitet (*nur innerhalb zulässiger Abweichungen!*). Den Mittelwert erzeugt bei F 6213 und F 6214 der zugehörige Baustein, bei F 6217 das Anwenderprogramm. Im Fehlerfall wird nur der Wert der funktionsfähigen Baugruppe verarbeitet.

5.5.1 Testroutinen

Die Baugruppen schalten über den Test-DA-Wandler Testwerte auf und prüfen diese über den AD-Wandler, mit dem auch das Eingangssignal digitalisiert wird.

5.5.2 Reaktionen auf festgestellte Fehler bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6213, F 6214

Fehlerart	Systemreaktion im Fehlerfall	Bemerkung
Baugruppen- oder Kanalfehler bei einkanaligen analogen Eingängen	Verarbeitung des konfigurierten Wertes am Softwarebaustein HA-RTE-3 (s. Anhang).	Im Fehlerfall kann nur in sicherer Richtung reagiert werden.
Baugruppen- oder Kanalfehler bei redundanten analogen Eingangsbaugruppen und redundanten Transmittern	Im Fehlerfall einer Eingangsbaugruppe wird der Wert der redundanten Baugruppe oder der konfigurierte Fehlerwert verarbeitet.	Wahlweise Min-, Max- oder Mittelwertbildung über Softwarebaustein HA-RTE-3 (s. Anhang).
Kurzschluss im Transmitterkreis	Anzeige der Baugruppenposition und des fehlerhaften Kanals auf der Diagnoseanzeige	nur bei Einsatz 4...20 mA

Tabelle 19: Fehlerreaktion bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6213, F 6214

5.5.3 Reaktionen auf festgestellte Fehler bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6217

Fehlerart	Systemreaktion im Fehlerfall	Bemerkung
Kanalfehler	Analogwert = 0000 Kanalfehlerbit = TRUE	Kanalfehlerbit ist im Anwenderprogramm sicherheitsgerichtet zu verarbeiten
Baugruppenfehler	Alle Analogwerte = 0000 Alle Kanalfehlerbits = TRUE	siehe Kanalfehler, betrifft alle Kanalfehlerbits
Überschreiten des Messbereichs (22 mA)	max. Analogwert = 4095 Kanalfehlerbit = TRUE	max. zulässiger Wert ist im Anwenderprogramm zu definieren.

Tabelle 20: Fehlerreaktion bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6217

Die Baugruppe hat ein eigenes 1oo2-Mikroprozessorsystem, das sicherheitsgerichtete Online-Tests automatisch durchführt und die sicheren Daten für die sichere Verarbeitungseinheit bereitstellt. Für jeden Kanal existiert der Analogwert und ein zugehöriges Kanalfehlerbit.

WARNUNG



Warnung! Personenschaden durch fehlerhaften Messwert möglich!
Für jeden sicherheitsgerichteten Analogeingang ist eine sicherheitsgerichtete Reaktion bei gesetztem Kanalfehlerbit zu programmieren.

5.6 Sicherheitsgerichtete analoge eigensichere Thermoelement-Eingangsbaugruppe F 6220

Die Thermoelementbaugruppe hat acht Kanäle zum Anschluss von Thermoelementen verschiedener Typen (je nach Parametrierung an den Bausteinen HF-TMP-3) und einen Eingang zum Anschluss eines Widerstandsthermometers Pt 100 als Vergleichstemperatureingang. Sie hat ein eigenes Doppelprozessorsystem und wird über den Softwarebaustein HF-TMP-3 (siehe Kapitel 2.12 im Anhang und die Online-Hilfe ELOP II) für jeden belegten Kanal parametriert.

Die Eingänge sind auch zur Messung von niedrigen Spannungen verwendbar, siehe Datenblatt.

5.6.1 Testroutinen

Die Baugruppe hat ein eigenes 1oo2-Mikroprozessorsystem, das sicherheitsgerichtete Online-Tests automatisch durchführt und die sicheren Daten für die sichere Signalverarbeitung am Softwarebaustein HF-TMP-3 bereitstellt. Jeder der 8+1 Kanäle liefert sichere Eingangswerte und einen sicheren Fehlerstatus.

5.6.2 Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten Thermoelementbaugruppe F 6220

Zustand	Systemreaktion	Bemerkung
Baugruppenfehler	Ausgang <i>Kanalfehler</i> am Baustein HF-TMP-3 schaltet auf TRUE.	Reaktion ist im Anwenderprogramm unter Verwendung des Ausgangssignals <i>Kanalfehler</i> zu realisieren.
Kanalfehler	Ausgang <i>Kanalfehler</i> am Baustein HF-TMP-3 schaltet auf TRUE.	Reaktion ist im Anwenderprogramm zu realisieren.
Unterlauf	Ausgang <i>Unterlauf</i> am Baustein HF-TMP-3 schaltet auf TRUE.	Reaktion ist im Anwenderprogramm zu realisieren.
Überlauf	Ausgang <i>Überlauf</i> am Baustein HF-TMP-3 schaltet auf TRUE.	Reaktion ist im Anwenderprogramm zu realisieren.

Tabelle 21: Fehlerreaktion bei der sicherheitsgerichteten Thermoelementbaugruppe F 6220

Die Grenzwerte für Unterlauf bzw. Überlauf werden an den Eingängen *Unterlaufschwelle* bzw. *Überlaufschwelle* des Bausteins HF-TMP-3 festgelegt. Wenn der Messwert diese parametrisierten Schwellenwerte unter- bzw. überschreitet, wird das entsprechende Signal TRUE, ohne dass ein Fehler bei der Baugruppe vorliegt.

5.6.3 Projektierungshinweise

- Nicht benutzte Eingänge sind kurzzuschließen.
- Bei SIL 3 ist die Referenztemperatur aus dem Anwenderprogramm heranzuziehen oder als Vergleich der Referenztemperaturen zweier Baugruppen zu ermitteln.
- Es sind alle denkbaren Abweichungen zu betrachten und in der Auswertung der Messwerte zu berücksichtigen.
- Die Temperatur der Thermoelemente ist bei SIL 3 jeweils als Vergleich zweier Thermoelemente zu ermitteln.

5.7 Sicherheitsgerichtete analoge eigensichere Eingangsbaugruppe F 6221

Die analoge Eingangsbaugruppe hat acht Kanäle zum direkten Anschluss von analogen Transmittern aus dem (Ex)-Bereich. Die Transmitter-Speisespannung kann durch die Ausgangsbaugruppe F 3325 (oder einen anderen Geber entsprechend den Datenblattvorgaben) erfolgen. Diese Transmitter-Speisespannung ist zur Überwachung über die Baugruppe F 6221 anzuschließen.

Jeder belegte Kanal wird über einen eigenen Softwarebaustein HF-AIX-3 parametrisiert.

5.7.1 Testroutinen

Die Baugruppe hat ein eigenes 1oo2-Mikroprozessorsystem, das sicherheitsgerichtete Online-Tests automatisch durchführt und die sicheren Daten für die sichere Signalverarbeitung am Softwarebaustein HF-AIX-3 bereitstellt. Jeder der acht Kanäle liefert sichere Eingangswerte und einen sicheren Fehlerstatus.

5.7.2 Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten analogen Eingangsbaugruppe F 6221

Zustand	Systemreaktion	Bemerkung
Baugruppenfehler	Ausgang <i>Wert</i> (INT) am Baustein HF-AIX-3 führt Zahlenwert 0. Ausgang <i>Kanalfehler</i> am Baustein HF-AIX-3 schaltet auf TRUE.	Im Anwenderprogramm ist ein Fehlerwert unter Verwendung des Bausteineingangssignals <i>Wert im Fehlerfall</i> zu vereinbaren.
Kanalfehler	Ausgang <i>Kanalfehler</i> am Baustein HF-AIX-3 schaltet auf TRUE.	
Unterlauf	Ausgang <i>Unterlauf</i> am Baustein HF-AIX-3 schaltet auf TRUE.	
Überlauf	Ausgang <i>Überlauf</i> am Baustein HF-AIX-3 schaltet auf TRUE.	

Tabelle 22: Fehlerreaktion bei der sicherheitsgerichteten analogen Eingangsbaugruppe F 6221

Die Grenzwerte für Unterlauf bzw. Überlauf werden an den Eingängen *Unterlaufschwelle* bzw. *Überlaufschwelle* des Bausteins HF-AIX-3 festgelegt. Wenn der Messwert diese parametrisierten Schwellenwerte unter- bzw. überschreitet, wird das entsprechende Signal TRUE, ohne dass ein Fehler bei der Baugruppe vorliegt.

5.7.3 Weitere Projektierungshinweise

- Nicht benutzte Spannungseingänge 0...1 V sind auf der Klemmleiste kurzzuschließen.
- Nicht benutzte Stromeingänge sind durch den Shunt im Kabelstecker abgeschlossen.
- Nur die im Datenblatt der F 6221 aufgeführten Verwendungen sind zulässig.
- Die Ex-Schutzbestimmungen und Ex-Anschlussbedingungen sind einzuhalten.

5.8 Hinweis zum Wechseln von Eingangsbaugruppen

Im Fehlerfall oder im Wartungsfall sind beim Austausch folgende Arbeitsschritte einzuhalten:

1. Kabelstecker abschrauben oder Eingangsbaugruppe mit aufgestecktem Kabelstecker ziehen.
2. Neue Eingangsbaugruppe ohne Kabelstecker einstecken und verschrauben.
3. Kabelstecker aufstecken und verschrauben.
4. Quittungstaste (Taster ACK auf der Zentralbaugruppe) betätigen.

i

Betriebsunterbrechung möglich!
Ein Austausch von defekten Eingangsbaugruppen wird dringend empfohlen.

5.9 Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsgerichteten Eingangsbaugruppen

Für jede einzelne der in einem System eingesetzten sicherheitsgerichteten Eingangsbaugruppen ist im Rahmen der Projektierung bzw. Inbetriebnahme eine eigene Checkliste zur Kontrolle der zu berücksichtigenden Anforderungen auszufüllen. Nur dann kann sichergestellt werden, dass die Anforderungen vollständig und übersichtlich erfasst werden. Die Checklisten dienen gleichzeitig als Nachweisdokumente für eine sorgfältig durchgeführte Projektierung.

Die Checklisten dieses Sicherheitshandbuchs sind als MS Word-Dateien (*.doc) auf der HIMA DVD und im Internet unter www.hima.de erhältlich.

SDIGE-F3236	für sicherheitsgerichtete digitale Baugruppen
SDIGE-F3237	für sicherheitsgerichtete digitale Baugruppen
SDIGE-F3238	für sicherheitsgerichtete digitale Baugruppen
SDIGE-F3240	für sicherheitsgerichtete digitale Baugruppen
SDIGE-F3248	für sicherheitsgerichtete digitale Baugruppen
SDIGE-F5220	für sicherheitsgerichtete Zähler-Baugruppen
SANAE-F6213 / F6214	für sicherheitsgerichtete analoge Baugruppen
SANAE-F6217	für sicherheitsgerichtete analoge Baugruppen
SANAE-F6220	für sicherheitsgerichtete analoge Baugruppen
SANAE-F6221	für sicherheitsgerichtete analoge Baugruppen

6 Ausgangsbaugruppen

6.1 Gesamtübersicht der Ausgangsbaugruppen für die Systeme H41q, H41qc und H51q

Baugruppe	Bezeichnung	sicherheitsgerichtet	rückwirkungsfrei	Belastbarkeit	dazugehöriger SW-Baustein
Digitale Ausgangsbaugruppen					
F 3322	16fach digitale Ausgangsbaugruppe		•	≤ 0,5 A	
F 3325	6fach Speisegerät (Ex)		•	22 V ≤ 0,02 A	
F 3330	8fach digitale Ausgangsbaugruppe	•	•	≤ 0,5 A	
F 3331	8fach digitale Ausgangsbaugruppe	•	•	≤ 0,5 A	HB-BLD-3, HB-BLD-4 ¹⁾
F 3333	4fach digitale Ausgangsbaugruppe	•	•	≤ 2 A	
F 3334	4fach digitale Ausgangsbaugruppe	•	•	≤ 2 A	HB-BLD-3, HB-BLD-4 ¹⁾
F 3335	4fach digitale Ausgangsbaugruppe (Ex)	•	•	22 V ≤ 0,053 A	
F 3348	8fach digitale Ausgangsbaugruppe	•	•	≤ 0,5 A	
F 3349	8fach digitale Ausgangsbaugruppe	•	•	≤ 0,5 A ≤ 48 V	HB-BLD-3, HB-BLD-4 ¹⁾
F 3422	8fach Relaisbaugruppe		•	≤ 2 A, ≤ 60 V	
F 3430 ²⁾	4fach Relaisbaugruppe	•	•	≤ 4 A, ≤ 250 V	
Analoge Ausgangsbaugruppen					
F 6705	2fach D/A-Konverter	•	•	0...20 mA	HZ-FAN-3 ³⁾
F 6706	2fach D/A-Konverter		•	0...20 mA	

1) Zur Fehleranzeige und Parametrierung von anderen Betriebsarten (nicht Ruhestrom)

2) Die Baugruppe F 3430 ist nicht nach EN/ISO 13849-1 zertifiziert.

3) Notwendig im Stromsenkenbetrieb zur Fehlerauswertung

Tabelle 23: Ausgangsbaugruppen für die Systeme H41q, H41qc und H51q

6.2 Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsgerichteten Ausgangsbaugruppen

Die sicherheitsgerichteten Ausgangsbaugruppen werden in jedem Zyklus beschrieben, die Ausgangssignale zurückgelesen und mit den vom Anwenderprogramm berechneten Ausgangsdaten verglichen.

Zusätzlich wird innerhalb der Mehrfhereintrittszeit (MEZ) ein Walking-Bit-Test über alle Ausgänge durchgeführt, dabei steht das Testsignal für die Dauer von max. 200 µs an. Damit

wird die Schaltbarkeit der Ausgänge geprüft, ohne die Funktion der angeschlossenen Stellglieder zu beeinflussen. Es wird ein Einfrieren jedes Ausgangs erkannt, auch wenn das Ausgangssignal statisch ist.

Sicherheitsgerichtete Ausgangsbaugruppen mit Leitungsüberwachung können Fehler auf der Zuleitung zum Verbraucher feststellen. Die Leitungsüberwachung genügt den Sicherheitsanforderungen bis SIL 1. Dies hat nur Bedeutung, wenn die Leitungsüberwachung in sicherheitsgerichteten Stromkreisen verwendet wird. Das Ausgangssignal ist in allen Anwendungen für Sicherheitsanforderungen bis SIL 3 einsetzbar.

System H41q, H41qc	System H51q
Die Ausgangsbaugruppen werden in den Systembaugruppenträger gesteckt. Es stehen Bausätze mit 12 Steckplätzen (H41q) oder 13 Steckplätzen (H41qc) für E/A-Baugruppen zur Verfügung.	Die Ausgangsbaugruppen werden in eigens dafür vorgesehenen E/A-Baugruppenträgern (EABTs) mit jeweils maximal 16 Steckplätzen für E/A-Baugruppen gesteckt. Die erforderlichen Grundkomponenten für EABTs sind in Bausätzen zusammengefasst (siehe Kapitel 4 auf Seite 21).

Tabelle 24: Steckplätze für Ausgangsbaugruppen bei Systemen H41q, H41qc und H51q

6.2.1 Sicherheitsgerichtete digitale Ausgangsbaugruppen

Die Testroutinen stellen einen Fehler durch einen Vergleich der zurückgelesenen Ausgangssignale mit den internen Ausgangsdaten fest. Das Betriebssystem bringt eine Baugruppe auf einer als defekt erkannten Baugruppenposition in den sicheren Zustand und meldet dies auf der Diagnoseanzeige.

Bei Baugruppen mit Überwachung des Ausgangskreises wird ein erkannter Leitungsbruch durch Anzeigen des fehlerhaften Kanals der Baugruppe auf der Diagnoseanzeige signalisiert. Die defekte Ausgangsbaugruppe wird durch die integrierte Sicherheitsabschaltung sicher abgeschaltet.

Zusätzlich lassen sich mit Hilfe des Softwarebaustein H8-STA-3 eine oder mehrere Abschaltgruppen definieren. Der Defekt einer Ausgangsbaugruppe führt dann zum Absteuern aller zu einer Abschaltgruppe gehörenden Ausgangsbaugruppen.

Abhängig von den Sicherheitsanforderungen der Anlage kann über die E/A-Parameter bei den Einstellungen für die Ressourcen auch eine Gesamtabstaltung der Steuerung konfiguriert werden.

6.2.2 Sicherheitsgerichtete analoge Ausgangsbaugruppen

Die sicherheitsgerichteten analogen Ausgangsbaugruppen sind im *Stromquellenbetrieb* oder im *Stromsenkenbetrieb* einsetzbar.

Im *Stromquellenbetrieb* führt die integrierte Sicherheitsabschaltung im Fehlerfall zum sicheren Zustand (Ausgangsstrom 0 mA).

Im *Stromsenkenbetrieb* ist der sichere Zustand nur durch zusätzliche Maßnahmen erreichbar. Das Anwenderprogramm muss die Versorgungsspannung für die Stromschleife sicher abschalten. Zur Fehlerauswertung ist dazu der Softwarebaustein HZ-FAN-3 zu verwenden.

6.3 Prinzipielle Arbeitsweise von sicherheitsgerichteten Ausgangsbaugruppen

In den sicherheitsgerichteten Ausgangsbaugruppen sind drei testbare Halbleiter-Schalter in Serie geschaltet. Somit ist der sicherheitstechnisch erforderliche unabhängige, zweite Abschaltweg auf der Ausgangsbaugruppe integriert. Diese integrierte Sicherheitsabschaltung schaltet im Fehlerfall alle Kanäle der defekten Ausgangsbaugruppe sicher ab (energieloser Zustand).

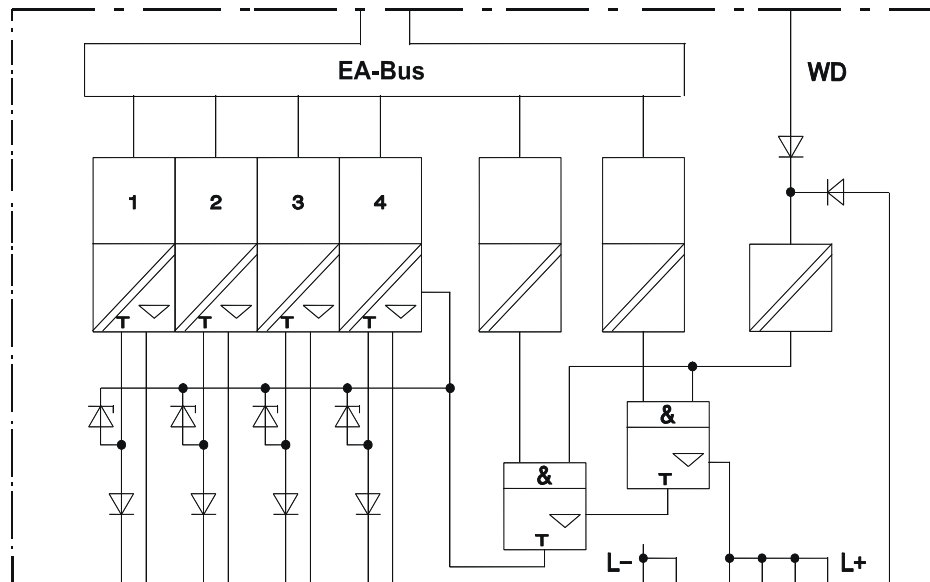


Abbildung 1: Prinzipschaltung der Ausgangsbaugruppen mit integrierter Sicherheitsabschaltung (hier mit 4 Ausgangskanälen)

6.4 Sicherheitsgerichtete digitale Ausgangsbaugruppen F 3330, F 3331, F 3333, F 3334, F3335, F 3348, F3349

6.4.1 Testroutinen

Die Baugruppen werden automatisch während des Betriebes getestet. Die wesentlichen Testfunktionen sind:

1. Rücklesen des Ausgangssignals des Schaltverstärkers. Die Schaltschwelle für einen rückgelesenen Low-Pegel ist $\leq 6,5$ V.
2. Lesen der Leitungsdiagnose der eingeschalteten Kanäle (nur bei F 3331, F 3334 und F 3349).
3. Aufschalten von Testmustern und Test auf Übersprechen (Walking-Bit-Test) im Rahmen der Mehrfahleintrittszeit.
4. Lesen der Leitungsdiagnose aller Kanäle (nur bei F 3331, F 3334 und F 3349).
5. Prüfen der integrierten Sicherheitsabschaltung.

6.4.2 Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Ausgangsbaugruppen

- Bei allen auf der Baugruppe erkannten Fehlern wird die Baugruppe in den sicheren, energielosen Zustand gebracht, d. h. die Baugruppe wird abgeschaltet.
- Bei externen Kurzschlüssen, die nicht von internen Fehlern unterscheidbar sind, wird die Baugruppe ebenfalls abgeschaltet.
- Leitungsfehler werden nur gemeldet und führen nicht zur Abschaltung.

6.5 Sicherheitsgerichtete digitale Relaisbaugruppe F 3430

6.5.1 Testroutinen

Die Baugruppe wird automatisch während des Betriebes getestet. Die wesentlichen Testfunktionen sind:

1. Rücklesen des Ausgangssignals des Schaltverstärkers für die diversitären 3fach Relais-Schalter.
2. Aufschalten von Testmustern und Test auf Übersprechen (Walking-Bit-Test) im Rahmen der Mehrfahleintrittszeit.
3. Prüfen der integrierten Sicherheitsabschaltung.

6.5.2 Reaktion auf festgestellte Fehler bei sicherheitsgerichteten digitalen Relaisbaugruppen

- Bei allen auf der Baugruppe erkannten Fehlern wird die Baugruppe in den sicheren, energielosen Zustand gebracht, d. h. die Baugruppe wird abgeschaltet.
- Bei externen Kurzschlüssen spricht die Sicherung für den relevanten Kanal an. Eine Fehlermeldung erfolgt nicht.

6.5.3 Hinweis zur Projektierung mit F 3430

Relais sind elektromechanische Bauelemente und haben konstruktionsbedingt eine begrenzte Lebensdauer. Die Lebensdauer der Relais richtet sich nach der Schaltleistung der Kontakte (Strom/Spannung) und der Anzahl der Schaltspiele.

Die Lebensdauer beträgt bei Nennbetriebsbedingungen 300.000 Schaltspiele bei 30 V DC und 4 A.

Zur Einhaltung der Anforderungen gemäß IEC 61508 (PFD/PFH, siehe Kapitel 3.2.1) gilt ein Offline-Proof-Test-Intervall von 5 Jahren bei SIL 3- und von 20 Jahren bei SIL 2-Anwendungen.

Die notwendigen Prüfungen werden beim Hersteller HIMA durchgeführt.

6.6 Sicherheitsgerichtete analoge Ausgangsbaugruppe F 6705

6.6.1 Testroutinen

Die Baugruppe wird automatisch während des Betriebes getestet. Die wesentlichen Testfunktionen sind:

1. Rücklesen des Ausgangssignals.
2. Test des DA-Wandlers auf Linearität.
3. Test auf Übersprechen zwischen den Ausgängen.
4. Prüfen der integrierten Sicherheitsabschaltung.

6.6.2 Reaktionen auf festgestellte Fehler bei der sicherheitsgerichteten analogen Ausgangsbaugruppe

Im Stromquellenbetrieb wird die Baugruppe bei allen auf der Baugruppe erkannten Fehlern in den sicheren, energielosen Zustand gebracht, d. h. die Baugruppe schaltet durch die integrierte Sicherheitsabschaltung ab.

Ein externer Leitungsbruch ist nicht von internen Fehlern unterscheidbar und führt zum Abschalten der Baugruppe.

Im Stromsenkenbetrieb ist der sichere, energielose Zustand nur durch ein externes

Abschalten erreichbar. Das Anwenderprogramm muss die Spannungsquelle für die Stromschleife sicher abschalten. Deshalb ist der Softwarebaustein HZ-FAN-3 zur Fehlerauswertung zu verwenden.

6.7 Hinweis zum Wechseln von Ausgangsbaugruppen

Im Fehlerfall oder im Wartungsfall sind beim Austausch folgende Arbeitsschritte einzuhalten:

Austausch einer Ausgangsbaugruppe:

1. Kabelstecker abschrauben oder Ausgangsbaugruppe mit aufgestecktem Kabelstecker ziehen.
2. Neue Ausgangsbaugruppe ohne Kabelstecker einstecken und verschrauben.
3. Kabelstecker aufstecken und verschrauben.
4. Quittungstaste (Taster ACK auf der Zentralbaugruppe) betätigen.

Die Ausgangsbaugruppe ist ausgetauscht.

i

Betriebsunterbrechung möglich!

Ein Austausch von defekten Ausgangsbaugruppen wird dringend empfohlen.

6.8 Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsgerichteten Ausgangsbaugruppen

Für jede einzelne der in einem System eingesetzten sicherheitsgerichteten Ausgangsbaugruppen ist im Rahmen der Projektierung bzw. Inbetriebnahme eine eigene Checkliste zur Kontrolle der zu berücksichtigenden Anforderungen auszufüllen. Nur dann kann sichergestellt werden, dass die Anforderungen vollständig und übersichtlich erfasst werden. Die Checklisten dienen gleichzeitig als Nachweisdokumente für eine sorgfältig durchgeführte Projektierung.

Die Checklisten dieses Sicherheitshandbuchs sind als MS Word-Dateien (*.doc) auf der HIMA DVD und im Internet unter www.hima.de erhältlich.

SDIGA-F3330	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3331	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3333	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3334	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3335	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3348	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3349	für sicherheitsgerichtete digitale Baugruppen
SDIGA-F3430	für sicherheitsgerichtete digitale Baugruppen
SANAA-F6705	für sicherheitsgerichtete analoge Baugruppen

7 Software

Die Software für sicherheitsgerichtete HIMA-Automatisierungsgeräte der Systemfamilien H41q, H41qc und H51q gliedert sich in die drei Blöcke:

- *Betriebssystem*,
- *Anwenderprogramm*
- *Programmierwerkzeug* nach IEC 61131-3 (ELOP II mit integriertem Sicherheitswerkzeug).

Das *Betriebssystem* ist in der jeweils gültigen, vom TÜV für sicherheitsgerichtete Anwendungen zertifizierten Form anzuwenden. Die jeweils gültige Version ist dem gemeinsamen Dokument *Versionsliste der Baugruppen und der Firmware des H41q/H51q Systems* zu entnehmen. Dieses Dokument wird von einem gemeinsamen Änderungsdienst der TÜV Rheinland Industrie Service GmbH und der Firma HIMA erstellt.

Das *Anwenderprogramm* wird mit dem Programmierwerkzeug ELOP II erstellt und enthält die anlagenspezifischen Funktionen, die das Automatisierungsgerät ausführen soll. Zur Parametrierung von Betriebssystemfunktionen dient ebenfalls ELOP II. Ein Codegenerator übersetzt das Anwenderprogramm in den Maschinencode. ELOP II überträgt diesen Maschinencode über eine serielle Schnittstelle oder Ethernet in die Flash-EPROMs in der Zentralbaugruppe des Automatisierungsgerätes.

Die wesentlichen Funktionen des Betriebssystems und die daraus abgeleiteten Vorgaben für das Anwenderprogramm sind im Betriebssystemhandbuch HI 800 104 D in der Tabelle *Funktionen des Betriebssystems* beschrieben.

7.1 Sicherheitstechnische Aspekte für das Betriebssystem

Dieses Kapitel beschreibt die Signatur und die prinzipielle Arbeitsweise des Betriebssystems.

7.1.1 Kennzeichnung, aktuelle freigegebene Version für sicherheitstechnische Anwendungen (CRC-Signatur)

Jedes neue Betriebssystem hat seine Bezeichnung mit Ausgabestand. Zur weiteren Kennzeichnung dient die Signatur des Betriebssystems, die im Betrieb des Automatisierungsgerätes auf der Diagnoseanzeige abgerufen werden kann.

Die jeweils gültigen, vom TÜV für sicherheitsgerichtete Automatisierungsgeräte zugelassenen Versionen des Betriebssystems und die dazugehörigen Signaturen (CRCs) sind der *Versionsliste der Baugruppen und der Firmware des H41q/H51q Systems* zu entnehmen.

7.1.2 Arbeitsweise und Funktionen des Betriebssystems

Das Betriebssystem arbeitet das Anwenderprogramm zyklisch ab. Die Reihenfolge ist in stark vereinfachter Form:

- Lesen der Eingangsdaten (Hardware-Eingänge)
- Bearbeiten der Logikfunktionen gemäß IEC 61131-3, Abschnitt 4.1.3
- Schreiben der Ausgangsdaten (Hardware-Ausgänge)

Hinzu kommen folgende wesentliche Funktionen:

- Umfangreiche Selbsttests
- Tests der E/A-Baugruppen während des Betriebs
- Datentransfer und Datenvergleich.

Ein Zyklus wird in sieben Phasen abgearbeitet. Diese Phasen sind detailliert im Betriebssystem-Handbuch HI 800 104 D beschrieben.

7.2 Sicherheitstechnische Aspekte des Anwenderprogramms

Allgemeiner Ablauf der Programmierung von Automatisierungsgeräten der Familien H41q/ H51q für sicherheitstechnische Anwendungen:

1. Spezifikation der Steuerungsfunktion
2. Schreiben des Anwenderprogramms
3. Verifizieren des Anwenderprogramms durch Offline-Simulation
4. Kompilieren des Anwenderprogramms mit dem C-Code-Generator
5. Der betriebsbewährte C-Compiler (GNU-CC) übersetzt den C-Code zweimal und erzeugt den Zielcode und den Vergleichscode.
6. Der Zielcode-Vergleicher vergleicht den Zielcode und den Vergleichscode. Fehler, die durch den nicht sicheren PC verursacht wurden, erkennt und meldet der Zielcode-Vergleicher.
7. Das so fehlerfrei erzeugte, ablauffähige Programm wird in das System H41q bzw. H51q geladen. Dort kann das Programm getestet werden
8. Nach dem erfolgreichen Abschluß der Tests nimmt das PES den sicheren Betrieb auf.

Begriffe

Laden	Unter diesem Begriff versteht man, dass ein Programm entweder mittels Download- oder mittels Reload in die Steuerung geladen wird.
Download	Beim Download eines Programms in die Steuerung werden alle Ausgänge der Steuerung zurückgesetzt und die Steuerung angehalten.
Reload	Beim Reload eines Anwenderprogramms in eine redundante Steuerung wird das geänderte Anwenderprogramm nacheinander in die Zentralbaugruppen geladen. Eine Zentralbaugruppe ist dabei immer im MONO-Betrieb. Es erfolgt keine Abschaltung. Bei einem PES mit nur einer Zentralbaugruppe werden die Ausgänge für die Dauer der Übertragung gehalten. Reload ist nur möglich, wenn reloadfähiger Code erzeugt wurde.

7.2.1 Vorgaben und Regeln für den Einsatz in sicherheitstechnischen Anwendungen (Auflagen aus Baumustergutachten etc.)

Das Anwenderprogramm wird mit dem Programmierwerkzeug ELOP II für Personalcomputer mit dem Betriebssystem Windows[®] eingegeben. Der PC muss zusätzlich mit einem Hardlock-Modul von HIMA ausgerüstet sein.

Das Programmierwerkzeug ELOP II enthält im wesentlichen:

- Eingabe (Funktionsbaustein-Editor), Überwachung und Dokumentation
- Variablen mit symbolischen Namen und Variablentyp (BOOL, UINT usw.)
- Zuordnung der Ressource (HIMA-Automatisierungssysteme H41q/H51q)
- Codegenerator (Übersetzen des Anwenderprogramms in den Maschinencode) mit C-Code-Generator und GNU-C Compiler.

7.2.1.1 Basis der Programmierung

Die Steuerungsaufgabe soll in Form einer Spezifikation oder eines Pflichtenheftes vorliegen. Diese Dokumentation ist die Basis der Überprüfung der korrekten Umsetzung in das Programm. Die Art der Darstellung der Spezifikation richtet sich nach der Aufgabenstellung. Dies kann sein:

- Kombinatorische Logik:
 - Ursache/Wirkungs-Schema
 - Logik der Verknüpfung mit Funktionen und Funktionsbausteinen
 - Funktionsblöcke mit spezifizierten Eigenschaften.
- Sequentielle Steuerungen (Ablauf-Steuerungen)
 - Verbale Beschreibung der Schritte mit Fortschaltbedingungen und zu steuernden

Aktoren

- Ablaufpläne nach DIN EN 60848
- Matrix- oder Tabellenform der Fortschaltbedingungen und der zu steuernden Aktoren
- Definition der Randbedingungen, z. B. Betriebsarten, NOTAUS usw.

Das Automatisierungskonzept der Anlage muss die Analyse der Feldkreise, d. h. die Art der Sensoren und Aktoren enthalten:

- Sensoren (digital oder analog)
 - Signal im Normalbetrieb (Ruhestromprinzip bei digitalen Sensoren, life-zero bei analogen Sensoren)
 - Signal im Fehlerfall
 - Festlegung von sicherheitstechnisch erforderlichen Redundanzen (1oo2, 2oo3)
 - Diskrepanzüberwachung und Reaktion.
- Aktoren
 - Stellung und Ansteuerung im Normalbetrieb
 - Sichere Reaktion/Stellung bei Abschaltung bzw. Energieausfall.

Ziele bei der Programmierung des Anwenderprogramms sollen sein:

- Leichte Verständlichkeit
- Nachvollziehbarkeit
- Änderungsfreundlichkeit.

7.2.2 Sicherheitstechnische Aspekte für die Programmierung mit ELOP II

Für die Erstellung der Applikationsprogramme wird das Programmierwerkzeug *ELOP II* verwendet.

Die Einsatzbedingungen, z. B. die unterstützte Windows-Version, sind der Dokumentation zur jeweiligen Version von ELOP II zu entnehmen.

Das Sicherheitskonzept von ELOP II gewährleistet Folgendes:

- Das Programmierwerkzeug arbeitet korrekt, d. h. Fehler des Programmierwerkzeugs werden entdeckt.
- Der Anwender setzt das Programmierwerkzeug korrekt ein, d. h. Anwenderfehler werden entdeckt.

Bei der ersten Inbetriebnahme einer sicherheitsgerichteten Steuerung wird die Sicherheit des gesamten Systems durch einen vollständigen Funktionstest geprüft. Nach einer Änderung des Anwenderprogramms musste bisher zur Gewährleistung der Sicherheit wieder ein vollständiger Funktionstest durchgeführt werden.

Das Sicherheitswerkzeug in ELOP II nach IEC 61131-3 ist so ausgelegt, dass nach einer Änderung des Anwenderprogramms nur die Änderungen zu überprüfen sind. Dieses Sicherheitswerkzeug dient zum Auffinden von Anwenderfehlern und Fehlern des Programmierwerkzeugs.

Das Sicherheitswerkzeug von ELOP II besteht aus drei, für die Sicherheit wichtigen Bausteinen:

- C-Code-Vergleicher
- Zielcode-Vergleicher
- betriebsbewährter GNU-C-Compiler.

Der C-Code-Vergleicher identifiziert Änderungen am Anwenderprogramm. Der Zielcode-Vergleicher vergleicht zwei durch den GNU-C-Compiler (GNU-CC) nacheinander erzeugte Zielcodes. Dadurch werden Fehler vermieden, die durch den nicht sicheren PC verursacht wurden.

Nicht sicherheitsgerichtete Hilfsmittel sind:

- Die in ELOP II integrierte Revisionsverwaltung. Diese kann zur eindeutigen Identifizierung der relevanten Projektversionen genutzt werden
- Die in dem Fluss-Diagramm Abbildung 2:dargestellte Offline-Simulation. Die Offline-Simulation verifiziert das Anwenderprogramm gegen die Spezifikation ohne Auswirkung auf den Prozess.

7.2.2.1 Anwendung des Sicherheitswerkzeugs von ELOP II bei der Programmerstellung

In Abbildung 2:sind Punkte zu finden, auf die im folgenden Text Bezug genommen wird.

1. Erstellung des Anwenderprogramms nach einer verbindlichen Spezifikation (z. B. nach IEC 61508, DIN V VDE 0801 oder entsprechender Anwendernorm), im Flussdiagramm Abbildung 2:die Punkte (1) bis (4).
2. Der C-Code-Generator kompiliert das Anwenderprogramm in den C-Code und erzeugt zusätzlich eine Vergleichsdatei, Punkt (5) im Flussdiagramm.

GEFAHR



Gefahr! Personenschaden durch Fehlfunktion möglich!

Für das Anwenderprogramm ist eine Cross-Referenzliste zu erzeugen und auf die korrekte Verwendung der Variablen zu überprüfen! Es ist zu überprüfen, dass alle Variablen nur dort verwendet werden, wo sie gemäß Spezifikation vorgesehen sind.

3. Der betriebsbewährte C-Compiler übersetzt den C-Code und die Vergleichsdatei, Punkt (6) und (13). Es wird der Zielcode und der Vergleichscode erzeugt.

GEFAHR



Gefahr! Personenschaden durch Fehlfunktion möglich!

Der Zielcode-Vergleicher muss aktiviert sein, Punkt (14). Er vergleicht den Zielcode und den Vergleichscode. Der Zielcode-Vergleicher erkennt und meldet durch den nicht sicheren PC verursachte Fehler.

4. Das so erzeugte, ablauffähige Programm in das System H41q/H51q laden (Punkt (7)). Dort ist das Programm vollständig zu testen und abzunehmen (Punkt (8)).
5. Ein Backup des Zielcodes erzeugen.
6. Das PES nimmt den sicheren Betrieb auf.

7.2.2.2 Anwendung des Sicherheitswerkzeugs von ELOP II bei der Programmänderung

1. Modifikation des Anwenderprogramms nach einer verbindlichen Spezifikation (z. B. nach IEC 61508, DIN V VDE 0801 oder entsprechender Anwendernorm), im Flussdiagramm die Punkte (1) bis (4).
Grundlage für die Änderung ist das Backup des laufenden Anwenderprogramms. Dieses Backup enthält:
 - VGL-Datei
 - Zielcode
 - Eingabedaten.
2. Der C-Code-Generator kompiliert das geänderte Anwenderprogramm in den C-Code (neu), Punkt (5).
3. Der C-Code-Vergleicher muss aktiviert sein, Punkt (12). Er vergleicht den C-Code (neu) mit dem C-Code (alt) der vorigen Programmversion, Punkt (11). Als Vergleichsdatei (C-Code (alt)) muss das Backup angegeben werden.
4. Das Ergebnis des Vergleichs, Punkt (15), wird dokumentiert
5. Überprüfen, ob der C-Code-Vergleicher die am Anwenderprogramm durchgeführten Änderungen anzeigt. Nur Code-relevante Änderungen werden angezeigt.
6. Ergebnis des C-Code-Vergleichers:

- a) meldet er Änderungen, die der Anwender nicht wiedererkennt, so kann dies folgende Gründe haben:
 - die vom Anwender durchgeführte Änderung hat weitergehende Änderungen zur Folge, die nicht vorhergesehen wurden
 - ein interner Fehler liegt vor.
- b) meldet er vom Anwender durchgeführte Änderungen nicht so kann dies liegen an:
 - Änderungen, die der C-Code-Vergleicher nicht erkennt, z. B. graphische Änderungen oder Änderungen von Initialwerten
 - Änderungen, die nicht korrekt übernommen wurden.
7. Der C-Compiler übersetzt den C-Code (neu) und die Vergleichsdatei (neu), Punkte (6) und (13). Er erzeugt den Zielcode und den Vergleichscode.
8. Der Zielcode-Vergleicher muss aktiviert sein, Punkt (14). Er vergleicht den Zielcode und den Vergleichscode. Fehler, die durch den nicht sicheren PC verursacht wurden, werden erkannt und gemeldet.
9. Das so erzeugte, ablauffähige Programm wird in das System H41q/H51q geladen. Dort sind alle Programmteile zu testen, die einer Änderung unterliegen. Der Test der Änderung prüft, ob der Zielcode korrekt ist.
10. Liegt keine Fehlfunktion vor, muss ein Backup des neuen, aktuellen Programms erzeugt werden. Das PES kann den sicheren Betrieb aufnehmen.

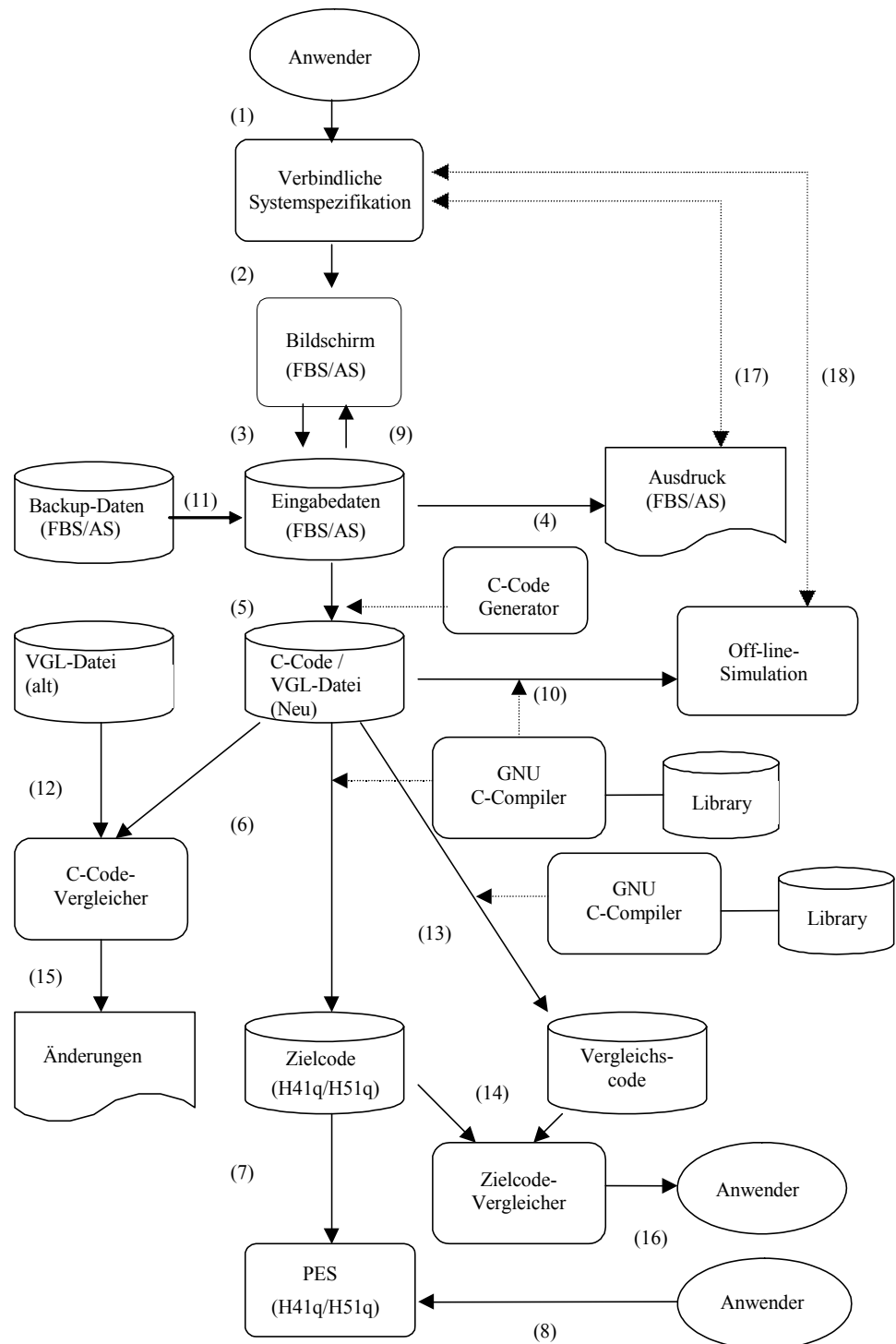


Abbildung 2: Flussdiagramm, Funktion des Sicherheitswerkzeugs

7.2.3 Verwendung von Variablen und PLT-Namen

Mit Hilfe des Variablen-Deklarations-Editors werden die Variablennamen und ihre Datentypen definiert. Allen Variablen des Anwenderprogramms werden symbolische Namen zugeordnet. Diese symbolischen Namen können aus maximal 256 Zeichen bestehen.

Für physikalische Ein- und Ausgänge werden symbolische PLT-Namen verwendet, diese können ebenfalls aus maximal 256 Zeichen bestehen.

Die Verwendung von symbolischen Namen anstelle der physikalischen Adresse hat für den Anwender zwei wesentliche Vorteile:

- Im Anwenderprogramm werden die Anlagenbezeichnungen von Ein- und Ausgängen verwendet.
- Änderungen der Zuordnung der Signale in den Ein- und Ausgangskanälen haben keinen Einfluss auf das Anwenderprogramm.

7.2.3.1 Zuordnung von PLT-Namen zu Variablennamen

Als Grundlage der Zuordnung von PLT-Namen zu Variablennamen sollte die Messstellenliste bzw. eine Liste der Sensoren und Aktoren dienen.

Die Zuordnung eines Variablennamens zur verwendeten Hardware erfolgt im Dialog für die Ressourcen unter *Schrank bearbeiten*. Dabei wird die gewünschte Baugruppenträgerposition (1-1 bis 1-8 bzw. 2-1 bis 2-8) und -typ, Steckplatz und -typ der benötigten Baugruppe sowie die den Variablennamen zuzuordnenden PLT-Namen eingetragen.

TIPP Variablenname und PLT-Name sollten praktischerweise gleich lauten.

Die Anzahl der Kanäle (Namen) pro Baugruppe ist abhängig vom verwendeten Typ der Baugruppe. Die erforderlichen Testroutinen für sicherheitsgerichtete E/A-Baugruppen werden vom Betriebssystem automatisch ausgeführt.

HIMA empfiehlt, die Ein- und Ausgangsbaugruppen in den E/A-Baugruppenträgern in funktionalen Gruppen zusammenzufassen.

Gesichtspunkte für die Gruppierung können sein:

- Gruppierung nach Anlagenteilen
gleichartige Anordnung der Baugruppen in den Gruppen, z. B.
 - digitale/analoge Anlagenteile
 - sicherheitsgerichtete/nicht sicherheitsgerichtete E/A-Baugruppen
- redundante Gruppierungen in den verschiedenen E/A-Baugruppenträgern in gleicher Reihenfolge
- Reservebaugruppen oder Reservekanäle für späteren Reload (Reloadbarer Code)

7.2.3.2 Arten von Variablen

Es können je nach Programmorganisationseinheit (POE) - Programm, Funktionsbaustein oder Funktion - verschiedene Variablenarten definiert werden. Eine Übersicht enthält nachstehende Tabelle:

Variablenart	Anwenderprogramm PROG	Funktionsbaustein FB	Funktion FUN	Verwendung
VAR	X (CONST ¹⁾ , RETAIN ²⁾)	X (CONST, RETAIN)	X (CONST)	lokale Variable
VAR_INPUT	-	X	X	Eingangs-Variable
VAR_OUTPUT	-	X (RETAIN)	X	Ausgangs-Variable
VAR_EXTERNAL	-	X (CONST)	-	extern von / an andere POE
VAR_GLOBAL	X (CONST, RETAIN)	-	-	global von anderer POE
VAR_ACTION	X	X	X	im Aktionsblock der Ablaufsprache

¹⁾ CONST: im Online-Test änderbare Konstante - ohne Neuübersetzung des Anwenderprogramms. Sie kann vom Anwenderprogramm nicht beschrieben werden.

²⁾ RETAIN: Variable mit Haftverhalten, d. h. der Wert geht nach einem Spannungsausfall und Wiederkehr der Spannung nicht verloren.

Tabelle 25: Arten von Variablen in ELOP II

Nicht initialisierte Variable sind nach einem Kaltstart auf den Wert Null oder FALSE gesetzt.

7.2.3.3 Digitale Ein- und Ausgänge für boolsche Variablen

Bei der Definition der Ressource wird unterschieden zwischen digitalen Ein- und Ausgängen und digitalen sicherheitsgerichteten Ein- und Ausgängen. Für sicherheitsgerichtete Funktionen dürfen nur sicherheitsgerichtete E/A-Baugruppen eingesetzt werden. Für die meisten sicherheitsgerichteten E/A-Baugruppen sind HIMA-Standardbausteine im Anwenderprogramm vorzusehen, siehe Anhang.

Die nicht sicherheitsgerichteten E/A-Baugruppen werden vom Betriebssystem nur gelesen bzw. beschrieben und keinen weiteren Testroutinen unterzogen. Ein Defekt wird daher vom Betriebssystem nicht erkannt, und es erfolgt keine Fehlermeldung. HIMA empfiehlt daher, wegen der erweiterten Diagnose nur sicherheitsgerichtete E/A-Baugruppen einzusetzen.

7.2.3.4 Analoge E/A-Baugruppen

Analoge Eingabegruppen wandeln die Analogwerte (Spannungen, Ströme) in Digitalwerte mit 12-Bit-Auflösung.

Analoge Ausgangsbaugruppen wandeln 12-Bit-Digitalwerte in Ströme 0...20 mA oder 4...20 mA.

Für die meisten analogen sicherheitsgerichteten und nicht sicherheitsgerichteten E/A-Baugruppen sind HIMA-Bausteine im Anwenderprogramm zu verwenden, siehe Anhang.

7.2.3.5 Importierte oder exportierte Variablen

Die Daten der zu importierenden oder exportierenden Variablen werden über die Schnittstellen entweder zur HIMA-Kommunikation über HIPRO (PES-Master) oder zu Fremdsystemen übertragen. Verfügbare Protokolle für Fremdsysteme sind Modbus, Modbus TCP, PROFIBUS-DP und 3964R. Die Daten können auch über ein Ethernet-Protokoll zu einem OPC-Server übertragen werden. Die Variablen für Import und Export werden im Anwenderprogramm wie normale Ein- und Ausgangsvariable verarbeitet. Sie werden in der Variablendeklaration der Programminstanz definiert.

Es ist möglich, boolesche Variablen mit dem Attribut Ereignis zu versehen. Ereignisse sind Signalwechsel von booleschen Variablen mit zusätzlicher Information über den Zeitpunkt (Datum und Uhrzeit). Der Zeitstempel eines Ereignisses entspricht millisekundengenau der Uhrzeit des Automatisierungsgeräts.

7.2.4 Signaturen des Anwenderprogramms

Unbeabsichtigte oder unautorisierte Veränderungen am Anwenderprogramm können durch mehrere CRC-Signaturen erkannt werden. Diese Signaturen heißen Versionsnummern. In ELOP II gibt es folgende Versionsnummern:

- Codeversionsnummer
- Runversionsnummer
- Datenversionsnummer
- Bereichsversionsnummer

7.2.4.1 Codeversionsnummer

Die Codeversionsnummer wird über die Funktionen der programmierten Logik gebildet. Nur wenn die Codeversion des Programms in der Steuerung und im Programmierwerkzeug übereinstimmen, kann über den PC die Funktion der Steuerung beobachtet werden.

Keinen Einfluss auf die Codeversionsnummer haben:

- Schreiben oder Löschen von Kommentaren
- Setzen oder Löschen von Online-Test-Feldern (OLT-Felder), d. h. von Force-Informationen
- Verschieben von Linien bzw. Bausteinen, wenn sich die Reihenfolge der Abarbeitung nicht ändert
- Änderungen der SIO-Parameter selbst, nicht aber Aktivieren/Deaktivieren der SIO-Parameter
- Bus-Parameter.

Änderungen der Basisadressen für Fremd-/Modbus-Kopplung können zu einer Änderung der Codeversionsnummer führen. Bei allen anderen Änderungen ändert sich auch die Codeversionsnummer.

7.2.4.2 Runversionsnummer

Die Steuerung bildet die Runversionsnummer während des Betriebs. Durch den Vergleich mit einer bisher gültigen und dokumentierten Runversionsnummer ist erkennbar, ob das Programm innerhalb der Steuerung zwischenzeitlich beeinflusst wurde (sichtbar durch Aufruf auf der Diagnoseanzeige).

Die Runversionsnummer wird geändert bei:

- anderer Codeversionsnummer (nicht bei allen Arten von Änderungen)
- Einfügen oder Löschen von Baugruppen
- anderen Systemparametern
- Einfügen oder Löschen von VAR_CONST
- Änderung von VAR_CONST-Werten
- Änderung des Ressourcetyps
- Online-Änderung von Einstellungen
- Forcen von E/A-Variablen im Online-Testfeld
- Änderung der Stellung des Force-Hauptschalters

7.2.4.3 Datenversionsnummer

Die Datenversionsnummer bezieht sich auf die Definition von nicht sicherheitsgerichteten importierten oder exportierten Variablen und ändert sich in folgenden Fällen:

- Wenn sich der Name einer Variable mit den Attributen für HIPRO-N (nicht sicherheitsgerichtet) ändert.
- Wenn solche Variablen bei der Erzeugung von nicht reloadbaren Code komprimiert werden (falls Speicherplatzlücken vorhanden sind).

7.2.4.4 Bereichsversionsnummer

Die Bereichsversionsnummer erfasst alle innerhalb eines Projekts definierten Variablen und ändert sich in folgenden Fällen:

- Löschen oder Hinzufügen von Baugruppen im Schrank.
- Wenn die Erzeugung reloadbaren Codes eingestellt ist und den Attributen folgenden Typs mehr Variable zugeordnet als gelöscht werden:
HIPRO-N, HIPRO-S, BUSCOM, Ereignis, 3964R.
- Wenn die Erzeugung nicht reloadbaren Codes eingestellt ist und den Attributen folgenden Typs zugeordnete Variable hinzugefügt oder gelöscht werden:
HIPRO-N, HIPRO-S, BUSCOM, Ereignis, 3964R.
- Wenn eine Neuorganisation des Speichers erforderlich ist, da die Speichergrenze erreicht ist.

Änderungen der Basisadressen für Fremd-/Modbus-Kopplung können zu einer Änderung der Bereichsversionsnummer führen.

7.2.5 Verwendung von Standardfunktionsbausteinen für sicherheitstechnische Anwendungen

In der nachfolgenden Liste sind die HIMA-Standardfunktionsbausteine für sicherheitstechnische Anwendungen aufgeführt. Die Funktionsbeschreibungen der Bausteine sind auf der Webseite www.hima.de und auf der HIMA-DVD verfügbar.

7.2.5.1 Standardfunktionsbausteine unabhängig von der E/A-Ebene

Typ	Funktion	TÜV-Prüfung ¹⁾	
		sicherheitsgerichtet	rückwirkungsfrei
H8-UHR-3	Datum und Uhrzeit		•
HK-AGM-3	PES-Master-Überwachung		•
HK-COM-3	Kommunikationsbaugruppenüberwachung		•
HK-LGP-3	LGP Auswertung und Konfigurieren		•
HK-MMT-3	Modbus-Master		•
HA-LIN-3	Temperaturlinearisierung	•	•
HA-PID-3	PID-Regler	•	•
HA-PMU-3	parametrierbarer Messumformer	•	•

Tabelle 26: Standardfunktionsbausteine unabhängig von der E/A-Ebene

¹⁾ In der Spalte *TÜV-Prüfung* bedeutet „•“, dass für den betreffenden Baustein ein Sicherheitsnachweis des TÜV vorliegt. Für die sicherheitstechnische Anwendung der Bausteine wird auf die Dokumentation der Bausteine verwiesen.

7.2.5.2 Standardfunktionsbausteine abhängig von der E/A-Ebene

Typ	Funktion	TÜV-Prüfung ¹⁾	
		sicherheitsgerichtet	rückwirkungs-frei
H8-STA-3	Gruppenbildung sicherheitsgerichteter, testbarer Ausgänge	•	•
HA-RTE-3	Überwachung analoger testbarer Eingangsbaugruppen F 6213 / F 6214	•	•
HB-BLD-3	Baugruppen- und Leitungsdiagnose testbarer Ausgänge	•	•
HB-BLD-4	Baugruppen- und Leitungsdiagnose testbarer Ausgänge	•	•
HB-RTE-3	Überwachung binärer, testbarer Eingangsbaugruppen	•	•
HF-AIX-3	Überwachung analoger testbarer Eingangsbaugruppen F 6221	•	•
HF-CNT-3	Zählerbaustein für Baugruppe F 5220	•	•
HF-CNT-4	Zählerbaustein für Baugruppe F 5220	•	•
HF-TMP-3	Konfigurierbaustein für F 6220	•	•
HZ-FAN-3	Fehleranzeige für testbare E/A-Baugruppen		•
HZ-DOS-3	Diagnose ohne Sicherheit		•

¹⁾ In der Spalte *TÜV-Prüfung* bedeutet „•“, dass für den betreffenden Baustein ein Sicherheitsnachweis des TÜV vorliegt. Für die sicherheitstechnische Anwendung der Bausteine wird auf die Dokumentation der Bausteine verwiesen.

Tabelle 27: Standardfunktionsbausteine abhängig von der E/A-Ebene

Die folgenden Bausteine dürfen in sicherheitstechnischen Anwendungen eingesetzt werden, jedoch nicht für sicherheitsgerichtete Aktionen:

- H8-UHR-3
- HK-AGM-3
- HK-LGP-3
- HK-MMT-3
- HZ-FAN-3
- HZ-DOS-3

Weitere Hinweise sind auf der Webseite www.hima.de und der HIMA-DVD zu erhalten.

7.2.6 Parametrierung des Automatisierungsgeräts

Die nachfolgend angeführten Parameter legen das Verhalten des Automatisierungsgeräts während des Betriebs fest und werden im Menü Eigenschaften der Ressource eingestellt.

7.2.6.1 Sicherheitsparameter

In den Eigenschaften der Ressource sind die Sicherheitsparameter einstellbar:

- die Parameter für den sicherheitsgerichteten Betrieb des Automatisierungsgeräts
- Die Aktionen, die mit dem Programmiergerät im sicherheitsgerichteten Betrieb zulässig sind

Sicherheitsgerichtete Parameter	empfohlene Einstellung
Parameter Online änderbar	rücksetzen, abhängig vom Projekt
Sicherheitsparameter	
Sicherheitszeit in s	prozessabhängig
Watchdog-Zeit in ms	maximal die halbe Sicherheitszeit
Anforderungsklasse	6, entspricht SIL 3, abhängig vom Projekt
Werte änderbar	
Konstanten	rücksetzen
Variablen	rücksetzen
E/A Forcen	rücksetzen
Erlaubte Aktionen	
Testbetrieb	rücksetzen
Start	rücksetzen
Reload	abhängig vom Projekt

Tabelle 28: Sicherheitsgerichtete Parameter

i

Bei Ausgaben des Betriebssystems vor (07.14) ist der Wert 255 s für die Sicherheitszeit nicht erlaubt!
Nur der Wertebereich 1 bis 254 s ist zulässig!

i

Die während des sicherheitsgerichteten Betriebs möglichen Belegungen sind nicht starr an eine bestimmte Sicherheitsanforderung (SIL) gebunden, sondern müssen für jeden Einsatz des Automatisierungsgeräts mit der zuständigen Prüfstelle abgestimmt werden.

7.2.6.2 Verhalten bei Fehlern in sicherheitsgerichteten Ausgangskanälen

Die folgende Tabelle zeigt die Einstellmöglichkeiten des Parameters *Verhalten bei Ausgabefehler* in den **Eigenschaften** einer Ausgangsbaugruppe.

Einstellung	Beschreibung
Nur Anzeige	Abschaltung über integrierte Sicherheitsabschaltung des Ausgangsverstärkers. Falls nicht möglich, Abschaltung des Watchdog-Signals im E/A-Baugruppenträger durch Verbindungsbaugruppe (nur Systeme H51q). Keine Abschaltung des Watchdog-Signals der zugehörigen Zentralbaugruppe (kein Fehlerstopp). Anwenderprogramm und Kommunikation laufen weiter. Nur bis SIL 1 zulässig!
Notaus	Abschaltung des Watchdogsignals der zugehörigen Zentralbaugruppe und damit Abschaltung der Ausgangsverstärker (Fehlerstopp). Anwenderprogramm und Kommunikation laufen nicht weiter.
Normaler Betrieb	Reaktion wie bei Parameter <i>Nur Anzeige</i> , zusätzlich Abschaltung der zugehörigen Gruppe, wenn - mit Hilfe des Bausteins H8-STA-3, Kapitel 2.1 im Anhang - eine Gruppe konfiguriert ist. Abschaltung des Watchdog-Signals der zugehörigen Zentralbaugruppe (Fehlerstopp), falls keine Gruppe konfiguriert oder das Gruppenrelais defekt ist. In diesem Fall laufen Anwenderprogramm und Kommunikation nicht weiter. Erforderlich ab SIL 2. Übliche und empfohlene Einstellung.

Tabelle 29: Einstellung des Parameters *Verhalten bei Ausgabefehlern*

Die Kommunikation mit dem PADT bei Auftreten eines Fehlers ist unabhängig von der Einstellung von *Verhalten bei Ausgabefehler* möglich.

7.2.7 Identifizierung des Programms

Das Anwenderprogramm ist an Hand der Codeversionsnummer eindeutig identifizierbar. Das dazu gehörige Backup (Archiv-Version) ist so eindeutig bestimmbar.

Besteht eine Unsicherheit, welches Backup korrekt ist, so kompiliert man das fragliche Backup mit Download-Option und vergleicht anschließend den Zielcode mit der Codeversion des geladenen Programms.

Bei reloadbarem Code ist dies nur dann möglich, wenn das Backup auf die folgende Weise erzeugt wurde:

1. Letzte Änderung durchführen
2. Reloadbaren Code generieren (kompilieren), ergibt Codeversion A
3. Steuerung mit der Codeversion A laden
4. Reloadbaren Code generieren, ergibt Codeversion B, kann identisch sein mit A
5. Steuerung mit Codeversion B laden
6. Bei jeder weiteren Codegenerierung ohne Änderung ergibt sich Codeversion B.

7.2.8 Überprüfung des erstellten Applikationsprogramms auf Einhaltung der spezifischen Sicherheitsfunktion

Für die Überprüfung ist einen geeigneter Satz Testfälle zu erzeugen, der die Spezifikation abdeckt. Dabei ist es nicht notwendig, bei einem 20-fach UND-Gatter 2^{20} Testsätze durchzuführen. In der Regel dürften der unabhängige Test jedes Eingangs und der aus Anwendungssicht wichtigen Verknüpfungen ausreichend sein. Dieser Testsatz ist ausreichend, da ELOP II und die in diesem Sicherheitshandbuch definierten Maßnahmen es hinreichend unwahrscheinlich machen, dass semantisch und syntaktisch korrekter Code erzeugt wird, der noch unerkannte systematische Fehler aus dem Prozess der Codeerzeugung enthält.

Auch bei der numerischen Auswertung von Formeln ist ein geeigneter Testsatz zu

generieren. Sinnvoll sind z. B. Äquivalenzklassentests, d. h. Tests innerhalb der definierten Wertebereiche, an den Grenzen und in unzulässigen Wertebereichen. Die Testfälle sind so zu wählen, dass die Korrektheit der Berechnung nachgewiesen wird. Die notwendige Anzahl der Testfälle hängt von der verwendeten Formel ab und muss kritische Wertepaarungen umfassen.

Der Online-Test kann hierbei unterstützend verwendet werden, um z. B. Werte vorzugeben und Zwischenwerte abzulesen. Eine aktive Simulation mit Quellen ist aber erforderlich, da nur so eine korrekte Verdrahtung der Sensoren und Aktoren nachzuweisen ist. Außerdem ist nur so die Systemkonfiguration überprüfbar.

7.3 **Checkliste: Maßnahmen zur Erstellung eines Anwenderprogramms**

Die Checkliste ist als Word-Datei MEAP-0001-D.doc auf der HIMA-DVD und im Internet unter www.hima.de erhältlich.

7.4 **Reload (Reloadbarer Code)**

i

Reload ist nur nach Rücksprache mit der für die Anlagenabnahme zuständigen Prüfstelle zulässig. Während des gesamten Reload muss der für den Reload Verantwortliche die sicherheitstechnische ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen sicherstellen.

⚠️ WARNUNG



Warnung! Personenschaden durch Fehlfunktion möglich!

- Vor jedem Reload sind die Änderungen im Anwenderprogramm gegenüber dem noch laufenden Anwenderprogramm mit Hilfe des C-Code-Vergleichers im Sicherheitswerkzeug von ELOP II zu ermitteln.
- Die Änderungen des Reload sind vor der Übertragung in das PES sorgfältig an Simulatoren zu testen.

Ist ein Reload des Anwenderprogramms in der (den) Zentralbaugruppe(n) möglich, wird das durch die Meldung *Code reloadbar* während des Übersetzungslaufs des Codegenerators angezeigt.

Bei folgenden Änderungen am Anwenderprogramm geht die Reloadfähigkeit verloren:

- Im Schrank werden Baugruppen gelöscht oder neue Baugruppen hinzugefügt.
- Den Attributen folgenden Typs werden mehr Variable zugeordnet als gelöscht: HIPRO-N, HIPRO-S, BUSCOM, Ereignis, 3964R
- Die Basisadressen für BUSCOM werden geändert, siehe Kapitel 7.2.4.4.
- Zuordnungen zu Systemvariable werden hinzugefügt oder geändert. Dies gilt nicht für alle Systemvariable (Einzelheiten siehe *Funktionen des Betriebssystems HI 800 104 D*).
- Namen von HIPRO-S-Variablen werden geändert.

7.4.1 **Systeme mit einer Zentralbaugruppe**

Während der Ladezeit des Anwenderprogramms findet kein Zugriff auf die E/A-Ebene statt, d. h. es werden keine E/A-Baugruppen gelesen, beschrieben oder getestet.

Während des Ladens des Anwenderprogramms bearbeitet dieses die Schnittstellen der Steuerung nicht, und es findet kein Durchreichen von importierten oder exportierten

Variablen über die Schnittstellen statt.

i

Betriebsunterbrechung möglich!

Wird bei Systemen mit einer Zentralbaugruppe ein Reload durchgeführt, so muss dieser innerhalb der Fehlertoleranzzeit des Prozesses abgeschlossen sein.

7.4.2 Systeme mit redundanten Zentralbaugruppen

Bei diesen Systemen ist ein Reload ohne die oben genannten Einschränkungen für einkanalige Systeme möglich.

Ablauf des Reload:

1. Beim Laden der ersten Zentralbaugruppe setzt die zweite Zentralbaugruppe die Bearbeitung des Anwenderprogramms im Mono-Betrieb fort.
2. Danach erhält die neu geladene Zentralbaugruppe die aktuellen Daten von der noch in Betrieb befindlichen Zentralbaugruppe und übernimmt den Mono-Betrieb mit dem neuen Anwenderprogramm.
3. Nach dem Laden der zweiten Zentralbaugruppe erhält diese die aktuellen Daten von der ersten und beide Zentralbaugruppen gehen in den redundanten Betrieb über.

7.4.3 Einschränkungen beim Reload

Die folgenden Punkte sind beim Reload zu beachten:

- Wird bei einem Reload ein Logikteil gelöscht, z. B. eine Funktion mit Ansteuerung eines physikalischen Ausgangs, so wird das Prozessabbild nicht geändert. Deshalb müssen alle von diesem Reload betroffenen Ausgänge gelöscht werden, d. h. die vom Reload betroffenen Ausgänge müssen vor dem Reload abgesteuert sein.
- Wird bei einem Reload die Eingangsvariable (VAR_INPUT) eines Funktionsbausteins nicht mehr beschrieben (z. B., weil die Variable oder Zuweisung vor dem Funktionsbaustein gelöscht wurde), so behält die Eingangsvariable ihren letzten Wert und wird nicht automatisch auf FALSE / 0 zurückgesetzt!
Dieses Verhalten betrifft alle Funktionsbausteine, nicht jedoch Funktionen.
Die Ursache für dieses Verhalten besteht darin, dass beim Reload die Werte aller Variablen gespeichert bleiben, um ein Weiterarbeiten möglich zu machen. Eingänge von Standard- wie von anwenderspezifischen Funktionsbausteinen werden intern als Variable verarbeitet.
Abhilfe: ein solcher Eingang muss mit einer neuen Variablen verbunden werden, die auf den gewünschten Wert gesetzt ist.
- Alle Variablen mit dem Attribut *const* nehmen nach einem Reload wieder ihren Initialwert an, auch wenn sie online auf einen anderen Wert gesetzt wurden.
- Alle Systemparameter nehmen beim Reload wieder ihren konfigurierten Wert an, auch wenn sie online auf einen anderen Wert gesetzt wurden. Dies hat Auswirkungen auf Watchdog-Zeit, Sicherheitszeit, Baudrate der Schnittstellen und vieles mehr.
- Wird in einem Anwenderprogramm mit einer Schrittkette der aktive Schritt gelöscht und anschließend ein Reload durchgeführt, dann geht die Fortschaltbedingung für den nächsten Schritt verloren. Das bedeutet, dass die Schrittkette nicht mehr ausgeführt werden kann.
- Wird bei der Übersetzung eines Programms der CRC 0 erzeugt, so darf das Programm nicht in die Steuerung geladen werden!
Abhilfe: das Programm muss geändert und neu übersetzt werden, so dass ein CRC entsteht, der nicht 0 ist. Die Änderungen dürfen die Funktion des Programms nicht verändern. Deshalb sollten nur Objekte grafisch vertauscht werden, die nicht voneinander abhängig sind, z. B. Eingänge eines UND-Bausteins.

7.5 Offline-Test

Änderungen im Anwendungsprogramm können mit dem Offline-Test in ELOP II simuliert werden. Diese Simulation ist ein gutes Hilfsmittel, um die Auswirkung einer Änderung zu beurteilen. Sie reicht nicht aus, um in den sicherheitsgerichteten Steuerungen die durchgeführten Änderungen zu validieren. Dazu ist ein Test an der tatsächlichen Steuerung oder einem Simulator erforderlich.

7.6 Forcen

Forcen ist nur nach Rücksprache mit der für die Anlagenabnahme zuständigen Prüfstelle zulässig. Während des Forcens muss der Verantwortliche die sicherheitstechnische ausreichende Überwachung des Prozesses durch andere technische und organisatorische Maßnahmen sicherstellen.

i

Beim Forcen in sicherheitsgerichteten Steuerungen ist die jeweils aktuelle Version des Dokuments *Wartungseingriffe, Maintenance Override* des TÜV Rheinland Industrie Service zu beachten. Das Dokument kann im Internet von der Seite www.tuvasi.com heruntergeladen werden.

Möglichkeiten beim Forcen:

- Forcen kann per Konfiguration verboten werden. Das PES nimmt dann keine Force-Werte, die anwenderspezifisch definiert werden, mehr an. In diesem Fall können neue Force-Werte erst wieder nach dem Abschalten des Systems gesetzt werden.
- Wenn der Anwender das Control-Panel verlässt, wird angezeigt, ob und wieviele Force-Werte noch gesetzt sind.
- Alle geforceden Ein- oder Ausgänge können durch zwei getrennte Force-Hauptschalter wieder zurückgesetzt werden

Weitere Details zur Prozedur des Forcens sind dem Betriebssystem-Handbuch HI 800 104 D und der Online-Hilfe von ELOP II zu entnehmen.

GEFAHR



Gefahr! Personenschaden durch Fehlfunktion möglich!

Vor der Aufnahme des sicherheitsgerichteten Betriebs sind alle Force-Marker aus dem Anwenderprogramm zu entfernen.

Einzelheiten zu Force-Markern sind in der Online-Hilfe von ELOP II beschrieben.

7.7 Schutz vor Manipulationen

Im PES und im Programmierwerkzeug ELOP II sind Schutzmechanismen integriert, die versehentliche oder unautorisierte Veränderungen am Sicherheitssystem verhindern.

1. Im PES können die Systemparameter so eingestellt werden, dass eine Programmänderung ohne Neuladen nicht möglich ist.
2. Das Programmierwerkzeug ELOP II hat einen Hardlock und kann zusätzlich durch die Passwortmechanismen von Windows® vor unberechtigtem Zugriff geschützt werden.

i

Die Anforderungen der Sicherheits- und Anwendungsnormen bezüglich des Schutzes vor Manipulationen sind zu beachten. Die Autorisierung von Mitarbeitern und die notwendigen Schutzmaßnahmen unterliegen der Verantwortung des Betreibers.

Der Betreiber muss zusammen mit der zuständigen Prüfstelle definieren, welche Maßnahmen zum Schutz vor Manipulation angewendet werden.

7.8 Funktionen des Anwenderprogramms

Die Programmierung unterliegt keiner Einschränkung durch die Hardware. Die Funktionen des Anwenderprogramms sind frei programmierbar. Bei der Programmierung ist zu beachten, dass das Ruhestromprinzip bei den Ein- und Ausgängen berücksichtigt wird. Ein Drahtbruch führt z. B. zur Abschaltung des betreffenden Aktors.

- Drahtbrüche sind innerhalb des Anwenderprogramms bei speicherprogrammierbaren Steuerungen im Gegensatz zu festverdrahteten Sicherheitssteuerungen nicht zu berücksichtigen.
- Es sind beliebige Negierungen zulässig.
- Aktive Signale zur Auslösung einer Aktion (z. B. Schiebetaktimpuls für ein Schieberegister) können für sicherheitstechnische Anwendungen genutzt werden.

Bei analogen, sicherheitsgerichteten Eingangsbaugruppen wird im Fehlerfall ein definierter Wert weiter verarbeitet. Nähere Angaben hierzu sind der Beschreibung der Softwarebausteine im Handbuch *ELOP II Ressourcety* zu entnehmen.

In einer digitalen, sicherheitsgerichteten E/A-Baugruppe wird im Fehlerfall der Eingang auf einen sicheren Wert 0 gesetzt, und die digitale Ausgangsbaugruppe wird durch die integrierte Sicherheitsabschaltung abgeschaltet. Nähere Angaben hierzu sind der Beschreibung der Softwarebausteine im Anhang zu entnehmen.

Gegenüber festverdrahteten Steuerungen ist in speicherprogrammierbaren Steuerungen ein erweiterter Funktionsumfang vorhanden, insbesondere Byte- und Wortverarbeitung.

7.8.1 Gruppenabschaltung

Die für einen bestimmten Anlagenbereich eingesetzten sicherheitsgerichteten Ausgangsbaugruppen (z. B. für einen Brenner) können in einer Gruppe zusammengefasst werden. Hierzu ist pro Gruppe der Softwarebaustein H8-STA-3 ins Anwenderprogramm einzufügen. Am Softwarebaustein sind alle Positionen der zu einer Gruppe gehörenden Ausgangsbaugruppen einzustellen. Im Fehlerfall einer Ausgangsbaugruppe werden alle zu dieser Gruppe gehörenden Ausgangsbaugruppen abgeschaltet. Zur Sicherheit des Systems genügt jedoch allein die integrierte Sicherheitsabschaltung der Ausgangsbaugruppen.

7.8.2 Softwarebausteine für einzelne sicherheitsgerichtete E/A-Baugruppen

Eingangsbaugruppe		Ausgangsbaugruppe	
digital		digital	
Tabelle 30: Zuordnung von Softwarebausteinen zu E/A-Baugruppen			
Typ	Softwarebaustein	Typ	Softwarebaustein
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
analog		analog	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		
F 6221	HF-AIX-3		

Für die sicherheitsgerichteten E/A-Baugruppen sind die zugehörigen Softwarebausteine in das Anwenderprogramm einzufügen. Nähere Angaben siehe Anhang bzw. Beschreibung der Softwarebausteine in der ELOP II Online-Hilfe.

7.8.3 Redundante E/A-Baugruppen

Zur Erhöhung der Verfügbarkeit ohne Einschränkung der Sicherheit können sicherheitsgerichtete Ein- oder Ausgangsbaugruppen parallel geschaltet werden, wie es in der nachfolgenden Skizze dargestellt ist. Höchste Verfügbarkeit wird erreicht, wenn in diesem Fall auch Automatisierungsgeräte mit zwei E/A-Bussen eingesetzt und die redundanten E/A-Signale auch auf getrennte E/A-Baugruppen geführt werden.

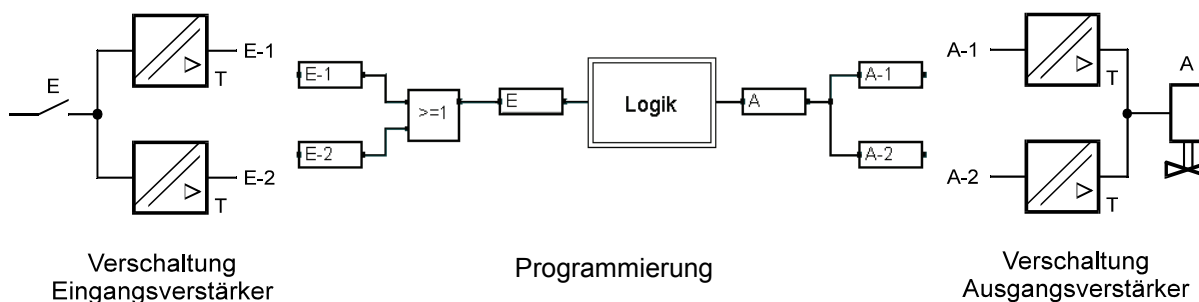


Abbildung 3: Redundante E/A-Baugruppen zur Erhöhung der Verfügbarkeit

7.8.3.1 Redundante, nicht sicherheitsgerichtete Sensoren

Hardware

Je nach Steuersignal (mechanischer Kontakt, Initiator, eigensicher / nicht eigensicher) sind Eingangsbaugruppen vom Typ F 3236, F 3237 oder F 3238 einzusetzen. Die beiden Sensoren werden in 1oo2-Schaltung betrieben, d. h. bei Ansprechen eines Sensors wird der sicherheitsgerichtete Schaltkreis sofort abgeschaltet. Eine Diskrepanz wird nach Ablauf der vorgegebenen Zeit gemeldet. Diese Funktionalität kann in einem Funktionsbaustein für die Eingangsbaugruppe F 3236 zusammengefasst sein. Für die Baugruppen F 3237 und F 3238 gibt es den Baustein HB-RTE-3 mit weiterer Überwachung der Initiatorkreise.

Anwenderprogramm, Eingangsbaugruppe F 3236

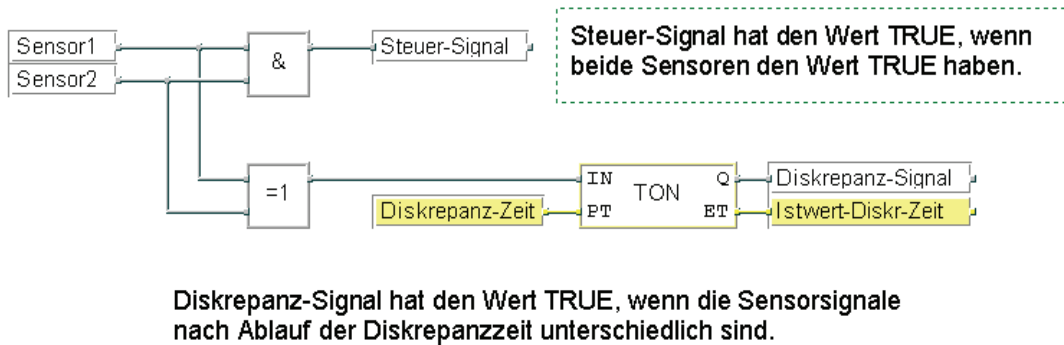
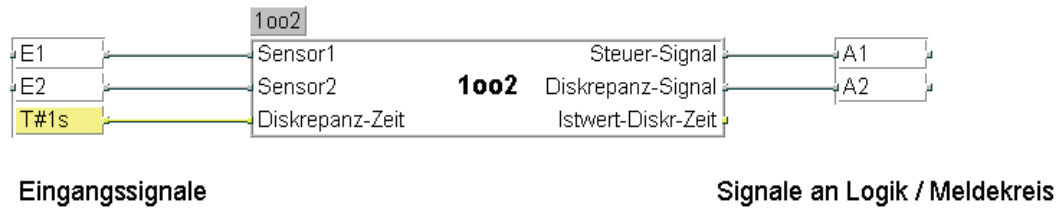


Abbildung 4: Beispiel für einen Funktionsbaustein 1002 und Logik des Bausteins

Anwenderprogramm, Eingangsbaugruppe F 3237 oder F 3238

Verwendung des Bausteins HB-RTE-3

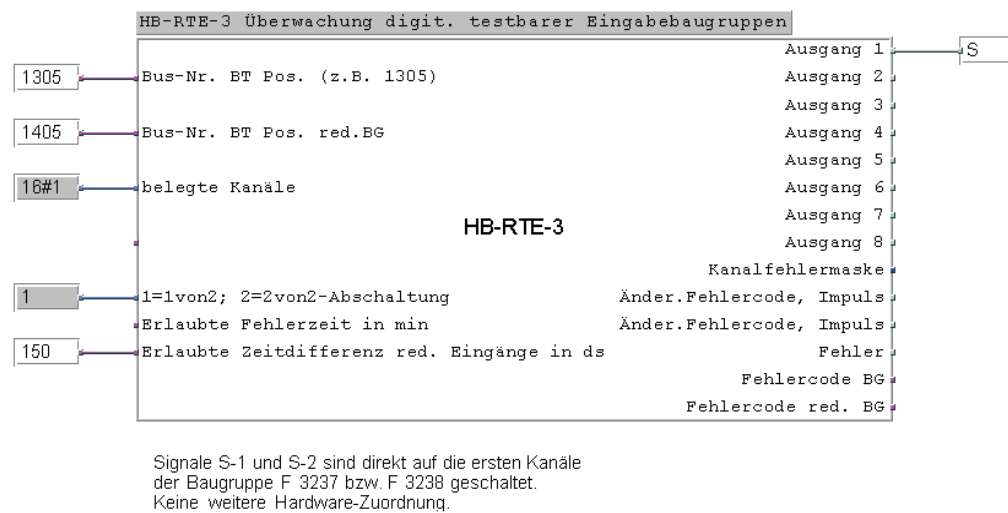


Abbildung 5: Verwendung des Bausteins HB-RTE-3

Sicherheitsbetrachtung

Beim Ansprechen einer der beiden Sensoren oder Ausfall einer Komponente innerhalb des Systems wird abgeschaltet.

Für die Applikationen der Sensoren sind die relevanten Normen zu beachten, z. B. IEC 61511.

Verfügbarkeitsbetrachtung

Keine Verfügbarkeit, da jeder Ausfall einer Komponente zur Abschaltung führt.

7.8.4 Analoge redundante Sensoren

Verschaltung, Hardware

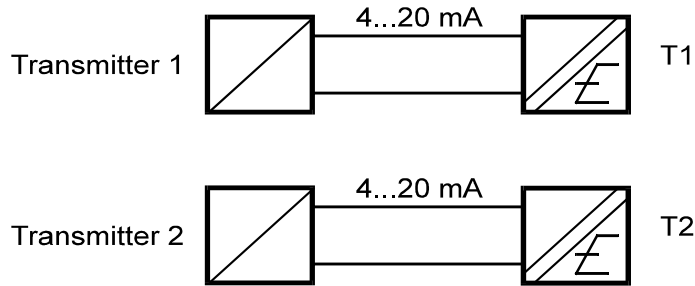
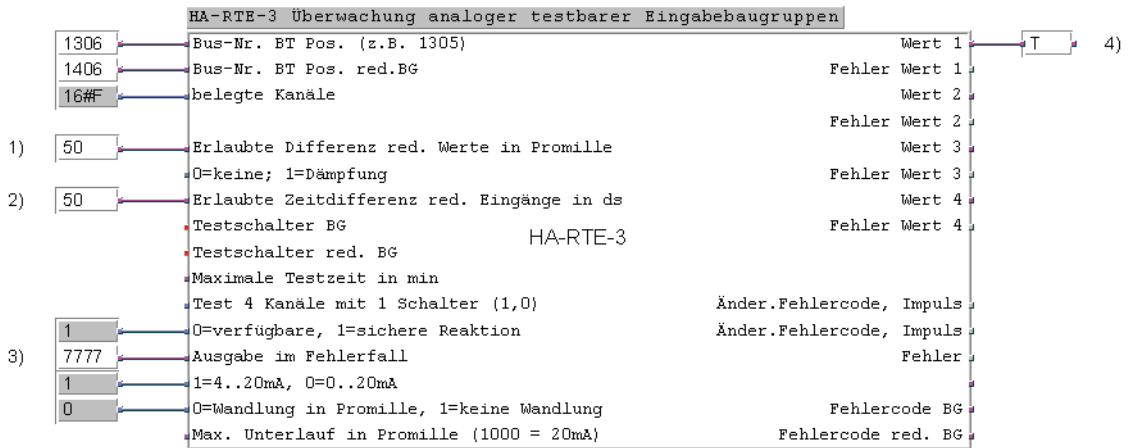


Abbildung 6: Verschaltung redundanter Sensoren

Anwenderprogramm, Eingangsbaugruppe F 6213 oder F 6214

Verwendung des Bausteins HA-RTE-3, Einzelheiten zum Baustein siehe Kapitel 2.5 im Anhang und die Online-Hilfe von ELOP II



Signale T1 und T2 sind direkt auf die ersten Kanäle der Baugruppe F 6213 bzw. F 6214 gelegt. Keine weitere Hardware-Zuordnung.

- 1) z. B. 50
- 2) z. B. 50
- 3) 7777, wenn physikalische Größe im Gefahrfall größer wird (alle vier Kanäle der Baugruppe), 0000, wenn physikalische Größe im Gefahrfall kleiner wird (alle vier Kanäle der Baugruppe)
- 4) Werte 0...1066

Abbildung 7: Verwendung von Baustein HA-RTE-3 bei F 6213 oder F 6214

Vergleicherelement zur Alarmierung oder Abschaltung bei Erreichen des zulässigen Grenzwerts

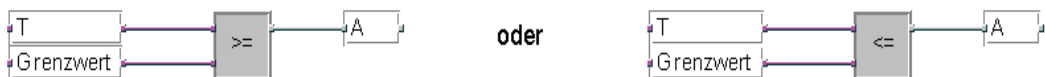


Abbildung 8: Vergleicherelement zur Alarmierung oder Abschaltung bei Erreichen des zulässigen Grenzwerts

Sicherheitsbetrachtung

Beim Ansprechen eines der beiden Sensoren oder Ausfall einer Komponente innerhalb des

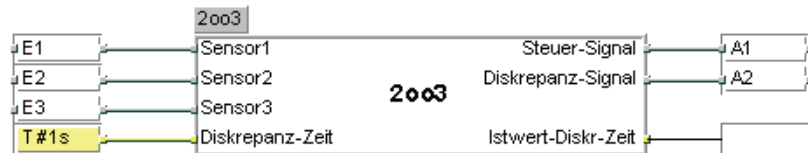
Systems hat der Ausgang A High-Pegel.

Für die Applikationen der Sensoren sind die relevanten Normen zu beachten, z. B. IEC 61511.

Verfügbarkeitsbetrachtung

Keine Verfügbarkeit, da jeder Ausfall einer Komponente oder das Ansprechen eines Sensors zur Abschaltung führt.

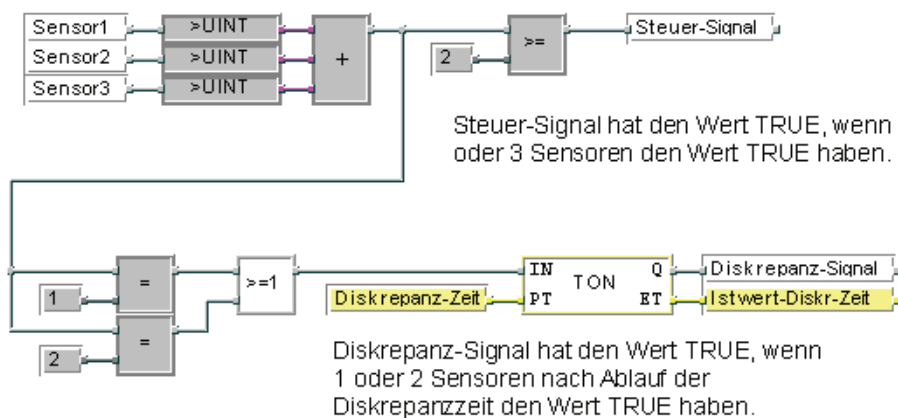
7.8.5 Eingangsbaugruppen mit 2oo3-Verschaltung



Signale von 3 verschiedenen Eingangsbaugruppen.

Funktionsbaustein 2oo3

Signale an Logik / Meldekreis



Steuer-Signal hat den Wert TRUE, wenn 2 oder 3 Sensoren den Wert TRUE haben.

Diskrepanz-Signal hat den Wert TRUE, wenn 1 oder 2 Sensoren nach Ablauf der Diskrepanzzeit den Wert TRUE haben.

Abbildung 9: Funktionsbaustein 2oo3 und Logik des Bausteins

i Die dargestellte Schaltung ist zweckmäßigerweise in einem Funktionsbaustein 2oo3 zusammengefasst.

Bei einem PES mit zwei E/A-Bussen wird das Signal des zweiten Sensors auf zwei Eingangskanäle (jeweils ein Kanal im E/A-Bus1 und ein Kanal im E/A-Bus2) verzweigt und im Anwenderprogramm über eine ODER-Funktion geführt. Es können auch alle Sensorsignale parallel auf Eingangskanäle an beiden E/A-Bussen geschaltet und über jeweils eine ODER-Funktion geführt werden. Anschließend wird der oben dargestellt Funktionsbaustein eingesetzt.

Für die Applikationen der Sensoren sind die relevanten Normen zu beachten, z. B. IEC 61511.

7.9 Programmdokumentation für sicherheitsgerichtete Anwendungen

Das Programmierwerkzeug ELOP II ermöglicht den automatischen Ausdruck der Dokumentation eines Projektes. Die wichtigsten Dokumentationsarten sind:

- Schnittstellendeklaration
- Variablenliste

- Logik
- Beschreibung der Datentypen
- Konfigurationen für Schrank, Baugruppenträger, Baugruppen und Systemparameter
- PLT/Variablen-Querverweis
- Codegenerator-Informationen

Das Layout der verschiedenen Dokumentationsarten kann beliebig vorgegeben werden.

Die Dokumentation ist Bestandteil einer Funktionsabnahme einer genehmigungspflichtigen Anlage durch eine Prüfstelle (TÜV). Die Funktionsabnahme bezieht sich nur auf die Anwenderfunktion, nicht aber auf die sicherheitsgerichteten HIMA-Automatisierungsgeräte H41q-MS, H51q-MS, H41q-HS, H51q-HS, H41q-HRS, H51q-HRS, die baumustergeprüft sind.

i

HIMA empfiehlt, bei abnahmepflichtigen Anlagen so früh wie möglich die Genehmigungsbehörde bei der Projektierung einzuschalten.

7.10 Sicherheitstechnische Aspekte für die Kommunikation (sicherheitsgerichtete Datenübertragung)

Das HIPRO-S-Protokoll ist zertifiziert für SIL 3.

7.10.1 Sicherheitsgerichtete Kommunikation

Im Dialogfenster *Eigenschaften* für die Ressourcen (Register **HIPRO-S, Bearbeiten** der markierten Ressource) kann der Datenaustausch zu sicherheitstechnisch zugeordneten Ressourcen über PES-Master überwacht werden. Hierzu kann eine Überwachungszeit als Parameter *Zeitintervall* angegeben sowie der Befehl *importierte Variablen rücksetzen* bei Überschreiten der Überwachungszeit aktiviert werden.

Die einzustellende Überwachungszeit ist prozessabhängig, die Abstimmung erfolgt mit der abnehmenden Behörde.

Die sicherheitsgerichtete Kommunikation kann auch über das TÜV-zertifizierte Protokoll **saferethernet** mit Hilfe der Ethernet-Kommunikationsbaugruppen F 8627 X oder F 8628 X erfolgen.

7.10.2 Zeitliche Anforderungen

Bei serieller Verbindung wird aus Gründen einer konstanten Übertragungszeit empfohlen, einen eigenen PES-Master und einen eigenen Bus für die sicherheitsgerichtete Datenübertragung mit einer Datenübertragungsrate von 57,6 kbit/s vorzusehen.

Die Datenübertragungszeit T_T vom Wechsel eines Geberwertes an einem PES bis zur Reaktion am Ausgang eines anderen PES ist:

$$T_T = 2 \cdot ZZ_1 + 2 \cdot T_D + 2 \cdot ZZ_2$$

ZZ_1 Zykluszeit von PES 1

ZZ_2 Zykluszeit von PES 2

T_D Datenübertragungszeit zwischen zwei PESen, diese hängt ab von der verwendeten Datenverbindung:

Serielle Übertragung: Hier muss man den Wert der Buszykluszeit annehmen. Zur Buszykluszeit siehe das Betriebssystem-Handbuch HI 800 104 D, Abschnitt

Sicherheitsgerichtete Datenübertragung über HIPRO-S.

Übertragung über Ethernet: in diesem Fall muss man die maximale Übertragungszeit (T_{\max}) annehmen, siehe den Abschnitt *Berechnung der Überwachungszeit für HIPRO-S / HIPRO-S DIRECT Verbindungen* im Datenblatt der Baugruppe F 8627 X.

7.10.3 Hinweise für die Erstellung des Anwenderprogramms

Die Konfiguration des Ethernet-Netzwerkes in ELOP II für HIPRO-S erfolgt automatisch. Dennoch sind bei der Erstellung des Anwenderprogramms folgende Hinweise zu beachten:

- Der Resource-Name in ELOP II muss acht Zeichen umfassen, wobei die letzten zwei Zeichen Ziffern sein müssen. Dabei sind die Zahlen zwischen 1 bis 99 zulässig. Die Zahlen müssen einmalig sein, so dass sie kollisionsfrei zum Ermitteln der IP-Adresse der Kommunikationsbaugruppe verwendet werden können.
- Die sicherheitsgerichtete Kommunikation mit HIPRO-S im NORMAL-Mode ist so einzurichten, dass jedes Automatisierungsgerät zu jedem anderen einen sicherheitsgerichteten Datenaustausch konfiguriert hat. (d. h. Austausch von Dummydaten, falls keine Anwenderdaten ausgetauscht werden). Bei der Benutzung des HIPRO-S-DIRECT-Modes ist dies nicht nötig (es müssen keine Dummydaten übertragen werden). Einzelheiten siehe Datenblatt F 8627 X.
- Zur Kontrolle der HIPRO-S-Konfiguration ist das PES-Masterprogramm zu kompilieren. Anschließend sind die aufgetretenen Fehler zu korrigieren.
- Bei der sicherheitsgerichteten Kommunikation muss für die Übertragungsdaten Null der sichere Wert sein.

8 Einsatz für Brandmelderzentralen entsprechend DIN EN 54-2 und NFPA 72

Die Systeme H41q, H41qc und H51q sind für Brandmelderzentralen nach DIN EN 54-2 und NFPA 72 einsetzbar.

Hierzu ist es erforderlich, dass das Anwenderprogramm die Funktionalitäten für Brandmelderzentralen nach den genannten Normen erfüllt.

Die in DIN EN 54-2 geforderte maximale Zykluszeit von Brandmeldzentralen von 10 Sekunden ist mit den System H41q, H41qc und H51q leicht erfüllbar, da die Zykluszeiten dieser System im Bereich $< 0,5$ Sekunden liegen und ebenso die gegebenenfalls geforderte Sicherheitszeit von 1 Sekunde (Fehlerreaktionszeit).

Der Anschluss der Brandmelder erfolgt im Arbeitsstromprinzip mit Leitungsüberwachung auf Schluss und Bruch. Hierzu können die Eingangsbaugruppen F 3237/F 3238 für boolsche Anschlüsse oder F 6217/F 6221 für analoge Anschlüsse nach folgender Beschaltung verwendet werden:

Digitale Anschlüsse

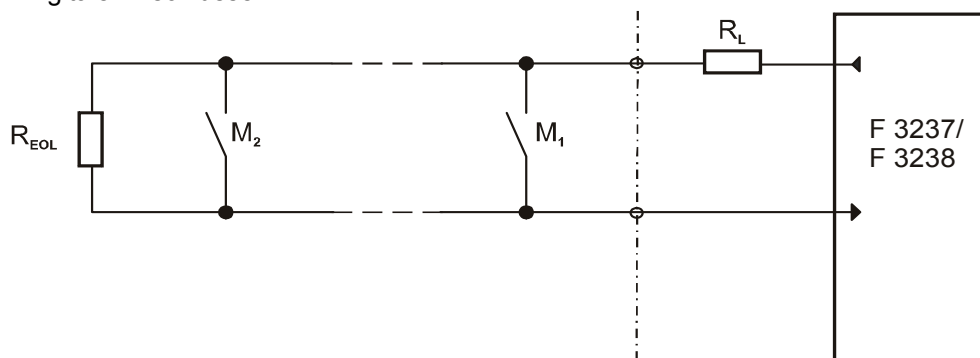


Abbildung 10: Digitale Anschlüsse von Brandmeldern

Analoge Anschlüsse

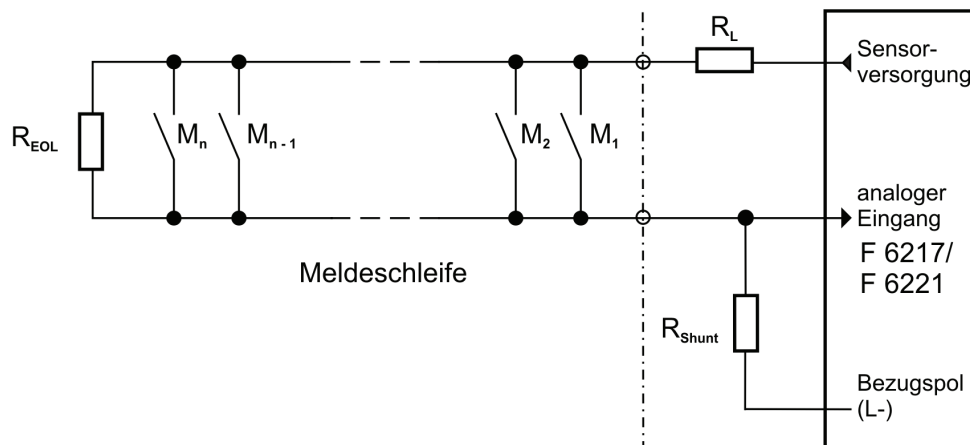


Abbildung 11: Verschaltung von Brandmeldern

Legende zu den Bildern:

M	Brandmelder
R_{EOL}	Abschlusswiderstand am letzten Sensor der Schleife
R_L	Begrenzung des maximal zulässigen Stromes der Schleife
R_{Shunt}	Messwiderstand

Für die Anwendungen sind die Widerstände R_{EOL} , R_L und R_{Shunt} abhängig von den

eingesetzten Sensoren und ihrer Anzahl pro Meldeschleife zu berechnen. Dazu sind auch die Datenblätter der Sensor-Hersteller zu berücksichtigen.

Zusätzlich ist auf die Einhaltung der spezifizierten Stromwerte der Baugruppen F 3237 bzw. F 3238 (siehe Datenblätter) zu achten. Dies gilt insbesondere, wenn die Brandmelder keine mechanischen Kontakte haben, sondern elektronische Ausgänge.

Die Alarmausgänge zur Ansteuerung von Lampen, Sirenen, Hupen usw. werden im Arbeitstromprinzip betrieben, d. h. es müssen Ausgangsbaugruppen mit Überwachung der Kreise auf Leitungsschluss und Leitungsbruch eingesetzt werden, z. B. die Baugruppentypen F 3331 oder F 3334.

Die Ansteuerung von Visualisierungssystemen, Leuchtmeldetableaus, LED-Anzeigen, alphanumerischen Displays, akustischen Alarmen usw. ist mit einem dafür angepassten Anwenderprogramm realisierbar.

Die Weiterleitung von Störungsmeldungen über Ein-/Ausgangsbaugruppen oder zu Übertragungseinrichtungen für Störungsmeldungen muss im Ruhestromprinzip erfolgen.

Die Übertragung von Brandmeldungen von HIMA-System zu HIMA-System ist mit den vorhandenen Kommunikationsstandards wie Modbus, HIPRO-S, OPC (Ethernet) realisierbar. Die Überwachung der Kommunikation ist Bestandteil des Anwenderprogramms. HIMA empfiehlt, diese Kommunikation redundant auszuführen, damit bei Störung einer Komponente einer Übertragungsstrecke (Leitung, Hardwarefehler usw.) trotzdem die Kommunikation gewährleistet ist. Der Ausfall der Komponente muss gemeldet werden und die defekte Komponente soll während des Betriebs getauscht oder repariert werden können.

Die Systeme H41q, H41qc bzw. H51q, die als Brandmelderzentrale eingesetzt werden, müssen eine redundante Stromversorgung haben. Auch müssen Vorkehrungen gegen einen Ausfall der Energieversorgung getroffen werden, z. B. batteriebetriebene Hupe. Die Umschaltung zwischen Netzversorgung und der Ersatzstromversorgung muss so schnell erfolgen, dass ein unterbrechungsfreier Betrieb gewährleistet ist. Spannungseinbrüche bis zu 10 ms sind zulässig.

Bei Störungen des Systems werden die im Anwenderprogramm definierten Systemvariablen vom Betriebssystem beschrieben. Somit ist eine Fehlersignalisierung auf die vom System erkannten Fehler programmierbar. Sicherheitsgerichtete Ein- und Ausgänge werden im Fehlerfall abgeschaltet, d. h. Verarbeitung von Low-Pegel in allen Kanälen der fehlerhaften Eingangsbaugruppe und Abschaltung aller Kanäle der fehlerhaften Ausgangsbaugruppe.

Bei Brandmeldeanlagen nach EN 54-2 und NFPA 72 ist eine Erdschlussüberwachung einzusetzen.

Anhang

1 Standard-Software-Bausteine für den Zentralbereich

Für Funktionen der Zentralbaugruppen können Standard-Softwarebausteine aufgerufen und belegt werden. Eine detaillierte Beschreibung dieser Bausteine findet sich in der Online-Hilfe des jeweiligen Bausteins.

1.1 Baustein HK-AGM-3

Mit diesem Baustein wird die Funktion eines Automatisierungsgeräts H41qc oder H51q als HIPRO-Master überwacht.

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

1.2 Baustein HK-COM-3

Mit diesem Baustein wird die Funktion der Kommunikationsbaugruppen in einem System H41qc oder H51q überwacht.

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

1.3 Baustein HK-MMT-3

Mit diesem Baustein kann ein Automatisierungsgerät H41q, H41qc oder H51q als Modbus-Master eingesetzt werden.

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

1.4 Baustein H8-UHR-3

Der Baustein ermöglicht das externe Stellen oder Ändern von Datum und Uhrzeit des Automatisierungsgeräts.

Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

2 Standard-Software-Bausteine für den E/A-Bereich

Alle nachfolgend beschriebenen Software-Bausteine sind für den Betrieb in sicherheitsgerichteten Automatisierungsgeräten zugelassen.

Die in diesem Kapitel beschriebenen besonderen Programmierhinweise sind zu beachten.

Für die genauen Informationen über die Funktionen der Software-Bausteine und die Belegung der Ein- und Ausgänge ist die Online-Hilfe des jeweiligen Bausteins zu verwenden.

2.1 Baustein H8-STA-3

Der Baustein wird zur Konfiguration einer Gruppenabschaltung verwendet. Er wird für jede Abschaltgruppe einmal im Anwenderprogramm eingesetzt.

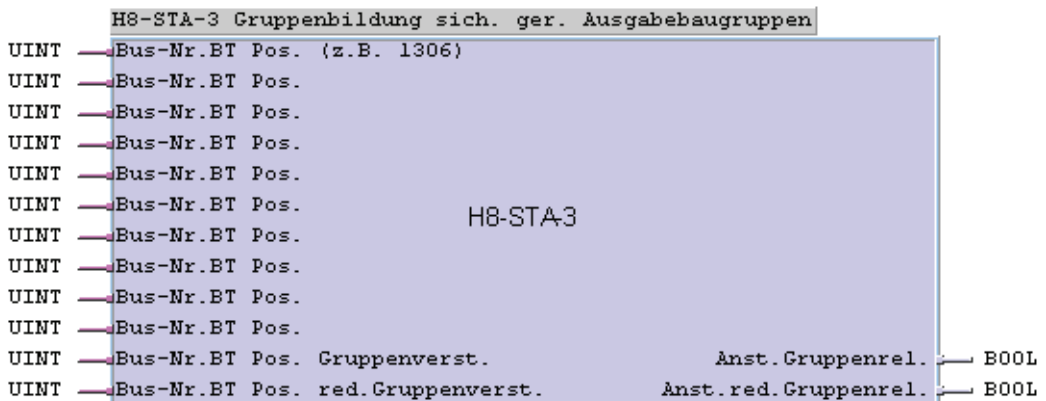


Abbildung 12:Anschlüsse des Bausteins H8-STA-3

Zum Verhalten bei Fehlern von Ausgangskanälen siehe Kapitel 7.2.6.2 .

2.1.1 Baustein-Eingänge

Die Positionen der zu einer Abschaltgruppe gehörenden Baugruppen werden als vierstellige Dezimalzahl eingegeben entsprechend der Festlegung in der gewählten Ressource.

Beispiel: „1306“ bedeutet:

Schrank 1, Baugruppenträger 3, Baugruppen-Position 06

Bei Einsatz von Baugruppen mit integrierter Sicherheitsabschaltung ist einer der Eingänge *Bus-Nr.BT Pos. Gruppenverst.* oder *Bus-Nr.BT Pos. red. Gruppenverst.* zu belegen. Hier ist ein vorhandener, aber nicht bestückter Steckplatz einzutragen.

2.1.2 Baustein-Ausgänge

Namen der Gruppenverstärkerkanäle. Weitere Programmierungen in der Logik des Anwenderprogramms sind nicht nötig.

i

Ausgangsbaugruppen mit integrierter Sicherheitsabschaltung benötigen keine Gruppenabschaltung. Sie kann aber auch für diese Baugruppen vorgegeben werden. Dann führt ein Fehler einer Ausgangsbaugruppe zur Abschaltung aller Baugruppen, die zu einer Gruppe gehören (entsprechend den Angaben am Baustein H8-STA-3).

2.2 Baustein HA-LIN-3

Der Baustein dient der Linearisierung von Temperaturmessungen mit Thermoelementen und Widerstandsthermometern Pt 100. Die korrekte Parametrierung ist zu überprüfen, wenn die Werte zur Abschaltung sicherheitstechnisch relevanter Kreise verwendet werden (siehe ELOP II Online-Hilfe).

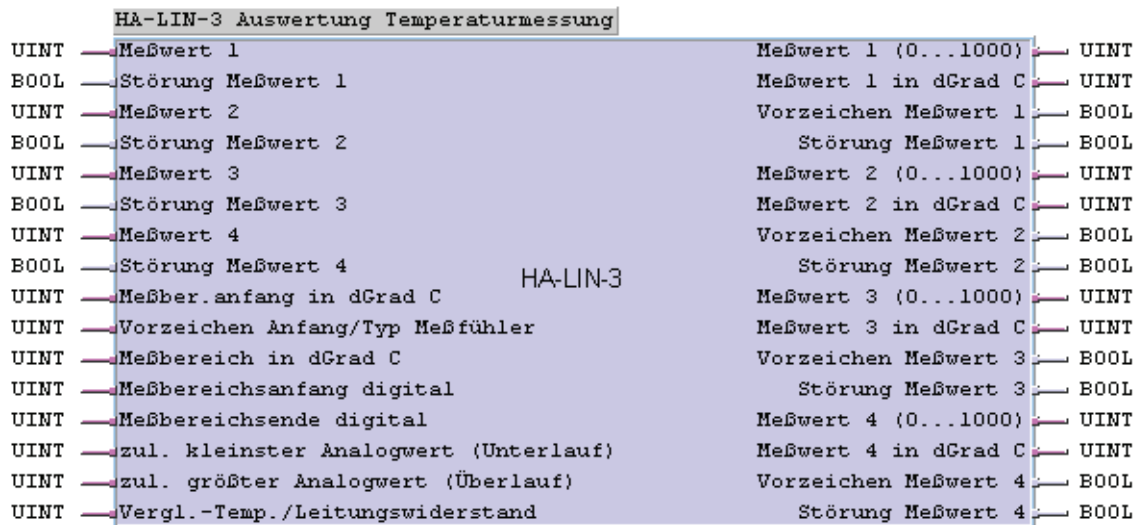


Abbildung 13:Anschlüsse des Bausteins HA-LIN-3

2.3 Baustein HA-PID-3

Der Baustein beinhaltet einen digitalen Regler, der durch Parametrierung in den Arbeitsweisen P, I, D, PI, PD und PID betrieben werden kann.

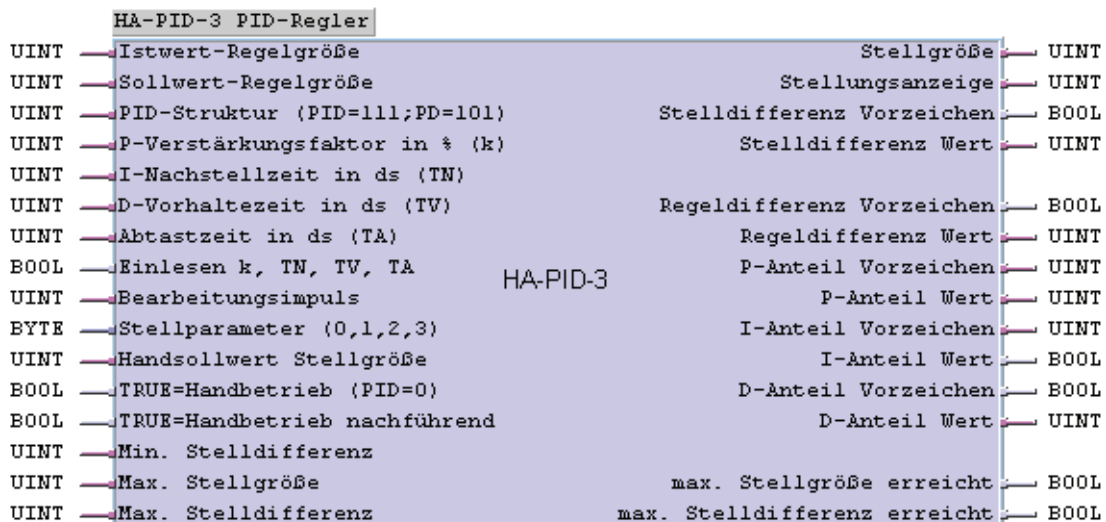


Abbildung 14:Anschlüsse des Bausteins HA-PID-3

2.3.1 Bausteineingänge

True=Handbetrieb (PID=0), True=Handbetrieb nachführend

Bei sicherheitsgerichtetem Betrieb des Regelbausteins dürfen diese Eingänge nicht belegt werden. Abweichungen davon sind durch die Abnahmebehörde zu genehmigen. Parameter- und Konstantenänderung an den Bausteineingängen im laufenden Betrieb sind nur mit Genehmigung der abnehmenden Behörde und im überwachten Betrieb erlaubt. Die Belegung der Bausteineingänge mit nicht sicherheitsgerichteten importierten Variablen ist nicht zulässig.

2.3.2 Bausteinausgänge:

Sicherheitsabschaltungen sind nur zugelassen über:
max. Stellgröße erreicht und *max. Stelldifferenz erreicht*
 Abweichungen davon sind durch die Abnahmebehörde zu genehmigen.

i Der Regelalgorithmus des Bausteins allein kann nicht in jedem Fall den sicheren Zustand einer Anlage erreichen. Im Einzelfall sind zusätzliche Maßnahmen notwendig.

2.4 Baustein HA-PMU-3

Der Baustein dient sowohl der Umformung digitalisierter Messwerte in Promillewerte als auch der Umformung von Promillewerten in digitalisierte Analogwerte. Die korrekte Parametrierung ist zu überprüfen, wenn die Werte zur Abschaltung sicherheitstechnisch relevanter Kreise verwendet werden (siehe ELOP II Online-Hilfe).

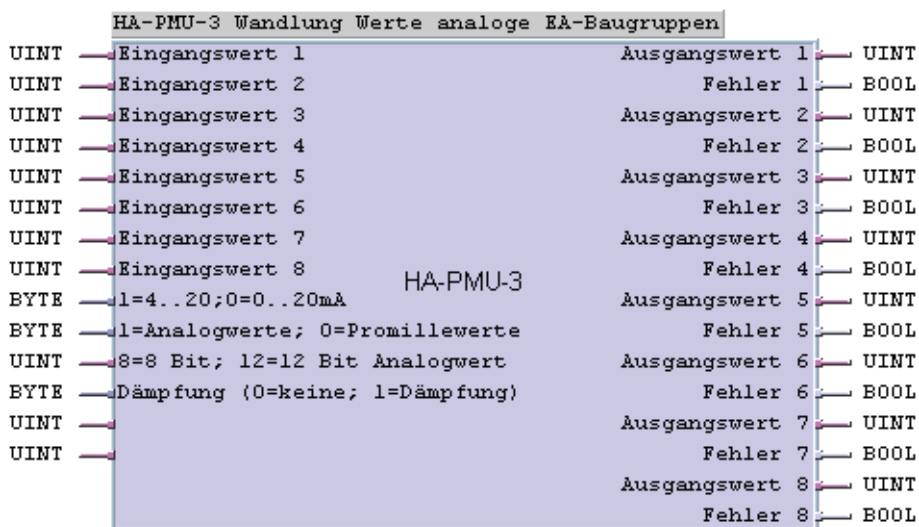


Abbildung 15:Anschlüsse des Bausteins HA-PMU-3

2.5 Baustein HA-RTE-3

Der Baustein dient zur Wertverarbeitung und zur Anzeige von Fehlern bei analogen sicherheitsgerichteten Eingangsbaugruppen bei einkanaligem oder redundantem Betrieb. Er muss für jede sicherheitsgerichtete analoge Eingangsbaugruppe (F 6213/F 6214) einmal im Anwenderprogramm eingesetzt werden. Für den Fall, dass zwei redundante E/A-Baugruppen verwendet werden, muss der Baustein nur einmal im Anwenderprogramm

vorhanden sein.

HA-RTE-3 Überwachung analoger testbarer Eingabebaugruppen			
UINT	Bus-Nr. BT Pos. (z.B. 1305)	Wert 1	UINT
UINT	Bus-Nr. BT Pos. red.BG	Fehler Wert 1	BOOL
BYTE	belegte Kanäle	Wert 2	UINT
		Fehler Wert 2	BOOL
UINT	Erlaubte Differenz red. Werte in Promille	Wert 3	UINT
BYTE	0=keine; 1=Dämpfung	Fehler Wert 3	BOOL
UINT	Erlaubte Zeitdifferenz red. Eingänge in ds	Wert 4	UINT
MOS A	Testschalter BG	Fehler Wert 4	BOOL
MOS A	Testschalter red. BG		
UINT	Maximale Testzeit in min		
BYTE	Test 4 Kanäle mit 1 Schalter (1,0)	Änder.Fehlercode, Impuls	BOOL
BYTE	0=verfügbare, 1=sichere Reaktion	Änder.Fehlercode, Impuls	BOOL
UINT	Ausgabe im Fehlerfall	Fehler	BOOL
BYTE	1=4..20mA, 0=0..20mA		UINT
BYTE	0=Wandling in Promille, 1=keine Wandlung	Fehlercode BG	UINT
UINT	Max. Unterlauf in Promille (1000 = 20mA)	Fehlercode red. BG	UINT

Abbildung 16:Anschlüsse des Bausteins HA-RTE-3

2.5.1 Eingänge

Bus-Nr. BT Pos.(z. B. 1305)

Bus-Nr. BT Pos. red. BG

Position der sicherheitsgerichteten analogen Eingangsbaugruppe und, falls vorhanden, der redundanten Baugruppe als 4-stellige Dezimalzahl:

Beispiel: „1305“ bedeutet:

Schrank 1, Baugruppenträger 3, Baugruppen-Position 05 (bei redundantem Betrieb muss die redundante Baugruppe eine unterschiedliche Position erhalten)

0 = keine; 1 = Dämpfung

1 nur bei redundantem Betrieb. Differenz aus dem aktuellen Wert und dem Wert des Vorzyklus wird zur erlaubten Differenz in ‰ (*Erlaubte Differenz red. Werte in Promille*) addiert. Begrenzung der Testzeit in Minuten. Nach Ablauf der Testzeit wird wieder der tatsächliche Wert in der Anwenderlogik verarbeitet. Siehe auch Mitteilung *Wartungseingriffe, Maintenance Override* auf der Webseite www.tuvasi.com des TÜV Rheinland.

Maximale Testzeit in min

2.5.2 Ausgänge

Wert 1...4

Die Verwendung der Werte muss überprüft werden, wenn diese zur Abschaltung sicherheitsgerichteter Kreise benutzt werden.

Fehler Wert 1...4

Die Ausgänge müssen belegt werden, um im Fehlerfall mit ihrem booleschen Signal eine Abschaltung auslösen zu können.

Die weiteren Ausgänge dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

2.6 Baustein HB-BLD-3

Der Baustein dient der kanalbezogenen Fehlerauswertung und Fehleranzeige für digitale sicherheitsgerichtete Ausgangsbaugruppen F 3331, F 3334 und F 3349. Er darf für jede

verwendete Baugruppe nur einmal eingesetzt werden.

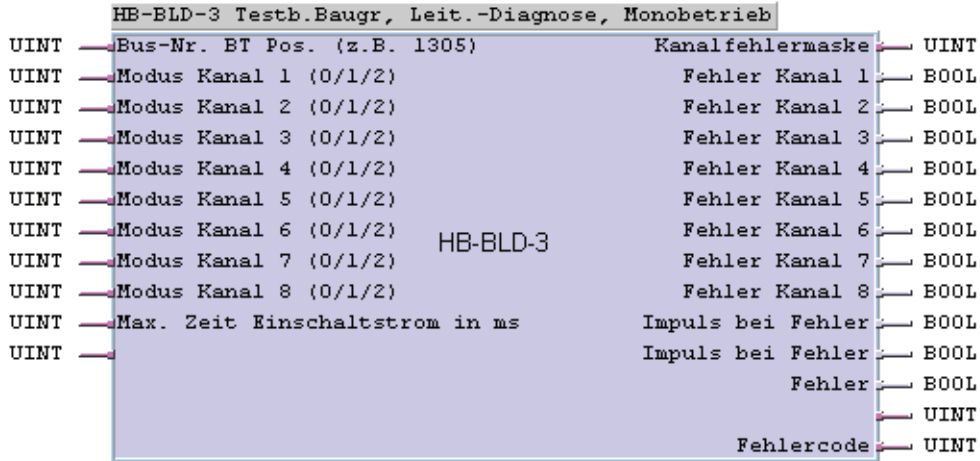


Abbildung 17:Anschlüsse des Bausteins HB-BLD-3

2.6.1 Eingänge

Bus-Nr. BT Pos. (z. B. 1305)

Position der sicherheitsgerichteten digitalen Ausgangsbaugruppe als 4stellige Dezimalzahl, Beispiel: „1305“ bedeutet: Schrank 1, Baugruppenträger 3, Baugruppen-Position 05

Modus Kanal n (0/1/2)

Belegung	Bedeutung
1	Normalbetrieb, erkannter Fehler wird mit High-Pegel an zugehörigem Ausgang <i>Fehler Kanal n</i> gemeldet, Ausgangskreis der Baugruppe ist geschlossen.
0	Fehlerauswertung, Fehlermeldungen werden unterdrückt
2	nur anlagenspezifisch erlaubt, inverser Betrieb, d. h. der Ausgangskreis soll offen sein
>2	Wertebereich überschritten: Der Kanal wird als fehlerhaft interpretiert (TRUE am Ausgang) und eine kanalbezogene Fehlermeldung wird ausgegeben.

In sicherheitsgerichteten Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Max. Zeit Einschaltstrom in ms

Festlegung der Wartezeit für die Erkennung des Leitungsbruchs bzw. Zeit für Tolerierung der Strombegrenzung. Für diese Zeit wird die Fehleranzeige unterdrückt. Eine Vergrößerung der Wartezeit bringt eine Erhöhung der Zykluszeit mit sich.

2.6.2 Ausgänge

Die Ausgänge *Impuls bei Fehler (2x)*, *Fehler* und *Fehlercode* dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

Die übrigen Ausgänge sind für sicherheitsgerichtete Aktionen verwendbar.

2.7 Baustein HB-BLD-4

Der Baustein dient der kanalbezogenen Fehlerauswertung und Fehleranzeige für digitale sicherheitsgerichtete Ausgangsbaugruppen F 3331, F 3334 und F 3349 bei redundantem

Betrieb. Er darf für ein redundantes Baugruppenpaar nur einmal eingesetzt werden.

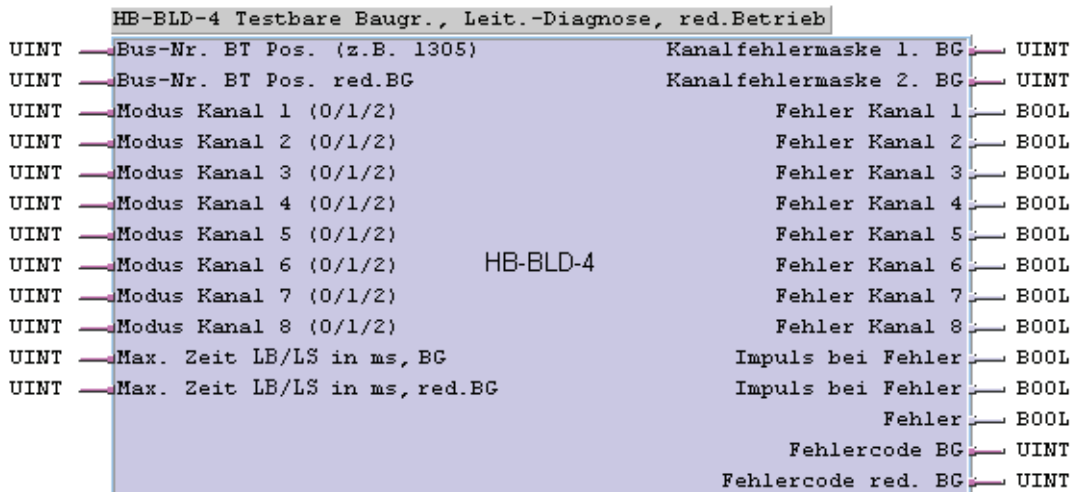


Abbildung 18:Anschlüsse des Bausteins HB-BLD-4

2.7.1 Eingänge

Bus-Nr. BT Pos.(z. B. 1305)
 Bus-Nr. BT Pos. red. BG

Position der sicherheitsgerichteten digitalen Ausgangsbaugruppe und falls vorhanden der redundanten Baugruppe als 4-stellige Dezimalzahl.

Beispiel: „1305“ bedeutet:

Schrank 1, Baugruppenträger 3, Baugruppen-Position 05

Modus Kanal n (0/1/2)

Belegung	Bedeutung
1	Normalbetrieb, ein erkannter Fehler wird mit High-Pegel an zugehörigem Ausgang <i>Fehler Wert Kanal n</i> gemeldet, Ausgangskreis der Baugruppe ist geschlossen.
0	Fehlerauswertung, Fehlermeldungen werden unterdrückt.
2	nur anlagenspezifisch erlaubt, inverser Betrieb d. h. der Ausgangskreis soll offen sein. Ein erkannter Fehler wird mit High-Pegel an zugehörigem Ausgang <i>Fehler Wert Kanal n</i> gemeldet,
>2	Wertebereich überschritten: Der Kanal wird als fehlerhaft interpretiert (TRUE am Ausgang) und eine kanalbezogene Fehlermeldung wird ausgegeben.

In sicherheitsgerichteten Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Max. Zeit Einschaltstrom in ms, BG Festlegung der Wartezeit für die Erkennung des Leitungsbruchs bzw. Zeit für Tolerierung der Strombegrenzung.

Max. Zeit Einschaltstrom in ms, red BG Für diese Zeit wird die Fehleranzeige unterdrückt. Eine Vergrößerung der Wartezeit bringt eine Erhöhung der Zykluszeit mit sich.

2.7.2 Ausgänge

Die Ausgänge *Impuls bei Fehler (2x)*, *Fehler*, *Fehlercode BG* und *Fehlercode red. BG* dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

Die übrigen Ausgänge sind für sicherheitsgerichtete Aktionen verwendbar.

2.8 Baustein HB-RTE-3

Der Baustein dient zur Auswertung und Anzeige von Fehlern bei digitalen sicherheitsgerichteten Eingangsbaugruppen bei einkanaligem oder redundantem Betrieb. Er muss für jede Eingangsbaugruppe Typ F 3237 oder F 3238 bzw. für zwei redundant arbeitende Eingangsbaugruppen F 3237 oder F 3238 je einmal im Anwenderprogramm eingesetzt werden.

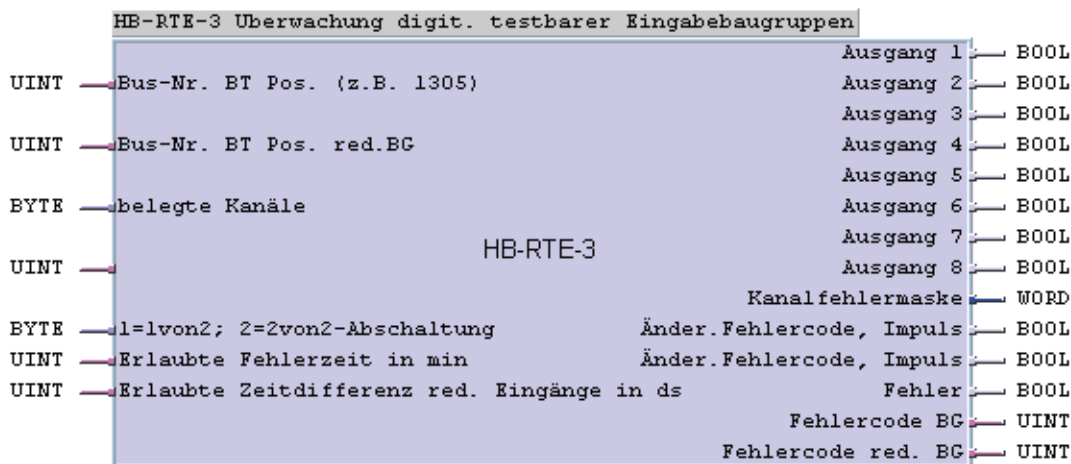


Abbildung 19:Anschlüsse des Bausteins HB-RTE3

2.8.1 Eingänge:

Bus-Nr. BT Pos.(z. B. 1305) Position der sicherheitsgerichteten digitalen Ausgangsbau-
 Bus-Nr. BT Pos. red. BG gruppe und falls vorhanden der redundanten Baugruppe als 4-
 stellige Dezimalzahl.
 Beispiel: „1305“ bedeutet:
 Schrank 1, Baugruppenträger 3, Baugruppen-Position 05

1 = 1 von 2; 2 = 2 von 2 -
Abschaltung

Belegung	Bedeutung
0	Belegung im einkanaligen Betrieb. Eingabe gemäß IEC 1131: 16#00 bzw. 2#00000000.
1	1 von 2-Abschaltung, entspricht UND-Verknüpfung. Bei der 1 von 2-Abschaltung wird die Redundanz der Baugruppen zur Erhöhung der Verfügbarkeit verwendet. Wenn keine Fehler der Eingabebaugruppen und der Eingangskreise anstehen, so werden die Eingangssignale der Kanäle 1...8 der Baugruppen an die zugehörigen Ausgänge des Bausteins UND-verknüpft. Beim Auftreten eines Fehlers in einem Kanal wird der letzte Zustand am zugehörigen Bausteinausgang gehalten und nach Ablauf der definierten Fehlerzeit auf FALSE zurückgesetzt, wenn der Fehler noch ansteht. Bei FALSE am anderen fehlerfreien Eingang oder beim gleichzeitigen Auftreten von Fehlern in beiden Kanälen (Doppelfehler) wird der Bausteinausgang ohne Verzögerung auf FALSE gesetzt.
2	2 von 2-Abschaltung, entspricht ODER-Verknüpfung. Bei der 2 von 2-Abschaltung wird die Redundanz der Baugruppen zur Erhöhung der Verfügbarkeit verwendet. Steht kein Fehler der Eingabebaugruppen oder der Eingangskreise an, so werden die Eingangssignale der Kanäle 1...8 der Baugruppen an die zugehörigen Ausgänge des Bausteins ODER-verknüpft übergeben. Bei Auftreten eines Fehlers in einem Kanal wird das Eingangssignal des anderen Kanals an den Bausteinausgang übergeben. Nur bei gleichzeitigem Auftreten von Fehlern in beiden Kanälen (Doppelfehler) wird der letzte Zustand am zugehörigen Bausteinausgang gehalten und nach Ablauf der definierten Fehlerzeit auf FALSE zurückgesetzt, wenn der Doppelfehler noch ansteht.

In sicherheitsgerichteten Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Erlaubte Fehlerzeit in min

Innerhalb der angegebenen Zeit nach Sensortest, Bauteil- oder Leitungsfehler keine Auswirkung auf die Abschaltung Abstimmung mit der abnehmenden Behörde notwendig.

Erlaubte Zeitdiff. red. Eingänge in ds

Zeitliche Differenz der Schaltpunkte zwischen zwei redundanten Gebern. Die Zeit ist geberabhängig, Abstimmung mit der abnehmenden Behörde notwendig.

2.8.2 Ausgänge

Die Ausgänge *Kanalfehlermaske*, *Änder. Fehlercode*, *Impuls (2x)*, *Fehler*, *Fehlercode BG* und *Fehlercode red. BG* dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

Die Ausgänge *Ausgang 1* bis *Ausgang 8* sind für sicherheitsgerichtete Aktionen verwendbar.

2.9 Baustein HF-AIX-3

Der Baustein HF-AIX-3 dient zur Parametrierung und Auswertung jeweils eines Kanals der sicherheitsgerichteten analogen (Ex)-Eingangsbaugruppe F 6221 mit einer Auflösung 0...10.000.

Der Baustein HF-AIX-3 muss für jeden Kanal der F 6221 einmal im Anwenderprogramm eingesetzt werden.

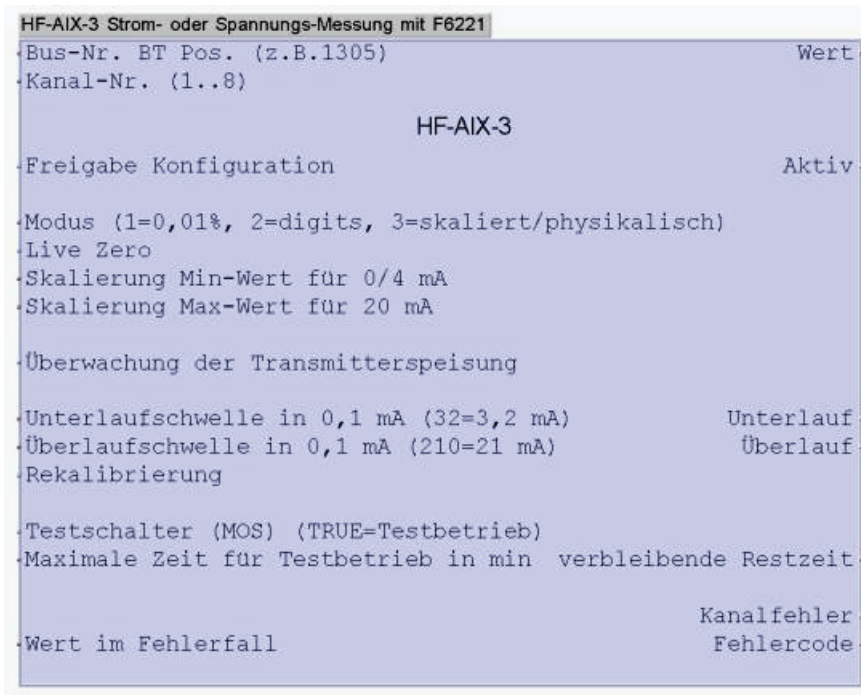


Abbildung 20: Anschlüsse des Bausteins HF-AIX-3

Die analoge Eingangsbaugruppe hat pro Kanal einen sicherheitsgerichteten Ausgang, der unabhängig vom Zyklus der Zentralbaugruppe gesteuert wird. Der Zustand dieses Ausgangs wird am Ausgang des Bausteins HF-AIX-3 angezeigt und kann im Anwenderprogramm weiter verarbeitet werden.

Über die Parametereinstellungen kann der Wert der analogen Eingangsbaugruppe gewandelt und gespreizt werden.

Ein am Bausteineingang *Wert im Fehlerfall* vorgegebener Wertes wird in folgenden Fällen auf den Ausgang *Wert* geschaltet:

- bei Kanalfehler
- bei Baugruppenfehler
- bei Messbereichsüber- oder -unterschreitung

In diesen Fällen verarbeitet das Anwenderprogramm den *Wert im Fehlerfall* an Stelle des Messwerts.

2.10 Baustein HF-CNT-3

Der Baustein HF-CNT-3 dient zur Parametrierung und Auswertung der beiden Kanäle der sicherheitsgerichteten Zählerbaugruppe F 5220 mit einer Auflösung von 24 Bit. Die Zählerbaugruppe kann eingesetzt werden zum Zählen von Impulsen, Erfassen von Frequenzen bzw. Drehzahlen sowie zum Erkennen der Drehrichtung.

Der Baustein HF-CNT-3 muss für jede Zählerbaugruppe F 5220 einmal im Anwenderprogramm eingesetzt werden.

```

HF-CNT-3 Zählerbaustein für F5220
Bus-Nr. BT Pos. (z.B. 1305)

      Zähler Kanal 1
Freigabe der Konfiguration
Impulsquelle (1=5V; 2=24V; 3= Initiator)           Zähler (24 Bit)
Vorgabewert                                       Zustand des Ausgangs
Torzeit in 50ms                                  Drehrichtung des Impuls
Maximalabweichung Frequenzmessung (TRUE = rechts; FALSE = links)
Zählmodus (1=rechts,links; 2=rechts; 3=links)     Leitungsbruch/-schluss
                                                    Aktiv
Reset des Zählers
Halt des des Zählers
Testschalter (MOS) (TRUE = Testbetrieb)
Maximale Zeit für Testbetrieb in min              verbleibende Restzeit
Forcewert im Testbetrieb

      Zähler Kanal 2
Freigabe der Konfiguration
Impulsquelle (1=5V; 2=24V; 3= Initiator)           Zähler (24 Bit)
Vorgabewert                                       Zustand des Ausgangs
Torzeit in 50ms                                  Drehrichtung des Impuls
Maximalabweichung Frequenzmessung (TRUE = rechts; FALSE = links)
Zählmodus (1=rechts,links; 2=rechts; 3=links)     Leitungsbruch/-schluss
                                                    Aktiv
Reset des Zählers
Halt des Zählers
Testschalter (MOS) (TRUE = Testbetrieb)
Maximale Zeit für Testbetrieb in min              verbleibende Restzeit
Forcewert im Testbetrieb

                                                    Fehlercode BG
  
```

Abbildung 21:Anschlüsse des Bausteins HF-CNT-3

Die Zählerbaugruppe hat pro Kanal einen sicherheitsgerichteten Ausgang, der unabhängig vom Zyklus der Zentralbaugruppe gesteuert wird. Der *Zustand des Ausgangs* wird am Ausgang des Zählerbausteins HF-CNT-3 angezeigt und kann im Anwenderprogramm weiter verarbeitet werden.

Mit TRUE-Signal am Eingang *Testschalter MOS* (Maintenance Override Switch) kann der Ausgang der Zählerbaugruppe für die vorgegebene Testbetriebszeit direkt gesteuert werden, d. h., der Ausgang führt das am Eingang *Forcewert im Testbetrieb* vorgegebene Signal. Siehe auch Mitteilung *Wartungseingriffe, Maintenance Override* auf der Webseite www.tuvasi.com des TÜV Rheinland.

i Bei Änderungen der Torzeit steht der korrekte Messwert erst nach drei Torzeiten (aktuell eingestellte) am Ausgang zur Verfügung!

2.11 Baustein HF-CNT-4

Dieser Baustein entspricht dem Baustein HF-CNT-3, besitzt aber zusätzlich je einen Ausgang *Kanalfehler*.

```

HF-CNT-4 Zählerbaustein für F5220
Bus-Nr. BT Pos. (z.B. 1305)

    Zähler Kanal 1
Freigabe der Konfiguration
Impulsquelle (1=5V; 2=24V; 3= Initiator)           Zähler (24 Bit)
Vorgabewert                                       Zustand des Ausgangs
Torzeit in 50ms                                  Drehrichtung des Impuls
Maximalabweichung Frequenzmessung (TRUE = rechts; FALSE = links)
Zählmodus (1=rechts,links; 2=rechts; 3=links)     Leitungsbruch/-schluss
                                                    Aktiv
Reset des Zählers                                Kanalfehler
Halt des des Zählers
Testschalter (MOS) (TRUE = Testbetrieb)
Maximale Zeit für Testbetrieb in min              verbleibende Restzeit
Forcewert im Testbetrieb

    Zähler Kanal 2           HF-CNT-4
Freigabe der Konfiguration
Impulsquelle (1=5V; 2=24V; 3= Initiator)           Zähler (24 Bit)
Vorgabewert                                       Zustand des Ausgangs
Torzeit in 50ms                                  Drehrichtung des Impuls
Maximalabweichung Frequenzmessung (TRUE = rechts; FALSE = links)
Zählmodus (1=rechts,links; 2=rechts; 3=links)     Leitungsbruch/-schluss
                                                    Aktiv
Reset des Zählers                                Kanalfehler
Halt des Zählers
Testschalter (MOS) (TRUE = Testbetrieb)
Maximale Zeit für Testbetrieb in min              verbleibende Restzeit
Forcewert im Testbetrieb

                                                    Fehlercode BC
    
```

Abbildung 22:Anschlüsse des Bausteins HF-CNT-4

Die Ausgänge *Kanalfehler* melden einen Kanalfehler..

Kanalfehler=

TRUE

Es liegt ein Kanalfehler vor.

Bei einem Baugruppenfehler sind beide Ausgänge *Kanalfehler*

TRUE

FALSE

Der Kanal arbeitet korrekt oder ist noch nicht parametrier.

2.12 Baustein HF-TMP-3

Der Baustein HF-TMP-3 wird für jeden Kanal der Thermoelementbaugruppe F 6220 eingesetzt. Ohne eine korrekte Parametrierung des Kanals über den Baustein HF-TMP-3 arbeitet der Kanal nicht, d. h. die Ausgangswerte sind 0 bzw. FALSE. Es gibt keine Default-Funktionalität bzw. -Einstellung. Der Sensor Typ 1 darf nur auf Kanal 9 eingegeben werden.

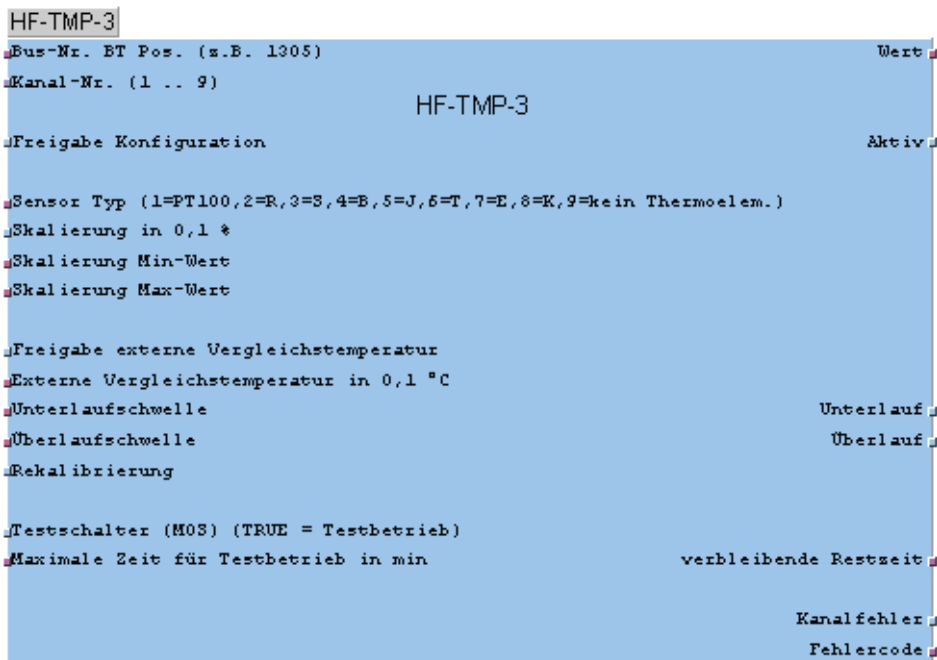


Abbildung 23: Anschlüsse des Bausteins HF-TMP-3

Das Signal *Freigabe externe Vergleichstemperatur* wird nur ausgewertet, wenn die Betriebsart *Temperaturmessung* eingestellt ist (Werte 2 bis 8 am Eingang *Typ*). Führt dieser Eingang TRUE, so wird die am Eingang *externe Vergleichstemperatur* anliegende Temperatur als Vergleichswert herangezogen. Führt dieser Eingang FALSE, wird der Temperaturwert des auf der Baugruppe befindlichen Widerstandsthermometers als Vergleichstemperatur verarbeitet.

Der Bausteinoutput *Wert* nimmt im Fehlerfall des Kanals bzw. der Baugruppe den Wert 0 an. Im Fehlerfall ist daher im Anwenderprogramm der Bausteinoutput *Kanalfehler* auszuwerten, damit der im Anwenderprogramm zu definierende Fehlerwert verarbeitet wird.

Bei sicherheitstechnischen Anwendungen in SIL 3 ist die Referenztemperatur als Vergleich der Referenztemperaturen auf zwei verschiedenen Baugruppen auszuwerten, ebenso die Temperatur zweier Thermoelemente.

Eine Rekalibrierung wird automatisch alle 5 Minuten durchgeführt zur automatischen Erfassung der an der Baugruppe vorhandenen Umweltbedingungen (z. B. Temperatur). Diese Funktion kann auch durch TRUE-Signal am Eingang *Rekalibrierung* im Anwenderprogramm erfolgen. Dieses Signal darf nur einen Zyklus lang anstehen.

Mit TRUE-Signal am Eingang *Testschalter MOS* (Maintenance Override Switch) wird der Wert an den Bausteinoutputs *Wert* und *Kanalfehler* eingefroren, wenn die Zeit für den Testbetrieb läuft. Siehe auch Mitteilung *Wartungseingriffe, Maintenance Override* auf der Webseite www.tuvasi.com des TÜV Rheinland.

2.13 Baustein HK-LGP-3

Der Baustein dient der Auswertung und Konfiguration der Ereignisaufzeichnung und der Umschaltung zwischen Modbus und LgP (Logikplan gesteuerte Protokollierung).

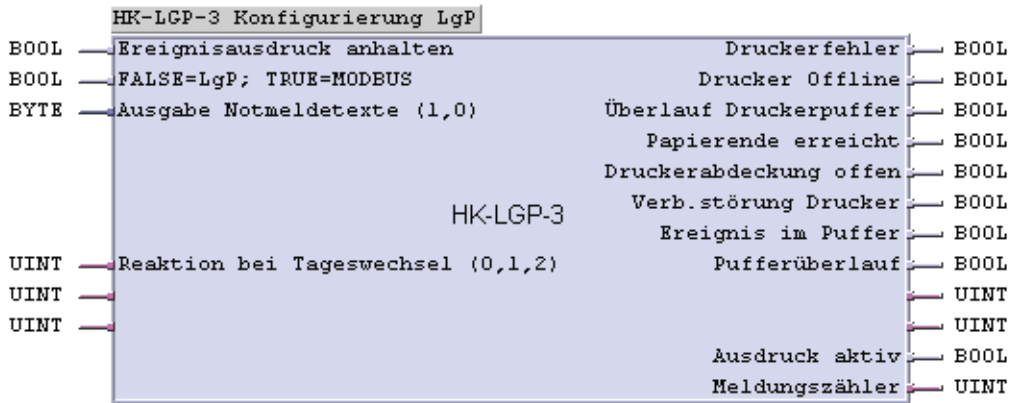


Abbildung 24:Anschlüsse des Bausteins HK-LGP-3

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

2.14 Baustein HZ-DOS-3

Der Baustein dient zur Festlegung, welche sicherheitsgerichteten E/A-Baugruppen nur im Diagnosemodus betrieben werden sollen. Mit einem Baustein können bis zu sechzehn Baugruppen überwacht werden. Der Baustein kann mehrfach im Anwenderprogramm eingesetzt werden.

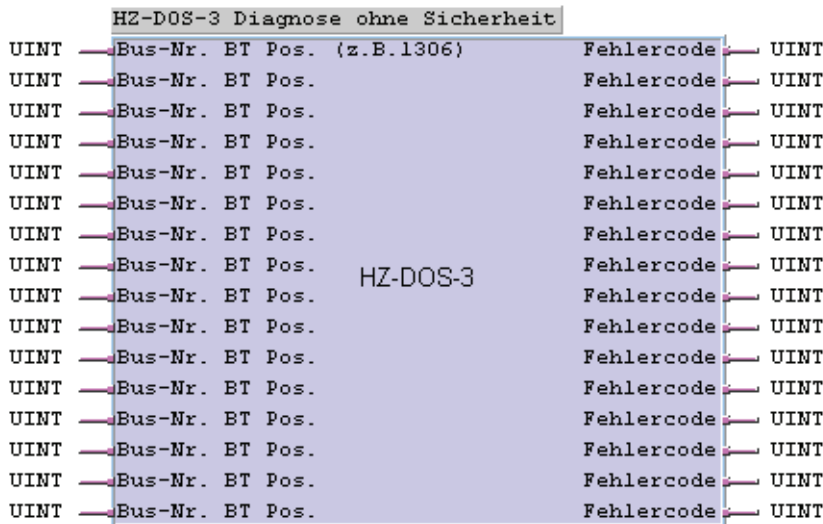


Abbildung 25:Anschlüsse des Bausteins HZ-DOS-3

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

Alle sicherheitsgerichteten E/A-Baugruppen, die am Baustein HZ-DOS-3 aufgelistet sind, dürfen nicht für Sicherheitsfunktionen verwendet werden.

2.15 Baustein HZ-FAN-3

Der Baustein dient zur Auswertung und Anzeige von Fehlern bei sicherheitsgerichteten E/A-Baugruppen. Mit einem Baustein können bis zu acht Baugruppen überwacht werden. Der Baustein kann mehrfach im Anwenderprogramm eingesetzt werden.

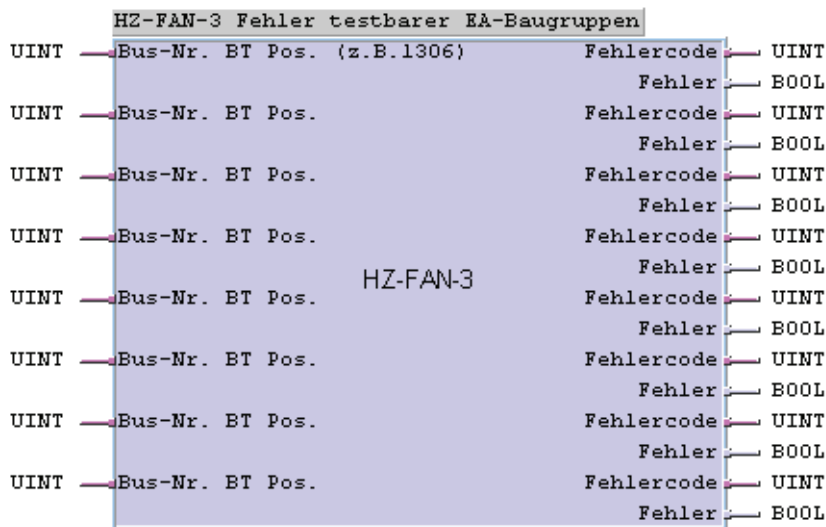


Abbildung 26: Anschlüsse des Bausteins HZ-FAN-3

2.15.1 Eingänge

Bus-Nr. BT Pos. (z. B. 1306) Die Positionen der sicherheitsgerichteten E/A-Baugruppen werden als vierstellige Dezimalzahl eingegeben.
 Beispiel: „1306“ bedeutet:
 Schrank 1, Baugruppenträger 3, Baugruppen-Position 06

2.15.2 Ausgänge

Alle Bausteinausgänge dienen nur zur Information, es dürfen hiervon keine sicherheitsgerichteten Aktionen im Anwenderprogramm abgeleitet werden.

Abbildungsverzeichnis

Abbildung 1:	Prinzipschaltung der Ausgangsbaugruppen mit integrierter Sicherheitsabschaltung (hier mit 4 Ausgangskanälen)	37
Abbildung 2:	Flussdiagramm, Funktion des Sicherheitswerkzeugs	46
Abbildung 3:	Redundante E/A-Baugruppen zur Erhöhung der Verfügbarkeit.	58
Abbildung 4:	Beispiel für einen Funktionsbaustein 1oo2 und Logik des Bausteins . 59	
Abbildung 5:	Verwendung des Bausteins HB-RTE-3	59
Abbildung 6:	Verschaltung redundanter Sensoren	60
Abbildung 7:	Verwendung von Baustein HA-RTE-3 bei F 6213 oder F 6214	60
Abbildung 8:	Vergleichelement zur Alarmierung oder Abschaltung bei Erreichen des zulässigen Grenzwerts	60
Abbildung 9:	Funktionsbaustein 2oo3 und Logik des Bausteins	61
Abbildung 10:	Digitale Anschlüsse von Brandmeldern	65
Abbildung 11:	Verschaltung von Brandmeldern.	65
Abbildung 12:	Anschlüsse des Bausteins H8-STA-3	68
Abbildung 13:	Anschlüsse des Bausteins HA-LIN-3	69
Abbildung 14:	Anschlüsse des Bausteins HA-PID-3	69
Abbildung 15:	Anschlüsse des Bausteins HA-PMU-3	70
Abbildung 16:	Anschlüsse des Bausteins HA-RTE-3.	71
Abbildung 17:	Anschlüsse des Bausteins HB-BLD-3.	72
Abbildung 18:	Anschlüsse des Bausteins HB-BLD-4.	73
Abbildung 19:	Anschlüsse des Bausteins HB-RTE3	74
Abbildung 20:	Anschlüsse des Bausteins HF-AIX-3	76
Abbildung 21:	Anschlüsse des Bausteins HF-CNT-3.	77
Abbildung 22:	Anschlüsse des Bausteins HF-CNT-4.	78
Abbildung 23:	Anschlüsse des Bausteins HF-TMP-3.	79
Abbildung 24:	Anschlüsse des Bausteins HK-LGP-3.	80
Abbildung 25:	Anschlüsse des Bausteins HZ-DOS-3.	80
Abbildung 26:	Anschlüsse des Bausteins HZ-FAN-3.	81

Tabellenverzeichnis

Tabelle 1: Umgebungsbedingungen	10
Tabelle 2: Normen	10
Tabelle 3: Klimatische Bedingungen	11
Tabelle 4: Mechanische Prüfungen	11
Tabelle 5: Prüfungen der Störfestigkeit	12
Tabelle 6: Prüfungen der Störfestigkeit	12
Tabelle 7: Prüfungen der Störaussendung	12
Tabelle 8: Nachprüfung der Eigenschaften der Gleichstromversorgung	12
Tabelle 9: Systembezeichnungen, Sicherheit, Verfügbarkeit und Systemkonfigurationen	16
Tabelle 10: Zentralbaugruppen und Bausätze für die Systeme H41q und H41qc	21
Tabelle 11: Zentralbaugruppen und Bausätze für das System H51q	21
Tabelle 12: Weitere zentrale Baugruppen für die Systeme H41q, H41qc und H51q	22
Tabelle 13: Sicherheit und Verfügbarkeit, Unterschiede H41q, H41qc und H51q	23
Tabelle 14: Selbsttestroutinen	24
Tabelle 15: Eingangsbaugruppen für die Systeme H41q, H41qc und H51q	27
Tabelle 16: Zulässige Steckplätze	28
Tabelle 17: Fehlerreaktion bei sicherheitsgerichteten digitalen Eingangsbaugruppen ..	29
Tabelle 18: Fehlerreaktion bei der sicherheitsgerichteten Zählerbaugruppe F 5220	30
Tabelle 19: Fehlerreaktion bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6213, F 6214	30
Tabelle 20: Fehlerreaktion bei sicherheitsgerichteten analogen Eingangsbaugruppen F 6217	31
Tabelle 21: Fehlerreaktion bei der sicherheitsgerichteten Thermoelementbaugruppe F 6220	32
Tabelle 22: Fehlerreaktion bei der sicherheitsgerichteten analogen Eingangsbaugruppe F 6221	33
Tabelle 23: Ausgangsbaugruppen für die Systeme H41q, H41qc und H51q	35
Tabelle 24: Steckplätze für Ausgangsbaugruppen bei Systemen H41q, H41qc und H51q	36
Tabelle 25: Arten von Variablen in ELOP II	48
Tabelle 26: Standardfunktionsbausteine unabhängig von der E/A-Ebene	50
Tabelle 27: Standardfunktionsbausteine abhängig von der E/A-Ebene	51
Tabelle 28: Sicherheitsgerichtete Parameter	52
Tabelle 29: Einstellung des Parameters <i>Verhalten bei Ausgabefehlern</i>	53
Tabelle 30: Zuordnung von Softwarebausteinen zu E/A-Baugruppen	58



SAFETY
NONSTOP

HIMA Paul Hildebrandt GmbH + Co KG

Industrie-Automatisierung

Postfach 1261 • 68777 Brühl

Telefon: (06202) 709-0 • Fax: (06202) 709-107

E-mail: info@hima.com • Internet: www.hima.de

(1045)