HIMA

SMART SAFETY.

Handbuch

HIQuad®

Sicherheitshandbuch

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

HIQuad®, HIQuad®X, HIMax®, HIMatrix®, SILworX®, XMR®, HICore® und FlexSILon® sind eingetragene Warenzeichen der HIMA Paul Hildebrandt GmbH.

Alle technischen Angaben und Hinweise in diesem Handbuch wurden mit größter Sorgfalt erarbeitet und unter Einschaltung wirksamer Kontrollmaßnahmen zusammengestellt. Bei Fragen bitte direkt an HIMA wenden. Für Anregungen, z. B. welche Informationen noch in das Handbuch aufgenommen werden sollen, ist HIMA dankbar.

Technische Änderungen vorbehalten. Ferner behält sich HIMA vor, Aktualisierungen des schriftlichen Materials ohne vorherige Ankündigungen vorzunehmen.

Alle aktuellen Handbücher können über die E-Mail-Adresse documentation@hima.com angefragt werden.

Kontakt

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Revisions-index	Änderungen	Art der Änderung	
		technisch	redaktionell
1.01	Gelöscht: Maintenance Override, Schutz vor Manipul., abgekünd. Baugruppen. Eingefügt: Automation-Security. Geändert: Zertifizierung, Sicherheitszeiten, Sicherheitsparameter, Reload, Forcen	X	X
1.02	Geändert: Kapitel 1.1 und Kapitel 3.4.7	X	X
2.02	Eingefügt: HIPRO-S V2, Zone 2	X	X
2.03	Geändert: Automation-Security, Reaktion auf festgestellte Fehler bei F 3349	X	X

Inhaltsverzeichnis

1 Einleitung

Dieses Handbuch enthält Informationen für den bestimmungsgemäßen Gebrauch der sicherheitsbezogenen 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 Systeme.
- 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 Systeme 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.

Dieses Sicherheitshandbuch ist die „Originalbetriebsanleitung“ im Sinne der Maschinenrichtlinie (Richtlinie 2006/42/EG).

Die „Originaldokumentation“ für das HIMA System ist in deutscher Sprache verfasst. Es gelten die Aussagen der deutschsprachigen Dokumentation.

1.1 Gültigkeit und Aktualität

Auch für ältere Versionen des Betriebssystems gilt jeweils die neueste Fassung dieses Sicherheitshandbuchs, die durch die höchste Revisionsnummer gekennzeichnet ist. Besonderheiten einzelner Versionen sind im Text erwähnt.

Die aktuelle Fassung ist auf der aktuellen HIMA DVD erhältlich oder kann von der HIMA-Website unter www.hima.de oder www.hima.com heruntergeladen werden.

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projekteure, Programmierer und Personen, die zur Inbetriebnahme, zur Wartung und zum Betreiben von Automatisierungsanlagen berechtigt sind. Vorausgesetzt werden spezielle Kenntnisse auf dem Gebiet der sicherheitsbezogenen Automatisierungssysteme.

1.3 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, die angeklickt werden können.
Kursiv	Parameter und Systemvariablen, Referenzen.
`Courier`	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen (Großbuchstaben).
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Im elektronischen Dokument (PDF): Wird der Mauszeiger auf einen Hyperlink positioniert, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.3.1 Sicherheitshinweise

Um ein möglichst geringes Risiko zu gewährleisten, sind die Sicherheitshinweise unbedingt zu befolgen.

Die Sicherheitshinweise im Dokument sind wie folgt dargestellt.

- Signalwort: Warnung, Vorsicht, Hinweis.
- Art und Quelle des Risikos.
- Folgen bei Nichtbeachtung.
- Vermeidung des Risikos.

Die Bedeutung der Signalworte ist:

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

⚠ SIGNALWORT

Art und Quelle des Risikos!
Folgen bei Nichtbeachtung.
Vermeidung des Risikos.

HINWEIS

Art und Quelle des Schadens!
Vermeidung des Schadens.

1.3.2 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.

1.4 Restrisiken

Von einem HIMA System selbst geht kein Risiko aus.

Restrisiken können ausgehen von:

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

2 Hinweise zum Einsatz von H41q/H51q Systemen

Die Sicherheitsinformationen, Hinweise und Anweisungen in diesem Handbuch unbedingt lesen. Das Produkt nur unter Beachtung aller Richtlinien und Sicherheitsrichtlinien einsetzen.

2.1 Bestimmungsgemäßer Einsatz

2.1.1 Anwendungsgebiet

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

Alle Eingangs- und Ausgangsbaugruppen sind sowohl bei redundanter als auch bei einkanaliger Ausführung der Zentralbaugruppen einsetzbar.

Bei der Verwendung der sicherheitsbezogenen Kommunikation zwischen verschiedenen Systemen muss beachtet werden, dass die Gesamt-Reaktionszeit des Systems nicht die Prozess-Sicherheitszeit 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.

2.1.1.1 Anwendung im Ruhestromprinzip

Die Automatisierungsgeräte sind für das Ruhestromprinzip konzipiert.

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

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

2.1.1.2 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 EN 54 und NFPA 72 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.

2.1.1.3 Explosionsschutz

Die sicherheitsbezogenen Automatisierungsgeräte H41q 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!

2.1.1.4 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!

2.1.2 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 Feldbus-Schnittstellen ist ohne sicherheitsbezogene Feldbus-Protokolle keine sicherheitsbezogene Kommunikation möglich.

2.2 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.

2.3 ESD-Schutzmaßnahmen

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

HINWEIS

Elektrostatische Entladung!

Nichtbeachtung kann zu Schäden an elektronischen Bauelementen führen.

- **Vor Arbeit mit HIMA Komponenten geerdetes Objekt berühren.**
- **Antistatisch gesicherten Arbeitsplatz benutzen und Erdungsband tragen.**
- **Komponenten 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.

3 Sicherheitskonzept für den Einsatz der PES

3.1 Sicherheit und Verfügbarkeit

Bereits als Monosysteme sind die Systemfamilien H41q 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.

3.1.1 Sicherheit

Für die sicherheitsbezogenen Systeme H41q 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}...10^{-3}
- eine PFH von 10^{-8}...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 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.

3.1.2 Übersicht

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

Systembezeichnung	H41q-MS H51q MS	H41q-HS H51q HS	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 7.8.3) 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 1: 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 für den Austausch von Baugruppen erhalten.
- Nach Austausch einer Baugruppe muss diese automatisch in Betrieb gehen.

Die HIMA Automatisierungssysteme in den entsprechenden Konfigurationen erfüllen diese Forderungen.

Für die Programmierung der Systeme wird ein PADT (Programmiergerät, PC) mit dem Programmierwerkzeug **ELOP II** nach IEC 61131-3 verwendet. Es bietet Unterstützung bei der Erstellung sicherheitsbezogener Programme und der Bedienung der Automatisierungsgeräte.

3.2 Sicherheitszeiten

Einzelfehler, die zu einem gefährlichen Betriebszustand führen können, werden durch die Selbsttesteinrichtungen innerhalb der Sicherheitszeit (≥ 1 s) erkannt.

- Prozess-Sicherheitszeit

  Prozesstechnische 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 Tests erkannt.

  Bei den Tests werden unterschieden:
  - Tests innerhalb der Sicherheitszeit

    Sie werden innerhalb der Sicherheitszeit durchgeführt (Vordergrundtests),

    Reaktionszeit: sofort, spätestens innerhalb der Sicherheitszeit.
  - Hintergrundtests

    Sie sind in viele Zyklen aufgeteilt,

    Die Reaktion erfolgt bei Erkennen eines Fehlers sofort, spätestens innerhalb einer Zeit, die durch den 3600-fachen Wert der Sicherheitszeit bestimmt ist.

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

  Die Fehlerreaktionszeit eines Automatisierungsgeräts entspricht der Sicherheitszeit (≥ 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 ms / 2 = 50 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 ms / 4 = 25 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…254 s ist zulässig!

3.3 Wiederholungsprüfung (Proof-Test nach IEC 61508)

Ziel der Wiederholungsprüfung ist die Aufdeckung versteckter gefahrbringender Ausfälle in einem sicherheitsbezogenen System, so dass das System, wenn nötig, wieder in den Zustand gebracht werden kann, indem es seine geplante Funktion erfüllt. Danach ist der sichere Betrieb einschließlich der Sicherheitsfunktionen wieder gewährleistet.

Die Durchführung der Wiederholungsprüfung ist abhängig von:

- Der Beschaffenheit der Anlage (EUC = equipment under control).
- Dem Risikopotenzial der Anlage.
- Den Normen, die für den Betrieb der Anlage zur Anwendung kommen.
- Den Normen, die von der Prüfstelle als Grundlage für die Genehmigung der Anlage benutzt wurden.

Nach den Normen IEC 61508 1-7, IEC 61511 1-3, IEC 62061 und VDI/VDE 2180 Blatt 1 bis 4 hat bei sicherheitsbezogenen Systemen der Betreiber für eine Wiederholungsprüfung zu sorgen. Bei einer Wiederholungsprüfung müssen die kompletten Sicherheitsfunktionen des sicherheitsbezogenen HIMA Systems überprüft werden.

HIMA Sicherheitssysteme sind in regelmäßigen Abständen einer Wiederholungsprüfung zu unterziehen. Für HIMA Steuerungen muss die Wiederholungsprüfung in einem Intervall erfolgen, welches dem applikationsspezifisch notwendigen Safety Integrity Level (SIL) entspricht.

Die Durchführung der Wiederholungsprüfung ist im Wartungshandbuch HI 800 438 D beschrieben.

3.4 Sicherheitsauflagen

Für den Einsatz der sicherheitsbezogenen Steuerungen der Systeme H41q und H51q gelten folgende Sicherheitsauflagen

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

3.4.1 Hardware-Projektierung: produktunabhängige Auflagen

Für den sicherheitsbezogenen Betrieb dürfen nur hierfür zugelassene fehlersichere Hardware-Baugruppen und Software-Komponenten verwendet werden. Die zugelassenen Hardware-Baugruppen und Software-Komponenten sind aufgeführt in dem gemeinsamen Dokument *Versionsliste der Baugruppen und der Firmware der H41q/H51q Systeme der HIMA Paul Hildebrandt GmbH*.

- 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 3.5.1) 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.

3.4.2 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 sind Netzteile in den Ausführungen PELV oder SELV einzusetzen.

3.4.3 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.

3.4.4 Programmierung: produktabhängige Auflagen

- Die Fehlerreaktion des Systems bei Fehlern in den fehlersicheren Eingangs- 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.

3.4.5 Kommunikation: produktabhängige Auflagen

- Bei der Verwendung der sicherheitsbezogenen Kommunikation zwischen verschiedenen Systemen ist zu beachten, dass die Gesamtreaktionszeit des Systems nicht die Prozess-Sicherheitszeit 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.

3.4.6 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 Prozess-Sicherheitszeit nicht überschreiten.
- 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.

3.4.7 Automation-Security

Industrielle Steuerungen müssen in ausreichendem Maß gegen Manipulation geschützt werden. Die Anforderungen der relevanten Normen, Richtlinien und Gesetze bezüglich des Schutzes vor Manipulationen sind zu beachten.

⚠ WARNUNG

Personenschaden durch unbefugte Manipulation an der Steuerung möglich!

Die Steuerung ist gegen unbefugte Zugriffe zu schützen!

Eine Risikoanalyse sollte die erforderlichen Maßnahmen ermitteln. Die benötigten Maßnahmen sind sorgfältig zu planen, zu ergreifen und müssen über den gesamten Lebenszyklus aktualisiert werden.

Die Einhaltung der notwendigen Schutzmaßnahmen unterliegen der Verantwortung des Betreibers.

Weitere Einzelheiten siehe HIMA Automation-Security Handbuch HI 801 372 D.

3.5 Zertifizierung

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

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

Zertifikat und Prüfbericht

Sicherheitsbezogene Automatisierungsgeräte

H41q-MS, H41q-HS, H41q-HRS

H51q-MS, H51q-HS, H51q-HRS

Die sicherheitsbezogen Automatisierungsgeräte der Systemfamilien H41q und H51q sind nach den im Folgenden aufgelisteten wichtigen Normen für die funktionale Sicherheit geprüft und zertifiziert:

IEC 61508, Teile 1-7: 2010	bis SIL 3
IEC 61511, Teile 1-3: 2004	bis SIL 3
EN 62061: 2005 +AC:2010 +A1: 2013 + A2:2015	
EN/ISO 13849-1: 2008 + AC: 2009	Kategorie 4, Performance Level e
EN 50156-1: 2015	
EN 12067-2: 2004	
EN 298: 2012	
NFPA 85: 2015	
NFPA 86: 2015	
EN 61131-2: 2007	
EN 61000-6-2: 2005	
EN 61000-6-4: 2007 + A1:2011	
EN 54-2:1997 + AC:1999 + A1: 2006	
NFPA 72: 2016	
EN 50130-4: 2011 + A1: 2014	

Das Kapitel 3.5.1 enthält eine detaillierte Aufstellung aller durchgeführten Umwelt- und EMV-Prüfungen.

3.5.1 Prüfbedingungen

3.5.1.1 Umgebungsbedingungen und technische Daten

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

Art der Bedingung	Inhalt der Bedingung
Schutzklasse	Schutzklasse II nach EN 61131-2
Umgebungs-temperatur	0...+60 °C
Lagertemperatur	-40...+80 °C (mit Batterie: nur -30...+75 °C)
Verschmutzung	Verschmutzungsgrad II
Aufstellhöhe	< 2000 m
Gehäuse	Standard: IP20 Falls es die zutreffenden Applikationsnormen (z. B. EN 60204) fordern, muss das System in ein Gehäuse der geforderten Schutzart (z. B. IP54) eingebaut werden.
Eingangsspannung Netzteil	24 VDC

Tabelle 2: Umgebungsbedingungen

Diverse Abweichungen sind dem entsprechenden Datenblatt zu entnehmen.

Die sicherheitsbezogenen Steuerungssysteme H41q/H51q wurden für die Einhaltung der Anforderungen der folgenden Normen für EMV, Klima und Umweltanforderungen entwickelt.

Norm	Inhalt
EN 61131-2: 2007	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: 2007	Elektromagnetische Verträglichkeit (EMV) Fachgrundnorm Störaussendung, Industriebereich

Tabelle 3: Normen

3.5.1.2 Klimatische Prüfungen

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

EN 61131-2	Klimaprüfungen
	Trockene Wärme und Kälte; Beständigkeitsprüfungen: +70 °C / -40 °C, 16 h, +85 °C, 1 h Stromversorgung nicht angeschlossen
	Temperaturwechsel; Beständigkeitsprüfung: Schneller Temperaturwechsel: -40 °C / +70 °C, Stromversorgung nicht angeschlossen
	Unempfindlichkeitsprüfung Langsamer Temperaturwechsel: -10 °C / +70 °C, Stromversorgung angeschlossen
	Zyklen mit feuchter Wärme; Beständigkeitsprüfungen: +25 °C / +55 °C, 95 % relative Feuchte, Stromversorgung nicht angeschlossen
EN 54-2	Feuchte Wärme 93 % relative Feuchte, 40 °C, 4 Tage in Betrieb 93 % relative Feuchte, 40 °C, 21 Tage, Stromversorgung nicht angeschlossen

Tabelle 4: Klimatische Bedingungen

3.5.1.3 Mechanische Prüfungen

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

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

Tabelle 5: Mechanische Prüfungen

3.5.1.4 EMV-Prüfungen

Eingehaltene Prüfbedingungen siehe EG-Konformitätserklärung.

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 sicherheitsbezogen.

3.5.1.5 Spannungsversorgung

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

EN 61131-2:	Nachprüfung der Eigenschaften der Gleichstromversorgung
	Das Netzgerät muss alternativ die folgenden Normen erfüllen: ▪ EN 61131-2 oder ▪ SELV (Safety Extra Low Voltage, EN 60950) oder ▪ PELV (Protective Extra Low Voltage, EN 60742)
	Die Absicherung der Systeme H41q/H51q muss gemäß den Angaben in den Datenblättern erfolgen.
	Prüfung des Spannungsbereichs: 24 VDC, -20...+25 % (19,2...30,0 VDC)
	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 6: Nachprüfung der Eigenschaften der Gleichstromversorgung

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

Baugruppe/ Bausatz	Bezeichnung	sicherheitsbezogen	rückwirkungsfrei
F 8652X	Zentralbaugruppe, Doppelprozessor 1oo2	•	•
B 4235	Bausatz Zentralgerät H41q-MS	•	•
B 4237-1	Bausatz Zentralgerät H41q-HS	•	•
B 4237-2	Bausatz Zentralgerät H41q-HRS	•	•

Tabelle 7: Zentralbaugruppen und Bausätze für die Systeme H41q

4.2 Zentralbaugruppen und Bausätze für das System H51q

Baugruppe/ Bausatz	Bezeichnung	sicherheitsbezogen	rückwirkungsfrei
F 8650X	Zentralbaugruppe, Doppelprozessor 1oo2	•	•
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 8: Zentralbaugruppen und Bausätze für die Systeme H51q

4.3 Weitere zentrale Baugruppen für die Systeme H41q und H51q

Baugruppe/ Bausatz	Bezeichnung	sicherheitsbezogen	rückwirkungsfrei
Stromverteilerbaugruppen			
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 8627X	Ethernet		•
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)		•
H 7506	Busanschlussklemme zum Aufbau von 2-Draht-Bussen		•

Tabelle 9: Zentralbaugruppen und Bausätze für die Systeme H51q

4.4 Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsbezogenen Zentralbaugruppen

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

Systeme H41q	System H51q
Im Systembaugruppenträger H41q sind einsetzbar: ▪ 2 Zentralbaugruppen ▪ 12 E/A-Baugruppen ▪ 2 Stromversorgungsbaugruppen ▪ 2 Sicherungsbaugruppen	Im Zentralbaugruppenträger sind einsteckbar: ▪ 2 Zentralbaugruppen ▪ pro Zentralbaugruppe 3 Coprozessorbaugruppen F 8621/A oder 5 Kommunikationsbaugruppen F 8627X, F 8628X

Tabelle 10: Unterschiede H41q und H51q

4.4.1 Netzgeräte

In sicherheitstechnischen Anwendungen ist immer ein Netzgerät 24 VDC / 5 VDC 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 sicherheitsbezogenen Zentralbaugruppen F 8652X/F 8650X

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

- zwei taktsynchrone 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 als Programmspeicher für Betriebssystem und Anwenderprogramm geeignet für min. 100 000 Speicherzyklen
- Datenspeicher in SRAM (statisches RAM)
- Multiplexer zum Anschluss von E/A-Bus, Dual-ported RAM (DPR) und redundanter Zentralbaugruppe
- Pufferung der SRAMs über Batterien auf der Zentralbaugruppe
- 2 Schnittstellen RS485 mit galvanischer Trennung, Übertragungsrate: max. 57600 bps; Einstellung auf 9600 bps und 57600 bps per Schalter oder Einstellung (auch anderer Übertragungsraten) per Software, wobei Software-Werte 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 (Systemspannung: 5 V)
- Batterieüberwachung

4.5 Prinzipielle Arbeitsweise von sicherheitsbezogenen Zentralbaugruppen

Sicherheitsbezogene 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 Selbst-Testroutinen, die immer wieder durchlaufen werden. Der Watchdog überwacht den Programmablauf.

4.5.1 Selbst-Testroutinen

In der Tabelle 11 sind die Selbst-Testroutinen der sicherheitsbezogenen Zentralbaugruppen F 8650X und F 8652X und der Ankopplung an die E/A-Ebene erläutert

Test	Beschreibung
CPU-Test	Geprüft werden: ▪ 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 Hardware-Vergleicher 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 Hardware-Vergleicher zwischen den beiden Speichern (direkt und invers) einen Unterschied feststellt. Durch einen weiteren Test wird die Abschaltbarkeit des Watchdog-Signals geprüft.
Test der Verbindung zur E/A-Ebene innerhalb der Zentralbaugruppe	Bei redundanten Zentralbaugruppen in Systemen H41q-HS und 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 Verbindungsbau-gruppe innerhalb der E/A-Baugruppenträger	Die Adressierung wird zyklisch nach jeder Bearbeitung einer sicherheitsbezogenen 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 11: Selbst-Testroutinen

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 Gesamtabschaltung 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 (05.34)) wird auch das Anwenderprogramm selbst von der noch laufenden Zentralbaugruppe in

die neue, «leere» Zentralbaugruppe geladen (self-education). Zu Einzelheiten siehe das Betriebssystem-Handbuch HI 800 104 D.

4.5.3 Diagnoseanzeige

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

- einer 4-stelligen alphanumerischen Anzeige für Texte und Werte
- einer LED *CPU* zur Anzeige von Zentralbaugruppenfehlern
- einer LED *IO* zur allgemeinen Fehleranzeige sicherheitsbezogener 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 4-stellige Anzeige zeigt STOP an. Es ist möglich, durch eine Bedienaktion den Fehlercode anzuzeigen. Eine Liste der Fehlercodes befindet sich im Betriebssystem-Handbuch HI 800 104 D.

Bei Fehlern von sicherheitsbezogenen Baugruppen in der E/A-Ebene leuchtet die LED *IO*. Die 4-stellige 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. Beim Hochfahren werden die Retain-Variablen 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

Baugruppe	Bezeichnung	Sicherheits-gerichtet	Rückwirkungs-frei	(Ex)i	Zugehöriger SW-Baustein
Digitale Eingangsbaugruppen					
F 3221	Eingangsbaugruppe, 16 Kanäle		•		
F 3222[1)]	Eingangsbaugruppe, 8 Kanäle		•		
F 3223	Eingangsbaugruppe, 4 Kanäle		•	•	
F 3224A	Eingangsbaugruppe, 4 Kanäle		•	•	
F 3236	Eingangsbaugruppe, 16 Kanäle	•	•		
F 3237	Eingangsbaugruppe, 8 Kanäle	•	•		HB-RTE-3
F 3238	Eingangsbaugruppe, 8 Kanäle	•	•	•	HB-RTE-3
F 3240	Eingangsbaugruppe, 8 Kanäle	•	•		
F 3248	Eingangsbaugruppe, 16 Kanäle	•	•		
F 5220	Zählerbaugruppe, 2 Kanäle	•	•		HF-CNT-3, -4
Analoge Eingangsbaugruppen					
F 6213[1)]	Eingangsbaugruppe, 4 Kanäle	•	•		HA-RTE-3
F 6214[1)]	Eingangsbaugruppe, 4 Kanäle	•	•		HA-RTE-3
F 6215	Eingangsbaugruppe, 8 Kanäle		•		
F 6217	Eingangsbaugruppe, 8 Kanäle	•	•		
F 6220	Thermoelement-Eingangsbaugruppe, 8 Kanäle	•	•	•	HF-TMP-3
F 6221	Eingangsbaugruppe, 8 Kanäle	•	•	•	HF-AIX-3
[1)] abgekündigte Baugruppe, nicht mehr lieferbar					

Tabelle 12: Übersicht über die Eingangsbaugruppen für die Systeme H41q und H51q

Die Anwendungsbereiche der Eingangsbaugruppen sind im HIQuad Betriebssystem Handbuch (HI 800 104 D) aufgeführt.

5.1 Sicherheit und Verfügbarkeit von sicherheitsbezogenen Eingangsbaugruppen

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

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

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

Sicherheitsbezogene Eingangsbaugruppen werden in den Systemen H41q und H51q während des Betriebes automatisch einem hochwertigen, zyklischen Selbsttest unterzogen. Die Eingangsbaugruppen enthalten Schaltungsteile, die einen Test der Eingangsbaugruppen-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 sicherheitsbezogene Reaktion des Systems herbei. Die Fehlermeldungen sind eine Diagnoseinformation für den Betreiber. Bei der Planung und Realisierung der Anlage kann somit flexibel ein Diagnosesystem erstellt werden.

Zur Erhöhung der Verfügbarkeit sind die sicherheitsbezogenen Eingangsbaugruppen auch redundant einsetzbar.

Der Einsatz redundanter Eingangsbaugruppen beeinträchtigt die Sicherheit des Systems nicht.

Sicherheitsbezogene Eingangsbaugruppen können sowohl für sicherheitsbezogene als auch für nicht sicherheitsbezogene Signale benutzt werden.

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

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

Tabelle 13: Zulässige Steckplätze

5.1.1 Sicherheit von Sensoren, Gebern, Transmittern

Sicherheitsbezogene 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 Betriebssystem-Handbuch 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 Norm IEC 61508 werden durch die Festlegung von Offline-Proof-Test-Intervallen entsprechende sicherheitstechnische Nachweise ermöglicht. Die Festlegungen im Detail sind hierzu anwendungsspezifisch zu definieren.

5.2 Sicherheitsbezogene digitale Eingangsbaugruppen F 3236, F 3237, F 3238, F 3240 und F 3248

5.2.1 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 sicherheitsbezogener Initiator angeschlossen werden. Durch die Selbsttests werden alle Anforderungen an die Erkennung der Schwellen der sicherheitsbezogenen Initiatoren erfüllt.

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

5.2.2 Reaktion auf festgestellte Fehler bei F 3236, F 3237, F 3238, F 3240 und F 3248

Fehlerart	Systemreaktion	Bemerkung
Baugruppen-defekt (Eingangsbau-gruppe)	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 sicherheitsbezogenen Eingängen ist dieses Signal mit dem Software-Baustein 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 sicherheitsbezogenen Eingängen ist dieses Signal mit dem Software-Baustein 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 Leitungsbruch und Kurzschluss des Geberkreises zeigt die Diagnoseanzeige neben der Baugruppenposition auch den fehlerhaften Kanal der Baugruppe an.	

Tabelle 14: Fehlerreaktion bei sicherheitsbezogenen digitalen Eingangsbaugruppen

5.3 Sicherheitsbezogene Zählerbaugruppe F 5220

Die zweikanalige Zählerbaugruppe hat ein eigenes Doppel-Prozessorsystem mit einem sicherheitsbezogenen Ausgang pro Kanal. Sie ist zur Impulszählung, 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!

5.3.1 Testroutinen

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

5.3.2 Reaktionen auf festgestellte Fehler

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

Tabelle 15: Fehlerreaktion bei der sicherheitsbezogenen Zählerbaugruppe F 5220

5.4 Sicherheitsbezogene analoge Eingangsbaugruppen F 6213, F 6214 und F 6217

Bei Redundanz von sicherheitsbezogenen 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.

5.4.1 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.

5.4.2 Reaktionen auf festgestellte Fehler bei F 6213 und F 6214

Fehlerart	Systemreaktion im Fehlerfall	Bemerkung
Baugruppen- oder Kanalfehler bei einkanaligen analogen Eingängen	Verarbeitung des konfigurierten Wertes am Software-Baustein HA-RTE-3 (siehe 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 Software-Baustein HA-RTE-3 (siehe Anhang)
Kurzschluss im Transmitterkreis	Anzeige der Baugruppenposition und des fehlerhaften Kanals auf der Diagnoseanzeige	nur bei Einsatz 4...20 mA

Tabelle 16: Fehlerreaktion bei sicherheitsbezogenen analogen Eingangsbaugruppen F 6213, F 6214

5.4.3 Reaktionen auf festgestellte Fehler bei F 6217

Fehlerart	Systemreaktion im Fehlerfall	Bemerkung
Kanalfehler	Analogwert = 0000 Kanalfehler-Bit = TRUE	Kanalfehler-Bit ist im Anwenderprogramm sicherheitsbezogen zu verarbeiten
Baugruppenfehler	Alle Analogwerte = 0000 Alle Kanalfehler-Bits = TRUE	Siehe Kanalfehler, betrifft alle Kanalfehler-Bits
Überschreiten des Messbereichs (22 mA)	Max. Analogwert = 4095 Kanalfehler-Bit = TRUE	Max. zulässiger Wert ist im Anwenderprogramm zu definieren.

Tabelle 17: Fehlerreaktion bei sicherheitsbezogenen analogen Eingangsbaugruppen F 6217

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

⚠ WARNUNG

Warnung! Personenschaden durch fehlerhaften Messwert möglich!

Für jeden sicherheitsbezogenen Analogeingang ist eine sicherheitsbezogene Reaktion bei gesetztem Kanalfehler-Bit zu programmieren.

5.5 Sicherheitsbezogene 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 Vergleichstemperatur-Eingang. Sie hat ein eigenes Doppel-Prozessorsystem und wird über den Software-Baustein HF-TMP-3 (siehe Kapitel 10.2.9 und die Online-Hilfe ELOP II) für jeden belegten Kanal parametriert.

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

5.5.1 Testroutinen

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

5.5.2 Reaktionen auf festgestellte Fehler bei F 6220

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

Tabelle 18: Fehlerreaktion bei der sicherheitsbezogenen Thermoelementbaugruppe F 6220

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

5.5.3 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.

5.6 Sicherheitsbezogene analoge eigensichere Eingangsbaugruppe F 6221

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

Jeder belegte Kanal wird über einen eigenen Software-Baustein HF-AIX-3 parametriert.

5.6.1 Testroutinen

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

5.6.2 Reaktionen auf festgestellte Fehler bei F 6221

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

Tabelle 19: Fehlerreaktion bei der sicherheitsbezogenen analogen Eingangsbaugruppe F 6221

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

5.6.3 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.

5.7 Hinweis zum Austausch von Eingangsbaugruppen

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

Eingangsbaugruppe austauschen

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.

► Die Eingangsbaugruppe ist ausgetauscht

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

5.8 Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Eingangsbaugruppen

Für jede einzelne der in einem System eingesetzten sicherheitsbezogenen Eingangsbaugruppen ist im Rahmen der Projektierung oder 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 auf der HIMA DVD und im Internet unter www.hima.de und www.hima.com erhältlich:

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

6 Ausgangsbaugruppen

Baugruppe	Bezeichnung	sicherheits bezogen	rückwirkungsfrei	Belastbar keit	Zugehöriger SW-Baustein
Digitale Ausgangsbaugruppen					
F 3322	Digitale Ausgangsbaugruppe, 16 Kanäle		•	≤ 0,5 A	
F 3325	Speisebaugruppe (Ex), 6 Kanäle		•	22 V ≤ 0,02 A	
F 3330	Digitale Ausgangsbaugruppe, 8 Kanäle	•	•	≤ 0,5 A	
F 3331	Digitale Ausgangsbaugruppe, 8 Kanäle	•	•	≤ 0,5 A	HB-BLD-3[1], HB-BLD-4[1]
F 3333	Digitale Ausgangsbaugruppe, 4 Kanäle	•	•	≤ 2 A	
F 3334	Digitale Ausgangsbaugruppe, 4 Kanäle	•	•	≤ 2 A	HB-BLD-3[1], HB-BLD-4[1]
F 3335	Digitale Ausgangsbaugruppe (Ex), 4 Kanäle	•	•	22 V ≤ 0,053 A	
F 3348 [4]	Digitale Ausgangsbaugruppe, 8 Kanäle	•	•	≤ 0,5 A 48 VDC	
F 3349	Digitale Ausgangsbaugruppe, 8 Kanäle	•	•	≤ 0,5 A ≤ 48 V	HB-BLD-3[1], HB-BLD-4[1]
F 3422	Digitale Relaisbaugruppe, 8 Kanäle		•	≤ 2 A ≤ 60 V	
F 3430[2]	Digitale Relaisbaugruppe	•	•	≤ 4 A ≤ 250 V	
Analoge Ausgangsbaugruppen					
F 6705	Analoge Ausgangsbaugruppe, 2 Kanäle	•	•	0...20 mA	HZ-FAN-3[3]
F 6706	Analoge Ausgangsbaugruppe, 2 Kanäle		•	0...20 mA	

[1] Zur Fehleranzeige und Parametrierung der Betriebsarten (Ruhestrom, Arbeitsstrom).

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

[3] Notwendig im Stromsenkenbetrieb zur Fehlerauswertung.

[4] Abgekündigte Baugruppe, nicht mehr lieferbar.

Tabelle 20: Übersicht über die Ausgangsbaugruppen für die Systeme H41q und H51q

Die Anwendungsbereiche der Ausgangsbaugruppen sind im HIQuad Betriebssystem Handbuch (HI 800 104 D) aufgeführt.

6.1 Allgemeines zur Sicherheit und Verfügbarkeit von sicherheitsbezogenen Ausgangsbaugruppen

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

Zusätzlich wird im Hintergrund ein Walking-Bit-Test über alle Ausgänge durchgeführt. Dabei steht das Testsignal für die Dauer von max. 250 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.

Sicherheitsbezogene 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 sicherheitsbezogenen Stromkreisen verwendet wird. Das Ausgangssignal ist in allen Anwendungen für Sicherheitsanforderungen bis SIL 3 einsetzbar.

System H41q	System H51q
Die Ausgangsbaugruppen werden in den Systembaugruppenträger gesteckt. Es stehen Bausätze mit 12 Steckplätzen (H41q) 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 4.2).
Steckplätze für Ausgangsbaugruppen bei Systemen H41q und H51q	Steckplätze für Ausgangsbaugruppen bei Systemen H41q und H51q

Tabelle 21: Steckplätze für Ausgangsbaugruppen bei Systemen H41q und H51q

6.1.1 Sicherheitsbezogene 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 Software-Baustein 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 Gesamtabschaltung der Steuerung konfiguriert werden.

6.1.2 Sicherheitsbezogene analoge Ausgangsbaugruppen

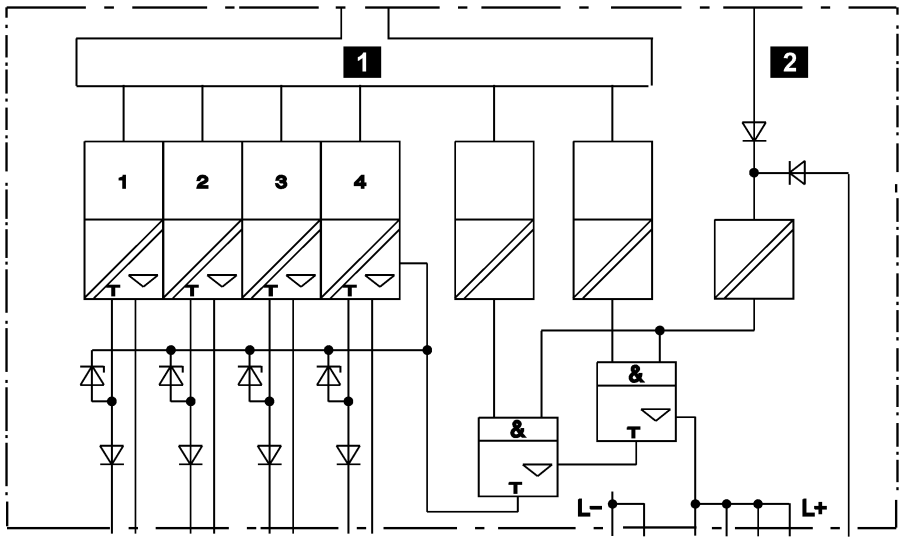
Die sicherheitsbezogenen analogen Ausgangsbaugruppen sind im Stromquellenbetrieb oder im Stromsenkenbetrieb einsetzbar.

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 Software-Baustein HZ-FAN-3 zu verwenden.

6.2 Prinzipielle Arbeitsweise von sicherheitsbezogenen Ausgangsbaugruppen

In den sicherheitsbezogenen 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).



1 E/A-Bus **2** Watchdog-Signal (WD)

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

6.3 Sicherheitsbezogene digitale Ausgangsbaugruppen F 3330, F 3331, F 3333, F 3334, F 3335, F 3349

6.3.1 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 ≤ 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 Hintergrundtests.
4. Lesen der Leitungsdiagnose aller Kanäle (nur bei F 3331, F 3334 und F 3349).
5. Prüfen der integrierten Sicherheitsabschaltung.

6.3.2 Reaktion auf festgestellte Fehler bei F 3330, F 3331, F 3333, F 3334, F 3335

- Alle auf der Baugruppe erkannten Fehler führen dazu, dass die Baugruppe in den sicheren, energielosen Zustand gebracht, d. h. abgeschaltet wird.
- Externe Kurzschlüsse, die nicht von internen Fehlern unterscheidbar sind, führen zur Abschaltung der Baugruppe.
- Leitungsfehler werden nur gemeldet und führen nicht zur Abschaltung.

6.3.3 Reaktion auf festgestellte Fehler bei F 3349

- Alle auf der Baugruppe erkannten Fehler führen dazu, dass die Baugruppe in den sicheren, energielosen Zustand gebracht, d. h. abgeschaltet wird.
- Nach externem Leitungsbruch oder Leitungsschluss wird der betroffene Kanal abgeschaltet und nach ca. 4,5 s wieder zugeschaltet, wenn der Leitungsbruch oder Leitungsschluss nicht mehr ansteht.

6.3.4 Hinweis zur Projektierung F 3330, F 3331, F 3333, F 3334

Vor dem Löschen der Baugruppen F 3330, F 3331, F 3333, F 3334 aus der Projektkonfiguration sind die Ausgänge zurückzusetzen! Zum Beispiel ist für Ausgänge, die auf 1-Signal geforcet sind, das Forcen zu beenden.

6.3.5 Hinweise zur Projektierung F 3349

Externer Kurzschlusse an einem Kanal führen nicht zum Ansprechen der integrierten Sicherheitsabschaltung. Die übrigen Kanäle bleiben aktiv.

6.4 Sicherheitsbezogene digitale Relaisbaugruppe F 3430

6.4.1 Testroutinen

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

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

6.4.2 Reaktion auf festgestellte Fehler bei sicherheitsbezogenen 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.

6.4.3 Hinweis zur Projektierung

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 VDC und 4 A.

Zur Einhaltung der Anforderungen gemäß IEC 61508 (PFD/PFH, siehe Kapitel 3.1.1) gilt ein Offline-Proof-Test-Intervall von 5 Jahren bei SIL-3-Anwendungen und von 20 Jahren bei SIL-2-Anwendungen.

Die notwendigen Prüfungen werden beim Hersteller HIMA durchgeführt.

6.5 Sicherheitsbezogene analoge Ausgangsbaugruppe F 6705

6.5.1 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.

6.5.2 Reaktionen auf festgestellte Fehler bei F 6705

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 Software-Baustein HZ-FAN-3 zur Fehlerauswertung zu verwenden.

6.6 Hinweis zum Austauschen 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.

6.7 Checklisten zur Projektierung, Programmierung und Inbetriebnahme von sicherheitsbezogenen Ausgangsbaugruppen

Für jede einzelne der in einem System eingesetzten sicherheitsbezogenen Ausgangsbaugruppen ist im Rahmen der Projektierung oder 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 auf der HIMA DVD und im Internet unter www.hima.de und www.hima.com erhältlich.

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

7 Software

Die Software für sicherheitsbezogene HIMA Automatisierungsgeräte der Systemfamilien H41q 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 sicherheitsbezogene Anwendungen zertifizierten Form anzuwenden. Die jeweils gültige Version ist dem gemeinsamen Dokument *Versionsliste der Baugruppen und der Firmware der H41q/H51q Systeme der HIMA Paul Hildebrandt GmbH* 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 und die übrige Projektkonfiguration über eine serielle Schnittstelle oder Ethernet in die Flash-EPROMs in der Zentralbaugruppe.

Die wesentlichen Funktionen des Betriebssystems und die daraus abgeleiteten Vorgaben für das Anwenderprogramm sind im Betriebssystem-Handbuch HI 800 104 D beschrieben.

7.1 Sicherheitstechnische Aspekte für das Betriebssystem

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

7.1.1 Kennzeichnung der aktuell 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.

7.1.2 Arbeitsweise und Funktionen des Betriebssystems

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

1. Lesen der Eingangsdaten (Hardware-Eingänge)
2. Bearbeiten der Logikfunktionen gemäß IEC 61131-3, Abschnitt 4.1.3
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 erstellt. 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, NOT-AUS 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 Anwenderprogramme 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 sicherheitsbezogenen 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 werden können.

Nicht sicherheitsbezogene Hilfsmittel sind:

- Die in ELOP II integrierte Revisionsverwaltung. Sie ist zur eindeutigen Identifizierung der relevanten Projektversionen nutzbar.
- Die in dem Fluss-Diagramm Bild 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

Im Flussdiagramm Bild 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 oder entsprechender Anwendernorm), im Flussdiagramm 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.

⚠ WARNUNG

Personenschaden durch Fehlfunktion möglich!

Für das Anwenderprogramm ist eine Querverweisliste 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). Der Compiler erzeugt den Zielcode und den Vergleichscode.

⚠ WARNUNG

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 Programmänderung

1. Modifikation des Anwenderprogramms nach einer verbindlichen Spezifikation (z. B. nach IEC 61508 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, 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, 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.

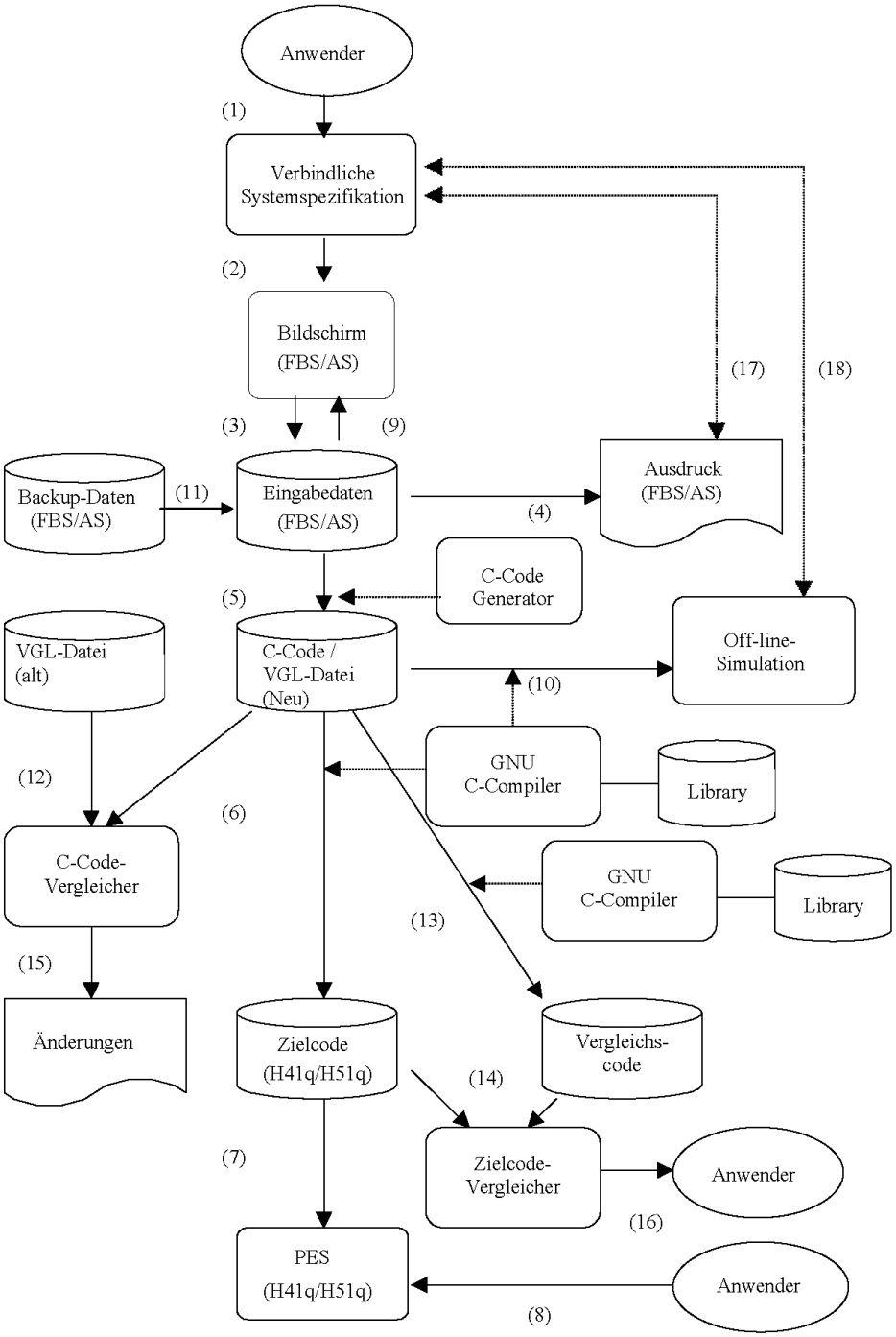


Bild 2: Flussdiagramm, Funktion des Sicherheitswerkzeugs

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 Eingänge 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 Eingängen und Ausgängen verwendet.
- Änderungen der Zuordnung der Signale in den Eingangs- 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 oder eine Liste der Sensoren und Aktoren dienen.

Die Zuordnung eines Variablennamens zur verwendeten Hardware erfolgt im Dialogfenster für die Ressourcen unter *Schrank bearbeiten*. Dabei sind die folgenden Angaben einzutragen:

- Position des Baugruppenträgers (1-1 bis 1-8 oder 2-1 bis 2-8)
- Typ des Baugruppenträgers
- Steckplatz und Typ der benötigten Baugruppe
- Die den Variablennamen zuzuordnenden PLT-Namen

TIPP Variablenname und PLT-Name sollten gleich lauten.

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

HIMA empfiehlt, die Eingangs- 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
  - sicherheitsbezogene/nicht sicherheitsbezogene 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 Programm-Organisationseinheit (POE) - Programm, Funktionsbaustein oder Funktion - verschiedene Variablenarten definiert werden. Nachstehende Tabelle enthält eine Übersicht:

Variablenart	Anwenderprogramm PROG	Funktions-baustein 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 22: 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 Eingänge und Ausgänge für boolesche Variablen

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

Die nicht sicherheitsbezogenen 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 sicherheitsbezogene 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 sicherheitsbezogenen und nicht sicherheitsbezogenen 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 Eingangs- 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 Versionen. In ELOP II gibt es folgende Versionen:

- Codeversion
- Runversion
- Datenversion
- Bereichsversion

7.2.4.1 Codeversion

Die Codeversion 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 Codeversion haben:

- Schreiben oder Löschen von Kommentaren
- Setzen oder Löschen von Online-Testfeldern (OLT-Felder), d. h. von Force-Informationen
- Verschieben von Linien oder 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 Codeversion führen. Bei allen anderen Änderungen ändert sich auch die Codeversion.

7.2.4.2 Runversion

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

Die Runversion wird geändert bei:

- anderer Codeversion (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 Datenversion

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

- Wenn sich der Name einer Variable mit den Attributen für HIPRO-N (nicht sicherheitsbezogen) ändert.

- Wenn solche Variablen bei der Erzeugung von nicht reloadbaren Code komprimiert werden (falls Speicherplatz-Lücken vorhanden sind).

7.2.4.4 Bereichsversion

Die Bereichsversion 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 Bereichsversion führen.

7.2.5 Parametrierung des Automatisierungsgeräts

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

7.2.5.1 Sicherheitsparameter

In den **Eigenschaften der Ressource** sind die Sicherheitsparameter einstellbar:

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

Sicherheitsbezogene 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 23: Sicherheitsbezogene Parameter

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

Nur der Wertebereich **1…254 s** ist zulässig!

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

Online-Änderung von Sicherheitsparametern

Im Control-Panel lässt sich das Dialogfenster *Systemparameter ändern* aufschalten. Das Register **Sicherheit** dient dazu, Sicherheitsparameter online zu ändern. Wird *Parameter Online änderbar* auf nicht änderbar gesetzt und zur Steuerung übertragen, so können keine weiteren dieser Parameter mehr online geändert werden.

Dies ist aber aus dem Inhalt des Registers nicht erkennbar. Deshalb ist es weiterhin möglich, Parameter zu ändern und online zur Steuerung zu übertragen. Die Steuerung ignoriert aber weitere Online-Änderungen, wenn *Parameter Online änderbar* einmal auf nicht änderbar gesetzt ist.

Weitere Online-Änderungen sind erst dann wieder möglich, wenn *Parameter Online änderbar* im Anwenderprogramm auf änderbar gesetzt und mittels Download in die Steuerung geladen ist.

7.2.5.2 Verhalten bei Fehlern in sicherheitsbezogenen Ausgangskanälen

Die folgende Tabelle zeigt die Einstellmöglichkeiten des Parameters *Verhalten bei Ausgabefehler*. Dieser befindet sich im Register **E/A-Parameter** des Dialogfensters *Eigenschaften* einer Ressource.

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 Ausgangskanäle (Fehlerstopp). Anwenderprogramm und Kommunikation laufen nicht weiter.
Normaler Betrieb	Reaktion wie bei Parameter *Nur Anzeige*, zusätzlich Abschaltung der zugehörigen Gruppe, wenn - mit Hilfe des Bausteins H8-STA-3, Kapitel 10.2.1 - 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 24: Einstellung des Parameters Verhalten bei Ausgabefehlern

7.2.6 Identifizierung des Programms

Das Anwenderprogramm ist an Hand der Codeversion eindeutig identifizierbar. Das dazugehörende 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

7.2.7 Überprüfung des erstellten Anwenderprogramms 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} Testfälle 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. Äquivalenzklassen-Tests, 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 MEAP-0001-D ist als Word-Datei auf der HIMA DVD und im Internet unter www.hima.de und www.hima.com 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 einigen Arten von Änderungen am Anwenderprogramm geht die Reloadbarkeit verloren. Einzelheiten hierzu und zu anderen Einschränkungen beim Reload siehe Betriebssystem-Handbuch HI 800 104 D.

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 Prozess-Sicherheitszeit 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. Beide Zentralbaugruppen gehen in den redundanten Betrieb über.

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 sicherheitsbezogenen Steuerungen die durchgeführten Änderungen zu validieren. Dazu ist ein Test an der tatsächlichen Steuerung oder einem Simulator erforderlich.

7.6 Forcen

Die Verantwortung für das Forcen liegt beim Betreiber!

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.

Möglichkeiten beim Forcen:

- Forcen kann per Konfiguration verboten werden. Das PES nimmt dann keine anwenderspezifisch definierten Force-Werte mehr an. In diesem Fall können neue Force-Werte erst wieder nach dem Abschalten des Systems gesetzt werden.
- Beim Schließen des Control-Panels wird angezeigt, ob Force-Werte gesetzt sind und wie viele.
- Alle geforcten 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.

⚠ WARNUNG

Personenschaden durch unbeabsichtigte Funktion möglich!

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

7.6.1 Löschen von geforcten Variablen

Vor dem Löschen von Variablen ist das Forcen dieser Variablen zu beenden!

Begründung:

- Löschen einer geforcten Variablen und Laden dieser Änderung in die Steuerung führt dazu, dass der Force-Editor die gelöschte Variable nicht mehr anzeigt. Dies gilt für alle Versionen von ELOP II bis einschließlich V5.1 730 IV3. Mit neueren Versionen von ELOP II kann das Forcen von gelöschten Variablen auch nach dem Ladevorgang im Force-Editor beendet werden.
- Die Erklärung dafür ist, dass der bisher dieser Variablen zugewiesene Eingang die Eigenschaft geforct und den Force-Wert behält.
- Das Einfügen einer Variablen zu einem späteren Zeitpunkt und die Zuweisung zu einem geforcten Eingang führt dazu, dass nach Laden mit Reload die neue Variable unmittelbar nach dem Reload geforct ist!

Dies kann Auswirkungen auf die Sicherheit der Anlage haben!

7.7 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 Eingängen und Ausgängen berücksichtigt wird. Ein Drahtbruch führt z. B. zur Abschaltung des betreffenden Aktors.

- Leitungsbrüche 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. Schiebe-Taktimpuls für ein Schieberegister) können für sicherheitstechnische Anwendungen genutzt werden.

Bei analogen, sicherheitsbezogenen Eingangsbaugruppen wird im Fehlerfall ein definierter Wert weiter verarbeitet. Nähere Angaben hierzu sind der Beschreibung der Software-Bausteine in Kapitel 10.2 zu entnehmen.

In einer digitalen, sicherheitsbezogenen 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 Software-Bausteine in Kapitel 10.2 zu entnehmen.

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

7.7.1 Gruppenabschaltung

Die für einen bestimmten Anlagenbereich eingesetzten sicherheitsbezogenen Ausgangsbaugruppen (z. B. für einen Brenner) können in einer Gruppe zusammengefasst werden. Hierzu ist pro Gruppe der Software-Baustein H8-STA-3 ins Anwenderprogramm einzufügen. Am Software-Baustein sind alle Positionen der zu einer Gruppe gehörenden Ausgangsbaugruppen einzustellen. Ein Fehler einer Ausgangsbaugruppe führt zur Abschaltung

aller zu dieser Gruppe gehörenden Ausgangsbaugruppen. Zur Sicherheit des Systems genügt jedoch allein die integrierte Sicherheitsabschaltung der Ausgangsbaugruppen.

7.7.2 Software-Bausteine für einzelne sicherheitsbezogene E/A-Baugruppen

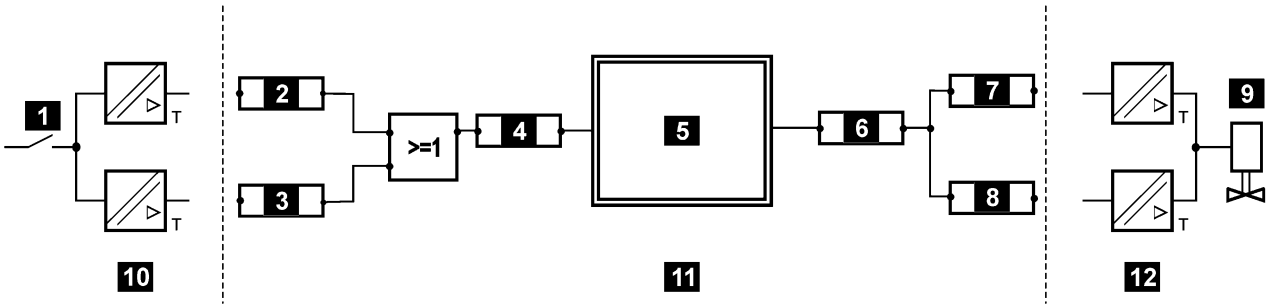
Eingangsbaugruppe		Ausgangsbaugruppe	
digital		digital	
Typ	Software-Baustein	Typ	Software-Baustein
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
analog		analog	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		
F 6221	HF-AIX-3		

Tabelle 25: Zuordnung von Software-Bausteinen zu E/A-Baugruppen

Für die sicherheitsbezogenen E/A-Baugruppen sind die zugehörigen Software-Bausteine in das Anwenderprogramm einzufügen. Nähere Angaben siehe Kapitel 10.2 oder die ELOP II Online-Hilfe.

7.8 Redundante E/A-Baugruppen

Zur Erhöhung der Verfügbarkeit ohne Einschränkung der Sicherheit können sicherheitsbezogene Eingangs- 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.



1 Sensor
2 Eingangssignal 1
3 Eingangssignal 2
4 Eingangsvariable
5 Programmlogik
6 Ausgangsvariable
7 Ausgangssignal 1
8 Ausgangssignal 2
9 Aktor
10 Verschaltung der Eingänge (Hardware)
11 Anwenderprogramm (Software)
12 Verschaltung der Ausgänge (Hardware)

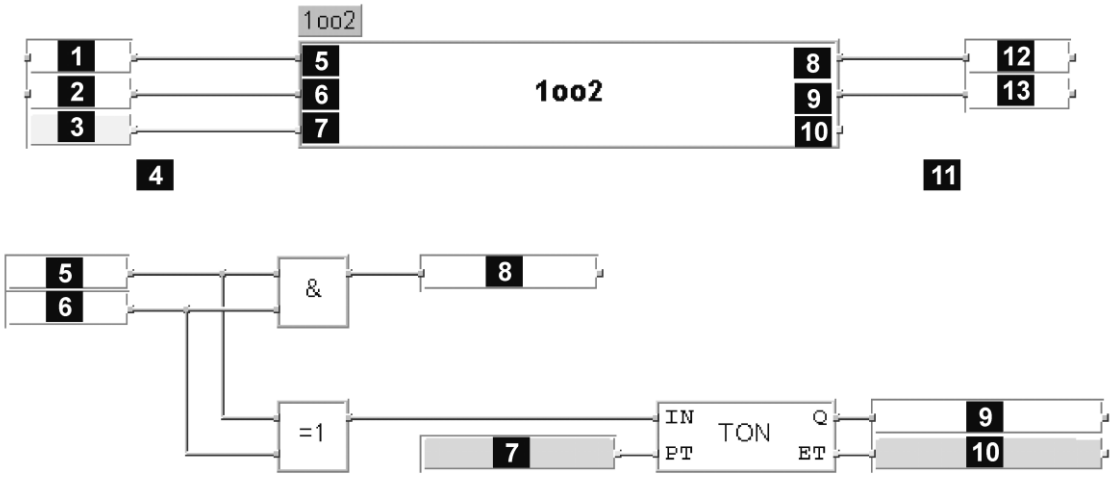
Bild 3: Redundante E/A-Baugruppen zur Erhöhung der Verfügbarkeit

7.8.1 Redundante, nicht sicherheitsbezogene Sensoren

7.8.1.1 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 sicherheitsbezogene 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.

7.8.1.2 Anwenderprogramm, Eingangsbaugruppe F 3236



1 Sensor-Signal 1
2 Sensor-Signal 2
3 Diskrepanz-Zeit, z. B. 1 s
4 Eingangssignale
5 Bausteineingang *Sensor1*
6 Bausteineingang *Sensor2*
7 Bausteineingang *Diskrepanz-Zeit*
8 Bausteinausgang *Steuer-Signal*
9 Bausteinausgang *Diskrepanz-Signal*
10 Bausteinausgang *Istwert-Diskr-Zeit*
11 Signale an Logik oder an Meldekreis
12 Variable zur Weiterverarbeitung des Steuer-Signals
13 Variable zur Weiterverarbeitung des Diskrepanz-Signals

Bild 4: Beispiel für einen Funktionsbaustein 1oo2 und Logik des Bausteins

Das Steuer-Signal hat den Wert TRUE, wenn beide Sensoren den Wert TRUE haben.

Das Diskrepanz-Signal hat den Wert TRUE, wenn die Sensorsignale nach Ablauf der Diskrepanzzeit unterschiedlich sind.

7.8.1.3 Anwenderprogramm, Eingangsbaugruppe F 3237 oder F 3238

Verwendung des Bausteins HB-RTE-3

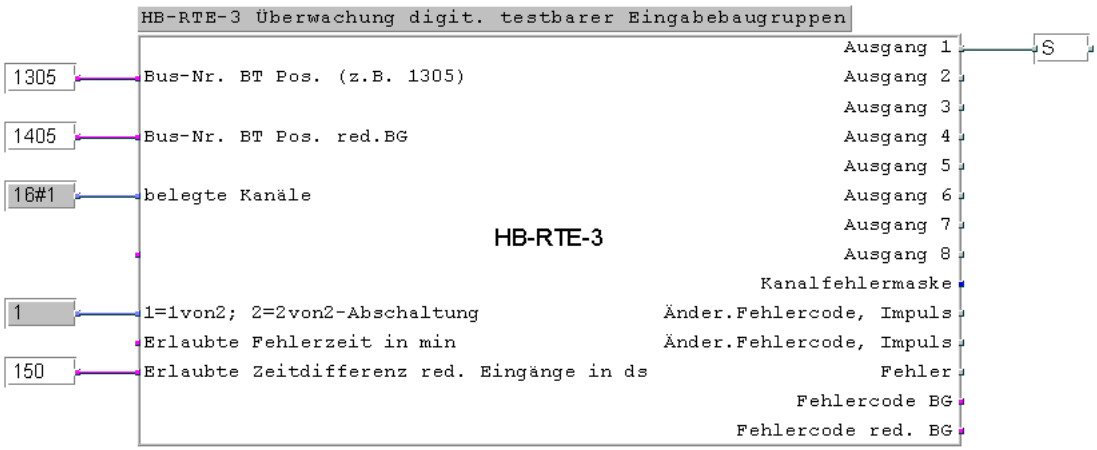


Bild 5: Verwendung des Bausteins HB-RTE-3

Die Signale S-1 und S-2 sind direkt auf die ersten Kanäle der Baugruppe F 3237 oder F 3238 geschaltet. Weitere Hardware ist nicht zugeordnet.

7.8.1.4 Sicherheitsbetrachtung

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

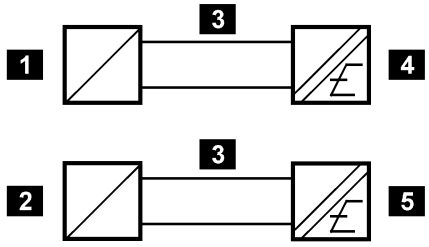
Für die Applikationen der Sensoren sind die relevanten Normen zu beachten, z. B. IEC 61511.

7.8.1.5 Verfügbarkeitsbetrachtung

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

7.8.2 Analoge redundante Sensoren

7.8.2.1 Verschaltung der Hardware

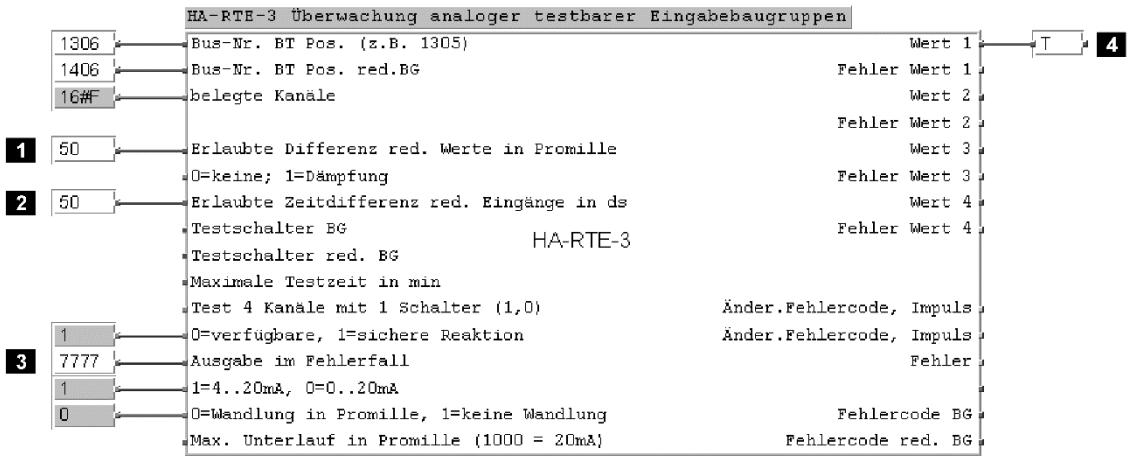


1 Transmitter 1
2 Transmitter 2
3 4…20 mA
4 T1
5 T2

Bild 6: Verschaltung redundanter Sensoren

7.8.2.2 Anwenderprogramm für Eingangsbaugruppe F 6213 oder F 6214

Verwendung des Bausteins HA-RTE-3, Einzelheiten zum Baustein siehe Kapitel 10.2.2 und die Online-Hilfe von ELOP II.



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

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

Die Signale T1 und T2 sind direkt auf die ersten Kanäle der Baugruppe F 6213 oder F 6214 gelegt. Eine weitere Hardware-Zuordnung erfolgt nicht.

Zwei Beispiele für ein Vergleicherelement zur Alarmierung oder Abschaltung bei Erreichen des zulässigen Grenzwerts:

1 Zu vergleichende Variable, z. B. Messwert

2 Vergleichswert

3 Vergleicherelement zur Alarmierung

4 Vergleichsergebnis

5 Vergleicherelement zur Abschaltung

Bild 8: Vergleicherelemente zur Alarmierung oder Abschaltung bei Erreichen des zulässigen Grenzwerts

7.8.2.3 Sicherheitsbetrachtung

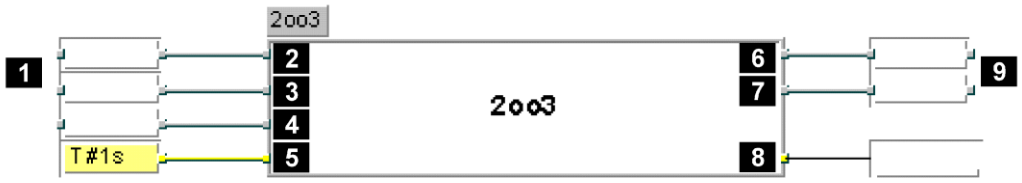
Beim Ansprechen eines der beiden Sensoren oder Ausfall einer Komponente innerhalb des Systems hat der entsprechende Ausgang *Fehler Wert x* (x = 1…4) High-Pegel.

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

7.8.2.4 Verfügbarkeitsbetrachtung

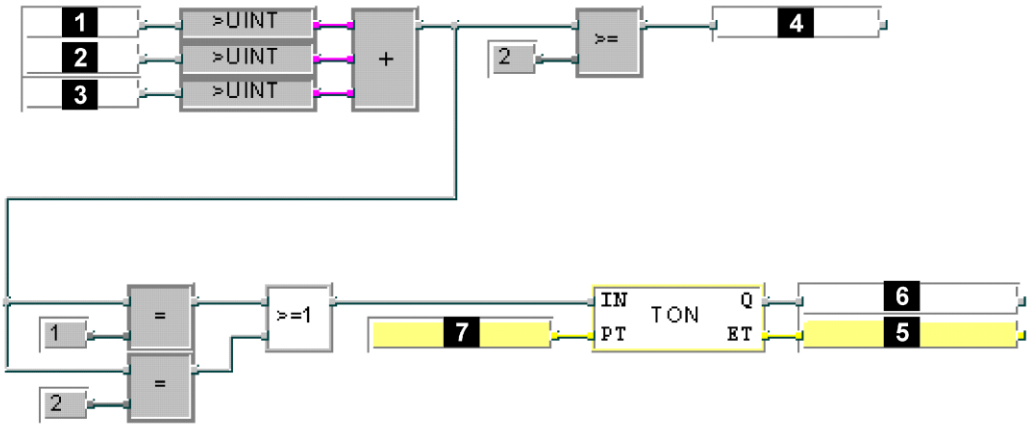
Keine Verfügbarkeit, da jeder Ausfall einer Komponente oder das Ansprechen eines Sensors zur Abschaltung führt.

7.8.3 Eingangsbaugruppen mit 2oo3-Verschaltung



1 Signale von drei verschiedenen Eingangsbaugruppen
2 Bausteineingang für Sensor1
3 Bausteineingang für Sensor2
4 Bausteineingang für Sensor3
5 Bausteineingang für die Diskrepanz-Zeit
6 Bausteinausgang für das Ergebnis-Signal
7 Bausteinausgang für das Diskrepanz-Signal
8 Bausteinausgang für den Istwert der Diskrepanz-Zeit
9 Signale an Logik oder Meldekreis

Bild 9: 2oo3-Funktionsbaustein



1 Sensor 1
2 Sensor 2
3 Sensor 3
4 Ergebnis-Signal
5 Diskrepanz-Zeit
6 Diskrepanz-Signal
7 Istwert der Diskrepanz-Zeit

Bild 10: Aufbau des 2oo3-Funktionsbausteins

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

Das Steuer-Signal hat den Wert TRUE, wenn zwei oder drei Sensoren den Wert TRUE haben.

Das Diskrepanz-Signal hat den Wert TRUE, wenn ein oder zwei Sensoren nach Ablauf der Diskrepanz-Zeit den Wert TRUE haben.

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 jeweils mit einer ODER-Funktion verknüpft werden.

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

7.9 Projektdokumentation für sicherheitsbezogene 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 (z. B. TÜV). Die Funktionsabnahme bezieht sich nur auf die Anwenderfunktion, nicht aber auf die sicherheitsbezogenen HIMA Automatisierungsgeräte H41q-MS, H51q MS, H41q-HS, H51q HS, H41q-HRS, H51q HRS, die baumustergeprüft sind.

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

7.10 Sicherheitstechnische Aspekte für die Kommunikation (sicherheitsbezogene Datenübertragung)

Das Protokoll HIPRO-S V2 ist zertifiziert für SIL 3.

i **HIMA empfiehlt dringend, für die sicherheitsbezogene Kommunikation HIPRO-S V2 über Ethernet einzusetzen!**

Zu Einzelheiten von HIPRO-S V2 siehe das HIPRO-S V2 Handbuch HI 800 722 D.

7.10.1 Sicherheitsbezogene Kommunikation

Der Datenaustausch zu sicherheitstechnisch zugeordneten Ressourcen wird über den Baustein HK-COM-3 überwacht. Hierzu kann eine Überwachungszeit als Parameter *Zeitintervall* angegeben sowie die Option *importierte Variablen rücksetzen* bei Überschreiten der Überwachungszeit aktiviert werden.

Die einzustellende Überwachungszeit ist prozessabhängig und ist mit der abnehmenden Behörde abzustimmen.

7.10.2 Zeitliche Anforderungen

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

$T_T = 2*ZZ_1 + 2*T_D + 2*ZZ_2$

- 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.
  - Übertragung über Ethernet: in diesem Fall ist die maximale Übertragungszeit (T_{max}) annehmen, siehe das Datenblatt der Baugruppe F 8627X, HI 800 264 D.

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 Ressource-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 eindeutig sein, so dass sie kollisionsfrei zum Ermitteln der IP-Adresse der Kommunikationsbaugruppe verwendet werden können.
- Zur Kontrolle der HIPRO-S Konfiguration ist das PES-Masterprogramm zu kompilieren. Anschließend sind die aufgetretenen Fehler zu korrigieren.
- Ein Parallelbetrieb von serieller und Ethernet-Schnittstelle für dieselbe HIPRO-S Verbindung (d. h. zum selben Kommunikationspartner) ist sicherheitstechnisch nicht zulässig.

  Es kann jederzeit zum Verbindungsabbruch kommen.

  Ein Parallelbetrieb liegt schon dann vor, wenn eine serielle Verbindung in Betrieb ist und eine Ethernet-Baugruppe im PES gesteckt ist.

  Abhilfen:

  - Wenn eine Ethernet-Baugruppe für andere Zwecke nötig ist, mittels kanalspezifisch eingestelltem Baustein HK-COM-3 und dessen Eingang *Funktion* die HIPRO-S Kommunikation verhindern.
  - Wenn eine Ethernet-Baugruppe für HIPRO-S Verbindungen zu anderen PES nötig ist, mittels verbindungsspezifisch eingestelltem Baustein HK-COM-3 und dessen Eingang *E5 – Verbindungs-Bitmaske* die spezielle Verbindung zum seriellen Partner verhindern.

8 Einsatz für Brandmelderzentralen

Die Systeme H41q 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.

DIN EN 54-2 fordert 10 s als maximale Zykluszeit von Brandmelderzentralen. Diese Zykluszeit ist mit den HIMA Systemen leicht erfüllbar, da die Zykluszeiten dieser Systeme im Bereich < 0,5 s liegen und ebenso die gegebenenfalls geforderte Sicherheitszeit von 1 s (Fehlerreaktionszeit).

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

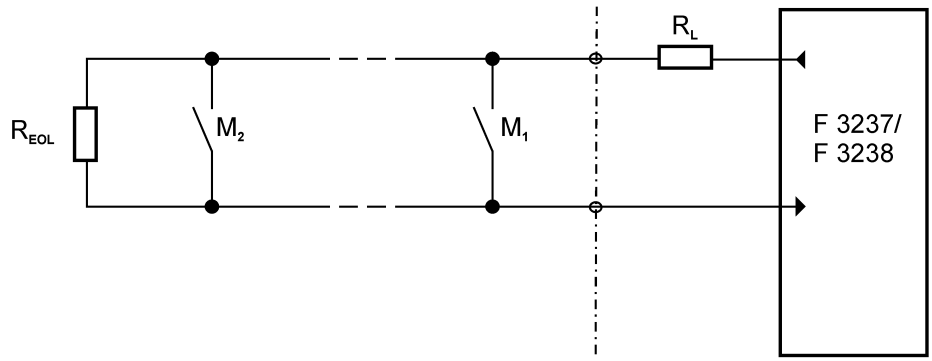
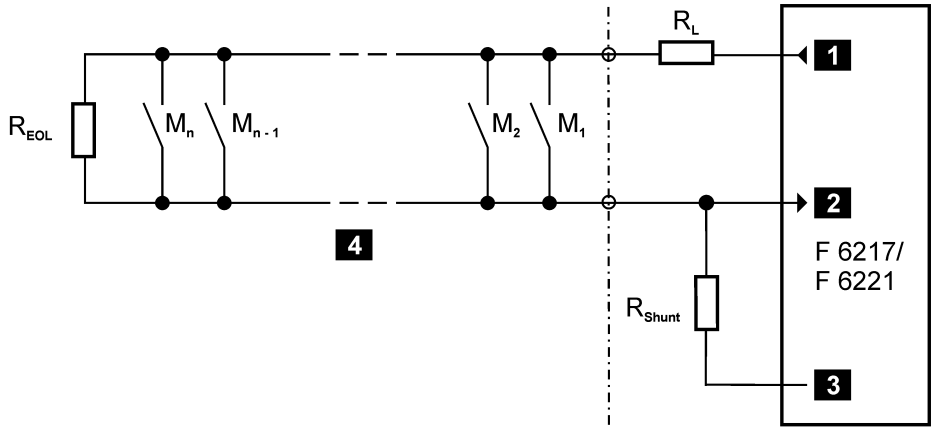


Bild 11: Verschaltung von Brandmeldern mit digitalen Eingängen



1 Sensor-Versorgung
2 Analoger Eingang
3 Bezugspol (L-)
4 Meldeschleife

Bild 12: Verschaltung von Brandmeldern mit analogen Eingängen

Legende zu Bild 11 und Bild 12:

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 Arbeitsstromprinzip 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 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, die 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 oder 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 beschreibt das Betriebssystem die im Anwenderprogramm auswertbaren Systemvariablen. Somit ist eine Fehlersignalisierung auf die vom System erkannten Fehler programmierbar. Sicherheitsbezogene Eingänge 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.

9 Einsatz von HIQuad Geräten in Zone 2

HIMA Komponenten sind zum Einbau in den explosionsgefährdeten Bereich der Zone 2 geeignet. Dazu sind, neben den besonderen Bedingungen, die Montage- und Installationsangaben in den Datenblättern der Baugruppen zu beachten.

Die Konformitätserklärung für die HIQuad Komponenten ist auf den HIMA Webseiten www.hima.de und www.hima.com zu finden.

HIMA Komponenten erfüllen die Anforderungen folgender Richtlinien und Normen:

Richtlinie	Norm	Beschreibung
IECEx	IEC 60079-0:2011	Explosionsgefährdete Bereiche – Teil 0: Betriebsmittel Allgemeine Anforderungen
2014/34/EU	EN 60079-0:2012 + A11:2013	
IECEx	IEC 60079-15:2010	Explosionsgefährdete Atmosphäre – Teil 15: Geräteschutz durch Zündschutzart «n»
2014/34/EU	EN 60079-15:2010	

Tabelle 26: Normen für HIMA Komponenten in Zone 2

Die HIMA Komponenten sind mit einer der folgenden Ex-Kennzeichnungen versehen:

 II 3G Ex nA IIC T4 Gc

 II 3G Ex nA nC IIC T4 Gc

Kennzeichnung	Beschreibung
	Ex-Kennzeichen nach Richtlinie
II	Gerätegruppe, für alle explosionsgefährdeten Bereiche außer schlagwettergefährdete Grubenbaue.
3G	Gerätekategorie, Bereich mit normalerweise keinem, oder nur kurzfristig auftretendem brennbarem Gasgemisch.
Ex	Ex-Kennzeichen nach Norm
nA	Zündschutzart für nicht funkende Einrichtung
nC	Zündschutzart für funkende, abgedichtete Einrichtung
IIC	Zündgruppe des Gases, typisches Gas ist Wasserstoff
T4	Temperaturklasse T4, mit einer maximalen Oberflächentemperatur von 135 °C
Gc	Geräteschutzniveau, entspricht der ATEX-Gerätekategorie 3G

Tabelle 27: Beschreibung Ex-Kennzeichnung HIQuad Komponenten

Besondere Bedingungen

1. HIMA Komponenten sind in ein Gehäuse einzubauen, das die Anforderungen der IEC 60079-15/EN 60079-15 mit der Schutzart IP54 oder besser erfüllt. Dieses Gehäuse muss mit folgendem Warnhinweis versehen sein:

   WARNUNG: Arbeiten nur im spannungslosen Zustand zulässig

   Ausnahme:

   Ist sichergestellt, dass keine explosionsfähige Atmosphäre vorhanden ist, darf auch unter Spannung gearbeitet werden.
2. Die HIMA Komponenten sind für den Betrieb mit maximalem Verschmutzungsgrad 2 ausgelegt.
3. Das verwendete Gehäuse muss die entstehende Verlustleistung sicher abführen können.
4. Die Versorgungsspannungen sind aus Netzgeräten mit sicherer Trennung zu entnehmen. Nur Netzgeräte in den Ausführungen PELV oder SELV einsetzen.
5. Die in den Baugruppenhandbüchern aufgeführten Betriebsbedingungen sind zu beachten.
6. Der E/A-Baugruppenträger muss zwangbelüftet sein.

Anwendbare Normen:

IEC 60079-14: 2013	Explosionsgefährdete Bereiche – Teil 14: Projektierung, Auswahl und Errichtung elektrischer Anlagen.
EN 60079-14: 2014	

Anforderungen für die Zündschutzart «n» sind zu beachten.

10 Standard-Funktionsbausteine

In den nachfolgenden Tabellen sind die HIMA Standard-Funktionsbausteine für sicherheitstechnische Anwendungen aufgeführt. Die Funktionsbeschreibungen der Bausteine sind in der Online-Hilfe des jeweiligen Bausteins verfügbar.

i Einige der in diesem Kapitel aufgeführten HIMA Standard-Funktionsbausteine haben zur erweiterten Diagnose den Ausgang Fehlercode. An diesem Ausgang wird immer nur ein Fehlercode angezeigt, auch wenn mehrere Fehler auftreten.

Der folgende Text nennt die Standard-Funktionsbausteine kurz «Bausteine».

10.1 Bausteine unabhängig von E/A-Baugruppen

Für Funktionen der Zentralbaugruppen können Bausteine in die Programmlogik eingefügt und belegt werden.

Typ	Funktion	TÜV-Prüfung[1)]	
		Sicherheits-gerichtet	Rückwirkungs-frei
H8-UHR-3	Datum und Uhrzeit		•
HA-LIN-3	Temperaturlinearisierung	•	•
HA-PID-3	PID-Regler	•	•
HA-PMU-3	Parametrierbarer Messumformer	•	•
HK-AGM-3	PES-Master-Überwachung		•
HK-COM-3	Kommunikationsbaugruppen-Überwachung	•[2)]	•
HK-LGP-3	LGP-Auswertung und -Konfiguration		•
HK-MMT-3	Modbus-Master		•

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.

2) Für sicherheitsbezogenes Protokoll HIPRO-S V2 ab Betriebssystem ≥ V7.0-8 BS (08.17).

Tabelle 28: Standard-Funktionsbausteine unabhängig von der E/A-Ebene

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

- H8-UHR-3
- HK-AGM-3
- HK-LGP-3
- HK-MMT-3

10.1.1 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 sicherheitsbezogenen Aktionen im Anwenderprogramm abgeleitet werden.

10.1.2 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).

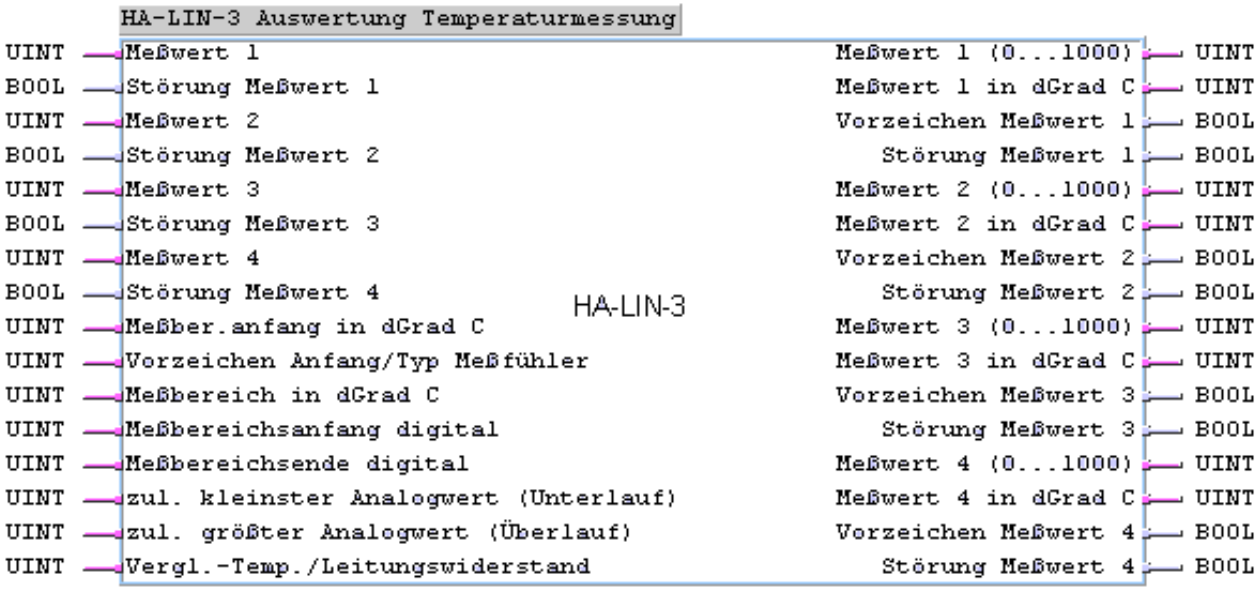


Bild 13: Anschlüsse des Bausteins HA-LIN-3

10.1.3 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.

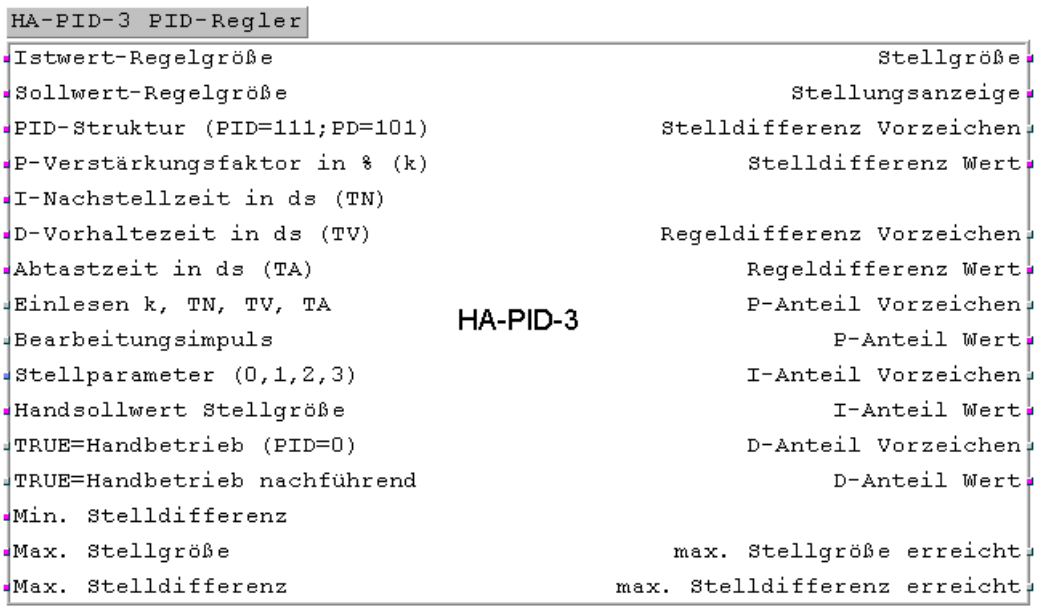


Bild 14: Anschlüsse des Bausteins HA-PID-3

10.1.3.1 Eingänge

True=Handbetrieb (PID=0), *True=Handbetrieb nachführend*	Bei sicherheitsbezogenem Betrieb des Regelbausteins dürfen diese Eingänge nicht belegt werden. Abweichungen davon sind durch die Genehmigungsbehörde zu genehmigen. Parameter- und Konstantenänderung an den Bausteineingängen im laufenden Betrieb sind nur mit Genehmigung der Genehmigungsbehörde und im überwachten Betrieb erlaubt. Die Belegung der Bausteineingänge mit nicht sicherheitsbezogenen importierten Variablen ist nicht zulässig.

10.1.3.2 Ausgänge

Sicherheitsabschaltungen sind nur zugelassen über:

max. Stellgröße erreicht und *max. Stelldifferenz erreicht*

Abweichungen davon sind durch die Genehmigungsbehörde 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.

10.1.4 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).

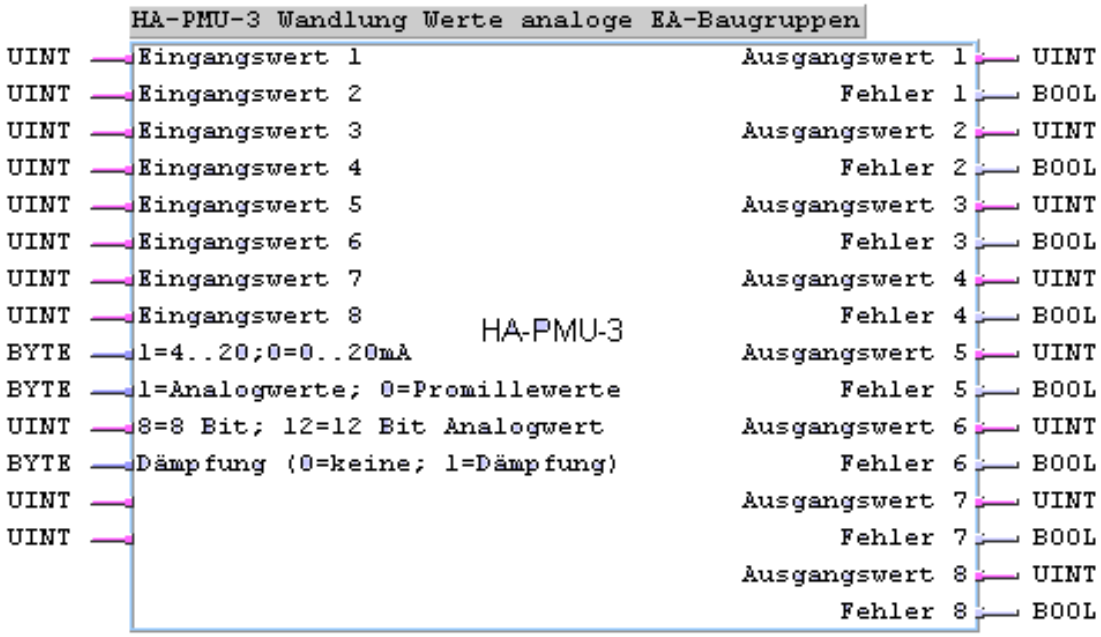


Bild 15: Anschlüsse des Bausteins HA-PMU-3

10.1.5 Baustein HK-AGM-3

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

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

10.1.6 Baustein HK-COM-3

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

Der Baustein ist für das sicherheitsbezogene Protokoll HIPRO-S V2 ab Betriebssystem V7.0-8 BS (08.17) sicherheitstechnisch relevant. Für alle anderen Protokolle dienen die Ausgänge des Bausteins nur zur Information, es dürfen hiervon keine sicherheitsbezogenen Aktionen im Anwenderprogramm abgeleitet werden.

10.1.7 Baustein HK-LGP-3

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

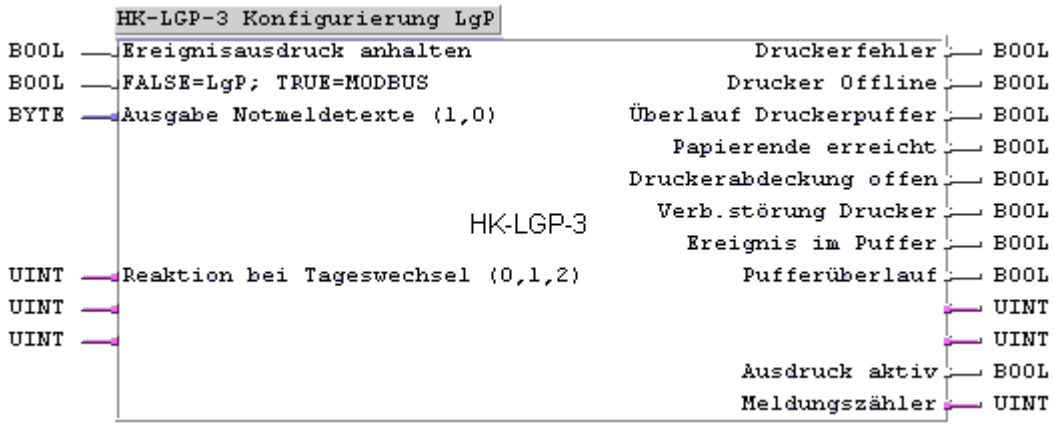


Bild 16: Anschlüsse des Bausteins HK-LGP-3

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information. Sie dürfen nicht zum Programmieren sicherheitsbezogener Reaktionen im Anwenderprogramm verwendet werden.

10.1.8 Baustein HK-MMT-3

Mit diesem Baustein kann ein Automatisierungsgerät H41q 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 sicherheitsbezogenen Aktionen im Anwenderprogramm abgeleitet werden.

10.2 Bausteine abhängig von E/A-Baugruppen

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

Typ	Funktion	TÜV-Prüfung[1)]	
		sicherheits bezogen	rückwirkungsfrei
H8-STA-3	Gruppenbildung sicherheitsbezogener, 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-DOS-3	Diagnose ohne Sicherheit		•
HZ-FAN-3	Fehleranzeige für testbare E/A-Baugruppen		•

[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 29: Standardfunktionsbausteine abhängig von der E/A-Ebene

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

- HZ-FAN-3
- HZ-DOS-3

Die in diesem Kapitel beschriebenen besonderen Programmierhinweise sind zu beachten.

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

10.2.1 Baustein H8-STA-3

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

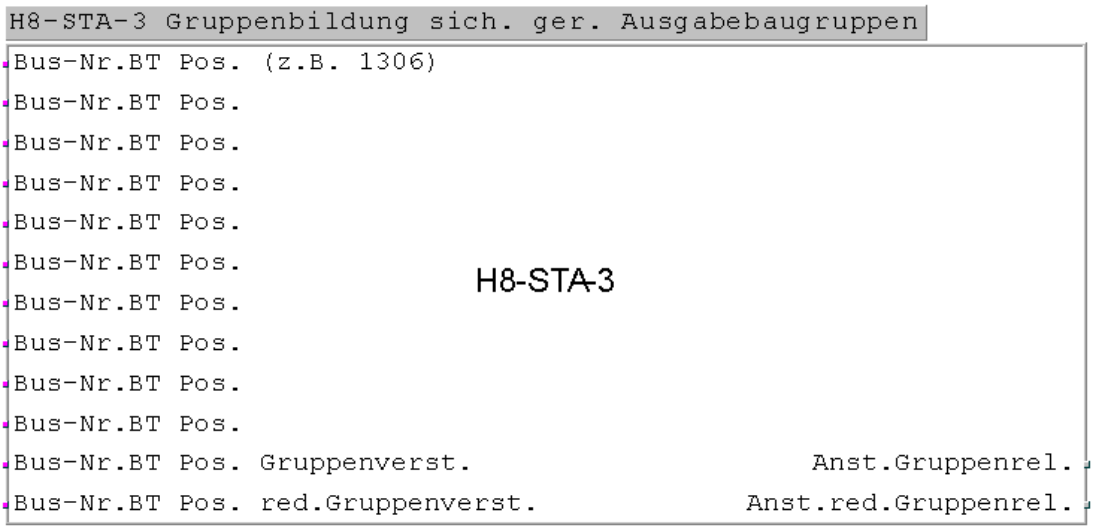


Bild 17: Anschlüsse des Bausteins H8-STA-3

Zum Verhalten bei Fehlern von Ausgangskanälen siehe Kapitel 6.

10.2.1.1 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.

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).

10.2.2 Baustein HA-RTE-3

Der Baustein dient zur Wertverarbeitung und zur Anzeige von Fehlern bei analogen sicherheitsbezogenen Eingangsbaugruppen bei einkanaligem oder redundantem Betrieb. Er muss für jede sicherheitsbezogene analoge Eingangsbaugruppe (F 6213) 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.

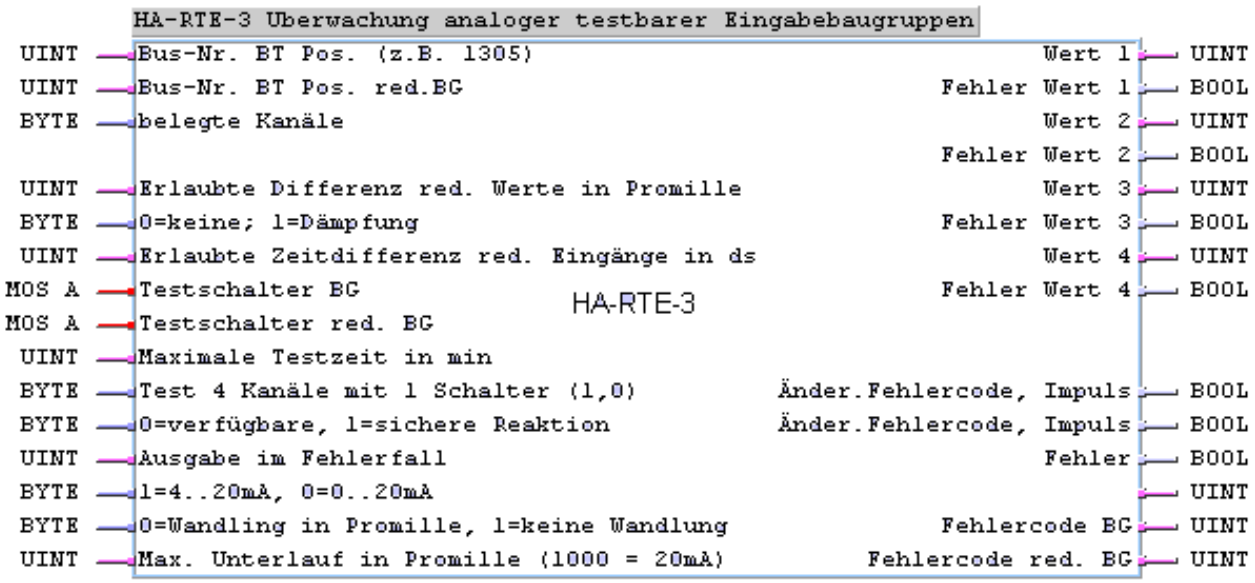


Bild 18: Anschlüsse des Bausteins HA-RTE-3

10.2.2.1 Eingänge

Bus-Nr. BT Pos.(z. B. 1305) *Bus-Nr. BT Pos. red. BG*	Position der sicherheitsbezogenen 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.
Maximale Testzeit in min	Begrenzung der Testzeit in Minuten. Nach Ablauf der Testzeit wird wieder der tatsächliche Wert in der Anwenderlogik verarbeitet.

10.2.2.2 Ausgänge

Wert 1...4	Die Verwendung der Werte muss überprüft werden, wenn diese zur Abschaltung sicherheitsbezogener Kreise benutzt werden.
Fehler Wert 1...4	Die Ausgänge müssen belegt werden, um im Fehlerfall mit ihrem boolschen Signal eine Abschaltung auslösen zu können.

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

10.2.3 Baustein HB-BLD-3

Der Baustein dient der kanalbezogenen Fehlerauswertung und Fehleranzeige für digitale sicherheitsbezogene Ausgangsbaugruppen F 3331, F 3334 und F 3349. Er darf für jede verwendete Baugruppe nur einmal eingesetzt werden.

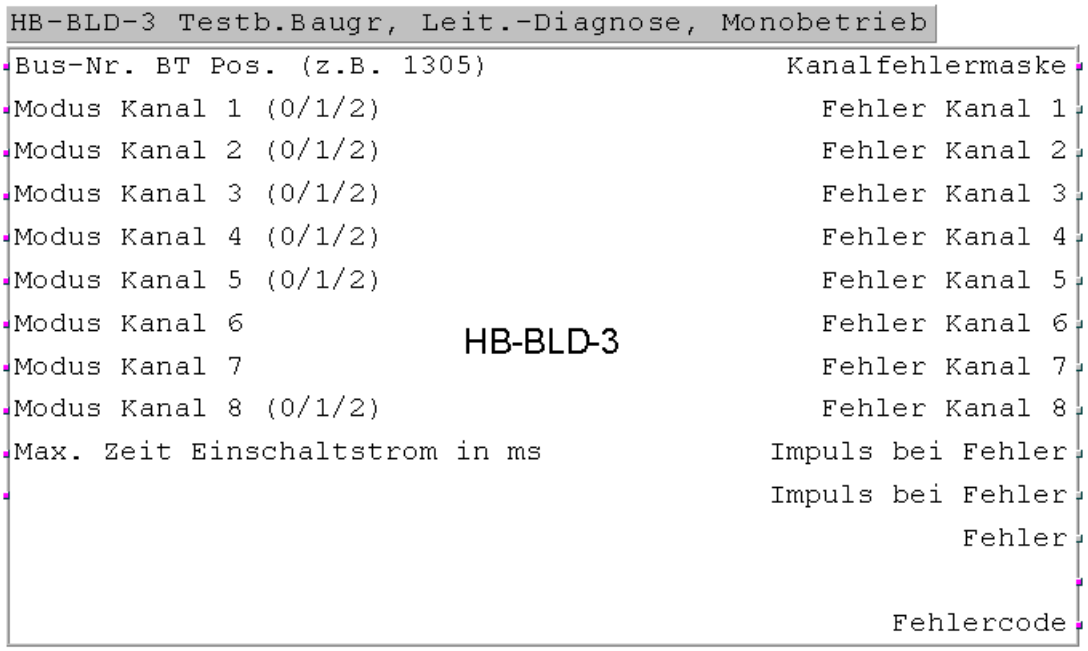


Bild 19: Anschlüsse des Bausteins HB-BLD-3

10.2.3.1 Eingänge

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

Position der sicherheitsbezogenen digitalen Ausgangsbaugruppe als 4-stellige 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 *Fehler Kanal* **n** 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 sicherheitsbezogenen Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Max. Zeit Einschaltstrom in ms

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

10.2.3.2 Ausgänge

Die Ausgänge *Impuls bei Fehler (2x)*, *Fehler* und *Fehlercode* dienen nur zur Information, sie dürfen nicht zur Programmierung sicherheitsbezogener Reaktionen im Anwenderprogramm verwendet werden.

Die übrigen Ausgänge sind für sicherheitsbezogene Reaktionen verwendbar.

10.2.4 Baustein HB-BLD-4

Der Baustein dient der kanalbezogenen Fehlerauswertung und Fehleranzeige für digitale sicherheitsbezogene Ausgangsbaugruppen F 3331, F 3334 und F 3349 bei redundantem Betrieb. Er darf für ein redundantes Baugruppenpaar nur einmal eingesetzt werden.

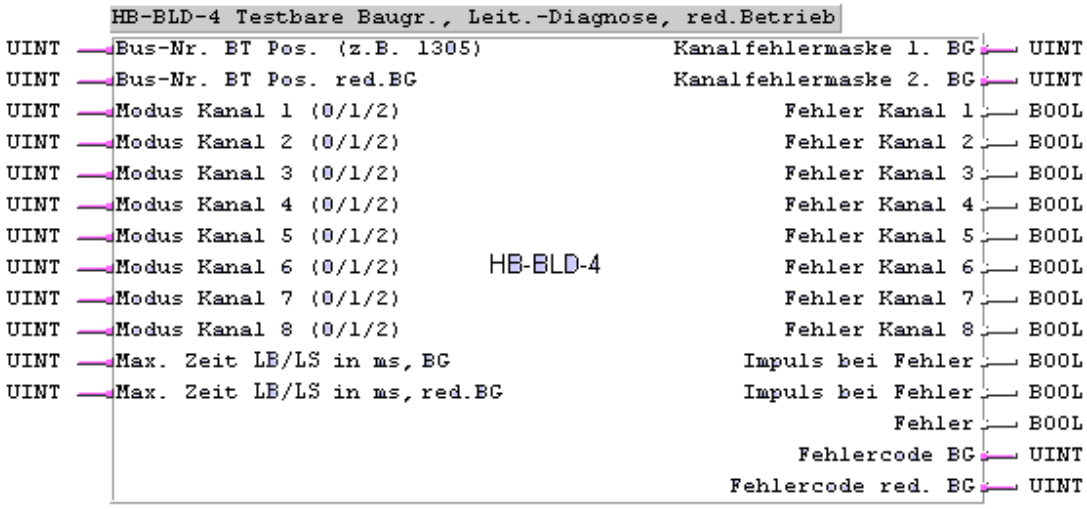


Bild 20: Anschlüsse des Bausteins HB-BLD-4

10.2.4.1 Eingänge

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

Position der sicherheitsbezogenen 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 am zugehörigen Ausgang *Fehler Kanal* **n** 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 am zugehörigen Ausgang *Fehler Kanal* **n** gemeldet.
> 2	Wertebereich überschritten: Der Kanal wird als fehlerhaft interpretiert (TRUE am Ausgang) und eine kanalbezogene Fehlermeldung wird ausgegeben.

In sicherheitsbezogenen Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Max. Zeit Einschaltstrom in ms, BG *Max. Zeit Einschaltstrom in ms, red BG*	Festlegung der Wartezeit für die Erkennung des Leitungsbruchs, d. h., Zeit für Tolerierung der Strombegrenzung. Für diese Zeit wird die Fehleranzeige unterdrückt. Eine Vergrößerung der Wartezeit bringt eine Erhöhung der Zykluszeit mit sich.

10.2.4.2 Ausgänge

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

Die übrigen Ausgänge sind für sicherheitsbezogene Aktionen verwendbar.

10.2.5 Baustein HB-RTE-3

Der Baustein dient zur Auswertung und Anzeige von Fehlern bei digitalen sicherheitsbezogenen 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.

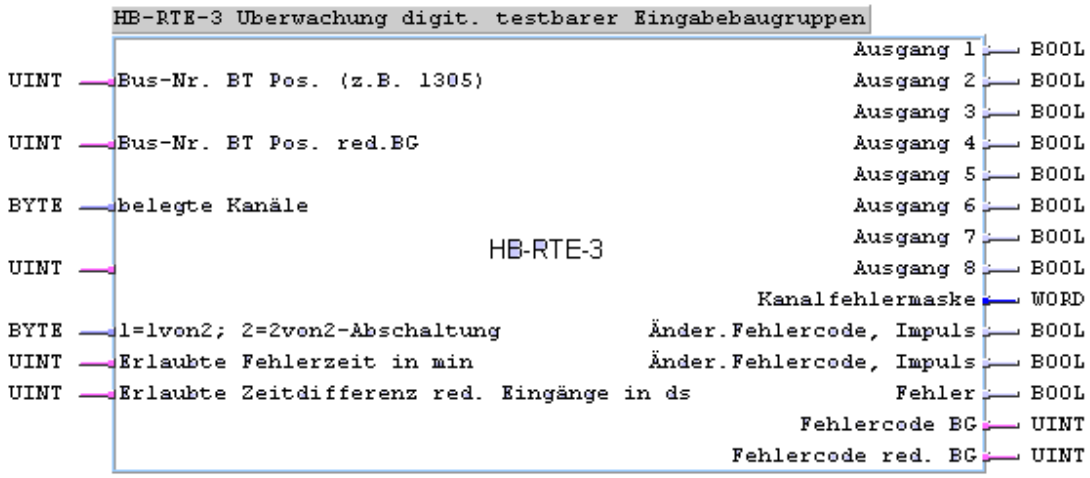


Bild 21: Anschlüsse des Bausteins HB-RTE-3

10.2.5.1 Eingänge

Bus-Nr. BT Pos.(z. B. 1305) *Bus-Nr. BT Pos. red. BG*	Position der sicherheitsbezogenen digitalen Ausgangsbaugruppe 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 61131: 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 Eingangsbaugruppen 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. Nach Ablauf der definierten Fehlerzeit wird der Bausteinausgang 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 sicherheitsbezogenen Steuerkreisen ist grundsätzlich das Ruhestromprinzip anzuwenden.

Erlaubte Fehlerzeit in min
Innerhalb der angegebenen Zeit nach Sensortest, Bauteil- oder Leitungsfehler erfolgt keine Fehlerreaktion.
Abstimmung mit der abnehmenden Behörde notwendig.

Erlaubte Zeitdiff. red. Eingänge in ds
Zeitliche Differenz der Schaltpunkte zwischen zwei redundanten Gebern. Die Zeit ist geberabhängig und mit der abnehmenden Behörde abzustimmen.

10.2.5.2 Ausgänge

Die Ausgänge *Kanalfehlermaske*, *Änder. Fehlercode*, *Impuls (2x)*, *Fehler*, *Fehlercode BG* und *Fehlercode red. BG* dienen nur zur Information. Sie dürfen nicht für die Programmierung sicherheitsbezogener Reaktionen im Anwenderprogramm verwendet werden.

Die Ausgänge *Ausgang 1*…*Ausgang 8* sind für sicherheitsbezogene Reaktionen verwendbar.

10.2.6 Baustein HF-AIX-3

Der Baustein HF-AIX-3 dient zur Parametrierung und Auswertung jeweils eines Kanals der sicherheitsbezogenen analogen (Ex)i-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.

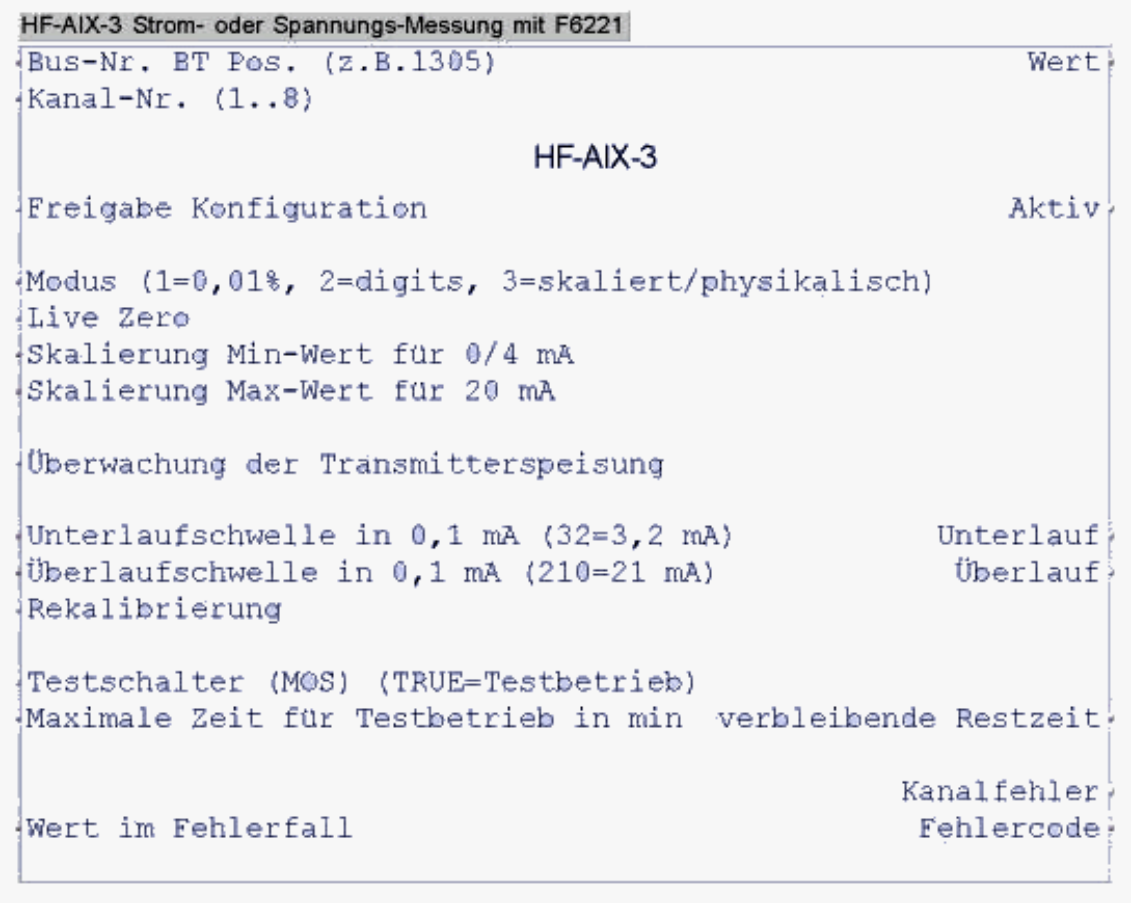


Bild 22: Anschlüsse des Bausteins HF-AIX-3

Die analoge Eingangsbaugruppe hat pro Kanal einen sicherheitsbezogenen 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 skaliert werden.

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

- bei Kanalfehler
- bei Baugruppenfehler
- bei Über- oder Unterschreitung desMessbereichs

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

10.2.7 Baustein HF-CNT-3

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

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

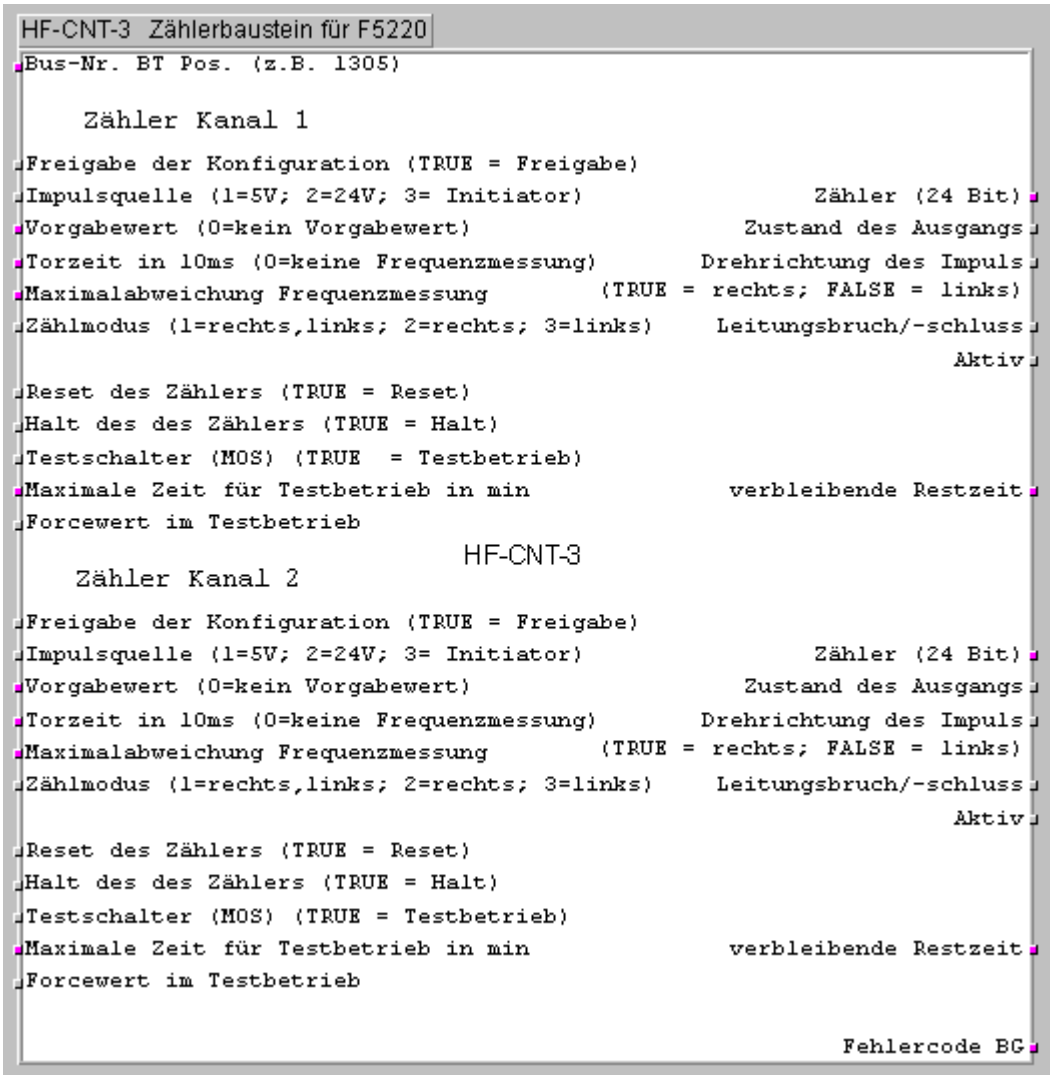


Bild 23: Anschlüsse des Bausteins HF-CNT-3

Die Zählerbaugruppe hat pro Kanal einen sicherheitsbezogenen 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.

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

10.2.8 Baustein HF-CNT-4

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

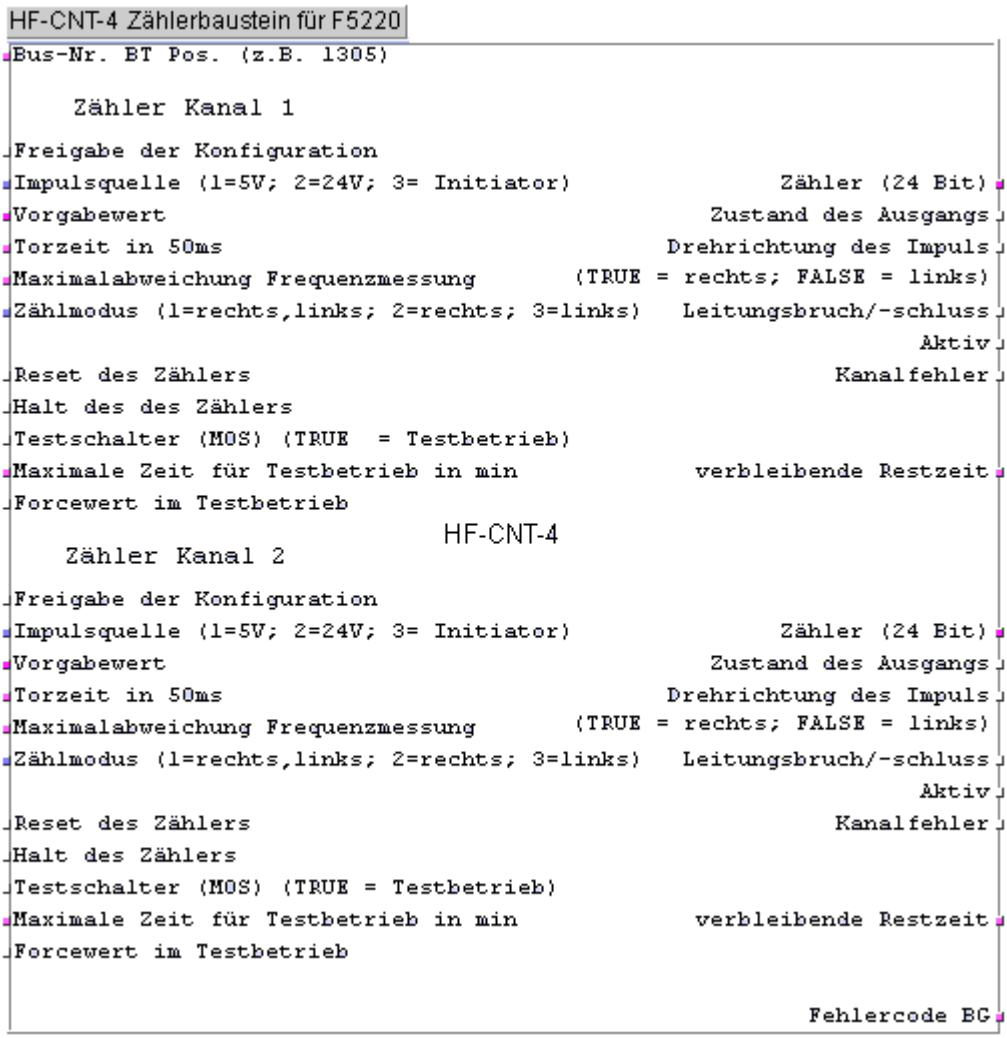


Bild 24: Anschlüsse des Bausteins HF-CNT-4

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 parametriert.

10.2.9 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 oder FALSE. Es gibt keine Default-Funktionalität und keine Default-Einstellung. Der Sensor-Typ 1 darf nur auf Kanal 9 eingegeben werden.

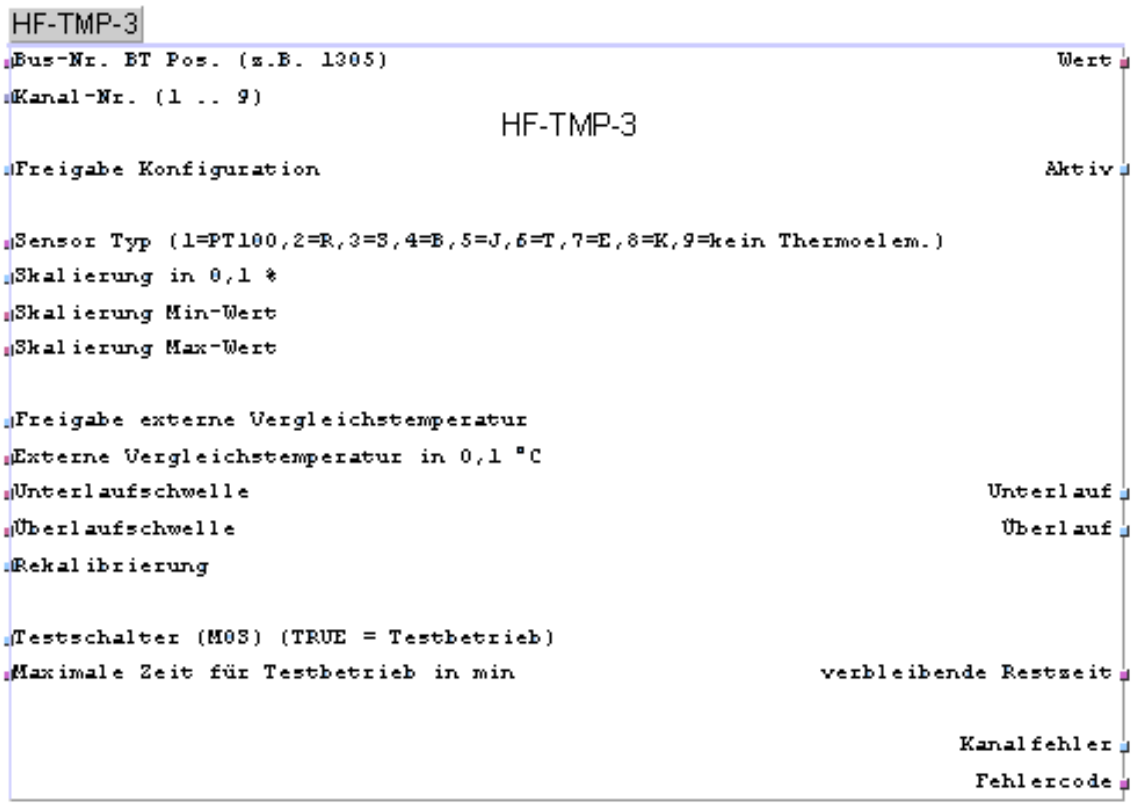


Bild 25: Anschlüsse des Bausteins HF-TMP-3

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

Bei sicherheitstechnischen Anwendungen für 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, um die an der Baugruppe vorhandenen Umweltbedingungen (z. B. Temperatur) automatisch zu erfassen. Eine Rekalibrierung kann auch durch TRUE am Eingang *Rekalibrierung* ausgelöst werden. Dieses Signal darf nur einen Zyklus lang anstehen.

Mit TRUE am Eingang *Testschalter MOS* (Maintenance Override Switch) wird der Wert an den Bausteinausgängen *Wert* und *Kanalfehler* eingefroren, wenn die Zeit für den Testbetrieb läuft.

10.2.10 Baustein HZ-DOS-3

Der Baustein dient zur Festlegung, welche sicherheitsbezogenen 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.

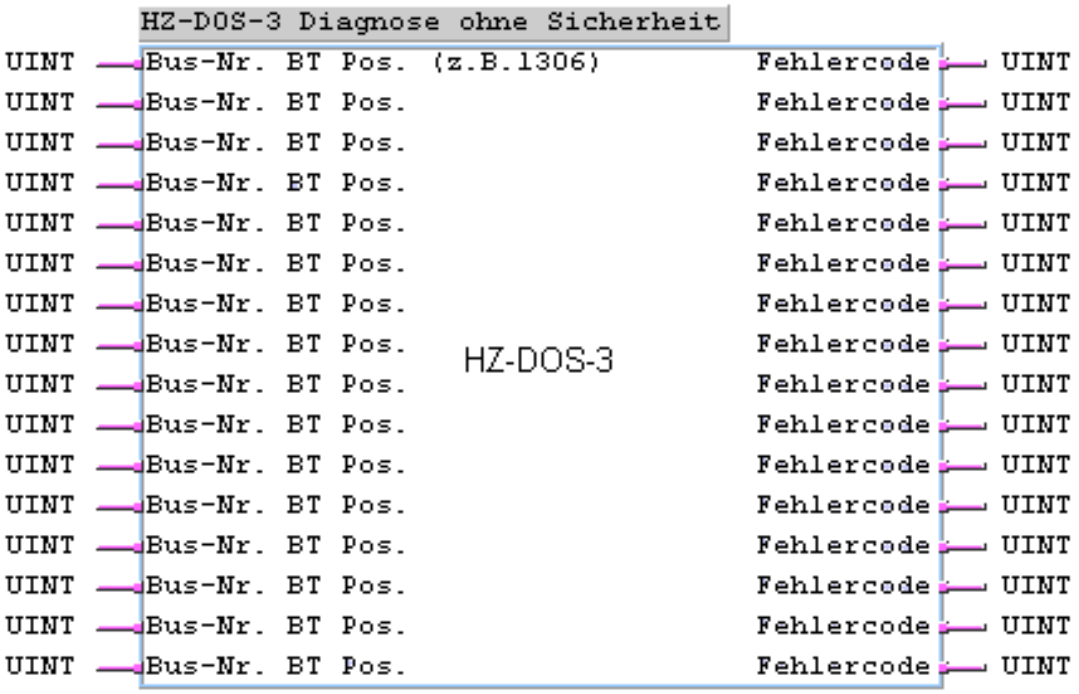


Bild 26: Anschlüsse des Bausteins HZ-DOS-3

Der Baustein ist sicherheitstechnisch nicht relevant. Die Ausgänge des Bausteins dienen nur zur Information. Sie dürfen nicht zum Programmieren sicherheitsbezogener Reaktionen im Anwenderprogramm verwendet werden.

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

10.2.11 Baustein HZ-FAN-3

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

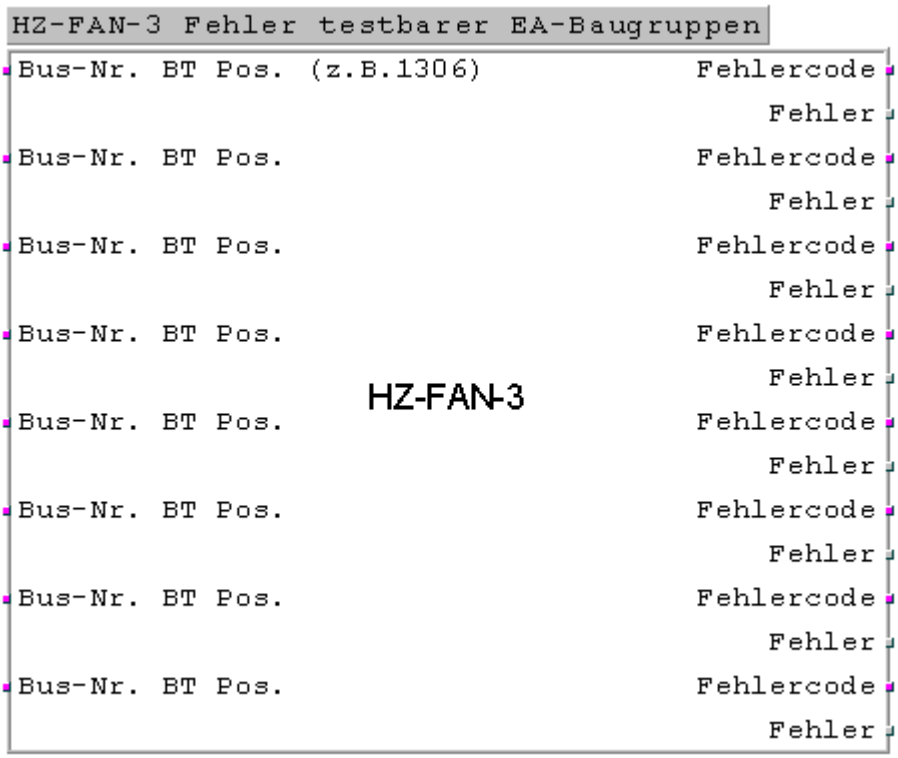


Bild 27: Anschlüsse des Bausteins HZ-FAN-3

10.2.11.1 Eingänge

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

10.2.11.2 Ausgänge

Alle Bausteinausgänge dienen nur zur Information. Sie dürfen nicht zum Programmieren sicherheitsbezogener Reaktionen im Anwenderprogramm verwendet werden.

Anhang

Glossar

Begriff	Beschreibung
AI	Analog Input, Analoger Eingang
ARP	Address Resolution Protocol: Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardwareadressen
COM	Kommunikationsmodul
CRC	Cyclic Redundancy Check, Prüfsumme
DI	Digital Input, digitaler Eingang
DO	Digital Output, digitaler Ausgang
ELOP II	Programmierwerkzeug für H41q/H51q
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Normen
ESD	ElectroStatic Discharge, elektrostatische Entladung
FB	Feldbus
FBS	Funktionsbausteinsprache
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen
IEC	Internationale Normen für die Elektrotechnik
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control)
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit ELOP II
PE	Schutzerde
PELV	Protective Extra Low Voltage: Funktionskleinspannung mit sicherer Trennung
PES	Programmierbares Elektronisches System
PFD	Probability of Failure on Demand: Wahrscheinlichkeit eines Fehlers bei Anforderung einer Sicherheitsfunktion
PFH	Probability of Failure per Hour: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
PLT-Name	Name eines E/A-Signals oder einer Systemvariablen
R	Read
R/W	Read/Write
rückwirkungsfrei	Es seien zwei Eingangsschaltungen an dieselbe Quelle (z. B. Transmitter) angeschlossen. Dann wird eine Eingangsschaltung «rückwirkungsfrei» genannt, wenn sie die Signale der anderen Eingangsschaltung nicht verfälscht.
SELV	Safety Extra Low Voltage: Schutzkleinspannung
SFF	Safe Failure Fraction, Anteil der sicher beherrschbaren Fehler
SIL	Safety Integrity Level (nach IEC 61508)
SIO	Serial I/O, serielle Schnittstelle für Eingabe/Ausgabe
SNTP	Simple Network Time Protocol (RFC 1769)
SW	Software
TMO	Timeout
W	Write
Watchdog (WD)	Zeitüberwachung für Module oder Programme. Bei Überschreiten der Watchdog-Zeit geht das Modul oder Programm in den Fehlerstopp.
WDZ	Watchdog-Zeit

Abbildungsverzeichnis

Tabellenverzeichnis

Index

HANDBUCH
Sicherheitshandbuch
HI 800 012 D

Für weitere Informationen kontaktieren Sie:

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Telefon +49 6202 709-0
Fax +49 6202 709-107
E-Mail info@hima.com

Erfahren Sie online mehr über HIQuad:

www.hima.com/de/produkte-services/hiquad/

www.hima.com