Modicon M580

Sicherheitshandbuch

Übersetzung der Originalbetriebsanleitung

QGH46984.05
11/2021

www.se.com

Rechtliche Hinweise

Die Marke Schneider Electric sowie alle anderen in diesem Handbuch enthaltenen Markenzeichen von Schneider Electric SE und seinen Tochtergesellschaften sind das Eigentum von Schneider Electric SE oder seinen Tochtergesellschaften. Alle anderen Marken können Markenzeichen ihrer jeweiligen Eigentümer sein. Dieses Handbuch und seine Inhalte sind durch geltende Urheberrechtsgesetze geschützt und werden ausschließlich zu Informationszwecken bereitgestellt. Ohne die vorherige schriftliche Genehmigung von Schneider Electric darf kein Teil dieses Handbuchs in irgendeiner Form oder auf irgendeine Weise (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen oder anderweitig) zu irgendeinem Zweck vervielfältigt oder übertragen werden.

Schneider Electric gewährt keine Rechte oder Lizenzen für die kommerzielle Nutzung des Handbuchs oder seiner Inhalte, ausgenommen der nicht exklusiven und persönlichen Lizenz, die Website und ihre Inhalte in ihrer aktuellen Form zurate zu ziehen.

Produkte und Geräte von Schneider Electric dürfen nur von Fachpersonal installiert, betrieben, instand gesetzt und gewartet werden.

Da sich Standards, Spezifikationen und Konstruktionen von Zeit zu Zeit ändern, können die in diesem Handbuch enthaltenen Informationen ohne vorherige Ankündigung geändert werden.

Soweit nach geltendem Recht zulässig, übernehmen Schneider Electric und seine Tochtergesellschaften keine Verantwortung oder Haftung für Fehler oder Auslassungen im Informationsgehalt dieses Dokuments oder für Folgen, die aus oder infolge der Verwendung der hierin enthaltenen Informationen entstehen.
Als verantwortungsbewusstes Inklusionsunternehmen aktualisieren wir unsere Inhalte, die nicht-inklusive Terminologie enthalten. Bis dieser Vorgang abgeschlossen ist, können unsere Inhalte allerdings nach wie vor standardisierte Branchenbegriffe enthalten, die von unseren Kunden als unangemessen betrachtet werden.

Inhaltsverzeichnis

Sicherheitshinweise

Wichtige Informationen

Lesen Sie sich diese Anweisungen sorgfältig durch und machen Sie sich vor Installation, Betrieb, Bedienung und Wartung mit dem Gerät vertraut. Die nachstehend aufgeführten Warnhinweise sind in der gesamten Dokumentation sowie auf dem Gerät selbst zu finden und weisen auf potenzielle Risiken und Gefahren oder bestimmte Informationen hin, die eine Vorgehensweise verdeutlichen oder vereinfachen.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs „Gefahr“ oder „Warnung“ angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfälle zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge hat.**

⚠ WARNUNG

WARNUNG macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, Tod oder schwere Verletzungen **zur Folge haben kann.**

⚠ VORSICHT

VORSICHT macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, leichte Verletzungen **zur Folge haben kann.**

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Bitte beachten

Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, bedient und gewartet werden. Schneider Electric haftet nicht für Schäden, die durch die Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Bevor Sie beginnen

Dieses Produkt nicht mit Maschinen ohne effektive Sicherheitseinrichtungen im Arbeitsraum verwenden. Das Fehlen effektiver Sicherheitseinrichtungen im Arbeitsraum einer Maschine kann schwere Verletzungen des Bedienpersonals zur Folge haben.

⚠WARNUNG

UNBEAUFSICHTIGTE GERÄTE

- Diese Software und zugehörige Automatisierungsgeräte nicht an Maschinen verwenden, die nicht über Sicherheitseinrichtungen im Arbeitsraum verfügen.
- Greifen Sie bei laufendem Betrieb nicht in das Gerät.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Dieses Automatisierungsgerät und die zugehörige Software dienen zur Steuerung verschiedener industrieller Prozesse. Der Typ bzw. das Modell des für die jeweilige Anwendung geeigneten Automatisierungsgeräts ist von mehreren Faktoren abhängig, z. B. von der benötigten Steuerungsfunktion, der erforderlichen Schutzklasse, den Produktionsverfahren, außergewöhnlichen Bedingungen, behördlichen Vorschriften usw. Für einige Anwendungen werden möglicherweise mehrere Prozessoren benötigt, z. B. für ein Backup-/Redundanzsystem.

Nur Sie als Benutzer, Maschinenbauer oder -integrator sind mit allen Bedingungen und Faktoren vertraut, die bei der Installation, der Einrichtung, dem Betrieb und der Wartung der Maschine bzw. des Prozesses zum Tragen kommen. Demzufolge sind allein Sie in der Lage, die Automatisierungskomponenten und zugehörigen Sicherheitsvorkehrungen und Verriegelungen zu identifizieren, die einen ordnungsgemäßen Betrieb gewährleisten. Bei der Auswahl der Automatisierungs- und Steuerungsgeräte sowie der zugehörigen Software für eine bestimmte Anwendung sind die einschlägigen örtlichen und landesspezifischen Richtlinien und Vorschriften zu beachten. Das National Safety Council's Accident Prevention

Manual (Handbuch zur Unfallverhütung; in den USA landesweit anerkannt) enthält ebenfalls zahlreiche nützliche Hinweise.

Für einige Anwendungen, z. B. Verpackungsmaschinen, sind zusätzliche Vorrichtungen zum Schutz des Bedienpersonals wie beispielsweise Sicherheitseinrichtungen im Arbeitsraum erforderlich. Diese Vorrichtungen werden benötigt, wenn das Bedienpersonal mit den Händen oder anderen Körperteilen in den Quetschbereich oder andere Gefahrenbereiche gelangen kann und somit einer potenziellen schweren Verletzungsgefahr ausgesetzt ist. Software-Produkte allein können das Bedienpersonal nicht vor Verletzungen schützen. Die Software kann daher nicht als Ersatz für Sicherheitseinrichtungen im Arbeitsraum verwendet werden.

Vor Inbetriebnahme der Anlage sicherstellen, dass alle zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen installiert und funktionsfähig sind. Alle zum Schutz des Arbeitsraums vorgesehenen Sicherheitseinrichtungen und Verriegelungen müssen mit dem zugehörigen Automatisierungsgerät und der Softwareprogrammierung koordiniert werden.

HINWEIS: Die Koordinierung der zum Schutz des Arbeitsraums vorgesehenen mechanischen/elektronischen Sicherheitseinrichtungen und Verriegelungen geht über den Umfang der Funktionsbaustein-Bibliothek, des System-Benutzerhandbuchs oder andere in dieser Dokumentation genannten Implementierungen hinaus.

Start und Test

Vor der Verwendung elektrischer Steuerungs- und Automatisierungsgeräte ist das System zur Überprüfung der einwandfreien Funktionsbereitschaft einem Anlauftest zu unterziehen. Dieser Test muss von qualifiziertem Personal durchgeführt werden. Um einen vollständigen und erfolgreichen Test zu gewährleisten, müssen die entsprechenden Vorkehrungen getroffen und genügend Zeit eingeplant werden.

⚠WARNUNG

GEFAHR BEIM GERÄTEBETRIEB

- Überprüfen Sie, ob alle Installations- und Einrichtungsverfahren vollständig durchgeführt wurden.
- Vor der Durchführung von Funktionstests sämtliche Blöcke oder andere vorübergehende Transportsicherungen von den Anlagekomponenten entfernen.
- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Führen Sie alle in der Dokumentation des Geräts empfohlenen Anlauftests durch. Die gesamte Dokumentation zur späteren Verwendung aufbewahren.

Softwaretests müssen sowohl in simulierten als auch in realen Umgebungen stattfinden.

Sicherstellen, dass in dem komplett installierten System keine Kurzschlüsse anliegen und nur solche Erdungen installiert sind, die den örtlichen Vorschriften entsprechen (z. B. gemäß dem National Electrical Code in den USA). Wenn Hochspannungsprüfungen erforderlich sind, beachten Sie die Empfehlungen in der Gerätedokumentation, um eine versehentliche Beschädigung zu verhindern.

Vor dem Einschalten der Anlage:

- Entfernen Sie Werkzeuge, Messgeräte und Verschmutzungen vom Gerät.
- Schließen Sie die Gehäusetür des Geräts.
- Alle temporären Erdungen der eingehenden Stromleitungen entfernen.
- Führen Sie alle vom Hersteller empfohlenen Anlauftests durch.

Betrieb und Einstellungen

Die folgenden Sicherheitshinweise sind der NEMA Standards Publication ICS 7.1-1995 entnommen (die Englische Version ist maßgebend):

- Ungeachtet der bei der Entwicklung und Fabrikation von Anlagen oder bei der Auswahl und Bemessung von Komponenten angewandten Sorgfalt, kann der unsachgemäße Betrieb solcher Anlagen Gefahren mit sich bringen.
- Gelegentlich kann es zu fehlerhaften Einstellungen kommen, die zu einem unbefriedigenden oder unsicheren Betrieb führen. Für Funktionseinstellungen stets die Herstelleranweisungen zu Rate ziehen. Das Personal, das Zugang zu diesen Einstellungen hat, muss mit den Anweisungen des Anlagenherstellers und den mit der elektrischen Anlage verwendeten Maschinen vertraut sein.
- Bediener sollten nur über Zugang zu den Einstellungen verfügen, die tatsächlich für ihre Arbeit erforderlich sind. Der Zugriff auf andere Steuerungsfunktionen sollte eingeschränkt sein, um unbefugte Änderungen der Betriebskenngrößen zu vermeiden.

Informationen zum Dokument

Geltungsbereich

Das Sicherheitshandbuch beschreibt die Module des M580-Sicherheitssystems mit besonderem Schwerpunkt auf die Erfüllung der Sicherheitsanforderungen nach IEC 61508. Das Handbuch enthält detaillierte Informationen zur ordnungsgemäßen Installation, zum Betrieb und zur Verwaltung des Systems, damit der Schutz des Personals gewährleistet und Schäden für Umwelt, Geräte und Produktion vermieden werden können.

Diese Dokumentation richtet sich an qualifiziertes Fachpersonal, das mit funktionaler Sicherheit und der Sicherheit von Control Expert vertraut ist. Inbetriebnahme und Bedienung des M580-Sicherheitssystems dürfen nur von Personal ausgeführt werden, das zur Inbetriebnahme und Bedienung von Systemen in Übereinstimmung mit den geltenden Standards für funktionale Systeme berechtigt ist.

HINWEIS:

- Die englische Version dieses Handbuchs ist die Originalversion.
- Im Falle von Änderungsanforderungen oder Qualitätsproblemen in Bezug auf das M580-Sicherheitsangebot wenden Sie sich an die Kundenbetreuung. Weitere Informationen finden Sie auf der Website von Schneider Electric auf der Seite *Support/Kontakt*:

  www.se.com/b2b/en/support/

Gültigkeitsanmerkung

Diese Dokumentation gilt für ™EcoStruxure Control Expert Safety 15.0 oder höher.

Informationen zur Produktkonformität sowie Umwelthinweise (RoHS, REACH, PEP, EOLI usw.) finden Sie unter www.se.com/ww/en/work/support/green-premium/.

Die technischen Merkmale der hier beschriebenen Geräte sind auch online abrufbar. Um auf die Online-Informationen zuzugreifen, gehen Sie zur Homepage von Schneider Electric www.se.com/ww/en/download/.

Die in diesem Handbuch vorgestellten Merkmale sollten denen entsprechen, die online angezeigt werden. Im Rahmen unserer Bemühungen um eine ständige Verbesserung werden Inhalte im Laufe der Zeit möglicherweise überarbeitet, um deren Verständlichkeit und Genauigkeit zu verbessern. Sollten Sie einen Unterschied zwischen den Informationen im Handbuch und denen online feststellen, nutzen Sie die Online-Informationen als Referenz.

Weiterführende Dokumentation

Titel der Dokumentation	Referenznummer
M580 Safety SRAC — SRAC Verification Plan	EIO0000004540 (Englisch)
Modicon M580, Sicherheitssystem, Planungshandbuch	QGH60283 (Englisch), QGH60284 (Französisch), QGH60285 (Deutsch), QGH60286 (Spanisch), QGH60287 (Italienisch), QGH60288 (Chinesisch)
EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek	QGH60275 (Englisch), QGH60278 (Französisch), QGH60279 (Deutsch), QGH60280 (Italienisch), QGH60281 (Spanisch), QGH60282 (Chinesisch)
Modicon-Steuerungsplattform – Cybersicherheit, Referenzhandbuch	EIO0000001999 (Englisch), EIO0000002001 (Französisch), EIO0000002000 (Deutsch), EIO0000002002 (Italienisch), EIO0000002003 (Spanisch), EIO0000002004 (Chinesisch)
Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen	NHA58880 (Englisch), NHA58881 (Französisch), NHA58882 (Deutsch), NHA58883 (Italienisch), NHA58884 (Spanisch), NHA58885 (Chinesisch)
Modicon M580 – Hardware, Referenzhandbuch	EIO0000001578 (Englisch), EIO0000001579 (Französisch), EIO0000001580 (Deutsch), EIO0000001582 (Italienisch), EIO0000001581 (Spanisch), EIO0000001583 (Chinesisch)
Modicon M580 Einzelgerät, Systemplanungshandbuch für häufig verwendete Architekturen	HRB62666 (Englisch), HRB65318 (Französisch), HRB65319 (Deutsch), HRB65320 (Italienisch), HRB65321 (Spanisch), HRB65322 (Chinesisch)
Modicon M580 – Systemplanungshandbuch für komplexe Topologien	NHA58892 (Englisch), NHA58893 (Französisch), NHA58894 (Deutsch), NHA58895 (Italienisch), NHA58896 (Spanisch), NHA58897 (Chinesisch)
EcoStruxure™ Automation Device Maintenance - Benutzerhandbuch	EIO0000004033 (Englisch), EIO0000004048 (Französisch), EIO0000004046 (Deutsch), EIO0000004049 (Italienisch), EIO0000004047 (Spanisch), EIO0000004050 (Chinesisch)
Unity Loader - Benutzerhandbuch	33003805 (Englisch), 33003806 (Französisch), 33003807 (Deutsch), 33003809 (Italienisch), 33003808 (Spanisch), 33003810 (Chinesisch)
EcoStruxure™ Control Expert – Betriebsarten	33003101 (Englisch), 33003102 (Französisch), 33003103 (Deutsch), 33003104 (Spanisch), 33003696 (Italienisch), 33003697 (Chinesisch)
EcoStruxure™ Control Expert – Systembits und -wörter, Referenzhandbuch	EIO0000002135 (Englisch), EIO0000002136 (Französisch), EIO0000002137 (Deutsch), EIO0000002138 (Italienisch), EIO0000002139 (Spanisch), EIO0000002140 (Chinesisch)

Diese technischen Veröffentlichungen, das vorliegende Dokument sowie andere technische Informationen stehen auf unserer Website www.se.com/en/download/ zum Download bereit.

M580-Sicherheitsfunktion

Inhalt dieses Kapitels

Einführung

In diesem Kapitel wird die M580-Sicherheitsfunktion für das M580-Sicherheitssystem und die einzelnen Sicherheitsmodule erläutert.

M580-Sicherheitsfunktion

Einführung in die M580-Sicherheitsfunktion von Schneider Electric

Control Expert mit Sicherheitfunktion ermöglicht Ihnen die Programmierung, Konfiguration und Wartung von Sicherheitsanwendungen. Bei der Entwicklung und Programmierung Ihrer Sicherheitsanwendung sollten Sie nur den Komponenten einer Sicherheitsschleife Sicherheitsfunktionen hinzufügen.

HINWEIS: Nur Sicherheitsmodule, ihre Konfigurationseinstellungen und Daten sollten Teil der Sicherheitsschleife sein.

Nach der Inbetriebnahme liest, während Ihr M580-Sicherheitssystem im Sicherheitsmodus läuft, das Sicherheitssystem regelmäßig die Sicherheitseingänge, verarbeitet die Programmsicherheitslogik der Anwendung, führt Diagnoseschritte durch und wendet die Logikergebnisse auf die Sicherheitsausgänge an.

Wenn die CPU oder die E/A-Diagnose einen Fehler erkennt, wird der betroffene Teil des Systems in einen sicheren Zustand versetzt. Abhängig von der Art des entdeckten Fehlers handelt es sich dabei um einen einzelnen E/A-Kanal, ein E/A-Modul oder das gesamte System.

Der sichere Zustand ist immer der deaktivierte Zustand. Beispiel:

- Wenn das analoge Eingangsmodul BMXSAI0410 oder das digitale Eingangsmodul BMXSDI1602 einen kritischen Fehler erkennt, wird der Wert seiner CPU-Eingänge auf 0 (deaktiviert) gesetzt. Dieser Zustand wird aufrechterhalten, bis das zugrundeliegende Problem gelöst wird.
- Wenn das digitale Ausgangsmodul BMXSDO0802 oder das digitale Relaisausgangsmodul BMXSRA0405 einen kritischen internen Fehler erkennt, werden die Ausgänge in den deaktivierten Zustand versetzt. Dieser Zustand wird aufrechterhalten, bis das zugrundeliegende Problem gelöst und das Modul neu gestartet wird.
- Wenn das digitale Ausgangsmodul BMXSDO0802 oder das digitale Relaisausgangsmodul BMXSRA0405 auf einem schwarzen Kanal zur CPU einen Kommunikationsfehler erkennen, versetzt das Ausgangsmodul seine Ausgänge in den Fehlerausweichzustand.

  HINWEIS: Mit Control Expert Safety können Sie den Fehlerausweichzustand konfigurieren (erregt, entregt oder letzten Wert beibehalten), falls die Kommunikation über einen schwarzen Kanal zwischen CPU und Ausgangsmodul verloren geht.

- Wenn eine Standalone-CPU BMEP58•040S oder eine Hot Standby-CPU BMEH58•040S einen Kommunikationsfehler entdeckt, der auf einem schwarzen Kanal zu einem Sicherheitseingangsmodul vorliegt, wird der Zustand der betroffenen Eingänge auf 0 (entregter Zustand) gesetzt, bis der schwarze Kanal wieder funktionsfähig ist und die CPU die tatsächlichen Eingangswerte lesen kann.

Sicherheitsschleife

Eine Sicherheitsschleife ist die Zusammenstellung von Geräten und Logik, über die ein Sicherheitsprozess ausgeführt wird. Ein Sicherheitsprojekt kann mehrere Sicherheitsschleifen umfassen. Für jede Sicherheitsschleife müssen Sie Folgendes überprüfen:

- Die Prozesssicherheitsdauer, Seite 156 ist länger als die Systemantwortzeit, Seite 156.
- Die Summe der PFD- oder PFH-Werte, Seite 149 für alle Komponenten der Sicherheitsschleife überschreitet nicht den zulässigen Höchstwert für:
  - Sicherheitsintegritäts-Level (1, 2, 3, oder 4)
  - Betriebsmodus (hohes oder niedriges Anforderungsniveau)
  - Prüfabstand

Nur Sicherheitsausrüstung sollte Teil der Sicherheitsschleife sein. Sie können zwar nicht-störende Module, Seite 29 in Ihr Sicherheitsprojekt aufnehmen, aber diese sollten Sie nur für nicht-sichere Tasks (MAST, FAST, AUX0 oder AUX1) einsetzen.

⚠WARNUNG

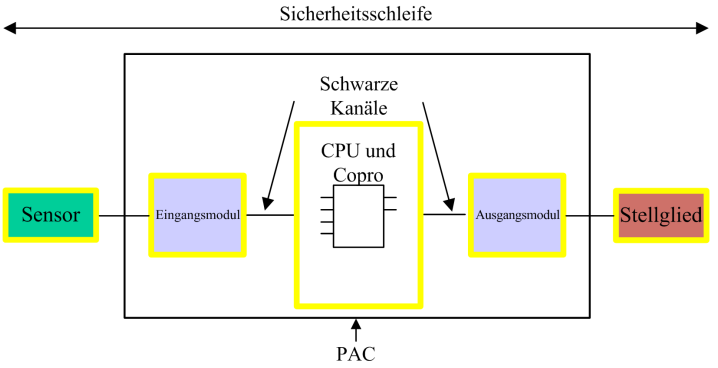
VERLUST DER FÄHIGKEIT ZUR AUSFÜHRUNG VON SICHERHEITSFUNKTIONEN

- Nutzen Sie nur Sicherheitsmodule, um Sicherheitsfunktionen durchzuführen.
- Nutzen Sie für Sicherheitsfunktionen keine Ein- oder Ausgänge nicht-störender Module.
- Nutzen Sie für Sicherheitsfunktionen keine Variablen aus dem globalen Bereich.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Eine Beschreibung der Variablen aus dem globalen Bereich finden Sie unter *Datentrennung in einem M580-Sicherheitsprojekt*, Seite 174.

Sicherheitsschleife:



Zur Sicherheitsausrüstung gehören die folgenden M580-Sicherheitsmodule von Schneider Electric:

- CPU für BME•58•040S und Koprozessor für BMEP58CPROS3:

  CPU und Koprozessor führen zusammen Tasks wie das Lesen von Sicherheitseingängen, Verarbeiten der Sicherheitslogik, Durchführen der Diagnose und Anwenden der Ergebnisse auf Ausgänge durch. All diese Tasks sind Teil der Sicherheitsschleife. Ports, die für die Kommunikation über schwarze Kanäle genutzt werden, sind ebenfalls Teil der Sicherheitsschleife. Andere CPU-Komponenten – USB-Port, SD-Speicherkarte und nicht-flüchtiger, statischer Arbeitsspeicher (nvSRAM) – sind jedoch nicht Teil der Sicherheitsschleife.

  HINWEIS: Sowohl bei einem Kalt- als auch bei einem Warmstart des Systems laden CPU und Koprozessor keine Daten aus dem nvSRAM in die Sicherheitstask. (nvSRAM-Daten werden nur in nicht-sicheren MAST-, FAST- und AUX-Tasks verwendet.) Stattdessen wenden CPU und Koprozessor zunächst Standardkonfigurationseinstellungen von der SD-Speicherkarte an und anschließend Werte, die sie während des Betriebs direkt von den Eingängen erhalten.

- E/A-Sicherheitsmodul (BMXSAI0410, BMXSDI1602, BMXSDO0802 und BMXSRA0405):

  Die Funktionen zum Senden von Eingangssignalen, Empfangen von Ausgangssignalen und Durchführen von Diagnoseelementen sind Teil der Sicherheitsschleife.

- Spannungsversorgungen BMXCPS4002S, BMXCPS4022S und BMXCPS3522S:

  Diese Sicherheitsspannungsversorgungen erkennen Überspannungen, was auch zur Sicherheitsschleife gehört. Da die Zuverlässigkeit jeder Spannungsversorgung (d. h. die Rate gefährlicher Fehler) hundertfach besser ist als vom SIL3-Standard vorgegeben, werden diese Sicherheitsspannungsversorgungen nicht in die Berechnung des Sicherheitsintegritäts-Levels für die Sicherheitsschleife einbezogen.

Die Sicherheitsschleife umfasst zudem die folgenden nicht-sicheren Elemente:

- Sensoren, Stellglieder und die Verkabelung, die sie mit den E/A-Sicherheitsmodulen verbinden. Das E/A-Sicherheitsmodul führt eine Verdrahtungsdiagnose für Sensoren und Stellglieder durch, um bei der Verwaltung der Sicherheitsschleife zu helfen.

  HINWEIS: Beim Entwickeln Ihrer Sicherheitsanwendung müssen Sie die Eigenschaften der Sensoren und Stellglieder festlegen (insbesondere die PFD/PFH-Werte).

Zertifizierungsstandards

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die Zertifizierungsstandards beschrieben, die für das M580-Sicherheitssystem und seine Komponenten und Module gelten.

Zertifizierungen

Zertifizierungsstandards für den M580-Sicherheits-PAC

Der M580-Sicherheits-PAC wurde von der TÜV Rheinland Group für den Einsatz in Anwendungen zertifiziert bis:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat 4 / ISO 13849-1

Detaillierte Informationen zur SIL-Bewertung finden Sie unter Beschreibung der SIL-Bewertung, Seite 406.

Technische Daten der programmierbaren Steuerung

- IEC 61131-2 Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittelanforderungen und Prüfungen.
- IEC/EN 61010-2-201, UL 61010-2-201, CSA-C22.2 Nr. 61010-2-201: Sicherheitsanforderungen für elektrische Anlagen - Teil 2-201: Besondere Anforderungen an Steuergeräte.

Umgebungsspezifische Kenndaten

Informationen zu Umgebungsteststufen finden Sie unter M580-Normen und -Zertifizierungen, Seite 25.

Technische Daten für explosionsgefährdete Bereiche

Für die USA und Kanada: Gefahrenbereich Klasse I, Division 2, Gruppen A, B, C und D

- CSA 22.2 Nr. 213, ANSI/ISA12.12.01 und FM3611

Für andere Länder: CE ATEX (Richtlinie 2014/34/EU) oder IECEx in definierter Atmosphäre Zone 2 (Gas) und/oder Zone 22 (Staub)

- IEC/EN 60079-0 ; IEC/EN 60079-7; IEC/EN 60079-15

Technische Daten für Automatisierungssysteme für die Energieversorgung

- IEC/EN 61000-6-5 Elektromagnetische Verträglichkeit - Teil 6-5: Allgemeine Normen - Störfestigkeit für Kraftwerke und Trafostationen.
- IEC/EN 61850-3 Kommunikationsnetzwerke und -systeme für die Automatisierung von Energieversorgungsunternehmen - Teil 3: Allgemeine Anforderungen

Informationen zu Installationsbeschränkungen finden Sie unter M580 Normen und Zertifizierungen, Seite 25.

Technische Daten für den Bahnsektor

- EN 50126 / IEC 62278: Bahnanwendungen - Spezifikation und Demonstration von Zuverlässigkeit, Verfügbarkeit, Wartbarkeit und Sicherheit (RAMS).
- EN 50128 / IEC 62279: Bahnanwendungen - Kommunikations-, Signal- und Verarbeitungssysteme - Software für Bahnleitungs- und Schutzsysteme.
- EN 50129 / IEC 62245: Bahnanwendungen - Kommunikations-, Signal- und Verarbeitungssysteme - Sicherheitsbezogene elektronische Systeme für die Signalisierung.
- EN 50155 / IEC 60571: Bahnanwendungen - Schienenfahrzeuge - Elektronische Anlagen.
- EN 50121-3-2 / IEC 62236-3-2: Bahnanwendungen - Elektromagnetische Verträglichkeit - Teil 3-2: Triebfahrzeug - Gerät.
- EN 50121-4 / IEC 62236-4: Bahnanwendungen - Elektromagnetische Verträglichkeit - Teil 4: Störaussendung und Störfestigkeit des Signalgerätes und des Telekommunikationsgeräts.
- EN 50121-5 / IEC 62236-5: Bahnanwendungen - Elektromagnetische Verträglichkeit - Teil 5: Störaussendung und Störfestigkeit von Anlagen und Geräten zur Spannungsversorgung in Festeinbau.
- EN 50125-1: Bahn - Umgebungsbedingungen für Anlagen - Teil 1: Schienenfahrzeuge und Bordausrüstung.
- EN 50125-3: Bahn - Umgebungsbedingungen für Anlagen - Teil 3: Geräte für Signalübertragung und Telekommunikation.
- EN 50124-1: Schienenverkehr - Isolationskoordination - Teil 1: Grundlegende Anforderungen - Abstände und Kriechstrecken für alle elektrischen und elektronischen Geräte.

Informationen zu Installationsbeschränkungen finden Sie unter M580 Normen und Zertifizierungen, Seite 25.

Technische Daten für die funktionale Sicherheit

- IEC/EN 61000-6-7 Elektromagnetische Verträglichkeit - Teil 6-7: Allgemeine Normen - Anforderungen an die Störfestigkeit von Geräten, die für die Ausführung von Funktionen in einem sicherheitsbezogenen System (funktionale Sicherheit) an industriellen Standorten bestimmt sind.
- IEC 61326-3-1: Elektrische Ausrüstung für Messung, Steuerung und Laborverwendung - Teil 3-1: Anforderungen an die Störfestigkeit von sicherheitsbezogenen Systemen und Anlagen zur Ausführung sicherheitsbezogener Funktionen - Allgemeine industrielle Anwendung.
- IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1-7, Ausgabe 2.0.
- IEC 61511-1: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Framework, Definitionen, System-, Hardware- und Softwareanforderungen.
- IEC 61511-2: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 2: Richtlinien für die Anwendung von IEC 61511-1.
- IEC 61511-3: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 3: Anleitung zur Bestimmung der erforderlichen Sicherheitsanforderungsstufen.

Technische Daten für die Maschinensicherheit

- IEC/EN 62061 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und elektronisch programmierbarer Steuerungssysteme
- ISO EN 13849-1: Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze.

Technische Daten für die funktionale Sicherheit in Systemen

- EN 54-2: Brandmelde- und Brandmeldeanlagen Teil 2: Steuerungs- und Anzeigegeräte.
- EN 50156-1: Elektrische Ausrüstung für Öfen und Zusatzausrüstung - Teil 1: Anforderungen an Anwendungsdesign und -installation.
- EN 50130-4: Alarmsysteme - Teil 4: Elektromagnetische Verträglichkeit - Produktnorm: Anforderungen an die Störfestigkeit von Feuer-, Eindringschutz-, Halte-, CCTV-, Zugangskontrolle- und sozialen Alarmsystemen.

- EN 298: Automatische Brennersteuerungen für Brenner und Geräte, die gasförmige oder flüssige Brennstoffe verbrennen.
- NFPA 85: Code für Gefahr von Kesselanlagen und Verbrennungsanlagen.
- NFPA 86: Standard für Öfen und Brennöfen.
- NFPA 72: Nationaler Feueralarm-/Brandmeldecode.

Hinweis:

Eine vollständige Liste der Normen (mit Überarbeitungen und Datumsangaben), die vom TÜV zertifiziert sind, finden Sie auf folgender Website:

www.certipedia.com or www.fs-products.com.

Normen und Zertifizierungen

Download

Klicken Sie auf die Verknüpfung für Ihre bevorzugte Sprache, um die Normen und Zertifizierungen für die Module dieser Produktfamilie (im PDF-Format) herunterzuladen:

Titel	Sprachen
Modicon M580, M340 und X80 I/O-Plattformen, Normen und Zertifizierungen	• Englisch: EIO0000002726 • Französisch: EIO0000002727 • Deutsch: EIO0000002728 • Italienisch: EIO0000002730 • Spanisch: EIO0000002729 • Chinesisch: EIO0000002731

Vom M580-Sicherheitssystem unterstützte Module

Inhalt dieses Kapitels

Einführung

Ein M580-Sicherheitsprojekt kann sowohl Sicherheitsmodule als auch nicht-sichere Module umfassen. Sie können folgende Komponenten verwenden:

- Sicherheitsmodule in der SAFE-Task
- Nicht-sichere Module nur in nicht-sicheren Tasks (MAST, FAST, AUX0 und AUX1)

  HINWEIS: In einem Sicherheitsprojekt können nur nicht-sichere Module hinzugefügt werden, die sich nicht störend auf die Sicherheitsfunktion auswirken.

Verwenden Sie für die Programmierung, Inbetriebnahme und Bedienung Ihrer M580-Sicherheitsanwendung nur die Programmiersoftware Control Expert von Schneider Electric.

- Control Expert L Safety stellt den gesamten Funktionsumfang von Control Expert L bereit und kann mit den Sicherheits-CPUs BMEP582040S und BMEH582040S eingesetzt werden.
- Control Expert XL Safety bietet den gesamten Funktionsumfang von Control Expert XL und kann mit der kompletten Baureihe der Sicherheits-CPUs BMEP58•040S und BMEH58•040S verwendet werden.

In diesem Kapitel werden die vom M580-Sicherheitssystem unterstützten sicherheitsspezifischen und nicht-sicheren Module aufgeführt.

Für das M580-Sicherheitssystem zertifizierte Module

Zertifizierte Module

Der M580 -Sicherheits-PAC ist ein von der TÜV Rheinland Group zertifiziertes Sicherheitssystem:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

Es basiert auf der Produktfamilie der M580-PACs (Programmable Automation Controller). Die folgenden M580-Sicherheitsmodule von Schneider Electric sind zertifiziert:

- Standalone-CPU BMEP582040S
- Standalone-CPU BMEP584040S
- Standalone-CPU BMEP586040S
- Hot Standby-CPU BMEH582040S
- Hot Standby-CPU BMEH584040S
- Hot Standby-CPU BMEH586040S
- Koprozessor BMEP58CPROS3
- Analoges Eingangsmodul BMXSAI0410
- Digitales Eingangsmodul BMXSDI1602
- Digitales Ausgangsmodul BMXSDO0802
- Digitales Relaisausgangsmodul BMXSRA0405
- Spannungsversorgung BMXCPS4002S
- Spannungsversorgung BMXCPS4022S
- Spannungsversorgung BMXCPS3522S

HINWEIS: Zusätzlich zu den oben aufgeführten Sicherheitsmodulen können in ein Sicherheitsprojekt ebenfalls nicht-störende, nicht-sichere Module, Seite 29 aufgenommen werden.

HINWEIS: Das Modicon-Sicherheitsangebot gilt bis SIL3 (Reg. IEC 61508) und ist PLe-konform (Register ISO 13849), d. h. es ist auch SIL1/SIL2- und PLa/b/c/d-fähig.

HINWEIS:

- Jedes Mal, wenn im Dokument SIL2 oder SIL3 ohne Standardreferenz erwähnt wird, gilt dies für IEC 61508 / IEC 61511.
- Jedes Mal, wenn SIL2 erwähnt wird, handelt es sich um SIL3 in Bezug auf EN 50126 / EN 50128 / EN 50129.
- Jedes Mal, wenn SIL3 erwähnt wird, gilt dies SIL4 in Bezug auf EN 50126 / EN 50128 / EN 50129.

Aktuelle Informationen zu den zertifizierten Produktversionen finden Sie auf der Website der TÜV Rheinland AG: www.certipedia.com oder www.fs-products.com.

Ersetzen einer CPU

Eine CPU BME•58•040S kann durch eine andere CPU BME•58•040S ersetzt werden. Der Austausch funktioniert allerdings nur, wenn die folgenden Einschränkungen berücksichtigt werden:

- Anzahl der E/A
- Anzahl der E/A-Stationen
- Anzahl der Variablen
- Größe des Anwendungsspeichers

Siehe folgende Themen:

- Unter *Konfigurationskompatibilität* im *Modicon M580 Hot Standby Systemplanungshandbuch für häufig verwendete Architekturen* finden Sie eine Beschreibung der mit Sicherheits- und Hot Standby-CPUs kompatiblen Control Expert-Anwendungen.
- Für eine Beschreibung der CPU-Einschränkungen siehe M580 CPU- und Koprozessor-Leistungsmerkmale im *Modicon M580 Sicherheitssystem - Planungshandbuch*.

Nicht-störende Module

Einführung

Ein M580-Sicherheitsprojekt kann sowohl Sicherheitsmodule als auch nicht-sichere Module umfassen. Sie können Nicht-Sicherheitsmodule nur für nicht-sichere Tasks einsetzen. In einem Sicherheitsprojekt können nur solche nicht-sicheren Module hinzugefügt werden, die sich nicht störend auf die Sicherheitsfunktion auswirken.

Definition eines nicht-störenden Moduls

⚠VORSICHT

UNSACHGEMÄSSE VERWENDUNG SICHERHEITSBEZOGENER DATEN

Stellen Sie sicher, dass weder die Eingangs- noch die Ausgangsdaten nicht-störender Module zur Steuerung sicherheitsbezogener Ausgänge verwendet werden. Nicht-sichere Module können nur nicht-sichere Daten verarbeiten.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Ein nicht-störendes Modul ist ein Modul, das sich nicht störend auf die Sicherheitsfunktion auswirkt. Für rackinterne M580-Module (BMEx, BMXx, PMXx und PMEx) sind zwei Typen nicht-störender Module verfügbar:

- **Typ 1**: Ein Modul des Typs 1 kann im gleichen Rack wie Sicherheitsmodule installiert werden (an der Stelle, an der das Sicherheitsmodul im Haupt- oder Erweiterungsrack platziert ist).
- **Typ 2**: Ein nicht-störendes Modul des Typs 2 kann nicht im gleichen Hauptrack wie die Sicherheitsmodule installiert werden (egal, wo das Sicherheitsmodul platziert ist, im Haupt- oder Erweiterungsrack).

  HINWEIS: Die Module vom Typ 1 und Typ 2 sind auf der Website von TÜV Rheinland unter www.certipedia.com aufgeführt.

  Für nicht-rackinterne Mx80-Module können alle Ethernet-Geräte (DIO oder DRS) als nicht-störend eingestuft und folglich als Teil eines M580-Sicherheitssystems eingesetzt werden.

Nicht-störende Module des Typs 1 für SIL3-Anwendungen

Die folgenden nicht-sicheren Module können als nicht-störende Module des Typs 1 in einem M580 -Sicherheitssystem eingesetzt werden.

HINWEIS: Die Liste der nicht-störenden, nicht-sicheren Module des Typs 1 kann sich von Zeit zu Zeit ändern. Die aktuelle Liste finden Sie auf der Website von TÜV Rheinland unter www.certipedia.com.

Modultyp	Modulreferenz
Baugruppenträger mit 4 Steckplätzen	BMEXBP0400
Baugruppenträger mit 8 Steckplätzen	BMEXBP0800
Baugruppenträger mit 12 Steckplätzen	BMEXBP1200
Baugruppenträger mit 4 Steckplätzen	BMXXBP0400
Baugruppenträger mit 6 Steckplätzen	BMXXBP0600
Baugruppenträger mit 8 Steckplätzen	BMXXBP0800
Baugruppenträger mit 12 Steckplätzen	BMXXBP1200
Baugruppenträger mit 6 Steckplätzen und Dual-Steckplätzen für redundante Spannungsversorgungen	BMEXBP0602
Baugruppenträger mit 10 Steckplätzen und Dual-Steckplätzen für redundante Spannungsversorgungen	BMEXBP1002
Kommunikation: Performance X80 Ethernet-Stationsadapter, 1 K	BMXCRA31210
Kommunikation: Performance X80 Ethernet-Stationsadapter, 1 K	BMECRA31210
Kommunikation: Ethernet-Modul mit Standard-Webdiensten	BMENOC0301
Kommunikation: Ethernet-Modul mit IP-Weiterleitung	BMENOC0321
Kommunikation: Ethernet-Modul mit FactoryCast-Webdiensten	BMENOC0311
Kommunikation: Rack-Erweiterungsmodul	BMXXBE1000
Kommunikation: AS-Schnittstelle	BMXEIA0100
Kommunikation: Globale Daten	BMXNGD0100
Kommunikation: Glasfaserkonverter MM/LC, 2 Kanäle, 100 MB	BMXNRP0200
Kommunikation: Glasfaserkonverter SM/LC, 2 Kanäle, 100 MB	BMXNRP0201
Kommunikation: Kommunikationsmodul M580 IEC 61850	BMENOP0300
Kommunikation: Integrierter OPC UA-Server	BMENUA0100
Beim Aufwärtszählen: SSI-Modul 3 CH	BMXEAE0300

Modultyp	Modulreferenz
Beim Aufwärtszählen: Hochgeschwindigkeitszähler 2 Kanäle	BMXEHC0200
Beim Aufwärtszählen: Hochgeschwindigkeitszähler, 8 Kanäle	BMXEHC0800
Bewegung: Impulswellenausgang, 2 unabhängige Kanäle	BMXMSP0200
Analog: 8 potenzialgetrennte analoge HART-Eingänge	BMEAHI0812
Analog: 4 potenzialgetrennte analoge HART-Ausgänge	BMEAHO0412
Analog: 4 potentialgetrennte analoge Hochgeschwindigkeitseingänge U/I	BMXAMI0410
Analog: 4 nicht potentialgetrennte analoge Hochgeschwindigkeitseingänge U/I	BMXAMI0800
Analog: 8 potentialgetrennte analoge Hochgeschwindigkeitseingänge U/I	BMXAMI0810
Analog: 4 Analogeingänge U/I, 4 Analogausgänge U/I	BMXAMM0600
Analog: 2 potentialgetrennte Analogausgänge U/I	BMXAMO0210
Analog: 4 potentialgetrennte Analogausgänge U/I	BMXAMO0410
Analog: 8 nicht potentialgetrennte Analogausgänge Strom	BMXAMO0802
Analog: 4 potentialgetrennte Analogeingänge TC/RTD	BMXART0414.2
Analog: 8 potentialgetrennte Analogeingänge TC/RTD	BMXART0814.2
Digital: 8 Digitaleingänge 220 VAC	BMXDAI0805
Digital: 8 potenzialgetrennte Digitaleingänge 100 bis 120 VAC	BMXDAI0814
Digital: 16 Digitaleingänge 24 VAC/24 VDC, Source (Strom lieferend)	BMXDAI1602
Digital: 16 Digitaleingänge 48 VAC	BMXDAI1603
Digital: 16 Digitaleingänge 100 bis 120 VAC, 20-polig	BMXDAI1604
Digital: 16 überwachte digitale Eingangskanäle 100 bis 120 VAC, 40-polig	BMXDAI1614
Digital: 16 überwachte digitale Eingangskanäle 200 bis 240 VAC, 40-polig	BMXDAI1615
Digital: 16 Triacs-Digitalausgänge, 100 bis 240 VAC, 20-polig	BMXDAO1605
Digital: 16 Triacs-Digitalausgänge, 24 bis 240 VAC, 40-polig	BMXDAO1615
Digital: 16 Digitaleingänge 24 VDC, Sink (Strom ziehend)	BMXDDI1602
Digital: 16 Digitaleingänge 48 VDC, Sink	BMXDDI1603
Digital: Digitaleingänge 125 VDC, Sink	BMXDDI1604T
Digital: 32 Digitaleingänge 24 VDC, Sink	BMXDDI3202K
Digital: 64 Digitaleingänge 24 VDC, Sink	BMXDDI6402K
Digital: 8 Digitaleingänge 24 VDC, 8 digitale Transistorausgänge Source	BMXDDM16022

Modultyp	Modulreferenz
Digital: 8 Digitaleingänge 24 VDC, 8 digitale Relaisausgämge	BMXDDM16025
Digital: 16 Digitaleingänge 24 VDC, 16 digitale Transistorausgänge Source	BMXDDM3202K
Digital: 16 digitale Transistorausgänge, Source 0,5 A	BMXDDO1602
Digital: 16 digitale Transistorausgänge, Sink	BMXDDO1612
Digital: 32 digitale Transistorausgänge, Source 0,1 A	BMXDDO3202K
Digital: 64 digitale Transistorausgänge, Source 0,1 A	BMXDDO6402K
Digital: 8 Digitalausgänge 125 VDC	BMXDRA0804T
Digital: 8 potenzialgetrennte digitale Relaisausgänge 24 VDC oder 24 bis 240 VAC	BMXDRA0805
Digital: 16 nicht potenzialgetrennte digitale Relaisausgangskanäle 5 bis 125 VDC oder 25 bis 240 VAC	BMXDRA0815
Digital: 16 digitale Relaisausgänge	BMXDRA1605
Digital: Digitaler NC-Relaisausgang 5 bis 125 VDC oder 24 bis 240 VAC	BMXDRC0805
Digital: 16 Digitaleingänge 24/125 VDC, TSTAMP	BMXERT1604
Mx80-Schalter für Netzwerkoptionen	BMENOS0300
Turbomaschinen Frequenzeingang, 2 Kanäle	BMXETM0200
Unterstützung für Profibus DP/DPV1-Mastermodul	PMEPXM0100
Erweitertes Mx80-RTU-Modul	BMENOR2200H

Nicht-störende Module des Typs 2 für SIL2/3-Anwendungen

Die folgenden rackinternen, nicht-sicheren Module können als nicht-störende Module des Typs 2 in einem M580-Sicherheitssystem betrachtet werden.

HINWEIS: Die Liste der nicht-störenden, nicht-sicheren Module des Typs 2 kann sich von Zeit zu Zeit ändern. Die aktuelle Liste finden Sie auf der Website von TÜV Rheinland unter www.certipedia.com.

Modultyp	Modulreferenz
Kommunikation: Standard-X80-Ethernet-Stationsadapter, 1 K	BMXCRA31200
AC-Standardspannungsversorgung	BMXCPS2000
DC-Standardspannungsversorgung, potenzialgetrennt	BMXCPS2010

Modultyp	Modulreferenz
Hochleistungsspannungsversorgung 24 bis 48 VDC, potenzialgetrennt	BMXCPS3020
Redundante Standardspannungsversorgung, 125 VDC	BMXCPS3522
Redundante Standardspannungsversorgung, 24/48 VDC	BMXCPS4022
Redundante AC-Standardspannungsversorgung	BMXCPS4002
AC-Hochleistungsspannungsversorgung	BMXCPS3500
DC-Hochleistungsspannungsversorgung	BMXCPS3540T
Kommunikation: Busmodul 2 RS485/232-Ports	BMXNOM0200
Digital: 32 Digitaleingänge 12/24 VDC, Sink oder Source	BMXDDI3232
Digital: 32 Digitaleingänge 48 VDC, Sink	BMXDDI3203
CANopen-X80-Master	BMECXM0100
Wägemodul	PMESWT0100
Diagnose-Partnermodul	PMXCDA0400
Ethernet TCP Open Universal-Kommunikationsmodul	PMEUCM0302

HINWEIS: Alle autorisierten Geräte eines M580-Systems, die per Ethernet mit Sicherheitsmodulen verbunden sind, werden als nicht-störend eingestuft. Infolgedessen sind alle Module der Betriebsreihen Quantum und STB Advantys (nicht im gleichen Rack wie M580-Sicherheitsmodule einsetzbar) nicht-störende Module des Typs 2.

Cybersicherheit für das M580-Sicherheitssystem

Inhalt dieses Kapitels

Einführung

In diesem Kapitel finden Sie verfügbares Material für die Entwicklung eines passenden Ansatzes zur Cybersicherheit für den M580-Sicherheits-PAC.

Cybersicherheit für das M580-Sicherheitssystem

Referenzhandbuch für die Cybersicherheit

Der Zweck einer Cybersicherheit-Richtlinie ist eine größtmögliche Verringerung von Schwachstellen in einem Sicherheitssystem, über die Cyberangriffe geschehen können. Informationen zur Entwicklung einer Cybersicherheitsrichtlinie für Ihr M580-Sicherheitssystem finden Sie im *Modicon-Steuerungsplattform Cybersicherheit, Referenzhandbuch* (Referenznummer EIO0000002000 (DE)).

Anwendungslebenszyklus

Inhalt dieses Kapitels

Einführung

Anwendungslebenszyklus

Einführung

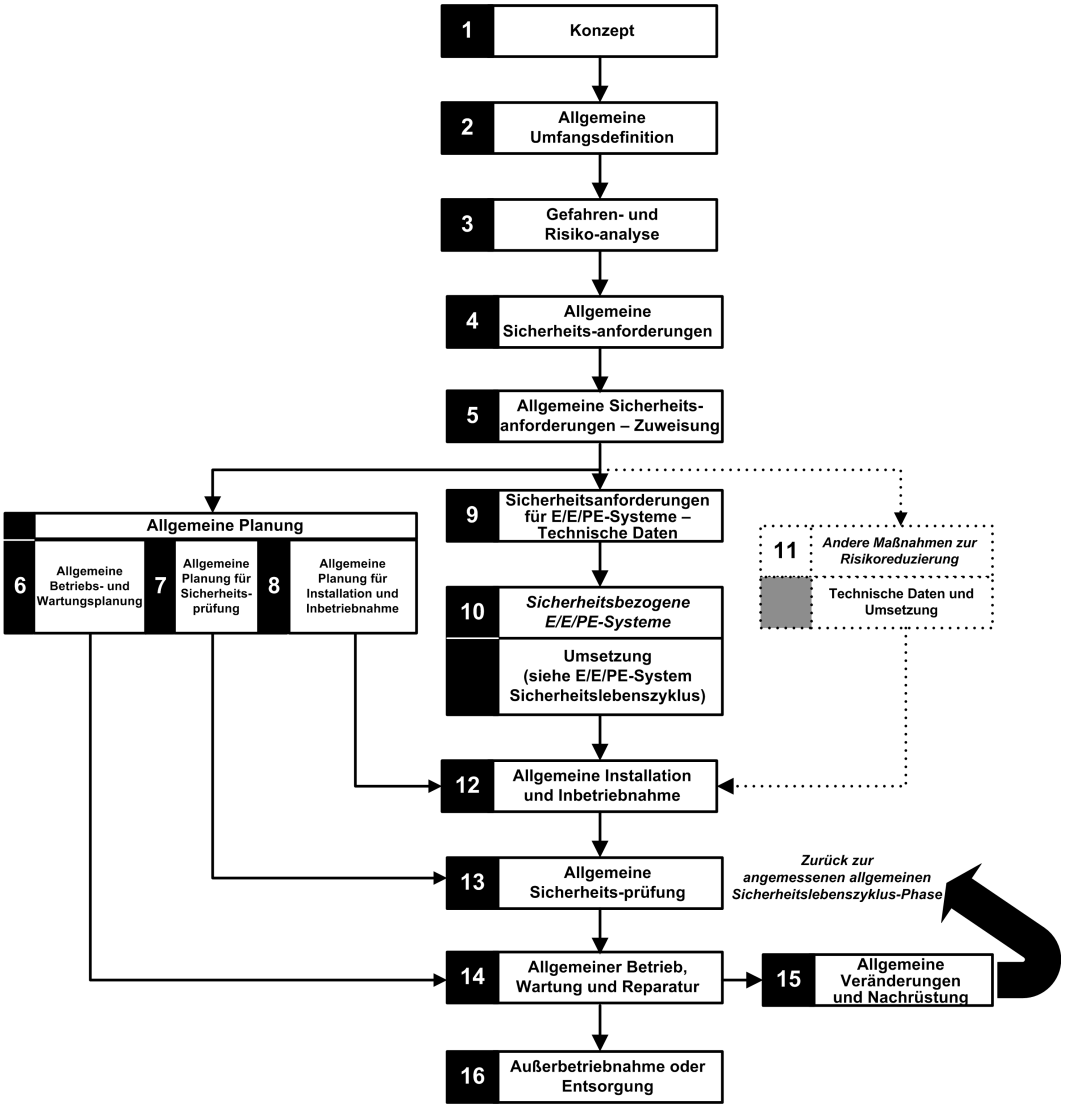
Wenn Sie eine sichere Anwendung entwickeln, sollten Sie sich an die Empfehlungen des Sicherheitsstandards halten, der für Ihren Anwendungsbereich gilt. Die meisten Anwendungsnormen stammen von der generischen Norm IEC 61508 oder sind mit ihr verknüpft. Dazu gehören z. B. die Norm für die Prozessindustrie (IEC 61511), die Normen für die Maschinenindustrie (IEC 62061 und ISO 13489), die Norm für die Atomindustrie (IEC 61513), die Bahnnormen (EN 5012x) usw.

In IEC 61508 wird ein Anwendungslebenszyklus als eine Reihe von Schritten definiert. Jeder Schritt verfügt über eine definierte Rolle, benötigt obligatorisch Eingangsdokumente und produziert Ausgangsdokumente. Die Entscheidung, ein SIS (Safety Integrated System) zu nutzen, wird am Ende des Schritts für die allgemeinen Sicherheitsanforderungen und Zuweisungen getroffen (Schritt 5).

Im Folgenden werden die erforderlichen Prüfungen erläutert, die für die Verwendung eines M580-Sicherheitssystems erforderlich sind und die zu den folgenden Zeitpunkten ausgeführt werden müssen:

9.	Sicherheitsanforderungen für E/E/PE-Systeme – Technische Daten
10.	Einrichtung von sicherheitsbezogenen E/E/PE-Systemen
12.	Allgemeine Installation und Inbetriebnahme
13.	Allgemeine Sicherheitsprüfung
14.	Allgemeiner Betrieb, Wartung und Reparatur
15.	Allgemeine Änderungen und Nachrüstung

Die folgende Abbildung zeigt den allgemeinen Sicherheitslebenszyklus:



Schritt 9: Sicherheitsanforderungen für E/E/PE-Systeme – Technische Daten

Dieser Schritt wird ausgeführt, wenn die Risikoanalyse abgeschlossen ist und u. a. die folgenden Informationen bereitgestellt hat:

- Definition der integrierten Sicherheitsfunktionen
- Deren erforderliche Leistung (Zeit, Risikoverringerung, SIL ...)
- Ausfallarten

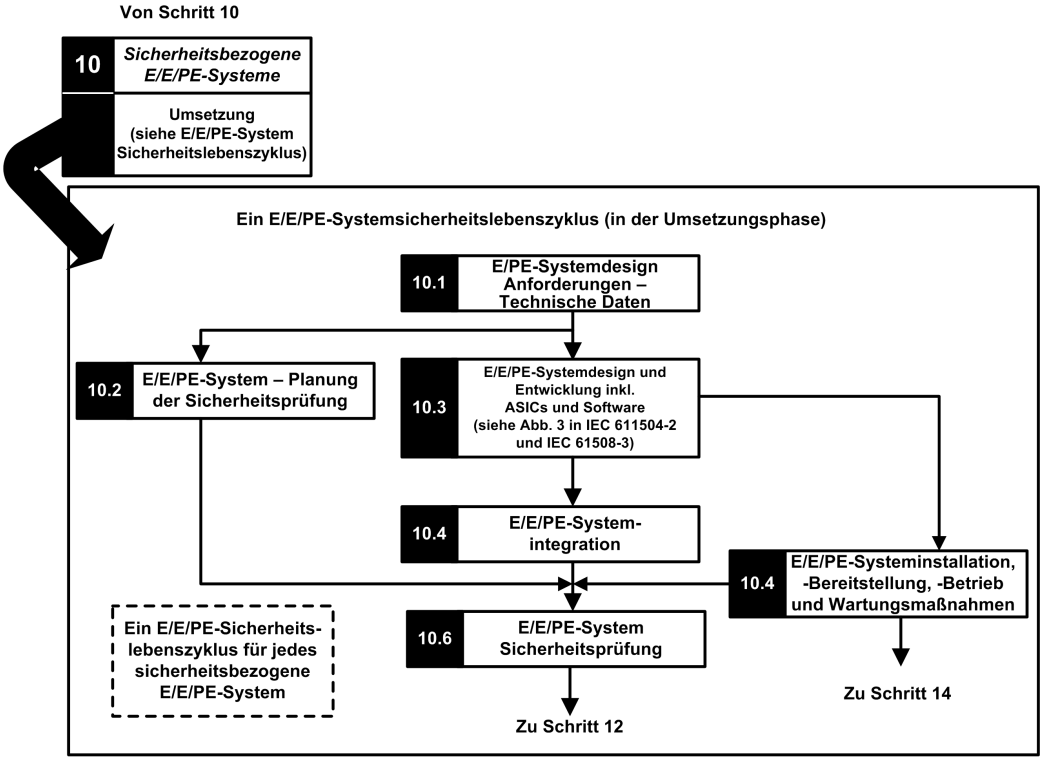
Dadurch sollten die technischen Daten und Sicherheitsanforderungen festgelegt werden, die mindestens die folgenden Informationen bereitstellen, die für die Gestaltung einer sicheren Anwendung mit einem Sicherheits-PAC beliebigen Typs erforderlich sind:

- Sicherer Zustand der integrierten Sicherheitsfunktionen
- Analyse des SIS-Betriebsmodus (inklusive Verhalten während der Laufzeit, beim Anhalten, beim Hochfahren, bei Wartung und Reparatur ...)
- SIF-Testintervall
- MTTR des SIS
- Auswahl des erregten oder deaktivierten SIF-Zustands
- Leistung der Logiklöser (Reaktionszeit, Präzision ...)
- Leistungsanforderungen
  - Fehlertoleranz
  - Integrität
  - Maximale Spurious Trip Rate
  - Maximale Dangerous Fault Rate
- Umgebungsspezifische Kenndaten (EMV, mechanisch, chemisch, klimatisch ...)

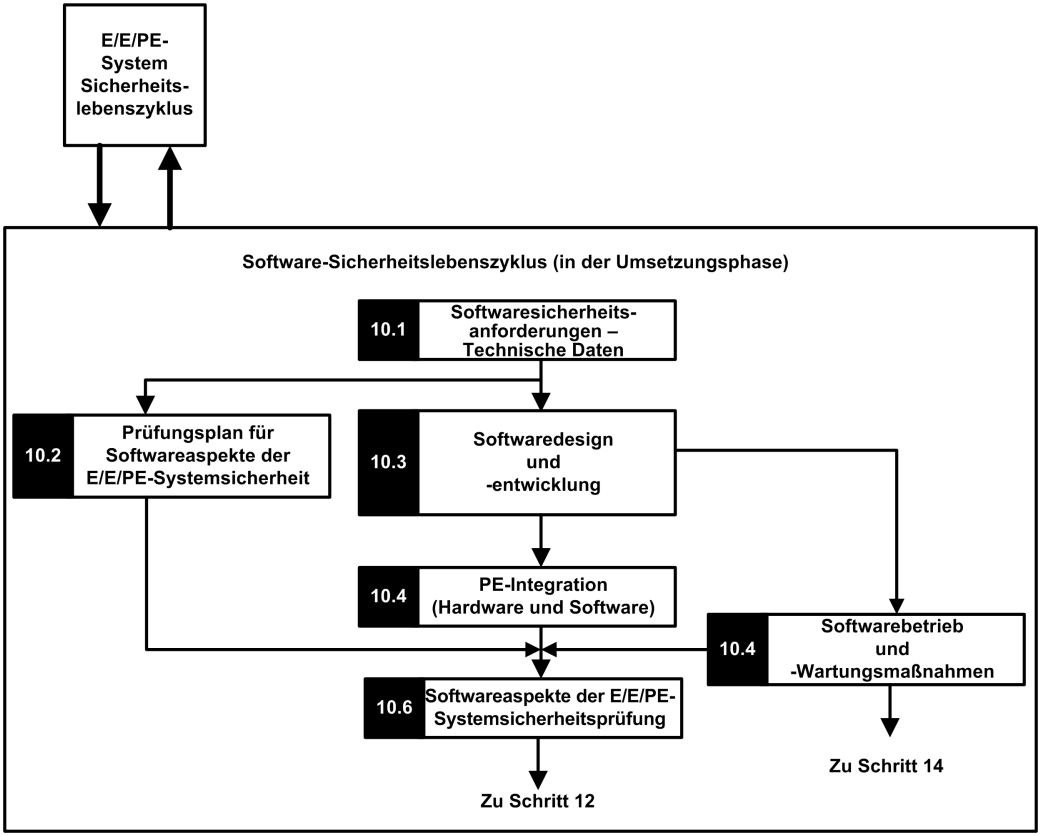
Schritt 10: Einrichtung von sicherheitsbezogenen E/E/PE-Systemen

Die Norm IEC 61508 teilt diesen Schritt in zwei Lebenszyklen auf – einen für die Systementwicklung, einen für die Softwareentwicklung.

Systementwicklung:



Softwareentwicklung:



Ziel des ersten Unterschritts (10.1) ist die Umwandlung der SIS-Sicherheitsanforderungen in eine Spezifikation für Hardwaredesign, Hardwaretests, Softwaredesign, Softwaretests und Integrationstests. Dadurch sollten mindestens die folgenden Informationen zusammengestellt werden, die für die Entwicklung einer sicheren Anwendung mit M580 erforderlich sind:

- Architektur der Hardware mit den folgenden Aufgaben:
  - Einhaltung der M580-Regeln zur Kombination von nicht-sicheren Modulen und Sicherheitsmodulen: Alle Sicherheitsmodule (E/A-Sicherheitsmodule und sichere CPU/KOPRO) werden in Racks positioniert, in denen das Hauptrack und seine Erweiterung über eine sichere Spannungsversorgung gespeist werden und die nur sichere oder nicht-störende Module vom Typ 1 enthalten.
  - Stromverbrauch pro Rack
  - Herabsetzungsregeln

- Architektur der Spannungsversorgung:
  - Nur SELV/PELV-Spannungsversorgung
- Architektur der Software:
  - Umfasst die Verwendung der globalen M580-Variablen. Eine globale Variable sollte das System nur dann davon abhalten, Sicherheitsaktionen auszulösen, wenn ein „sicheres Anwendungsprotokoll“ verwendet wird.
- Integration der Hardware (Verkabelung, Schrank usw.):
  - Sicherungsschutz
  - Zubehör für Verkabelungsdiagnose
- Mensch-Maschine-Schnittstellen (HMIs):
  - Umfasst die Verwendung der globalen M580-Variablen. Eine globale Variable sollte das System nur dann davon abhalten, Sicherheitsaktionen auszulösen, wenn ein „sicheres Anwendungsprotokoll“ verwendet wird.
- Elektrische/numerische Schnittstellen:
  - Sicherheitsstatus
  - Sensor und Aktor
- Algorithmus
- Leistung (inklusive Task-Periode, Watchdog und Timeout-Definition), Vorhersage eines guten Verhaltens anhand folgender Formel:

$$\Sigma_{alle\ Tasks} \frac{Ausf_{Task}}{Zeitraum_{Task}} < 80\%$$

  HINWEIS: Die Formel ist nur anwendbar, wenn die MAST-Task nicht im zyklischen Modus ausgeführt wird.
- Verhalten im Fall von:
  - Entsperrkonfiguration
  - Wartungsmodus
  - Wartungseingang
  - Ungültiger Kanal
  - Verdrahtungsfehler
  - Kanalfunktionsfähigkeit
  - Modulfunktionsfähigkeit
- Verwaltung der UID der E/A-Sicherheitsmodule (Definition des Zeitpunkts einer UID-Änderung)

- NTP-Server:
  - Auswahl des PAC als NTP-Server oder externer NTP-Server (je nach Verwendung der E/A-Zeitstempelung in der Prozessanwendung).
  - Serverredundanz
  - Serververlust

In den nächsten Unterschritten werden aus den Spezifikationen detaillierte technische Daten erarbeitet, die Entwicklung wird ausgeführt, alle Testpläne werden umgesetzt und Berichte bereitgestellt.

Schritt 12: Allgemeine Installation und Inbetriebnahme

Ziel dieses Schritts ist die Definition der Anforderungen für Installation, Aufgabenplanung, Toolerstellung, Inbetriebnahmeverfahren und dann die Generierung des Systems und die Prüfung seiner Korrektheit.

- Stellen Sie bei Hot Standby-Anwendungen sicher, dass das Fallback-Timeout, Seite 159 der Sicherheitsausgangsmodule den für Austausch, Seite 161- und Umschaltungsvorgänge, Seite 162 vorgegebenen Bedingungen entspricht, und prüfen Sie die CRA-Wartezeit.
- Vergewissern Sie sich, dass das Fallback-Sicherheitstimeout (S_TO) für die Sicherheitsausgangsmodule mindestens auf einen Wert gesetzt wurde, der 40 ms bzw. (2,5 * T_{SAFE}) überschreitet, je nachdem, welcher Wert größer ist. Hierbei gilt, dass T_{SAFE} der konfigurierten Dauer der SAFE-Task entspricht.
- Löschen Sie alle bereits in der SPS vorhandenen Anwendungen oder setzen Sie eine Anwendung ein, die ohne CIP-Safety-Geräte konfiguriert wurde, bevor Sie das Sicherheitsgerät in einem Ethernet-Sicherheitsnetzwerk (mit CIP-Safety-Geräten) installieren.

In einem M580-Sicherheitssystem sollte das Inbetriebnahmeverfahren die folgenden Punkte umfassen:

- Prüfung der Integrität von Control Expert, Prüfung der Version von Control Expert.
- Korrektheit der Firmwareversionen für CPU und Koprozessor durch Überwachung der Systemwörter %SW14 (Firmwareversion des SPS-Prozessors) und %SW142 (Firmwareversion des Koprozessors)
- Korrektheit der jeweiligen Moduladressen (Position im Rack, CRA-Switches)
- Korrektheit der Verkabelung:
  - Punkt-zu-Punkt-Prüfung: von interner Variable zum E/A-Modul zum Aktor/Sensor
  - Sicherungen
  - Zubehör für Verkabelungsdiagnose

- Am Ende des Vorgangs befinden sich alle Sicherheitsmodule im gesperrten Zustand. (Es wird empfohlen, dass die Sicherheitsanwendung dies selbst prüft.)
- Korrektheit der einzelnen Modulkonfigurationen (inklusive Timeouts):
  - Lesen der Konfiguration im Control Expert-Fenster und Vergleich mit den Spezifikationen.
- Alle Sicherheitsanwendungen wurden mit der Option **Gesamtes Projekt generieren** neu generiert und dann in die einzelnen SPS heruntergeladen. Ihre SAId sowie das Anwendungsarchiv wurden gespeichert.
- Taskzeitraum und Task-Watchdog sind korrekt.
- Modulreferenzen und -versionen.
- Nur Verwendung von SELV/PELV.
- Wenn CIP-Safety-Geräte in der Sicherheitsanwendung eingesetzt werden:
  - Nach dem Benutzertest kann die ID-Signatur der Sicherheitskonfiguration (SCID) als geprüft (Option im CIP-Safety-DTM in Control Expert aktiviert) und die Zielkonfiguration als gesperrt betrachtet werden.
  - Um sicherzustellen, dass die vom Benutzer mit dem Softwaretool Control Expert erstellte Ursprungskonfiguration ordnungsgemäß an das M580-CIP-Safety-Ursprungsgerät gesendet und dort gespeichert wurde, vergleichen Sie alle in den Ziel-DDDTs (im verbundenen Modus mit dem PAC mithilfe einer Animationstabelle) angezeigten Konfigurationsparameterwerte des CIP-Safety-Zielgeräts visuell mit den auf der Registerkarte „Konfigurationsprüfung“, Seite 374 des Ziel-DTM angezeigten und konfigurierten Parameterwerte. Sämtliche Werte müssen identisch sein.
  - Testen Sie alle Sicherheitsverbindungskonfigurationen nach deren Anwendung im M580-CIP-Safety-Ursprungsgerät, um sicherzustellen, dass jede Zielverbindung erwartungsgemäß funktioniert.
  - Vor der Installation von CIP-Safety-Geräten im Sicherheitsnetzwerk müssen alle Sicherheitsgeräte mit entsprechender MacId und Baudrate in Betrieb genommen werden.
- Benutzertests sind eine Möglichkeit zur Validierung aller Anwendungsdownloads.

Schritt 13: Allgemeine Sicherheitsprüfung

In diesem Schritt wird überprüft, ob die integrierten Sicherheitssysteme alle Anforderungen erfüllen. Die Tests werden ausgeführt und die Berichte bereitgestellt, die in Schritt 7 des Sicherheitslebenszyklus definiert wurden. Dazu gehört Folgendes:

- Stellen Sie sicher, dass es in keinem Systemzustand zu einem Überlauf kommt (Prüfung des Systembits %S19 in der MAST-, FAST- und AUX0-Task) und dass die maximale und die aktuelle Ausführungszeit der SAFE-Task (%SW42 und %SW43) kürzer ist als die Periode der SAFE-Task.

- Überprüfen Sie die CPU-Lastformel: $\Sigma_{alle\ Tasks} \frac{Ausf_{Task}}{Zeitraum_{Task}} < 80\%$

  HINWEIS: Mithilfe der Systemwörter %SW110 bis %SW115, Seite 414 können Sie eine Echtzeit-Prüfung der durchschnittlichen Last für die CPU-Tasks durchführen (wenn alle Tasks periodisch sind, sollte %SW116 unter 80 liegen).
- Überprüfen Sie die speziellen Betriebsmodi (Modul entsperren, Wartungseingang, ungültiger Kanal, Verdrahtung defekt).
- Stellen Sie bei Hot Standby-Anwendungen sicher, dass alle Tasks ordnungsgemäß über die Hot Standby-Verbindung synchronisiert wurden. Prüfen und verwenden Sie dazu die Bits MAST_SYNCHRONIZED, FAST_SYNCHRONIZED und SAFE-SYNCHRONIZED im DDT T_M_ECPU_HSBY. Siehe *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen* für eine Beschreibung des DDT T_M_ECPU_HSBY.

Schritt 14: Allgemeiner Betrieb, Wartung und Reparatur

- Führen Sie im richtigen Zeitraum die Prüftests aus.
- Überwachen Sie die SAId siehe Hinweis.

  HINWEIS: Solange sich die SAId nicht geändert hat, wurde auch der Sicherheitsteil der Anwendung nicht geändert. Details zum SAId-Verhalten finden Sie im Funktionsbaustein S_SYST_STAT_MX.
- Überwachen Sie den Konfigurationssperrstatus der einzelnen Sicherheitsmodule.
- Erfassen Sie die Wartungsvorgänge.
- Beim Auswechseln eines Moduls muss das Ersatzgerät ordnungsgemäß konfiguriert und dessen Betrieb (vom Benutzer) geprüft werden. Führen Sie (mindestens) die Inbetriebnahmeprozesse in Verbindung mit dem Modul durch.
- Erfassen Sie die Abweichungen.

Schritt 15: Allgemeine Änderungen und Nachrüstung

Alle Änderungen sollten als neue Bauweise erfasst werden. Eine Folgenanalyse kann dabei helfen, den Teil des ehemaligen Sicherheitssystems zu ermitteln, den Sie behalten können, sowie den Teil, der neu entwickelt werden muss.

HINWEIS: Wenn eine Anwendungsänderung die SAFE-Anwendung nicht betrifft, können Sie die Signatur der SAFE-Quelle heranziehen, um sicherzustellen, dass keine unerwünschte Änderung in den SAFE-Code eingeführt wurde. Die Signatur der SAFE-Quelle ist eine *Vorabkontrolle*, um sich zu vergewissern, dass die Anwendung unverändert ist. Die Signatur der SAFE-Quelle ersetzt nicht die SAId - das einzige zuverlässige Mittel zur Überprüfung, dass ein PAC die SAFE-Anwendung ausführt, die validiert wurde.

M580-E/A-Sicherheitsmodule

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die M580-E/A-Sicherheitsmodule beschrieben.

M580-E/A-Sicherheitsmodul – Gemeinsame Funktionen

Einführung

In diesem Abschnitt werden die gemeinsamen oder geteilten Funktion von M580-E/A-Sicherheitsmodulen erläutert.

Einführung in die M580-E/A-Sicherheitsmodule

Einführung

Die vier folgenden M580-E/A-Sicherheitsmodule sind für die Verwendung in Sicherheitsanwendungen zertifiziert:

- BMXSAI0410 (Analogeingang)
- BMXSDI1602 (Digitaleingang)
- BMXSDO0802 (Digitalausgang)
- BMXSRA0405 (Digitaler Relaisausgang)

Die drei E/A-Sicherheitsmodule ermöglichen Ihnen den Anschluss des Sicherheits-PAC an die Sensoren und Stellglieder, die Teil der Sicherheitsschleife sind. Jedes E/A-Sicherheitsmodul umfasst einen dedizierten Sicherheitsprozessor. Sie können diese E/A-Module im lokalen Baugruppenträger oder in RIO-Stationen installieren.

Installations- und Gehäuseanforderungen

Installieren Sie Ihre M580-Sicherheitsanlage auf folgende Weise:

- IEC-60950-Verschmutzungsgrad 2 für die Sicherheit der IT-Geräte
- IEC-60529-Standard für IP54-Schutz:
  - Der Gerätebetrieb darf nicht durch Eindringen von Staub behindert werden.
  - Spritzwasser darf keinen Einfluss auf die Geräte und den Betrieb haben.

Üblicherweise werden diese Standards eingehalten, indem die Sicherheitsanlage in einem Gehäuse, z. B. einem Schaltschrank, untergebracht wird.

Maximale Betriebshöhe

Die maximale Betriebshöhe für die M580-E/A-Sicherheitsmodule beträgt 2000 m über NN.

Kommunikation zwischen PAC und E/A

Die M580-Sicherheits-CPU und der -Koprozessor steuern gemeinsam den gesamten Datenaustausch des Baugruppenträgers, während die Sicherheits-E/A auf die Befehle der CPU und des Koprozessors reagieren. E/A-Sicherheitsmodule können in einem X Bus-Rack vom Typ BMXXBP•••• oder in einem Ethernet-Rack vom Typ BMEXBP•••• untergebracht werden.

Die Kommunikation zwischen dem Sicherheits-PAC und den E/A-Sicherheitsmodulen im lokalen Hauptrack erfolgt über die Bauträgergruppe.

Die Kommunikation zwischen dem Sicherheits-PAC und den in einer RIO-Station installierten E/A-Sicherheitsmodulen erfolgt über ein Adaptermodul in der RIO-Station:

- Ein Adapter vom Typ BMECRA31210 für ein Ethernet-Rack
- Ein Adapter vom Typ BMXCRA31210 für ein X-Bus-Rack

  HINWEIS: Bei einer CPU-Firmware ab Version 3.20 ist für die Kommunikation zwischen PAC und Sicherheits-E/A ein BM•CRA31210 mit einer Firmware ab Version 2.60 erforderlich.

  HINWEIS: Ein Adapter vom Typ BMXCRA31200 kann nicht genutzt werden, um die E/A-Sicherheitsmodule mit dem M580-Sicherheits-PAC zu verbinden.

Optional können Sie Glasfaser-Repeater-Module vom Typ BMXNRP0200 oder BMXNRP0201 einsetzen, um die physische Verbindung zwischen CPU und Koprozessor im lokalen Rack und dem Adapter in der RIO-Station zu verstärken. Glasfaser-Repeater-Module sorgen für eine verbesserte Störfestigkeit des RIO-Netzwerks und unterstützen längere Kabelstrecken. Gleichzeitig bleiben der volle Dynamikbereich des Netzwerks und das Sicherheitsintegritäts-Level gewährleistet.

Das Kommunikationsprotokoll zwischen E/A-Sicherheitsmodul und PAC gewährleistet den Datenaustausch. Dadurch können beide Geräte die Genauigkeit der empfangenen Daten prüfen, beschädigte Daten und Betriebsstörungen des übertragenden Moduls erkennen. Dementsprechend kann eine Sicherheitsschleife nicht-störende, Seite 29 RIO-Adapter und einen Baugruppenträger umfassen.

Externe Spannungsversorgung mit digitalem E/A-Sicherheitsmodul

Die digitalen Module BMXSDI1602 und BMXSDO0802 erfordern eine externe Spannungsversorgung mit 24-VDC-Schutzkleinspannung (SELV/PELV), um Sensoren und

Aktoren mit Strom zu versorgen. Die E/A-Sicherheitsmodule überwachen die nicht-sichere Prozessspannungsversorgung auf Über- und Unterspannung.

⚠⚠ GEFAHR

SELV/PELV-SPANNUNGSVERSORGUNG, ÜBERSPANNUNGSKATEGORIE II, ERFORDERLICH

Verwenden Sie für die Spannungsversorgung von Sensoren und Aktoren nur eine SELV/PELV-Spannungsversorgung der Kategorie II mit einer maximalen Abgabe von 60 VDC.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

Diagnose-Überblick für M580-E/A-Sicherheitsmodule

Einführung

Das M580-E/A-Sicherheitsmodul verfügt über die folgenden Diagnosefunktionen:

- Selbsttest beim Hochfahren
- Ständiger, integrierter Laufzeit-Selbsttest
- LEDs für Modul- und Kanaldiagnose

Zudem führen die digitalen E/A-Sicherheitsmodule eine Verdrahtungsdiagnose durch.

Selbsttest beim Start

Beim Start führen die E/A-Module eine umfangreiche Serie an Selbsttests durch. Folgende Ergebnisse sind möglich:

- Erfolgreich: Die Module sind in gutem Zustand und funktionsfähig.
- Nicht erfolgreich: Die Module sind nicht in gutem Zustand und nicht funktionsfähig. In diesem Fall werden die Eingänge auf 0 gesetzt und die Ausgänge deaktiviert.

  HINWEIS: Wenn die externe 24-VDC-Spannungsversorgung nicht an ein digitales Ein- oder Ausgangsmodul angeschlossen ist, werden die Selbsttests beim Hochfahren nicht durchgeführt und die Module starten nicht.

Ständige, integrierte Tests

Während des Betriebs führen die E/A-Module ständig Selbsttests aus. Die Eingangsmodule überprüfen, ob sie im gesamten Bereich Daten von den Sensoren lesen können. Die

Ausgangsmodule überprüfen, ob der tatsächliche Zustand des Ausgangs mit dem des befohlenen Zustands übereinstimmt.

LEDs

An der Frontplatte jedes E/A-Sicherheitsmoduls stehen LEDs zur Modul- und Kanaldiagnose bereit:

- Die oberen 4 LED-Anzeigen (**Run**, **Err**, **I/O** und **Lck**) signalisieren zusammen den Zustand des Moduls.
- Die unteren zwei oder vier LEDs (je nach Modul) beschreiben gemeinsam mit den oberen vier LEDs den Zustand und die Funktionsfähigkeit jedes Ein- und Ausgangskanals.

Weitere Informationen zu den LEDs für dieses Modul finden Sie im Abschnitt zur LED-Diagnose für die folgenden E/A-Sicherheitsmodule:

- BMXSAI0410 Modul für analoge Sicherheitseingänge, Seite 238
- BMXSDI1602 Modul für digitale Sicherheitseingänge, Seite 244
- BMXSDO0802 Modul für digitale Sicherheitsausgänge, Seite 250
- BMXSRA0405 Modul für digitale Sicherheitsrelaisausgänge, Seite 255

Verdrahtungsdiagnose für digitale Module

Das digitale Sicherheitseingangsmodul und das digitale Sicherheitsausgangsmodul können beide die folgende Diagnose für die Kanalverdrahtung durchführen:

- Offener (oder unterbrochener) Draht
- Masseschlusserkennung an 0 VDC
- Kurzschlusserkennung an 24 VDC
- Querschluss zwischen zwei Kanälen.

  HINWEIS: Die Verfügbarkeit dieser Diagnosefunktionen ist von der Verdrahtung des Moduls mit den anderen Geräten abhängig. Sehen Sie sich die Verdrahtungsbeispiele für die folgenden digitalen E/A-Sicherheitsmodule an, um weitere Informationen zu erhalten:

  - BMXSDI1602 Modul für digitale Sicherheitseingänge, Seite 72
  - BMXSDO0802 Modul für digitale Sicherheitsausgänge, Seite 102

Analoges Eingangsmodul BMXSAI0410

Einführung

In diesem Abschnitt wird das Modul BMXSAI0410, d. h. das analoge M580-Sicherheitseingangsmodul, beschrieben.

Analoges Sicherheitseingangsmodul BMXSAI0410

Einführung

Das analoge Sicherheitseingangsmodul BMXSAI0410 weist folgende Funktionen auf:

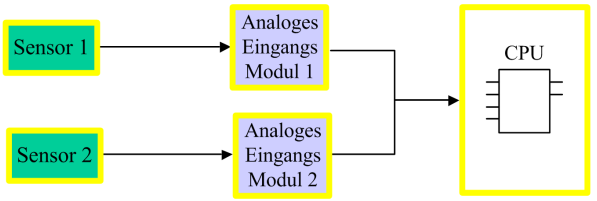
- 4 isolierte, analoge Eingangskanäle mit 4 bis 20 mA
- 12500 Auflösungsimpulse im Datenbereich von 0 bis 25 mA
- Erkennung von Stromstärken außerhalb des Bereichs für Werte unter 3,75 mA und über 20,75 mA
- Unterstützung der folgenden SIL3-Standards (IEC61508):
  - Das Modul kann bis zu Kategorie 2 (Cat2) / Performance Level d (PLd) mit 1 Eingangskanal erreichen (1oo1-Prüfung (one-out-of-one)). Somit können Cat1 und Cat2 / PL a, b, c, d über 1 Eingangskanal erreicht werden.
  - Das Modul kann bis zu Kategorie 4 (Cat4) / Performance Level e (PLe) mit 2 Eingangskanälen erreichen (1oo2-Prüfung (one-out-of-two)). Dadurch können Cat3 und Cat4 / PL d e über 2 Eingangskanäle erreicht werden.
- Für das Modul und die einzelnen Eingangskanäle steht eine Anzeige für die LED-Diagnose, Seite 238 zur Verfügung.
- Hot-Swapping des Moduls während der Laufzeit.
- CCOTF des Moduls im Wartungsmodus, Seite 265 (CCOTF wird nicht im Sicherheitsmodus, Seite 264 unterstützt)

Hohe Verfügbarkeit

Sie können Ihre Sicherheitsanwendung mit verschiedenen Anforderungen für Leistung und Verfügbarkeit konfigurieren, indem Sie einfache oder redundante Eingangskanäle und -module verwenden:

Bauweise:	**Sicherheitsfunktionsebenen:**			
Eingangskanäle => Module	**SIL**	**Cat**	**PL**	**Hohe Verfügbarkeit?**
Einfacher Eingangskanal für einfaches Eingangsmodul, Seite 56	SIL3	Cat 2	PLd	–
Einfacher Eingangskanal für redundante Eingangsmodule, Seite 57	SIL3	Cat 2	PLd	✓
Redundante Eingangskanäle für einfaches Eingangsmodul, Seite 58	SIL3	Cat 4	PLe	–
Redundante Eingangskanäle für redundante Eingangsmodule, Seite 59	SIL3	Cat 4	PLe	✓
✓: Bereitgestellt -: Nicht bereitgestellt				

Die folgende Abbildung zeigt die Konfiguration für redundante Analogeingänge:



Der Wert des analogen Eingangsstroms von Sensor 1 und Sensor 2 wird von Eingangsmodul 1 und Eingangsmodul 2 über einen Black Channel an eine Sicherheits-CPU gesendet. Die CPU führt in zwei separaten, kompilierten Logikprogrammen einen dedizierten Funktionsbaustein aus (`S_AIHA`), um die Daten der zwei Eingangsmodule zu verwalten und auszuwählen. Dieser Funktionsbaustein funktioniert wie folgt:

- Wenn der Zustand der Eingangsdaten von Modul 1 in Ordnung ist, werden die Eingangsdaten dieses Moduls in der Sicherheitsfunktion verwendet.
- Wenn der Zustand der Eingangsdaten von Modul 1 nicht in Ordnung ist, aber der Zustand der Eingangsdaten von Modul 2, werden die Eingangsdaten von Modul 2 verwendet.
- Wenn der Zustand der Eingangsdaten von Modul 1 und Modul 2 nicht in Ordnung ist, aktiviert das System die Sicherheitsfunktion.

BMXSAI0410 - Verdrahtungsanschlüsse

Einführung

Das analoge Eingangsmodul BMXSAI0410 verfügt über vier analoge Eingänge. Das Modul besitzt zwei Paar Stifte – zwei positive Kanalstifte (Ch) und zwei negative allgemeine Stifte (Com) – für jeden Eingang.

Für jeden Eingang gilt Folgendes:

- Die zwei Kanalstifte (Ch*n*) sind intern verbunden.
- Die zwei allgemeinen Stifte (Com*n*) sind ebenfalls intern verbunden.

Um einen analogen Sensor mit einem Eingang zu verbinden, können Sie einen beliebigen Kanalstift und einen beliebigen allgemeinen Stift verwenden.

Klemmenleisten

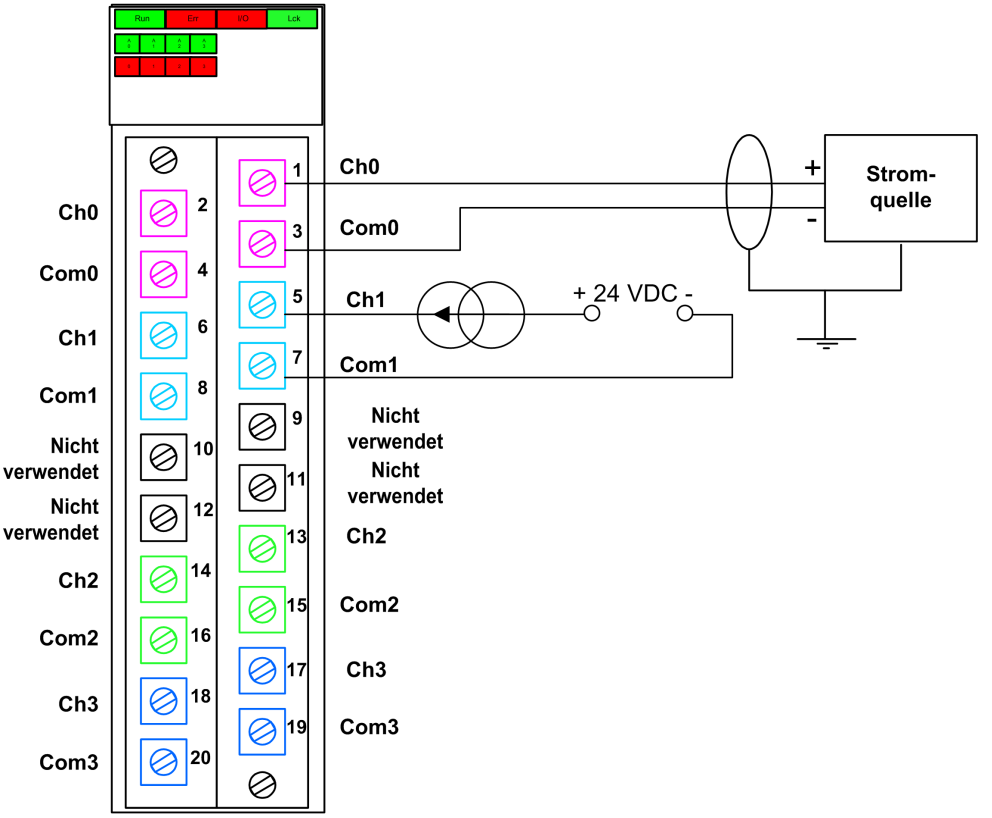
Die folgenden 20-Punkt-Klemmenleisten von Schneider Electric können für den 20-Stift-Anschluss vorn am Modul genutzt werden:

- Schraubklemmenleiste BMXFTB2010
- Käfigfederzugklemmenleiste BMXFTB2000
- Federklemmenleiste BMXFTB2020

HINWEIS: Die Klemmenleisten können nur entfernt werden, wenn die Modulspannung abgeschaltet ist.

Verdrahtungsanschlüsse

Das nachstehende Beispiel zeigt einen allgemeinen Verdrahtungsplan für die Eingänge am Modul:



HINWEIS: Das Modul erkennt einen getrennten Draht und meldet ihn als außer Reichweite (weniger als 3,75 mA), indem das Element `OOR` der Struktur `T_U_ANA_SIS_CH_IN, Seite 63` auf 1 gesetzt wird.

Zuweisung von Eingängen und Anschlussstiften

Es folgt eine Beschreibung der einzelnen Stifte des analogen Eingangsmoduls BMXSAI0410:

Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung
Eingang (+) von Kanal 0	2	1	Eingang (+) von Kanal 0
Eingang (–) von Kanal 0	4	3	Eingang (–) von Kanal 0

Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung
Eingang (+) von Kanal 1	6	5	Eingang (+) von Kanal 1
Eingang (–) von Kanal 1	8	7	Eingang (–) von Kanal 1
Nicht verwendet	10	9	Nicht verwendet
Nicht verwendet	12	11	Nicht verwendet
Eingang (+) von Kanal 2	14	13	Eingang (+) von Kanal 2
Eingang (–) von Kanal 2	16	15	Eingang (–) von Kanal 2
Eingang (+) von Kanal 3	18	17	Eingang (+) von Kanal 3
Eingang (–) von Kanal 3	20	19	Eingang (–) von Kanal 3

HINWEIS: Da die zwei positiven Stifte der beiden Eingänge intern verbunden sind, müssen Sie für einen Eingangskanal nur einen positiven Stift nutzen. Ebenfalls gilt: Da die zwei negativen Stifte der beiden Eingänge intern verbunden sind, müssen Sie für einen Eingangskanal nur einen negativen Stift nutzen.

Um z. B. einen analogen Sensor mit Eingangskanal 0 zu verbinden, können Sie Folgendes verbinden:

- Den positiven Draht des Sensors mit Stift 1 oder Stift 2
- Den negativen Draht des Sensors mit Stift 3 oder Stift 4

BMXSAI0410 - Verdrahtungsbeispiele für Eingänge

Einführung

Um das analoge Sicherheitseingangsmodul BMXSAI0410 mit analogen Sensoren zu verdrahten und SIL3 einzuhalten, gibt es verschiedene Möglichkeiten. Abhängig ist dies von:

- Den erforderlichen Standards für Kategorie (Cat2 oder Cat4) und Performance Level (PLd oder PLe)
- Den Anforderungen Ihrer Anwendung für hohe Verfügbarkeit

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Das maximale Sicherheitsintegritäts-Level (SIL) wird durch die Qualität des Sensors und die Länge des Prüfabstands gemäß IEC 61508 festgelegt. Wenn Sie Sensoren nutzen, die den Qualitätsansprüchen des gewünschten SIL-Standards nicht entsprechen, sollten diese Sensoren immer redundant mit zwei Kanälen verdrahtet werden.

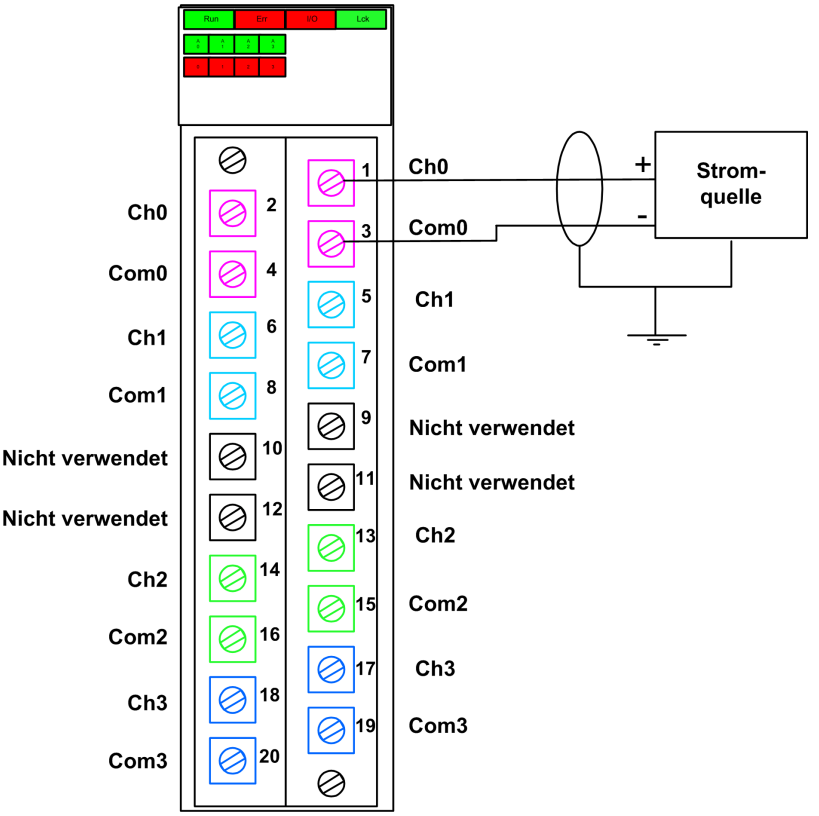
Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Im Folgenden werden verschiedene Verdrahtungsbeispiele für die digitale SIL3-Eingangsanwendung erläutert:

- Cat2/PLd:
  - Ein einziger Sensor, mit einem Eingang verbunden
- Cat2/PLd mit hoher Verfügbarkeit:
  - Zwei Sensoren, mit zwei Eingangspunkten auf verschiedenen Eingangsmodulen verbunden
- Cat4/PLe:
  - Zwei Sensoren, jeweils mit verschiedenen Eingangspunkten auf demselben Eingangsmodul verbunden
- Cat4/PLe mit hoher Verfügbarkeit:
  - Zwei Sensorpaare (für insgesamt vier Sensoren): Die Sensoren des ersten Paars werden jeweils mit einem anderen Eingangspunkt eines Moduls verbunden. Die Sensoren des zweiten Paars werden jeweils mit einem anderen Eingangspunkt eines zweiten Moduls verbunden.

SIL3 Cat2/PLd

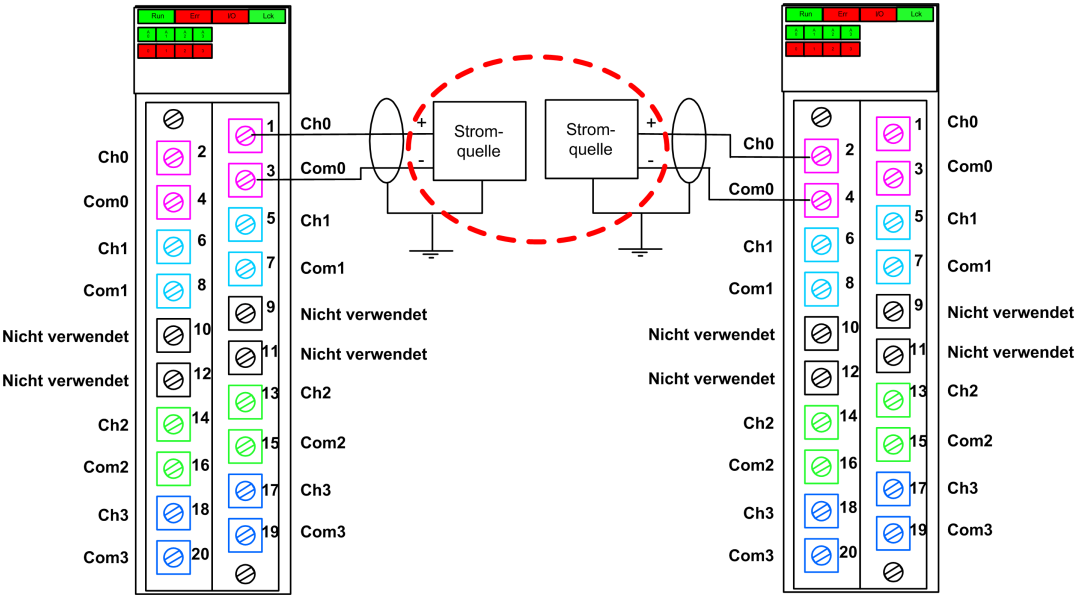
Das folgende Beispiel zeigt einen Sensor, der mit einem Eingangspunkt eines Eingangsmoduls verbunden ist. Die CPU führt eine 1oo1D-Prüfung für den überwachten Einzelwert durch:



⚠VORSICHT
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 2/Performance Level d gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwenden werden. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

SIL3 Cat2/PLd mit hoher Verfügbarkeit

Das folgende Beispiel zeigt zwei Sensoren, die dieselbe Prozessvariable überwachen. Jeder Sensor ist mit einem Eingangspunkt auf verschiedenen Eingangsmodulen verbunden. Die CPU führt eine 1oo1D-Prüfung für den überwachten Einzelwert durch:



HINWEIS: Bei dieser Bauweise können Sie in der SAFE-Task den Funktionsbaustein `S_AIHA` verwenden, um die zwei Prozessvariablenwerte zu verwalten, die von den beiden Sensoren gemeldet werden.

⚠VORSICHT

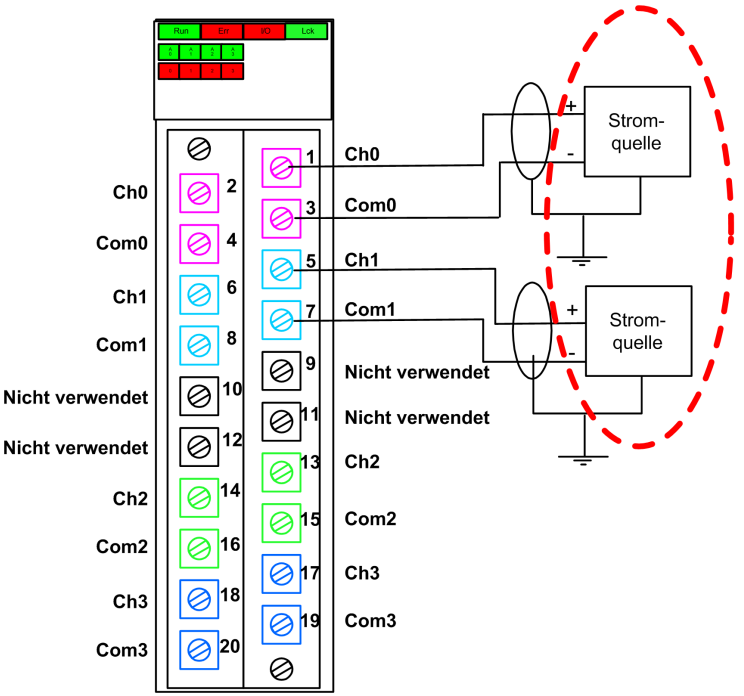
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 2/Performance Level d gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwenden werden.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

SIL3 Cat4/PLe

Das folgende Beispiel zeigt zwei Sensoren, die dieselbe Prozessvariable überwachen. Jeder Sensor ist mit einem Eingangspunkt auf demselben Eingangsmodul verbunden. Die CPU führt eine 1oo2D-Prüfung der konkurrierenden Werte durch, die von den zwei Sensoren für dieselbe Prozessvariable gemeldet werden:

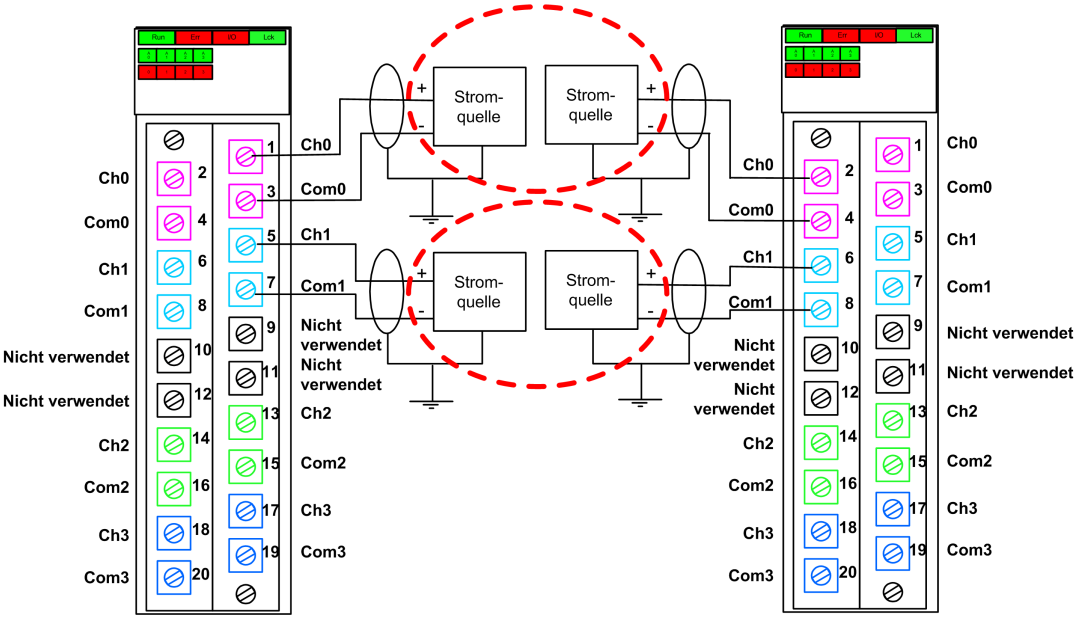


HINWEIS: Bei dieser Konzeption können Sie in der SAFE-Task den Funktionsbaustein `S_AI_COMP` verwenden, um die 1oo2-Prüfung der konkurrierenden Werte durchzuführen, die von den zwei Sensoren gemeldet werden.

⚠ VORSICHT
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwenden werden. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

SIL3 Cat4/PLe mit hoher Verfügbarkeit

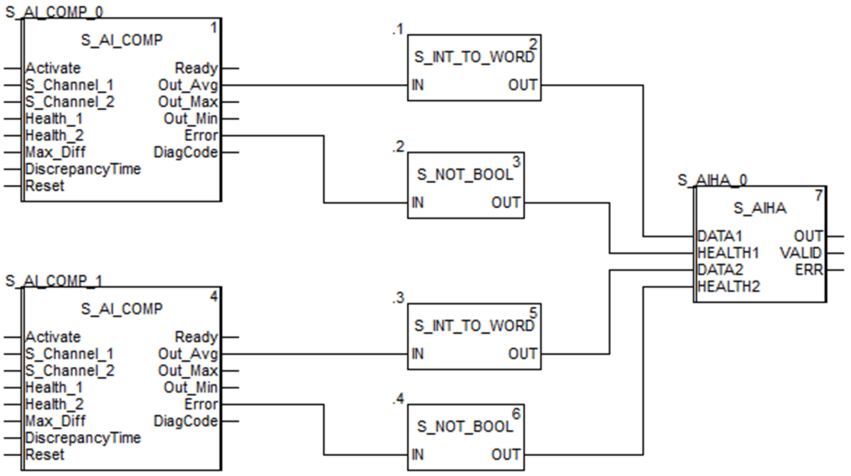
Das folgende Beispiel zeigt zwei Sensorpaare, die dieselbe Prozessvariable überwachen. Jeder Sensor ist mit einem Eingangspunkt auf zwei verschiedenen Eingangsmodulen verbunden (zwei Eingänge pro Modul). Bei dieser Konzeption kann die CPU eine 1oo2D-Prüfung durchführen:



HINWEIS: Bei dieser Bauweise können Sie in der SAFE-Task die Funktionsbausteine `S_AI_COMP` und `S_AIHA` nutzen, um die vier Eingangssignale zu verwalten.

- `S_AI_COMP` für die 1oo2-Prüfung zweier Wertepaare, die von beiden, mit demselben Modul verbundenen Sensoren kommen
- `S_AIHA` für die Verwaltung der Funktion für hohe Verfügbarkeit

Die folgende Darstellung der Funktionsbausteine zeigt die oben erläuterte Bauweise des Codesegments:



⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwenden werden.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

BMXSAI0410 - Datenstruktur

Einführung

Der gerätespezifische abgeleitete Datentyp (Device Derived Data Type, DDDT) `T_U_ANA_SIS_IN_4` ist die Schnittstelle zwischen dem analogen Eingangsmodul BMXSAI0410 und

der Anwendung, die auf der CPU läuft. Der DDDT `T_U_ANA_SIS_IN_4` umfasst die Datentypen `T_SAFE_COM_DBG_IN` und `T_U_ANA_SIS_CH_IN`.

All diese Strukturen werden im Folgenden beschrieben.

DDDT-Struktur `T_U_ANA_SIS_IN_4`

Die DDDT-Struktur `T_U_ANA_SIS_IN_4` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
MOD_HEALTH[1]	BOOL	• 1: Das Modul funktioniert ordnungsgemäß. • 0: Das Modul funktioniert nicht ordnungsgemäß.	RO
SAFE_COM_STS[1]	BOOL	• 1: Die Modulkommunikation ist gültig. • 0: Die Modulkommunikation ist nicht gültig.	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Debug-Struktur für sichere Kommunikation	RO
CONF_LOCKED	BOOL	• 1: Die Modulkonfiguration ist gesperrt. • 0: Die Modulkonfiguration ist nicht gesperrt.	RO
CH_IN	ARRAY[0 bis 3] von T_U_ANA_SIS_CH_IN	Array der Kanalstruktur	–
MUID[2]	ARRAY[0 bis 3] von DWORD	Eindeutige Modul-ID (automatisch von Control Expert zugewiesen)	RO
RESERVED	ARRAY[0 bis 9] von INT	–	–

1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. MOD_HEALTH und SAFE_COM_STS sind auf 0 gesetzt.

2. Dieser automatisch generierte Wert kann geändert werden, indem im Hauptmenü von Control Expert der Befehl **Generieren > IDs erneuern & Alles generieren** ausgeführt wird.

Struktur `T_SAFE_COM_DBG_IN`

Die Struktur `T_SAFE_COM_DBG_IN` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff[1]
S_COM_EST	BOOL	• 1: Die Kommunikation mit dem Modul wurde hergestellt. • 0: Die Kommunikation mit dem Modul wurde nicht hergestellt oder ist fehlerhaft.	RO
M_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Das Modul wird mit dem NTP-Server synchronisiert. • 0: Das Modul wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CPU_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Die CPU wird mit dem NTP-Server synchronisiert. • 0: Die CPU wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CHECKSUM	BYTE	Prüfsumme des Kommunikations-Frame	RO
COM_DELAY	UINT	Kommunikationsverzögerung zwischen zwei Werten, wie vom Modul erhalten: • 1 bis 65534: Die Zeit in ms, seitdem die CPU die letzte Kommunikation vom Modul empfangen hat. • 65535: Die CPU hat keine Kommunikation vom Modul empfangen.	RO
COM_TO	UINT	Timeout-Wert für die Kommunikation vom Modul **HINWEIS:** Sie können diesen Lese-/Schreibwert bearbeiten, um die tatsächliche Kommunikationszeit für das Modul zu erreichen oder zu überschreiten (z. B. in einer dezentralen RIO-Station).	R/W
STS_MS_IN	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der vom Modul empfangenen Daten	RO
S_NTP_MS	UINT	Sicherer Zeitwert für einen Sekundenbruchteil (bis zur nächsten ms) für den aktuellen Zyklus	RO
STS_S_IN	UDINT	Sicherer Zeitstempelwert (in Sekunden) der vom Modul empfangenen Daten	RO

Element	Datentyp	Beschreibung	Zugriff[1]
S_NTP_S	UDINT	Sicherer Zeitwert (in Sekunden) für den aktuellen Zyklus	RO
CRC_IN	UDINT	CRC-Wert für die vom Modul empfangenen Daten	RO

Struktur T_U_ANA_SIS_CH_IN

Die Struktur T_U_ANA_SIS_CH_IN umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
FCT_TYPE	WORD	• 1: Der Kanal ist aktiviert. • 0: Der Kanal ist nicht aktiviert.	RO
CH_HEALTH[1]	BOOL	• 1: Der Kanal ist funktionsfähig. • 0: Auf dem Kanal wurde ein Fehler entdeckt. Er ist nicht funktionsfähig. **Formel**: CH_HEALTH = not (OOR or IC) and SAFE_COM_STS	RO
VALUE	INT	Analoger Eingangswert **Formel**: VALUE = if (SAFE_COM_STS and not (IC)) then READ_VALUE else 0	RO
OOR	BOOL	• 1: Der Kanaleingangswert liegt außerhalb des Bereichs: ◦ <3,75 mA ◦ >20,75 mA • 0: Der Kanaleingangswert liegt nicht außerhalb des Bereichs.	RO
IC	BOOL	• 1: Das Modul hat einen ungültigen Kanal erkannt. • 0: Der Kanal wird intern vom Modul als funktionsfähig erklärt.	RO
1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. CH_HEALTH ist auf 0 gesetzt.			

Digitales Eingangsmodul BMXSDI1602

Einführung

In diesem Abschnitt wird das Modul BMXSDI1602, d. h. das digitale M580-Sicherheitseingangsmodul, beschrieben.

Digitales Sicherheitseingangsmodul BMXSDI1602

Einführung

Das digitale Sicherheitseingangsmodul BMXSDI1602 weist folgende Funktionen auf:

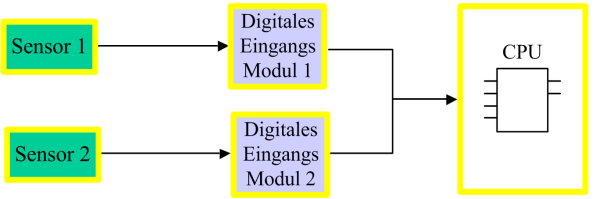
- 16 Eingänge vom Typ 3 (IEC61131-2) in zwei elektrisch nicht-isolierten Gruppen aus 8 Eingängen
- 24-VDC-Eingangsspannung
- Realisiert Folgendes:
  - SIL3 IEC61508, SILCL3 IEC62061.
  - SIL4 EN5012x.
  - Kategorie 2 (Cat2) / Performance Level d (PLd) ISO13849 mit 1 Eingangskanal (1oo1D-Prüfung („one-out-of-one“))
  - Kategorie 4 (Cat4) / Performance Level e (PLe) ISO13849 mit 2 Eingangskanälen (1oo2D-Prüfung („one-out-of-two“))
- Kompatibel mit 2- oder 3-Draht-Näherungssensoren
- Bietet optional zwei 24-VDC-Ausgänge (VS1 und VS2) für die Erkennung von Kurzschlüssen an 24 VDC:
  - VS1 für die Überwachung von Kurzschlüssen an den Eingängen 0 bis 3 (Rang A und B)
  - VS2 für die Überwachung von Kurzschlüssen an den Eingängen 4 bis 7 (Rang A und B)
- Überwachung der externen 24-VDC-Spannungsversorgung für Sensoren
- Für das Modul und die einzelnen Eingangskanäle steht eine Anzeige für die LED-Diagnose, Seite 244 zur Verfügung.

- Konfigurierbare Kanalverdrahtungsdiagnose (aktivieren/deaktivieren), Seite 73, mit der folgende Probleme erkannt werden:
  - Offener (oder unterbrochener) Draht
  - Masseschlusserkennung an 0 VDC
  - Kurzschlusserkennung an 24 VDC (falls die Sensorspannung intern bereitgestellt wird)
  - Querschlusserkennung zwischen zwei Kanälen (falls die Sensorspannung intern bereitgestellt wird)
- Hot-Swapping des Moduls während der Laufzeit
- CCOTF des Moduls im Wartungsmodus, Seite 265 (CCOTF wird nicht im Sicherheitsmodus, Seite 264 unterstützt)

Hohe Verfügbarkeit

Sie können mit zwei Sensoren an zwei unterschiedlichen Eingangskanälen auf unterschiedlichen Eingangsmodulen denselben physischen Wert überwachen und dadurch die Systemverfügbarkeit steigern.

Die folgende Abbildung zeigt die Konfiguration für redundante Digitaleingänge:



Der Wert des Eingangszustands von Sensor 1 und Sensor 2 wird von Eingangsmodul 1 und Eingangsmodul 2 über einen Black Channel an eine Sicherheits-CPU gesendet. Die CPU führt einen dedizierten Funktionsbaustein aus (S_DIHA), um die Daten der zwei Eingangsmodule zu verwalten und auszuwählen. Dieser Funktionsbaustein funktioniert wie folgt:

- Wenn der Zustand der Eingangsdaten von Modul 1 in Ordnung ist, werden die Eingangsdaten dieses Moduls in der Sicherheitsfunktion verwendet.
- Wenn der Zustand der Eingangsdaten von Modul 1 nicht in Ordnung ist, aber der Zustand der Eingangsdaten von Modul 2, werden die Eingangsdaten von Modul 2 verwendet.
- Wenn der Zustand der Eingangsdaten von Modul 1 und Modul 2 nicht in Ordnung ist, wird der Zustand des Eingangs in den sicheren Zustand (0) versetzt, um die Sicherheitsfunktion zu aktivieren.

Details zur Verdrahtung des Moduls für hohe Verfügbarkeit finden Sie in den Verdrahtungsbeispielen für Eingangsanwendungen, Seite 72.

Anschlussstecker BMXSDI1602

Einführung

Das digitale Eingangsmodul BMXSDI1602 umfasst 16 Eingänge in zwei Gruppen zu je 8 Eingängen. Die erste Gruppe besteht aus den Eingängen 0 bis 3 (Rang A und B), die zweite aus den Eingängen 4 bis 7 (Rang A und B). Zwischen diesen beiden Gruppen gibt es keine Isolierung.

Die Spannung für die Sensoren kann direkt über die externe Spannungsversorgung oder intern über die Spannungsversorgungen VS1 und VS2 bereitgestellt werden. Beide Bauweisen werden unten dargestellt.

Klemmenleisten

Die folgenden 20-poligen Klemmenleisten von Schneider Electric können für den 20-Punkt-Anschluss vorn am Modul genutzt werden:

- Schraubklemmenleiste BMXFTB2010
- Käfigfederzugklemmenleiste BMXFTB2000
- Federklemmenleiste BMXFTB2020

HINWEIS: Die Klemmenleisten können nur entfernt werden, wenn die Modulspannung abgeschaltet ist.

Prozessspannungsversorgung

Eine geschützte 24-VDC-Kleinspannungsversorgung (SELV/PELV) der Überspannungskategorie II ist erforderlich. Schneider Electric empfiehlt eine Spannungsversorgung, die nach einer Unterbrechung automatisch wieder hochfährt.

⚠ GEFAHR

VERLUST DER FÄHIGKEIT, SICHERHEITSFUNKTIONEN AUSZUFÜHREN

Verwenden Sie nur eine Prozessspannungsversorgung vom Typ SELV/PELV mit einer maximalen Abgabe von 60 V.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

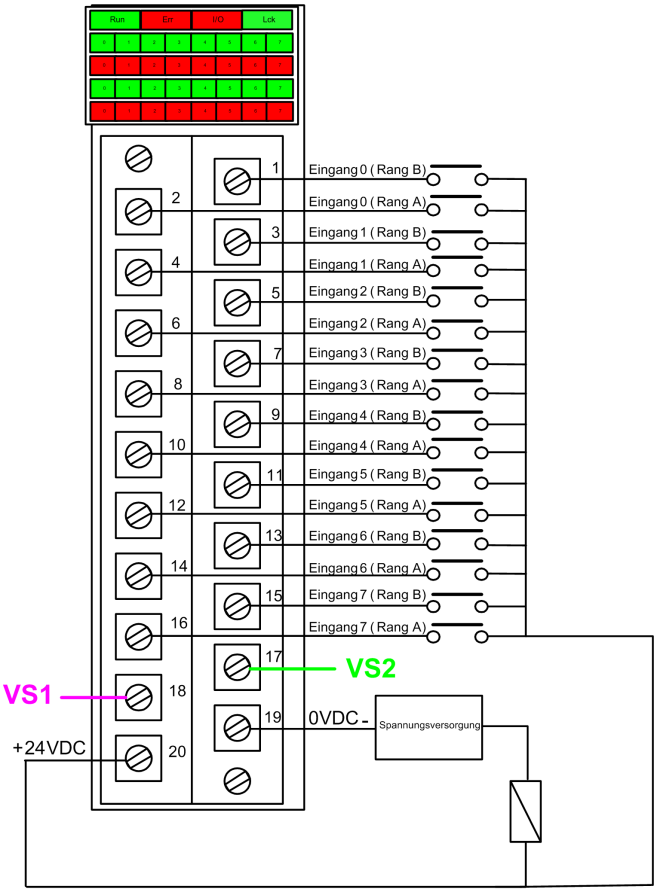
Sicherung

Es ist eine flinke Sicherung erforderlich, um die externe Spannungsversorgung vor Kurzschlüssen und Überspannung zu schützen.

HINWEIS
FALSCHE SICHERUNGSAUSWAHL Mit flinken Sicherungen schützen Sie die elektronischen Komponenten des digitalen Eingangsmoduls vor Überspannung. Die Auswahl einer falschen Sicherung kann zur Beschädigung des Eingangsmoduls führen. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Anschlussstecker: Über externe Spannungsersorgung gespeiste Sensoren

Bei der folgenden Bauweise werden die Sensoren direkt von einer externen Spannungsversorgung gespeist:



Spannungsversorgung: 24 VDC

Sicherung: Flinke Sicherung 0,5 A

HINWEIS: Durch eine externe Spannungsversorgung wird die Kanaldiagnose begrenzt, die das Modul durchführen kann. Bei dieser Bauweise kann das Modul Folgendes erkennen:

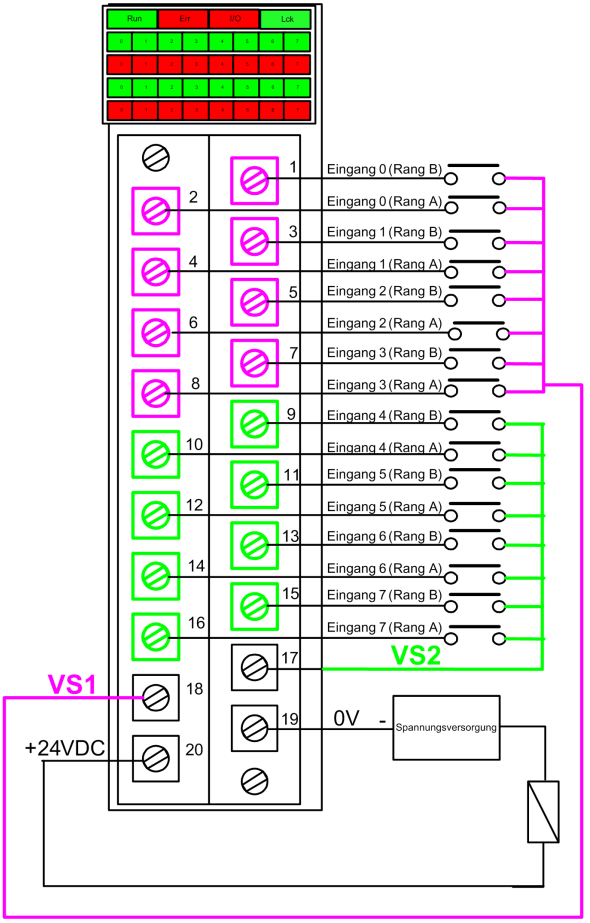
- Eine getrennte (oder offene) Verdrahtung (falls für den Kanal in Control Expert aktiviert)
- Einen Masseschluss

In dieser Bauweise erkennt das Modul Folgendes jedoch nicht:

- Einen Kurzschluss an 24 VDC
- Einen Querschluss an einem anderen Verdrahtungseingang

Anschlussstecker: Über interne Spannungsversorgung gespeiste Sensoren

Bei der folgenden Bauweise werden die Sensoren für die Kanäle 0 bis 3 über die überwachte Spannungsversorgung VS1 und die Sensoren für die Kanäle 4 bis 7 über die überwachte Bauweise VS2 gespeist:



Wenn Sie diese Bauweise verwenden, versorgen Sie die Kanalgruppen wie folgt mit interner Spannung:

- VS1 für die Spannungsversorgung der Kanäle 0 bis 3 (Rang A und B)
- VS2 für die Spannungsversorgung der Kanäle 4 bis 7 (Rang A und B)

HINWEIS: Bei dieser Bauweise kann das Modul Folgendes erkennen:

- Einen Kurzschluss an 24 VDC (falls für den Kanal in Control Expert aktiviert)
- Einen Querschluss an einem anderen Verdrahtungseingang
- Eine getrennte (oder offene) Verdrahtung (falls für den Kanal in Control Expert aktiviert)
- Einen Masseschluss

Zuweisung von Eingängen zu Anschlussstiften und Kanälen von Control Expert

Im Folgenden finden Sie eine Beschreibung der einzelnen Anschlussstifte am Eingangsmodul BMXSDI1602 sowie die Zuweisung der Stifte zu den Kanälen, wie es auf der Registerkarte **Konfiguration** des Modulkanals für das Modul in Control Expert Safety angezeigt wird:

Kanal in Control Expert	Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung	Kanal in Control Expert
0	Eingang 0 (Rang A)	2	1	Eingang 0 (Rang B)	8
1	Eingang 1 (Rang A)	4	3	Eingang 1 (Rang B)	9
2	Eingang 2 (Rang A)	6	5	Eingang 2 (Rang B)	10
3	Eingang 3 (Rang A)	8	7	Eingang 3 (Rang B)	11
4	Eingang 4 (Rang A)	10	9	Eingang 4 (Rang B)	12
5	Eingang 5 (Rang A)	12	11	Eingang 5 (Rang B)	13
6	Eingang 6 (Rang A)	14	13	Eingang 6 (Rang B)	14
7	Eingang 7 (Rang A)	16	15	Eingang 7 (Rang B)	15
–	VS1-Spannungsversorgung	18	17	VS2-Spannungsversorgung	–
–	24-VDC-Prozessspannungsversorgung	20	19	24-VDC-Prozessspannungsversorgung	–

BMXSDI1602 – Verdrahtungsbeispiele für Eingänge

Einführung

Um das digitale Sicherheitseingangsmodul BMXSDI1602 mit den Sensoren zu verdrahten und SIL3 einzuhalten, gibt es verschiedene Möglichkeiten. Abhängig ist dies von:

- Den erforderlichen Standards für Kategorie (Cat2 oder Cat4) und Performance Level (PLd oder PLe)
- Den Anforderungen Ihrer Anwendung für hohe Verfügbarkeit

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Das maximale Sicherheitsintegritäts-Level (SIL) wird durch die Qualität des Sensors und die Länge des Prüfabstands gemäß IEC 61508 festgelegt. Wenn Sie Sensoren nutzen, die den Qualitätsansprüchen des gewünschten SIL-Standards nicht entsprechen, sollten diese Sensoren immer redundant mit zwei Kanälen verdrahtet werden.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Im Folgenden werden verschiedene Verdrahtungsbeispiele für die digitale SIL3-Eingangsanwendung erläutert:

- Cat2/PLd:
  - Ein einziger Sensor, mit einem Eingang verbunden
- Cat2/PLd mit hoher Verfügbarkeit:
  - Ein einziger Sensor, mit zwei Eingangspunkten auf verschiedenen Eingangsmodulen verbunden
  - Zwei Sensoren, mit zwei Eingangspunkten auf verschiedenen Eingangsmodulen verbunden
- Cat4/PLe:
  - Ein einziger Sensor, mit zwei Eingangspunkten auf demselben Eingangsmodul verbunden
  - Zwei Sensoren, mit verschiedenen Eingangspunkten auf demselben Eingangsmodul verbunden
- Cat4/PLe mit hoher Verfügbarkeit:
  - Zwei Sensoren, mit zwei verschiedenen Eingangspunkten auf verschiedenen Eingangsmodulen verbunden

Konfigurierbare Verdrahtungsdiagnose in Control Expert

Für das digitale Eingangsmodul BMXSDI1602 nutzen Sie die entsprechende Seite **Konfiguration** in Control Expert:

- Aktivieren Sie die **Kurzschlusserkennung an 24 VDC** für alle erregten Kanäle. Mit diesem Test wird die folgende Stellglied-Verdrahtungsdiagnose für einen Kanal durchgeführt:
  - Kurzschlusserkennung an 24 VDC
  - Querschlusserkennung zwischen zwei Ausgangskanälen

  Das Prinzip besteht darin, die Sensoren in Gruppen von 8 Kanälen mit Spannung zu versorgen (VS1 für Kanäle 0 bis 3 (Rang A und B) und VS2 für Kanäle 4 bis 7 (Rang A und B)). An diese Spannungsausgänge wird regelmäßig ein OFF-Impuls gesendet (mit einem Abstand von unter 1 Sekunde und einer Dauer von unter 1 ms). Wenn die Spannung für den Eingang während dieses Impulses nicht null beträgt, liegt am Eingang ein Kurzschluss vor.
- Aktivieren Sie für alle acht Kanäle **Offene Draht-Erkennung**, wodurch die folgende Verdrahtungsdiagnose für den jeweiligen Kanal durchgeführt wird:
  - Erkennung offener (oder getrennter) Drähte (d. h. der Eingangskanal ist nicht mit dem Stellglied verbunden)
  - Masseschlusserkennung an 0 VDC

  Das Prinzip besteht in der künstlichen Erstellung und anschließenden Messung eines Fehlerstroms (Ileakage) auf der Leitung (mit einem parallel zum Sensor geschalteten Widerstand), wenn der Sensor geöffnet ist. Wenn der Fehlerstrom (0,4 mA <Ileakage < 1,3 mA) vom Modul an der Eingangsleitung nicht gemessen werden kann, wird die externe Leitung als durchtrennt eingestuft (oder als Kurzschluss nach Masse). Die Diagnose wird in einem Zeitraum von unter 10 ms durchgeführt.
  - Für Trockenkontaktsensoren empfehlen wir, parallel einen 33-kΩ-Widerstand zu nutzen.
  - Bei DDP-2- oder -3-Drähten muss der Ableitstrom zwischen den oben definierten Grenzwerten liegen. Sie müssen den Wert des parallel zum Sensor genutzten Widerstands definieren. Denken Sie dabei an den natürlichen Ableitstrom des Sensors und den internen Widerstand des Eingangs (7,5 K Ω).

⚠WARNUNG

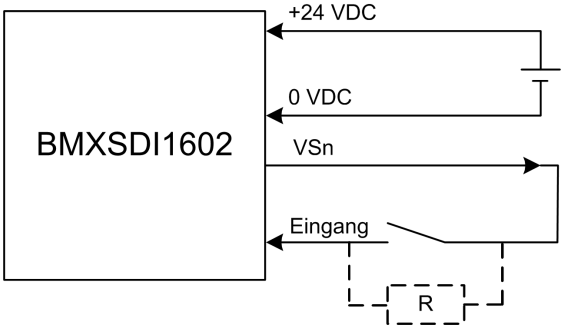
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Schneider Electric empfiehlt, die in Control Expert verfügbaren Diagnosetools zu aktivieren, um die obigen Probleme zu erkennen bzw. auszuschließen. Wenn ein Diagnosetest nicht aktiviert oder in Control Expert nicht vorhanden ist, müssen andere Sicherheitsmaßnahmen umgesetzt werden, um diese Probleme zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

SIL3 Cat2/PLd

Ein einziger Sensor, mit einem Eingang verbunden, Spannungsversorgung über interne VS:



Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

Da der Sensor intern über einen VS-Stift mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	

Problem	Erkennbar?	Übliche Erkennungszeit
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen[1]	Ja	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

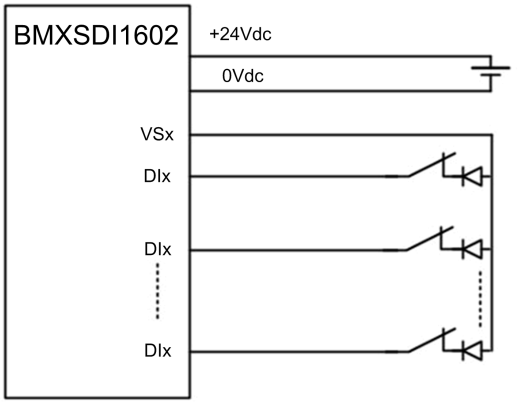
⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

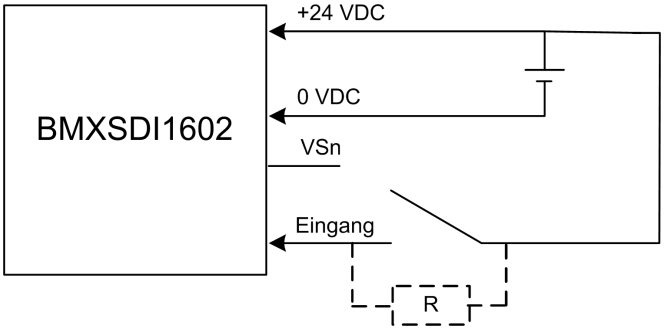
Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

HINWEIS: Fügen Sie ggf. der Eingangsschleife zwischen Sensor und Eingangspunkt eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.



Ein einziger Sensor, mit einem Eingang verbunden, externe Spannungsversorgung:



Da der Sensor extern mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC	Nein	–
Querschluss zwischen zwei Kanälen	Nein	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall eines einzigen Sensors, mit einem Eingang verbunden, externe Spannungsversorgung, siehe oben). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

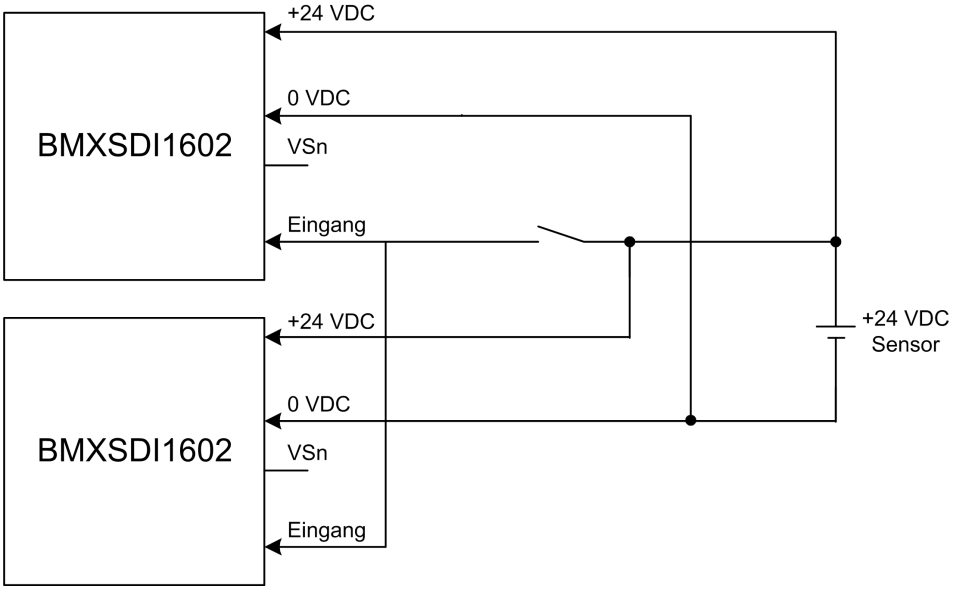
RISIKO EINES KURZSCHLUSSES AN 24 VDC

Das Modul kann keine Kurzschlüsse an 24 VDC erkennen (im Fall eines einzigen Sensors, mit einem Eingang verbunden, externe Spannungsversorgung, siehe oben). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

SIL3 Cat2/PLd mit hoher Verfügbarkeit

Ein einziger Sensor, mit zwei Eingängen verbunden, externe Spannungsversorgung:



Da der Sensor extern mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Nein	–
Masseschlusserkennung an 0 VDC	Nein	
Kurzschlusserkennung an 24 VDC[1]	Nein	

Problem	Erkennbar?	Übliche Erkennungszeit
Querschluss zwischen zwei Kanälen	Nein	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall eines einzigen Sensors, mit zwei Eingängen verbunden, externe Spannungsversorgung, siehe oben). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

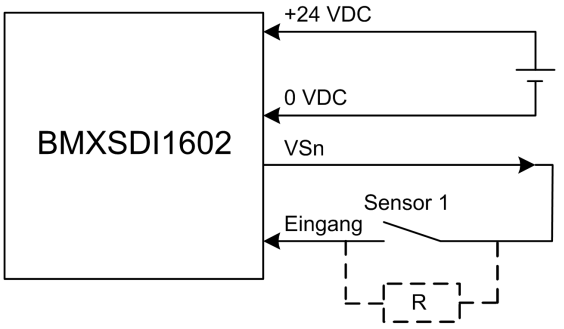
RISIKO EINES KURZSCHLUSSES AN 24 VDC

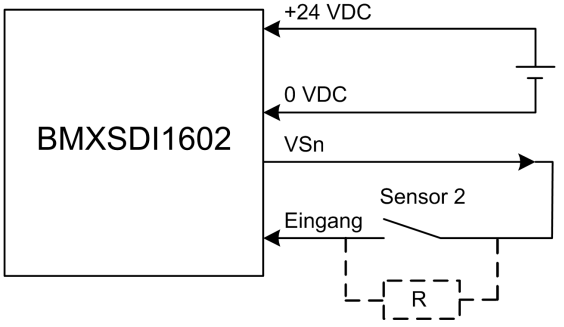
Das Modul kann keine Kurzschlüsse an 24 VDC erkennen (im Fall eines einzigen Sensors, mit zwei Eingängen verbunden, externe Spannungsversorgung, siehe oben). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Zwei redundante Sensoren, an verschiedenen Eingängen zweier Module mit Spannungsversorgung verbunden:

Das folgende Beispiel zeigt zwei redundante Sensoren (ggf. mechanisch verbunden), über die dieselbe Prozessvariable empfangen wird. Beide Sensoren sind mit einem einzigen Eingangspunkt auf verschiedenen Eingangsmodulen verdrahtet. Die Spannungsversorgung geschieht über die überwachte Spannungsversorgung:





Abhängig davon, ob die Spannung über VS1 oder V2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie den Funktionsbaustein `S_DIHA` nutzen, um die beiden Eingangssignale zu verwalten.
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Da der Sensor intern über einen VS-Stift mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Zwei redundante Sensoren, an verschiedenen Eingängen zweier Module mit externer Spannungsversorgung verbunden:

HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden. In diesem Fall wären ein Kurzschluss an 24 VDC und ein Querschluss zwischen zwei Kanälen nicht erkennbar.

Da der Sensor intern über einen VS-Stift mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC	Nein	–
Querschluss zwischen zwei Kanälen	Nein	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall zweier redundanter Sensoren, an einzelnen Eingängen zweier Module verbunden, externe Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO EINES KURZSCHLUSSES AN 24 VDC

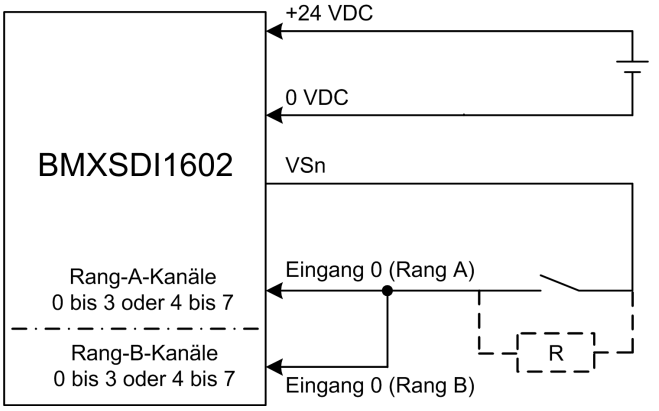
Das Modul kann keine Kurzschlüsse an 24 VDC erkennen (im Fall zweier redundanter Sensoren, an einzelnen Eingängen zweier Module verbunden, externe Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Cat4/PLe

Ein einziger Sensor, an zwei Eingängen desselben Moduls mit Spannungsversorgung verbunden:

Das folgende Beispiel zeigt einen Sensor, der mit zwei Eingangspunkten auf demselben Eingangsmodul verbunden ist. Die Spannungsversorgung erfolgt über die überwachte Spannungsversorgung:



Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie den Funktionsbaustein `S_EQUIVALENT` nutzen, um die beiden Eingangssignale zu verwalten.
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, Spannungsversorgung über VS-Stift:

Problem	**Erkennbar?**	**Übliche Erkennungszeit**
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Ein Sensor, an zwei Eingängen desselben Moduls mit externer Spannungsversorgung verbunden:

HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden. In diesem Fall wären ein Kurzschluss an 24 VDC und ein Querschluss zwischen zwei Kanälen nicht erkennbar.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, externe Spannungsversorgung:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Nein	–
Querschluss zwischen zwei Kanälen	Nein	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall eines einzigen Sensors, an zwei Eingängen desselben Moduls verbunden, externe Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

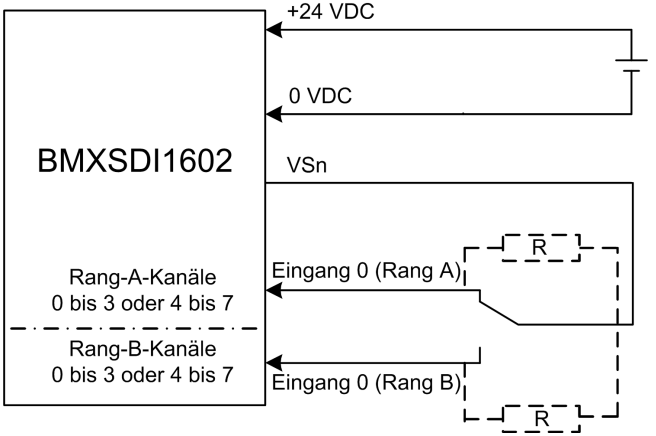
RISIKO EINES KURZSCHLUSSES AN 24 VDC

Das Modul kann keinen Kurzschluss an 24 VDC erkennen (im Fall eines einzigen Sensors, an zwei Eingängen desselben Moduls verbunden, externe Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Nicht äquivalenter Sensor, an zwei nicht äquivalenten Eingängen desselben Moduls mit Spannungsversorgung verbunden:

Das folgende Beispiel zeigt einen nicht äquivalenten Sensor, der mit zwei Eingangspunkten auf demselben Eingangsmodul verbunden ist. Die Spannungsversorgung erfolgt über die überwachte Spannungsversorgung: Das Modul führt eine 1oo2D-Prüfung durch:



Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie den Funktionsbaustein `S_ANTIIVALENT` nutzen, um die beiden Eingangssignale zu verwalten.
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Verdrahtungsdiagnose bei einem nicht äquivalenten Sensor, mit zwei Eingängen verbunden, Spannungsversorgung über VS-Stift:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

Nicht äquivalenter Sensor, an zwei nicht äquivalenten Eingängen desselben Moduls verbunden, externe Spannungsversorgung:

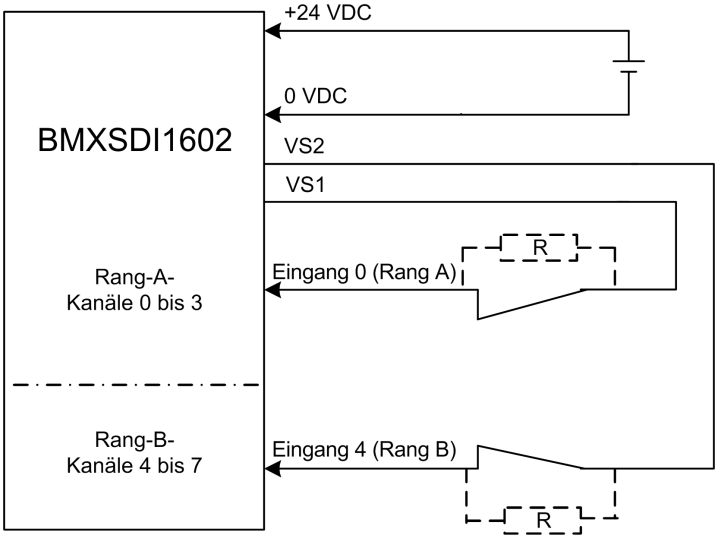
HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden. In diesem Fall wären ein Kurzschluss an 24 VDC und ein Querschluss zwischen zwei Kanälen nicht erkennbar.

Verdrahtungsdiagnose bei einem nicht äquivalenten Sensor, mit zwei Eingängen verbunden, externe Spannungsversorgung:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Nein	–
Querschluss zwischen zwei Kanälen	Nein	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

Empfang derselben Prozessvariable mit zwei separaten Sensoren (ggf. mechanisch verbunden) mit Spannungsversorgung:

Das folgende Beispiel zeigt zwei redundante Sensoren (ggf. mechanisch verbunden), über die dieselbe Prozessvariable empfangen wird. Beide Sensoren sind mit einem einzigen Eingangspunkt auf demselben Eingangsmodul verdrahtet. Die Spannungsversorgung geschieht über die überwachte Spannungsversorgung:



HINWEIS:

- Die Eingänge 0 bis 3 von Rang A werden mit den Eingängen 4 bis 7 von Rang B verwendet.
- Die Eingänge 0 bis 3 von Rang B werden mit den Eingängen 4 bis 7 von Rang A verwendet.

⚠WARNUNG

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwendet werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie den Funktionsbaustein `S_EQUIVALENT` nutzen, um die beiden Eingangssignale zu verwalten.
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, Spannungsversorgung über VS-Stift:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen (im Fall des Empfangs derselben Prozessvariable mit zwei separaten Sensoren mit Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO EINES KURZSCHLUSSES AN 24 VDC

Das Modul kann keine Kurzschlüsse an 24 VDC erkennen (im Fall des Empfangs derselben Prozessvariable mit zwei separaten Sensoren mit Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Empfang derselben Prozessvariable mit zwei separaten Sensoren (ggf. mechanisch verbunden) mit externer Spannungsversorgung:

HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden. In diesem Fall wären ein Kurzschluss an 24 VDC und ein Querschluss zwischen zwei Kanälen nicht erkennbar.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, externe Spannungsversorgung:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Nein	–
Querschluss zwischen zwei Kanälen	Nein	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall des Empfangs derselben Prozessvariable mit zwei separaten Sensoren mit externer Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

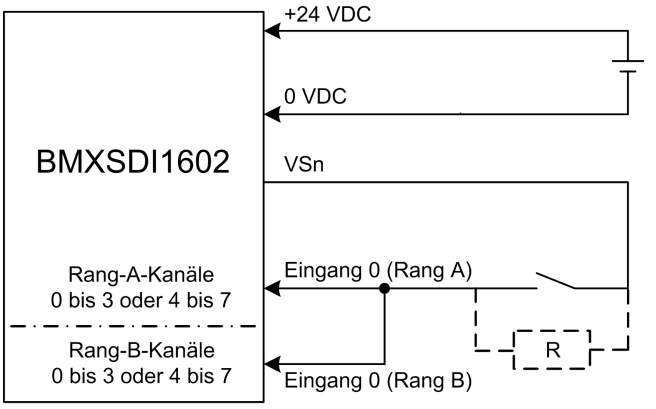
Um mit dieser Verdrahtung SIL3/Cat4/PLe zu erreichen, muss ein geeigneter, qualifizierter Sensor verwendet werden.

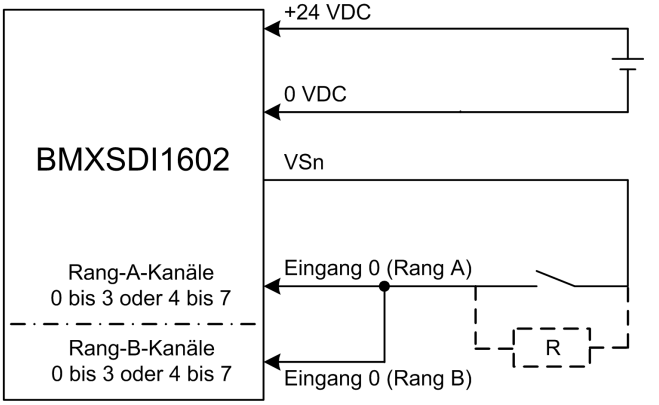
Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Cat4/PLe mit hoher Verfügbarkeit

Verdrahtungsschema mit Ein-Kanal-Verbindung zweier redundanter Ein-Kanal-Sensoren mit Spannungsversorgung:

Das folgende Beispiel zeigt zwei redundante Ein-Kanal-Sensoren (ggf. mechanisch verbunden), die mit zwei Eingangspunkten auf zwei verschiedenen Eingangsmodulen verbunden sind. Die Spannungsversorgung erfolgt über die überwachte Spannungsversorgung:





Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie die Funktionsbausteine `S_EQUIVALENT` und `S_DIHA` nutzen, um die vier Eingangssignale zu verwalten.
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, Spannungsversorgung über VS-Stift:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	
1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.		

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Verdrahtungsschema mit Ein-Kanal-Verbindung zwei redundanter Ein-Kanal-Sensoren mit externer Spannungsversorgung:

HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden. In diesem Fall wären ein Kurzschluss an 24 VDC und ein Querschluss zwischen zwei Kanälen nicht erkennbar.

Verdrahtungsdiagnose bei einem einzigen Sensor, mit zwei Eingängen verbunden, externe Spannungsversorgung:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	

Problem	Erkennbar?	Übliche Erkennungszeit
Kurzschlusserkennung an 24 VDC[1]	Nein	–
Querschluss zwischen zwei Kanälen	Nein	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen (im Fall einer Ein-Kanal-Verbindung von zwei redundanten Ein-Kanal-Sensoren mit externer Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

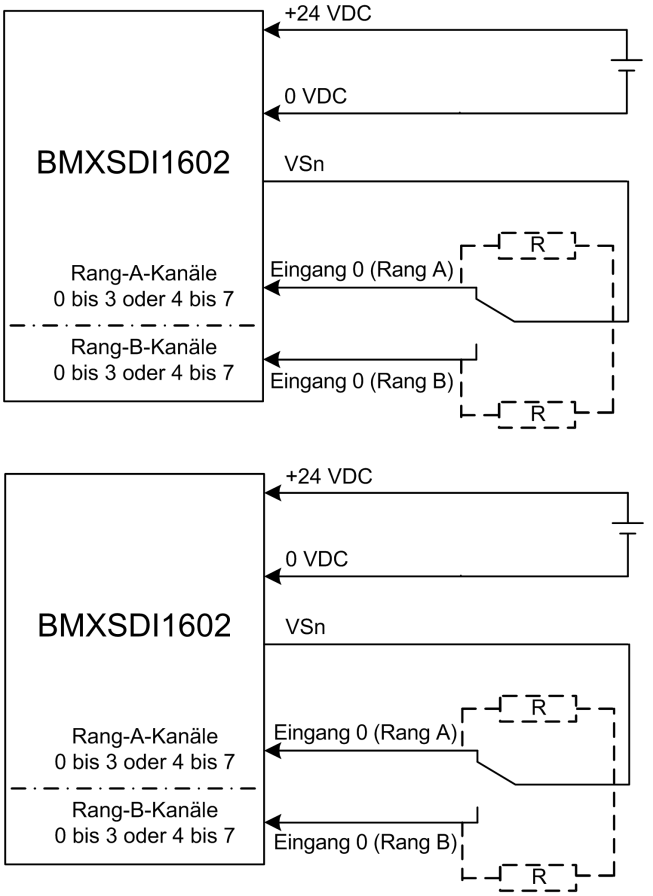
RISIKO EINES KURZSCHLUSSES AN 24 VDC

Das Modul kann keine Kurzschlüsse an 24 VDC erkennen (im Fall einer Ein-Kanal-Verbindung von zwei redundanten Ein-Kanal-Sensoren mit externer Spannungsversorgung). Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Nicht äquivalenter Sensor (ggf. mechanisch verbunden), an zwei nicht äquivalenten Eingängen zweier verschiedener Module mit Spannungsversorgung verbunden:

Das folgende Beispiel zeigt zwei redundante, nicht äquivalente Sensorpaare (ggf. mechanisch verbunden), die mit einem Eingangspunkt auf zwei verschiedenen Eingangsmodulen (zwei pro Modul) verbunden sind. Die Spannungsversorgung erfolgt über die überwachte Spannungsversorgung:



Abhängig davon, ob die Spannung über VS1 oder VS2 kommt, gilt Folgendes:

- Spannungsversorgung über VS1: Nutzen Sie Kanäle 0 bis 3, Rang A und B.
- Spannungsversorgung über VS2: Nutzen Sie Kanäle 4 bis 7, Rang A und B.

HINWEIS:

- Bei dieser Bauweise können Sie die Funktionsbausteine `S_ANTIVALENT` und `S_DIHA` nutzen, um die vier Eingangssignale zu verwalten.
  - `S_ANTIVALENT` für die 1oo2-Prüfung zweier Wertepaare, die von beiden, mit demselben Modul verbundenen Sensoren kommen
  - `S_DIHA` für die Verwaltung der Funktion für hohe Verfügbarkeit
- Fügen Sie der Eingangsschleife zwischen Sensor und Eingangspunkt ggf. eine Schottky-Diode hinzu, um die Wahrscheinlichkeit zu verringern, dass ein Kurzschluss an 24 VDC auf einem Kanal zu demselben Problem auf einem nebenliegenden Kanal führt.

Da der Sensor intern über einen VS-Stift mit Spannung versorgt wird, gilt die folgende Kanalverdrahtungsdiagnose:

Problem	Erkennbar?	Übliche Erkennungszeit
Offener (oder unterbrochener) Draht[1]	Ja	< 10 ms
Masseschlusserkennung an 0 V	Ja	
Kurzschlusserkennung an 24 VDC[1]	Ja	< 1 s
Querschluss zwischen zwei Kanälen	Ja	

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN DERSELBEN GRUPPE

Das Modul kann keine Querschlüsse zwischen zwei Kanälen in derselben VS-Kanalgruppe erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Nicht äquivalenter Sensor (ggf. mechanisch verbunden), an zwei nicht äquivalenten Eingängen zweier verschiedener Module mit externer Spannungsversorgung verbunden:

HINWEIS: Alternativ können die Sensoren über eine externe Spannungsversorgung versorgt werden (im Fall eines nicht äquivalenten Sensors, der mit zwei nicht äquivalenten Eingängen zweier unterschiedlicher Module verbunden ist und eine externe Spannungsversorgung hat). In diesem Fall wäre ein Querschluss zwischen zwei Kanälen nicht erkennbar.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN ZWISCHEN KANÄLEN

Das Modul kann keine Querschlüsse zwischen zwei Kanälen erkennen. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Um mit dieser Verdrahtung SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 zu erlangen, müssen geeignete, qualifizierte Sensoren verwendet werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

BMXSDI1602 - Datenstruktur

Einführung

Der gerätespezifische abgeleitete Datentyp (Device Derived Data Type, DDDT) `T_U_DIS_SIS_IN_16` ist die Schnittstelle zwischen dem digitalen BMXSDI1602-Eingangsmodul und der Anwendung, die auf der CPU läuft. Der DDDT `T_U_DIS_SIS_IN_16` umfasst die Datentypen `T_SAFE_COM_DBG_IN` und `T_U_DIS_SIS_CH_IN`.

All diese Strukturen werden im Folgenden beschrieben.

DDDT-Struktur `T_U_DIS_SIS_IN_16`

Die DDDT-Struktur `T_U_DIS_SIS_IN_16` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
MOD_HEALTH[1]	BOOL	• 1: Das Modul funktioniert ordnungsgemäß. • 0: Das Modul funktioniert nicht ordnungsgemäß.	RO
SAFE_COM_STS[1]	BOOL	• 1: Die Modulkommunikation ist gültig. • 0: Die Modulkommunikation ist nicht gültig.	RO
PP_STS	BOOL	• 1: Die Prozessspannungsversorgung läuft. • 0: Die Prozessspannungsversorgung ist außer Betrieb.	RO
CONF_LOCKED	BOOL	• 1: Die Modulkonfiguration ist gesperrt. • 0: Die Modulkonfiguration ist nicht gesperrt.	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Debug-Struktur für sichere Kommunikation	RO
CH_IN_A	ARRAY[0 bis 7] von T_U_DIS_SIS_CH_IN	Array der Struktur des Kanals von Rang A	–
CH_IN_B	ARRAY[0 bis 7] von T_U_DIS_SIS_CH_IN	Array der Struktur des Kanals von Rang B	–
MUID[2]	ARRAY[0 bis 3] von DWORD	Eindeutige Modul-ID (automatisch von Control Expert zugewiesen)	RO
RESERVED	ARRAY[0 bis 9] von INT	–	–

1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. MOD_HEALTH und SAFE_COM_STS sind auf 0 gesetzt.

2. Dieser automatisch generierte Wert kann geändert werden, indem im Hauptmenü von Control Expert der Befehl **Generieren > IDs erneuern & Alles generieren** ausgeführt wird.

Struktur `T_SAFE_COM_DBG_IN`

Die Struktur `T_SAFE_COM_DBG_IN` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
S_COM_EST	BOOL	• 1: Die Kommunikation mit dem Modul wurde hergestellt. • 0: Die Kommunikation mit dem Modul wurde nicht hergestellt oder ist fehlerhaft.	RO
M_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10:	RO

Element	Datentyp	Beschreibung	Zugriff
		• 1: Das Modul wird mit dem NTP-Server synchronisiert. • 0: Das Modul wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	
CPU_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Die CPU wird mit dem NTP-Server synchronisiert. • 0: Die CPU wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CHECKSUM	BYTE	Prüfsumme des Kommunikations-Frame	RO
COM_DELAY	UINT	Kommunikationsverzögerung zwischen zwei Werten, wie vom Modul erhalten: • 1 bis 65534: Die Zeit in ms, seitdem die CPU die letzte Kommunikation vom Modul empfangen hat. • 65535: Die CPU hat keine Kommunikation vom Modul empfangen.	RO
COM_TO	UINT	Timeout-Wert für die Kommunikation vom Modul	R/W
STS_MS_IN	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der vom Modul empfangenen Daten	RO
S_NTP_MS	UINT	Sicherer Zeitwert für einen Sekundenbruchteil (bis zur nächsten ms) für den aktuellen Zyklus	RO
STS_S_IN	UDINT	Sicherer Zeitstempelwert (in Sekunden) der vom Modul empfangenen Daten	RO
S_NTP_S	UDINT	Sicherer Zeitwert (in Sekunden) für den aktuellen Zyklus	RO
CRC_IN	UDINT	CRC-Wert für die vom Modul empfangenen Daten	RO

Struktur `T_U_DIS_SIS_CH_IN`

Die Struktur `T_U_DIS_SIS_CH_IN` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
CH_HEALTH[1]	BOOL	• 1: Der Kanal ist funktionsfähig. • 0: Auf dem Kanal wurde ein Fehler entdeckt. Er ist nicht funktionsfähig. **Formel**: CH_HEALTH = not (OC or IC or SC) and SAFE_COM_STS	RO
VALUE[2]	EBOOL	• 1: Der Eingang ist erregt. • 0: Der Eingang ist deaktiviert. **Formel**: VALUE = if (SAFE_COM_STS and not (IC)) then READ_VALUE else 0	RO
OC	BOOL	• 1: Der Kanal ist offen oder es liegt ein Masseschluss vor. • 0: Der Kanal ist verbunden. Es liegt kein Masseschluss vor.	RO
SC	BOOL	• 1: Auf dem Kanal liegt ein Kurzschluss an einer 24-VDC-Quelle oder zwischen zwei Kanälen vor. • 0: Auf dem Kanal liegt kein Kurzschluss an einer 24-VDC-Quelle oder zwischen zwei Kanälen vor.	RO
IC	BOOL	• 1: Das Modul hat einen ungültigen Kanal erkannt. • 0: Der Kanal wird intern vom Modul als funktionsfähig erklärt.	RO
V_OC	BOOL	Konfigurationsstatus des Tests für einen offenen Kanal/Masseschluss: • 1: Aktiviert • 0: Deaktiviert	RO
V_SC	BOOL	Konfigurationsstatus des Tests für einen Kurzschluss an einer 24-VDC-Quelle: • 1: Aktiviert • 0: Deaktiviert	RO

1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. CH_HEALTH ist auf 0 gesetzt.

2. Das Element VALUE kann von BMX CRA oder BME CRA mit einem Zeitstempel versehen werden.

Digitales Ausgangsmodul BMXSDO0802

Einführung

In diesem Abschnitt wird das Modul BMXSDO0802, d. h. das digitale M580-Sicherheitsausgangsmodul, beschrieben.

Digitales Sicherheitsausgangsmodul BMXSDO0802

Einführung

Das digitale Sicherheitsausgangsmodul BMXSDO0802 weist folgende Leistungsmerkmale auf:

- 8 nicht-elektrisch isolierte 0,5-A-Ausgänge
- 24-VDC-Ausgangsspannung
- Realisiert Folgendes:
  - SIL3 IEC61508, SILCL3 IEC62061.
  - SIL4 EN5012x.
  - Kategorie 4 (Cat4) / Performance Level e (PLe) ISO13849.
- Überwacht die externe Spannungsversorgung des Voraktors.
- Anzeige für die LED-Diagnose, Seite 250 für das Modul und die einzelnen Ausgangskanäle.
- Automatisch bereitgestellte Diagnose der Kanalverdrahtung, mit denen die folgenden Probleme erkannt werden, während der Ausgang *erregt* ist:
  - Überlaststrom
  - Masseschlusserkennung an 0 VDC
- Konfigurierbare Kanalverdrahtungsdiagnose (aktivieren/deaktivieren), Seite 103, mit der folgende Probleme erkannt werden:
  - Offener (oder unterbrochener) Draht
- Konfigurierbare Diagnose der Kanalverdrahtung (aktivieren/deaktivieren), mit denen die folgenden Probleme erkannt werden, während der Ausgang *entregt* ist:
  - Masseschlusserkennung an 0 VDC

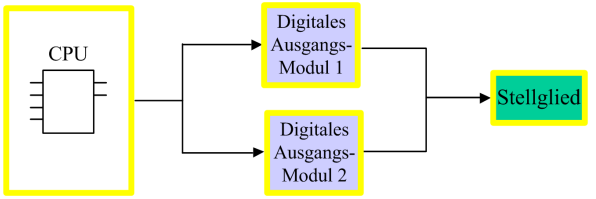
- Konfigurierbare Diagnose der Kanalverdrahtung (aktivieren/deaktivieren), mit denen die folgenden Probleme erkannt werden, während der Ausgang *erregt* oder *entregt* ist:
  - Kurzschlusserkennung an 24 VDC
  - Querschlusserkennung zwischen zwei Kanälen (falls die Sensorspannung intern bereitgestellt wird)
- Konfigurierbare Fehlerausweicheinstellungen für einzelne Kanäle, die angewendet werden, wenn die Kommunikation zwischen CPU und Ausgangsmodul verloren geht.
- Hot-Swapping des Moduls während der Laufzeit.
- CCOTF des Moduls funktioniert im Wartungsmodus, Seite 265. (CCOTF wird nicht im Sicherheitsmodus, Seite 264 unterstützt)

  HINWEIS: An jedem Ausgang wird ein Selbsttest durchgeführt, um dessen Fähigkeit zur Entregung und zur Erreichung des sicheren Zustands ohne Folgen für die Last zu überprüfen (Abschaltimpuls < 1 ms). Die Selbsttests erfolgen nacheinander - jeweils ein Ausgang zu einem Zeitpunkt - für jeden erregten Ausgang mit einer Dauer von unter 1 Sekunde. Wenn ein Ausgang mit einem statischen Eingang eines Produkts verbunden ist, erfasst der verbundene statische Eingang ggf. diesen Impuls. Es kann sinnvoll sein, einen Filter einzusetzen, um die potenziellen Folgen dieses Impulses für den Eingang zu vermeiden.

Hohe Verfügbarkeit

Sie können die CPU über einen Black Channel mit zwei Ausgangsmodulen verbinden und dann jedes Ausgangsmodul mit einem einzigen Aktor. Es ist kein Funktionsbaustein erforderlich, da das Signal von der CPU mit beiden Ausgangskanälen verbunden ist.

Die folgende Abbildung zeigt die Konfiguration für redundante Digitalausgänge für hohe Verfügbarkeit:



Der Zustand der einzelnen Ausgangsmodule kann aus den Elementen seiner DDDT-Struktur T_U_DIS_SIS_OUT_8, Seite 109 gelesen werden. Mit diesen Daten können Sie feststellen, ob ein Modul ausgetauscht werden muss. Wenn ein Modul nicht mehr funktionsfähig ist und ersetzt werden muss, läuft das System während des Austauschs in einer SIL3-kompatiblen Konfiguration weiter.

Details zu dieser Bauweise finden Sie im Verdrahtungsbeispiel für hoch verfügbare Ausgänge, Seite 106.

Anschlussstecker BMXSDO0802

Einführung

Das digitale Ausgangsmodul BMXSDO0802 umfasst eine einzelne Gruppe von 8 Ausgängen.

- Beide allgemeine +24-VDC-Spannungsversorgungsstifte (18 und 20) sind intern verbunden.
- Alle allgemeinen 0-V-Stifte (1, 3, 5, 7, 9, 11, 13, 15, 17 und 19) sind intern verbunden.

Klemmenleisten

Die folgenden 20-poligen Klemmenleisten von Schneider Electric können für den 20-Punkt-Anschluss vorn am Modul genutzt werden:

- Schraubklemmenleiste BMXFTB2010
- Käfigfederzugklemmenleiste BMXFTB2000
- Federklemmenleiste BMXFTB2020

HINWEIS: Die Klemmenleisten können nur entfernt werden, wenn die Modulspannung abgeschaltet ist.

Prozessspannungsversorgung

Eine geschützte 24-VDC-Kleinspannungsversorgung (SELV/PELV) der Überspannungskategorie II ist erforderlich. Schneider Electric empfiehlt eine Spannungsversorgung, die nach einer Unterbrechung automatisch wieder hochfährt.

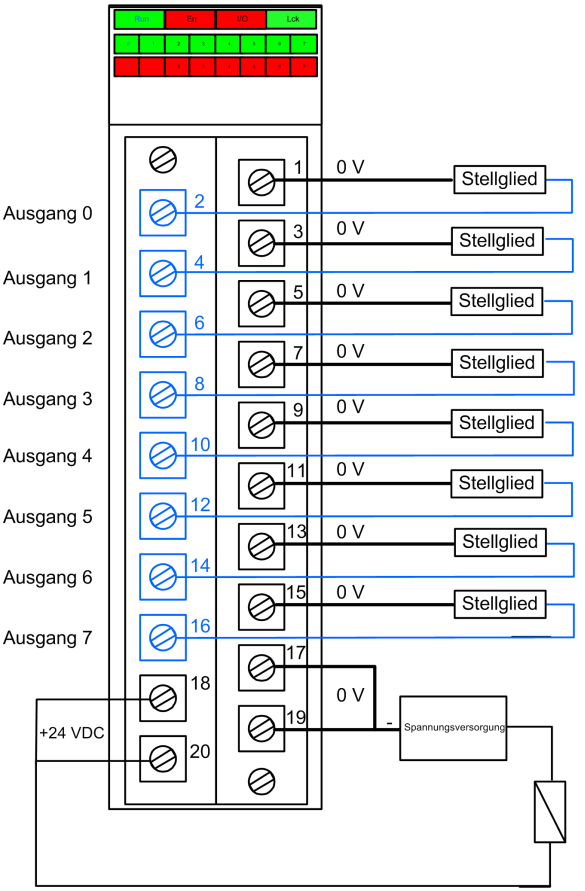
Sicherung

Es ist eine flinke Sicherung (max. 6 A) erforderlich, um die externe Spannungsversorgung vor Kurzschlüssen und Überspannung zu schützen.

⚠VORSICHT
FALSCHE SICHERUNGSAUSWAHL Mit flinken Sicherungen schützen Sie die elektronischen Komponenten des digitalen Ausgangsmoduls vor Überspannung. Die Auswahl einer falschen Sicherung kann zur Beschädigung des Ausgangsmoduls führen. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

Anschlusssteckerstifte

Die folgende Verdrahtungsdarstellung zeigt ein Ausgangsmodul, das mit 8 Aktoren verbunden ist:



Zuweisung von Ausgängen zu Anschlussstiften

Es folgt eine Beschreibung der einzelnen Stifte des BMXSDO0802-Ausgangsmoduls:

Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung
Ausgang 0	2	1	Allgemein 0 V
Ausgang 1	4	3	Allgemein 0 V
Ausgang 2	6	5	Allgemein 0 V
Ausgang 3	8	7	Allgemein 0 V
Ausgang 4	10	9	Allgemein 0 V
Ausgang 5	12	11	Allgemein 0 V
Ausgang 6	14	13	Allgemein 0 V
Ausgang 7	16	15	Allgemein 0 V
24-VDC-Prozessspannungsversorgung	18	17	Allgemein 0 V
24-VDC-Prozessspannungsversorgung	20	19	Allgemein 0 V

BMXSDO0802 – Verdrahtungsbeispiele für Ausgangsanwendung

Einführung

Sie können das digitale Sicherheitsausgangsmodul BMXSDO0802 auf verschiedene Weisen mit Stellgliedern verdrahten, um SIL3 Kategorie 4 (Cat4)/Performance Level e (PLe) zu erreichen, je nach Ihren Anforderungen für hohe Verfügbarkeit.

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Das maximale Sicherheitsintegritäts-Level (SIL) wird durch die Qualität des Stellglieds und die Länge des Prüfabstands gemäß IEC 61508 festgelegt. Wenn Sie Stellglieder nutzen, die den Qualitätsansprüchen des gewünschten SIL-Standards nicht entsprechen, sollten diese Stellglieder immer redundant mit zwei Kanälen verdrahtet werden.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Im Folgenden werden verschiedene Verdrahtungsbeispiele für die digitale SIL3-Cat4/PLe-Ausgangsanwendung erläutert:

- Cat4/PLe:
  - Ein Ausgangsmodulkanal, der eine Prozessvariable kontrolliert. Bei dieser Bauweise wird ein Stellglied eingesetzt.
- Cat4/PLe mit hoher Verfügbarkeit:
  - Zwei redundante Ausgangsmodule, bei denen je ein Kanal mit einem separaten Stellglied verbunden ist. Es wird aber dieselbe Prozessvariable kontrolliert.

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Wenn die Ausrüstung in Feuer- und Gasanwendungen genutzt wird oder wenn der Anforderungszustand des Ausgangs erregt ist:

- Ihr Prüftestvorgang muss einen Test umfassen, mit dem ermittelt wird, dass die Erkennung getrennter Drähte funktioniert, indem der Funktionsbaustein entfernt und sichergestellt wird, dass die entsprechenden Fehlerbits gesetzt sind.
- Stellen Sie sicher, dass die Masseschlusserkennung funktioniert, entweder indem die Diagnosefunktion **Impulstest für Zustand „Erregt“** auf der Modulregisterkarte **Konfiguration** aktiviert ist oder indem Sie einen anderen Vorgang implementieren (Ausgang auf 1 setzen, die Diagnose prüfen usw.).
- Vermeiden Sie lampenähnliche Stellglieder, da deren Impedanz sehr gering ist, wenn sie eingeschaltet sind. Dies kann zur falschen Erkennung eines Kurzschlusses oder einer Überladung führen.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Konfigurierbare Verdrahtungsdiagnose in Control Expert

Für das digitale Ausgangsmodul BMXSDO0802 nutzen Sie die entsprechende Seite **Konfiguration** in Control Expert:

- Aktivieren Sie die **Kurzschlusserkennung an 24 VDC** für alle erregten Kanäle. Mit diesem Test wird die folgende Stellglied-Verdrahtungsdiagnose für einen Kanal durchgeführt:
  - Kurzschlusserkennung an 24 VDC
  - Querschlusserkennung zwischen zwei Ausgangskanälen

- Aktivieren Sie für alle acht Kanäle **Offene Draht-Erkennung**, wodurch die folgende Verdrahtungsdiagnose für den jeweiligen Kanal durchgeführt wird:
  - Erkennung offener (oder getrennter) Drähte (d. h. der Ausgangskanal ist nicht mit dem Stellglied verbunden)
  - Masseschlusserkennung an 0 VDC
- Aktivieren Sie für jeden Ausgangskanal **Impulstest für Zustand „Erregt“**. Dieser Test wird regelmäßig ausgeführt, wenn sich der Ausgang im deaktivierten Zustand befindet. Es wird ein Impuls (mit einer Dauer von unter 1 ms) auf den Ausgang angewendet, um herauszufinden, ob ein Übergang in den erregten Zustand möglich ist. Wenn der Strom einen Schwellenwert von 0,7 A überschreitet, wird für den Ausgang ein Masseschluss gemeldet. Die Testzeitraum beträgt unter 1 s.

⚠WARNUNG

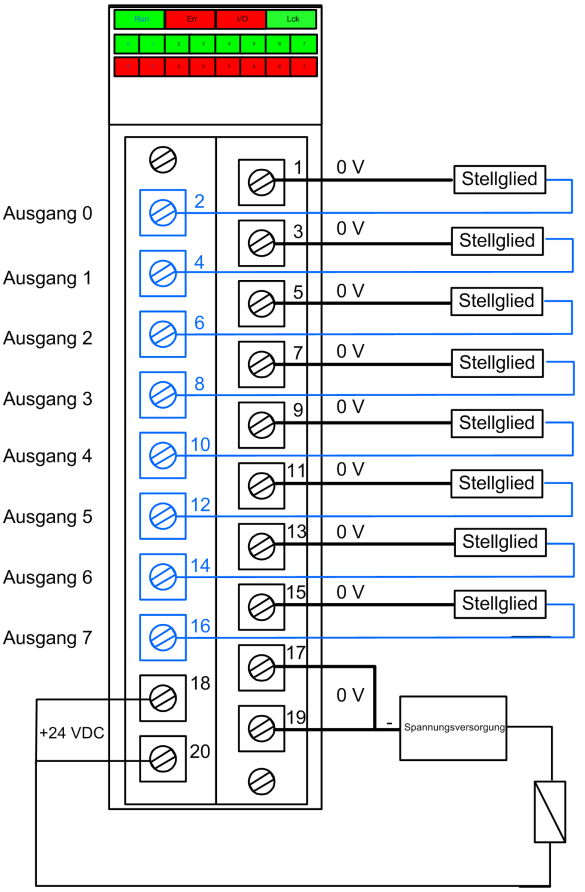
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Schneider Electric empfiehlt, die in Control Expert verfügbaren Diagnosetools zu aktivieren, um die obigen Probleme zu erkennen bzw. auszuschließen. Wenn ein Diagnosetest nicht aktiviert oder in Control Expert nicht vorhanden ist, müssen andere Sicherheitsmaßnahmen umgesetzt werden, um diese Probleme zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

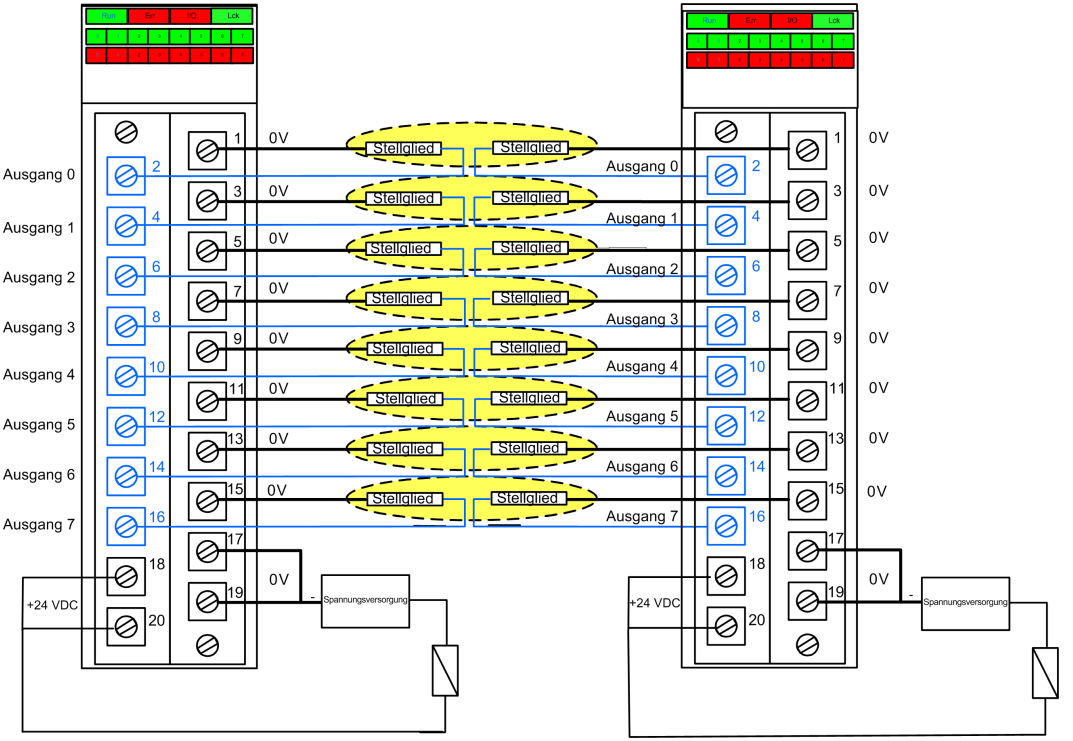
SIL 3 Cat4/PLe – Beispiel für ein digitales Ausgangsmodul

Das folgende Beispiel zeigt ein exklusives Stellglied, das mit einem Ausgangspunkt eines Ausgangsmoduls verbunden ist. Jede Schleife ist SIL 3 Cat4/PLe:



Beispiel für SIL 3 Cat4/PLe – Hohe Verfügbarkeit:

In der folgenden Abbildung kontrollieren zwei redundante Ausgänge dieselbe Prozessvariable. Wie unten dargestellt, ist jeder Ausgang mit separaten Stellgliedern verbunden. Dann führt jedes Stellglied denselben Befehl aus, der über unterschiedliche Kanäle gesendet wird. Alternativ können die zwei redundanten Ausgänge zusammen verdrahtet werden, um dasselbe Stellglied zu kontrollieren.



Zusammenfassung der Ausgangsverdrahtungsdiagnose

Die beiden Bauweisen ermöglichen die folgende Verdrahtungsdiagnose:

Problem	**Diagnose im Ausgangszustand verfügbar?**	
	Erregt	**Deaktiviert**
Offener (oder unterbrochener) Draht[1]	Ja. Wird in jedem Zyklus diagnostiziert.	Ja. Wird in jedem Zyklus diagnostiziert.
Ausgang überladen[2]	Ja. Wird in jedem Zyklus diagnostiziert.	Nein

Problem	Diagnose im Ausgangszustand verfügbar?	
	Erregt	**Deaktiviert**
Masseschlusserkennung an 0 VDC	Ja. Wird in jedem Zyklus diagnostiziert.	Ja. Diagnosezeitraum < 1 s.
Kurzschlusserkennung an 24 VDC[1]	Ja. Diagnosezeitraum < 1 s.	Ja. Wird in jedem Zyklus diagnostiziert.
Querschluss zwischen zwei Kanälen	Ja. Diagnosezeitraum < 1 s.	Ja. Wird in jedem Zyklus diagnostiziert.

1. Diese Diagnosefunktion wird ausgeführt, wenn sie auf der Modulregisterkarte **Konfiguration** in Control Expert aktiviert ist.

2. Machen Sie den Ausgang wieder funktionsbereit, nachdem Sie das Problem gelöst haben, indem Sie ihn deaktivieren.

⚠WARNUNG

RISIKO EINES MASSESCHLUSSES AN 0 VDC

Für den Masseschluss an 0 VDC mit dem Ausgang im deaktivierten Zustand wird empfohlen, die Option **Offene Draht-Erkennung** auf der Modulregisterkarte **Konfiguration** zu aktivieren. Alternativ ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO EINES KURZSCHLUSSES AN 24 VDC

Für den Kurzschluss an 24 VDC mit einem deaktivierten oder erregten Ausgangszustand wird empfohlen, die Option **Kurzschlusserkennung an 24 VDC** auf der Modulregisterkarte **Konfiguration** zu aktivieren. Alternativ ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN

Das Modul kann Querschlüsse zwischen zwei Kanälen nicht erkennen, wenn der Ausgang deaktiviert und der andere Kanal deaktiviert ist. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen, falls es auftritt, wenn der Ausgang in den erregten Zustand wechselt.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN

Für den Querschluss zwischen zwei Kanälen mit dem Ausgang im deaktivierten Zustand und dem anderen Kanal im erregten Zustand wird empfohlen, die Option **Kurzschlusserkennung an 24 VDC** auf der Modulregisterkarte **Konfiguration** zu aktivieren. Alternativ ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen, wenn der Ausgang in den erregten Zustand wechselt.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN

Das Modul kann Querschlüsse zwischen zwei Kanälen nicht erkennen, wenn der Ausgang erregt und der andere Kanal deaktiviert ist. Es ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

⚠WARNUNG

RISIKO VON QUERSCHLÜSSEN

Für den Querschluss zwischen zwei Kanälen mit dem Ausgang im erregten Zustand und dem anderen Kanal im erregten Zustand wird empfohlen, die Option **Kurzschlusserkennung an 24 VDC** auf der Modulregisterkarte **Konfiguration** zu aktivieren. Alternativ ist eine weitere Sicherheitsmaßnahme erforderlich, um dieses Problem zu erkennen oder auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

BMXSDO0802 - Datenstruktur

Einführung

Der gerätespezifische abgeleitete Datentyp (Device Derived Data Type, DDDT) `T_U_DIS_SIS_OUT_8` ist die Schnittstelle zwischen dem digitalen Ausgangsmodul BMXSDO0802 und der Anwendung, die auf der CPU läuft. Der DDDT `T_U_DIS_SIS_OUT_8` umfasst die Datentypen `T_SAFE_COM_DBG_OUT` und `T_U_DIS_SIS_CH_OUT`.

All diese Strukturen werden im Folgenden beschrieben.

DDDT-Struktur `T_U_DIS_SIS_OUT_8`

Die DDDT-Struktur `T_U_DIS_SIS_OUT_8` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
MOD_HEALTH[1]	BOOL	• 1: Das Modul funktioniert ordnungsgemäß. • 0: Das Modul funktioniert nicht ordnungsgemäß.	RO
SAFE_COM_STS[1]	BOOL	• 1: Die Modulkommunikation ist gültig. • 0: Die Modulkommunikation ist nicht gültig.	RO
PP_STS	BOOL	• 1: Die Prozessspannungsversorgung läuft. • 0: Die Prozessspannungsversorgung ist außer Betrieb.	RO
CONF_LOCKED	BOOL	• 1: Die Modulkonfiguration ist gesperrt.	RO

Element	Datentyp	Beschreibung	Zugriff
		• 0: Die Modulkonfiguration ist nicht gesperrt.	
S_COM_DBG	T_SAFE_COM_DBG_OUT	Debug-Struktur für sichere Kommunikation	RO
CH_OUT	ARRAY[0 bis 7] von T_U_DIS_SIS_CH_OUT	Array der Kanalstruktur	RO
S_TO	UINT	Sicherheitstimeout, der den Wechsel des Moduls in den Fehlerausweichzustand auslöst.	RO
MUID[2]	ARRAY[0 bis 3] von DWORD	Eindeutige Modul-ID (automatisch von Control Expert zugewiesen)	RO
RESERVED_1	ARRAY[0 bis 8] von INT	–	–
RESERVED_2	ARRAY[0 bis 6] von INT	–	–

1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. MOD_HEALTH und SAFE_COM_STS sind auf 0 gesetzt.

2. Dieser automatisch generierte Wert kann geändert werden, indem im Hauptmenü von Control Expert der Befehl **Generieren > IDs erneuern & Alles generieren** ausgeführt wird.

Struktur T_SAFE_COM_DBG_OUT

Die Struktur T_SAFE_COM_DBG_OUT umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
S_COM_EST	BOOL	• 1: Die Kommunikation mit dem Modul wurde hergestellt. • 0: Die Kommunikation mit dem Modul wurde nicht hergestellt oder ist fehlerhaft.	RO
M_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Das Modul wird mit dem NTP-Server synchronisiert. • 0: Das Modul wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CPU_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Die CPU wird mit dem NTP-Server synchronisiert. • 0: Die CPU wird nicht mit dem NTP-Server synchronisiert.	RO

Element	Datentyp	Beschreibung	Zugriff
		HINWEIS: Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	
CHECKSUM	BYTE	Prüfsumme des Kommunikations-Frame	RO
COM_DELAY	UINT	Kommunikationsverzögerung zwischen zwei Werten, wie vom Modul erhalten: • 1 bis 65534: Die Zeit in ms, seitdem die CPU die letzte Kommunikation vom Modul empfangen hat. • 65535: Die CPU hat keine Kommunikation vom Modul empfangen.	RO
COM_TO	UINT	Timeout-Wert für die Kommunikation vom Modul	R/W
STS_MS_IN	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der vom Modul empfangenen Daten	RO
S_NTP_MS	UINT	Sicherer Zeitwert für einen Sekundenbruchteil (bis zur nächsten ms) für den aktuellen Zyklus	RO
STS_S_IN	UDINT	Sicherer Zeitstempelwert (in Sekunden) der vom Modul empfangenen Daten	RO
S_NTP_S	UDINT	Sicherer Zeitwert (in Sekunden) für den aktuellen Zyklus	RO
CRC_IN	UDINT	CRC-Wert für die vom Modul empfangenen Daten	RO
STS_MS_OUT	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der an das Modul gesendeten Daten	RO
STS_S_OUT	UDINT	Sicherer Zeitstempelwert (in Sekunden) der an das Modul gesendeten Daten	RO
CRC_OUT	UDINT	CRC-Wert für die an das Modul gesendeten Daten	RO

Struktur `T_U_DIS_SIS_CH_OUT`

Die Struktur `T_U_DIS_SIS_CH_OUT` umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
CH_HEALTH[1]	BOOL	• 1: Der Kanal ist funktionsfähig. • 0: Auf dem Kanal wurde ein Fehler entdeckt. Er ist nicht funktionsfähig. **Formel**: CH_HEALTH = not (SC or OL or IC or OC) and SAFE_COM_STS and not (module in Fallback state)	RO
VALUE	EBOOL	Sicherer Befehl des Ausgabekanals: • 1: Befehl, den Ausgang zu schließen (erregt) • 0: Befehl, den Ausgang zu öffnen (deaktiviert)	R/W
TRUE_VALUE[2]	BOOL	Rücklesewert des Ausgangsrelaiskanals: • 1: Der Ausgang ist geschlossen (erregt). • 0: Der Ausgang ist offen (deaktiviert).	RO
OC	BOOL	• 1: Der Kanal ist offen oder es liegt ein Masseschluss vor. • 0: Der Kanal ist verbunden. Es liegt kein Masseschluss vor.	RO
SC	BOOL	• 1: Auf dem Kanal liegt ein Kurzschluss an einer 24-VDC-Quelle oder ein Querschluss mit einem anderen Kanal vor. • 0: Auf dem Kanal liegt kein Kurzschluss an einer 24-VDC-Quelle oder kein Querschluss vor.	RO
OL	BOOL	• 1: Der Kanal ist überladen oder es liegt ein Masseschluss an 0 VDC vor. • 0: Der Kanal ist nicht überladen oder es liegt kein Masseschluss an 0 VDC vor.	RO
IC	BOOL	• 1: Das Modul hat einen ungültigen Kanal erkannt. • 0: Der Kanal wird intern vom Modul als funktionsfähig erklärt.	RO
V_OC	BOOL	Konfigurationsstatus des Tests für einen offenen Kanal: • 1: Aktiviert • 0: Deaktiviert	RO
V_SC	BOOL	Konfigurationsstatus des Tests für einen Kurzschluss an einer 24-VDC-Quelle: • 1: Aktiviert • 0: Deaktiviert	RO

Element	Datentyp	Beschreibung	Zugriff
V_PULSE_ON	BOOL	Konfigurationsstatus des Impulstests (erregt): • 1: Aktiviert • 0: Deaktiviert	RO
CH_FBC	BOOL	Konfiguration der Fehlerausweicheinstellung für die Kanäle: • 1: Benutzerdefinierter Wert • 0: Letzten Wert halten	RO
CH_FBST	BOOL	Konfiguration des Fehlerausweichzustands der Kanäle bei Auswahl von „Benutzerdefinierter Wert“: • 1: Erregt • 0: Entregt	RO
1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. CH_HEALTH ist auf 0 gesetzt. 2. Das Element TRUE_VALUE kann von BMX CRA oder BME CRA mit einem Zeitstempel versehen werden.			

Digitales Relaisausgangsmodul BMXSRA0405

Einführung

In diesem Abschnitt wird das Modul BMXSRA0405, d. h. das digitale M580-Relaissicherheitsausgangsmodul, beschrieben.

Digitales Sicherheitsrelaisausgangsmodul BMXSRA0405

Einführung

Das digitale Sicherheitsrelaisausgangsmodul BMXSRA0405 weist folgende Leistungsmerkmale auf:

- 4 Relaisausgänge mit 5 A
- Ausgangsspannung 24 VDC und 24 bis 230 VAC (Überspannung Kategorie II)
- Erreicht SIL4 (EN5012x) / SIL3 (IEC61508) Kategorie 4 (Cat4) / Performance Level e (PLe).
- Unterstützt 8 vordefinierte Verdrahtungskonfigurationen
- Konfigurierbare, automatische Selbsttestüberwachung der Relaiskapazität für die Ausführung des befohlenen Ausgangszustands (abhängig von der ausgewählten Verdrahtungskonfiguration)
- Konfigurierbare Moduleinstellungen für Fehlerausweichmodus und -Timeout (in ms)
- Anzeige für die LED-Diagnose, Seite 255 für Modul und einzelne Ausgangskanäle
- Hot-Swapping des Moduls während der Laufzeit
- CCOTF des Moduls im Wartungsmodus, Seite 265. (CCOTF wird nicht im Sicherheitsmodus, Seite 264 unterstützt)

Verdrahtungsanschlüsse für BMXSRA0405

Einführung

Das digitale Relaisausgangsmodul BMXSRA0405 verfügt über 4 Relais und unterstützt bis zu 4 Ausgänge. Das Modul verfügt über ein Paar *a*- und ein Paar *b*-Stifte für jedes Relais. Folgendes gilt für alle Relais:

- Die zwei *a*-Stifte sind intern verbunden.

- Die zwei *b*-Stifte sind ebenfalls intern verbunden.

Klemmenleisten

Die folgenden 20-Punkt-Klemmenleisten von Schneider Electric können für den 20-Stift-Anschluss vorn am Modul genutzt werden:

- Schraubklemmenleiste BMXFTB2010
- Käfigfederzugklemmenleiste BMXFTB2000
- Federklemmenleiste BMXFTB2020

HINWEIS: Die Klemmenleisten können nur entfernt werden, wenn die Modulspannung abgeschaltet ist.

Prozessspannungsversorgung

Sie müssen die entsprechenden 24-VDC- oder 24-VAC-zu-230-VAC-Prozessspannungsversorgungen installieren.

Sicherung

Es ist eine schnell durchbrennende Sicherung (max. 6 A) erforderlich, die für die ausgewählte Anwendung und die Relaisbauweise geeignet ist. Installieren Sie immer eine externe Sicherung seriell mit der externen Spannungsversorgung, dem Relais und der Last.

⚠WARNUNG

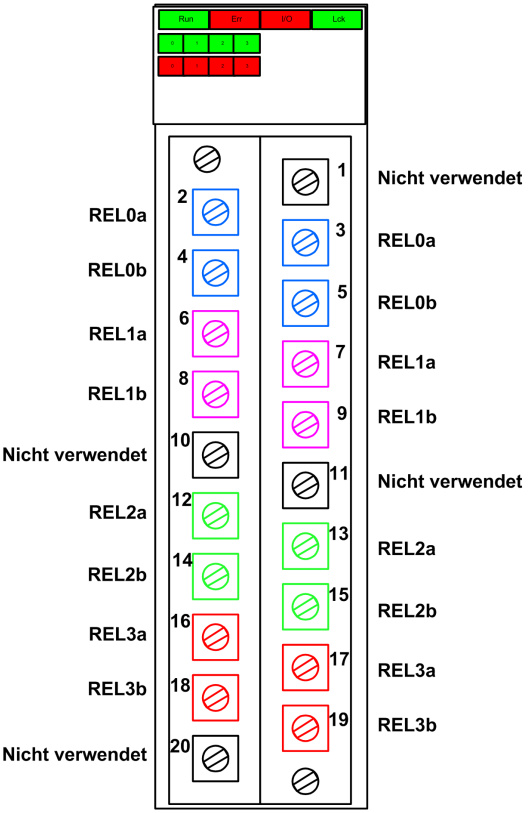
GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Es unterliegt Ihrer Verantwortung, eine ausreichende Verdrahtungsdiagnose einzusetzen, um Gefahren zu vermeiden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Verdrahtungsanschlüsse

Das folgende Beispiel zeigt die Stifte auf dem Relaismodul:



Zuweisung von Eingängen und Anschlussstiften

Es folgt eine Beschreibung der einzelnen Stifte des digitalen Relaisausgangsmoduls BMXSRA0405:

Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung
KEIN Kontakt, Relais 0a	2	1	Nicht verwendet
KEIN Kontakt, Relais 0b	4	3	KEIN Kontakt, Relais 0a
KEIN Kontakt, Relais 1a	6	5	KEIN Kontakt, Relais 0b
KEIN Kontakt, Relais 1b	8	7	KEIN Kontakt, Relais 1a
Nicht verwendet	10	9	KEIN Kontakt, Relais 1b

Stiftbeschreibung	Stiftnummer auf Klemmenleiste		Stiftbeschreibung
KEIN Kontakt, Relais 2a	12	11	Nicht verwendet
KEIN Kontakt, Relais 2b	14	13	KEIN Kontakt, Relais 2a
KEIN Kontakt, Relais 3a	16	15	KEIN Kontakt, Relais 2b
KEIN Kontakt, Relais 3b	18	17	KEIN Kontakt, Relais 3a
Nicht verwendet	20	19	KEIN Kontakt, Relais 3b

HINWEIS: Da die zwei *a*-Stifte der beiden Relais intern verbunden sind, müssen Sie für ein Relais nur einen *a*-Stift nutzen. Ebenfalls gilt: Da die zwei *b*-Stifte der beiden Relais intern verbunden sind, müssen Sie für ein Relais nur einen *b*-Stift nutzen.

BMXSRA0405 – Verdrahtungsbeispiele für Ausgangsanwendung

Einführung

Sie können das digitale Sicherheitsausgangsrelaismodul BMXSRA0405 auf verschiedene Weisen konfigurieren, um SIL2 Kategorie 2 (Cat2)/Performance Level c (PLc) oder SIL3 Cat4/PLe zu erreichen. Dies ist von folgenden Aspekten abhängig:

- Wie viele Ausgänge das Modul unterstützt
- Wie Sie die Fähigkeit des Moduls, das Stellglied in den gewünschten Anforderungszustand zu versetzen, testen möchten:
  - Automatisch vom Modul (in diesem Fall gibt es keinen Zustandsübergang für das Stellglied)
  - Über ein Verfahren, das den täglichen Übergang des Signals vom Modul zum Stellglied ausführt und überprüft (in diesem Fall wirkt sich der Übergang auf den Stellgliedzustand aus)

Konfigurieren Sie dies, indem Sie eine Anwendungsnummer auswählen (siehe Tabellen unten). Diese finden Sie in der Liste **Funktion** auf der Modulregisterkarte **Konfiguration** in Control Expert.

SIL2 Cat2/PLc – Anwendung und Verdrahtung:

Funktion	Anforderungs-zustand	Relais	Ausgän-ge	Signaltest?		Verdrahtungs-darstellung (s. u.)
				Automati-scher Signaltest?[1]	Täglicher Signalüber-gang?	
Anwendung_1	Deaktiviert	1	4	Nein	Ja	A
Anwendung_2	Deaktiviert	2	2	Ja	Nein	B
Anwendung_3	Erregt	1	4	Nein	Ja	A
Anwendung_4	Erregt	2	2	Ja	Nein	C
1. Der automatische Signaltest wirkt sich nicht auf den Stellgliedzustand aus.						

SIL3 Cat4/PLe – Anwendung und Verdrahtung:

Funktion	Anforderungs-zustand	Relais	Ausgän-ge	Signaltest?		Verdrahtungs-darstellung (s. u.)
				Automatischer Signaltest?[1]	Täglicher Signalüber-gang?	
Anwendung_5	Deaktiviert	2	2	Nein	Ja	A
Anwendung_6	Deaktiviert	4	1	Ja	Nein	D
Anwendung_7	Erregt	2	2	Nein	Ja	A
Anwendung_8	Erregt	2	2	Ja	Nein	C
1. Der automatische Signaltest wirkt sich nicht auf den Stellgliedzustand aus.						

Diese acht Anwendungsmöglichkeiten werden in den folgenden Verdrahtungsbeispielen erläutert.

Anwendung_1: 4 Ausgänge, SIL2/Cat2/PLc, deaktivierter Zustand, kein automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Deaktiviert“. Wenn das Modul einen internen Fehler eines Ausgangs erkennt, wird dieser Ausgang deaktiviert.

⚠VORSICHT
VERLUST DER FÄHIGKEIT, SICHERHEITSFUNKTIONEN AUSZUFÜHREN Um SIL2 gemäß IEC 61508 und Kategorie 2/Performance Level c gemäß ISO 13849 mit dieser Verdrahtung zu erreichen, müssen Sie einen täglichen Signalübergang vom erregten in den deaktivierten Zustand durchführen. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

Siehe Verdrahtung A, Seite 123 unten, wo die Verdrahtung für Anwendung_1 dargestellt wird.

Anwendung_2: 2 Ausgänge, SIL2 Cat2/PLc, deaktivierter Zustand, automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Deaktiviert“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais erkennt, werden beide Relais (Relais 0 und Relais 1 oder Relais 2 und Relais 3) für diesen Ausgang deaktiviert.

Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

Das Modul führt einen automatischen, regelmäßigen Impulstest für jedes Relais durch. Die Dauer des Tests beträgt weniger als 50 ms. Aufgrund der Konfiguration der zwei (parallel) verwendeten Relais hat der Test keine Auswirkungen auf die Ausgangslast (normalerweise *Erregt*). Sie können die Häufigkeit des Tests festlegen, indem Sie die **Überwachungsperiode** auf der Modulregisterkarte **Konfiguration** ändern. Gültige Testhäufigkeiten reichen von 1 bis 1440 Minuten.

Siehe Verdrahtung B, Seite 124 unten, wo die Verdrahtung für Anwendung_2 dargestellt wird.

Anwendung_3: 4 Ausgänge, SIL2/Cat2/PLc, erregter Zustand, kein automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Erregt“. Wenn das Modul einen internen Fehler eines Ausgangs erkennt, wird dieser Ausgang deaktiviert, um einen sicheren Zustand zu erreichen.

⚠VORSICHT
VERLUST DER FÄHIGKEIT, SICHERHEITSFUNKTIONEN AUSZUFÜHREN Um SIL2 gemäß IEC 61508 und Kategorie 2/Performance Level c gemäß ISO 13849 mit dieser Verdrahtung zu erreichen, müssen Sie einen täglichen Signalübergang vom erregten in den deaktivierten Zustand durchführen. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

Siehe Verdrahtung A, Seite 123 unten, wo die Verdrahtung für Anwendung_3 dargestellt wird.

Anwendung_4: 2 Ausgänge, SIL2 Cat2/PLc, erregter Zustand, automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Erregt“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais erkennt, werden beide Relais (Relais 0 und Relais 1 oder Relais 2 und Relais 3) für diesen Ausgang deaktiviert.

Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

Das Modul führt einen regelmäßigen Impulstest für jedes Relais durch. Die Dauer des Tests beträgt weniger als 50 ms. Aufgrund der Konfiguration der zwei (parallel) verwendeten Relais hat der Test keine Auswirkungen auf die Ausgangslast (normalerweise *Erregt*). Sie können die Häufigkeit des Tests festlegen, indem Sie die **Überwachungsperiode** auf der Modulregisterkarte **Konfiguration** ändern. Gültige Testhäufigkeiten reichen von 1 bis 1440 Minuten.

Siehe Verdrahtung C, Seite 125 unten, wo die Verdrahtung für Anwendung_4 dargestellt wird.

Anwendung_5: 2 Ausgänge, SIL3/Cat4/PLe, deaktivierter Zustand, kein automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Deaktiviert“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais erkennt, werden beide Relais (Relais 0 und Relais 1 oder Relais 2 und Relais 3) für diesen Ausgang deaktiviert.

Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

⚠VORSICHT

VERLUST DER FÄHIGKEIT, SICHERHEITSFUNKTIONEN AUSZUFÜHREN

Um SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 mit dieser Verdrahtung zu erreichen, müssen Sie einen täglichen Signalübergang vom erregten in den deaktivierten Zustand durchführen.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Siehe Verdrahtung C, Seite 125 unten, wo die Verdrahtung für Anwendung_5 dargestellt wird.

Anwendung_6: 1 Ausgang, SIL3/Cat4/PLe, deaktivierter Zustand, automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Deaktiviert“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais erkennt, werden alle Relais (Relais 0, Relais 1, Relais 2, Relais 3) für diesen Ausgang deaktiviert.

Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

Das Modul führt einen regelmäßigen Impulstest für jedes Relais durch. Die Dauer des Tests beträgt weniger als 50 ms. Aufgrund der Konfiguration der vier verwendeten Relais (2 Paare mit je zwei seriellen, parallel gesetzten Relais) hat der Test keine Auswirkungen auf die Ausgangslast (normalerweise *Erregt*). Sie können die Häufigkeit des Tests festlegen, indem Sie die **Überwachungsperiode** auf der Modulregisterkarte **Konfiguration** ändern. Gültige Testhäufigkeiten reichen von 1 bis 1440 Minuten.

Siehe Verdrahtung D, Seite 126 unten, wo die Verdrahtung für Anwendung_6 dargestellt wird.

Anwendung_7: 2 Ausgänge, SIL3/Cat4/PLe, erregter Zustand, kein automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Erregt“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais

erkennt, werden beide Relais (Relais 0 und Relais 1 oder Relais 2 und Relais 3) für diesen Ausgang deaktiviert.

Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

⚠VORSICHT

VERLUST DER FÄHIGKEIT, SICHERHEITSFUNKTIONEN AUSZUFÜHREN

Um SIL3 gemäß IEC 61508 und Kategorie 4/Performance Level e gemäß ISO 13849 mit dieser Verdrahtung zu erreichen, müssen Sie einen täglichen Signalübergang vom erregten in den deaktivierten Zustand durchführen.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Siehe Verdrahtung C, Seite 125 unten, wo die Verdrahtung für Anwendung_7 dargestellt wird.

Anwendung_8: 2 Ausgänge, SIL3 Cat4/PLe, erregter Zustand, automatischer Signaltest

Der Anforderungszustand für diese Anwendungsbauweise ist „Erregt“. Wenn das Modul einen internen Ausgangsfehler auf einem der für einen Ausgang verwendeten Relais erkennt, werden beide Relais (Relais 0 und Relais 1 oder Relais 2 und Relais 3) für diesen Ausgang deaktiviert.

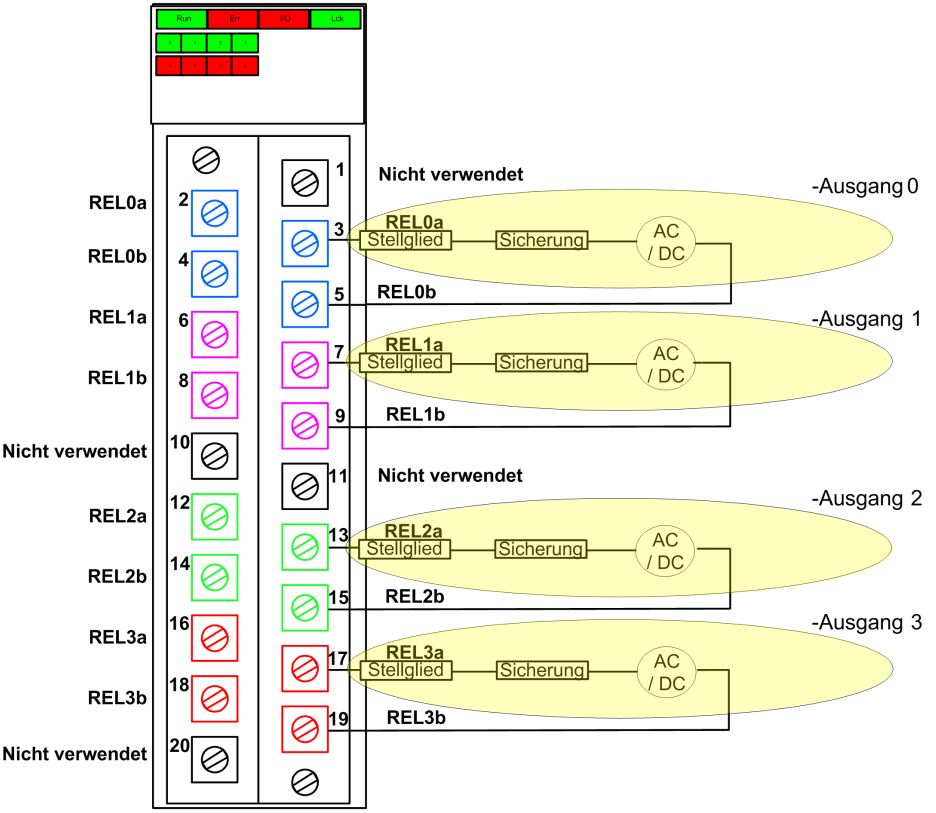
Ihr Anwendungsprogramm muss denselben Ausgangszustand an alle Relais kommunizieren, die dasselbe Stellglied aktivieren.

Das Modul führt einen regelmäßigen Impulstest für jedes Relais durch. Die Dauer des Tests beträgt weniger als 50 ms. Aufgrund der Konfiguration der zwei (seriell) verwendeten Relais hat der Test keine Auswirkungen auf die Ausgangslast (normalerweise *Deaktiviert*). Sie können die Häufigkeit des Tests festlegen, indem Sie die **Überwachungsperiode** auf der Modulregisterkarte **Konfiguration** ändern. Gültige Testhäufigkeiten reichen von 1 bis 1440 Minuten.

Siehe Verdrahtung C, Seite 125 unten, wo die Verdrahtung für Anwendung_8 dargestellt wird.

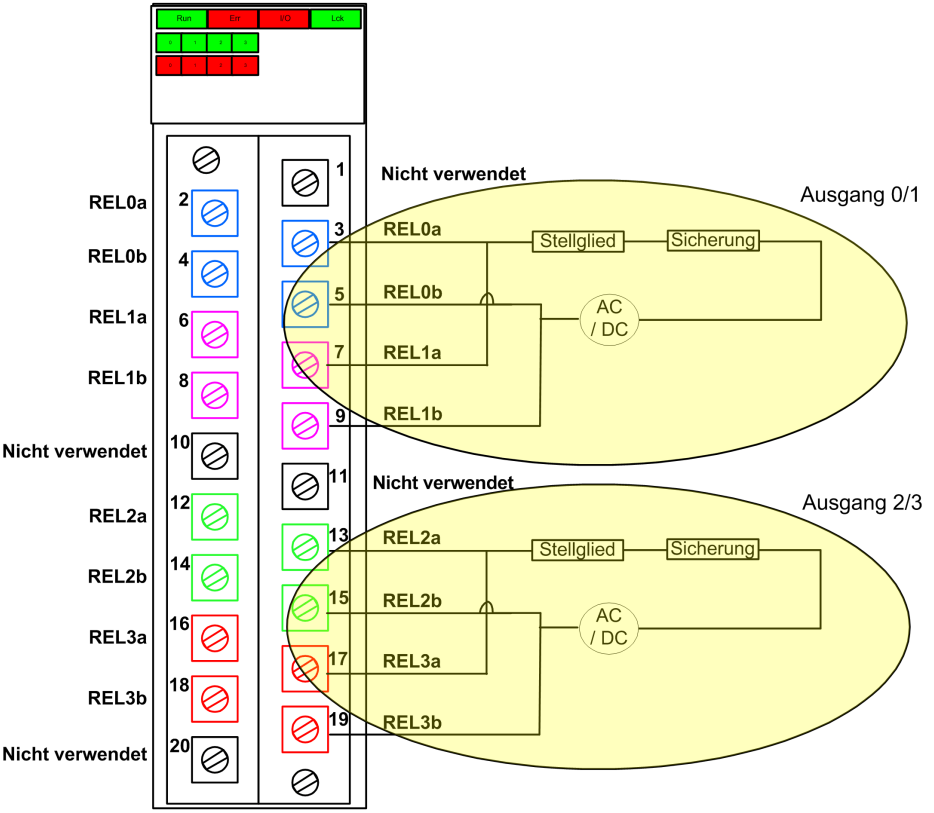
Verdrahtung A

Diese Verdrahtungsdarstellung bezieht sich auf Anwendung_1 und Anwendung_3:



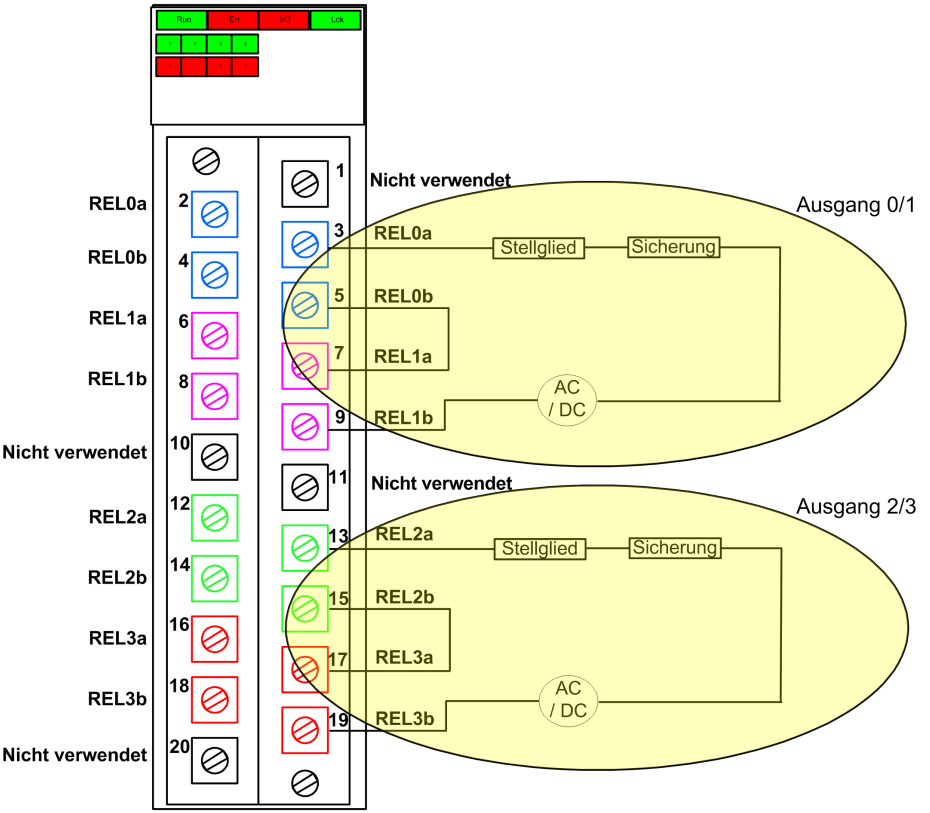
Verdrahtung B

Diese Verdrahtungsdarstellung bezieht sich auf Anwendung_2:



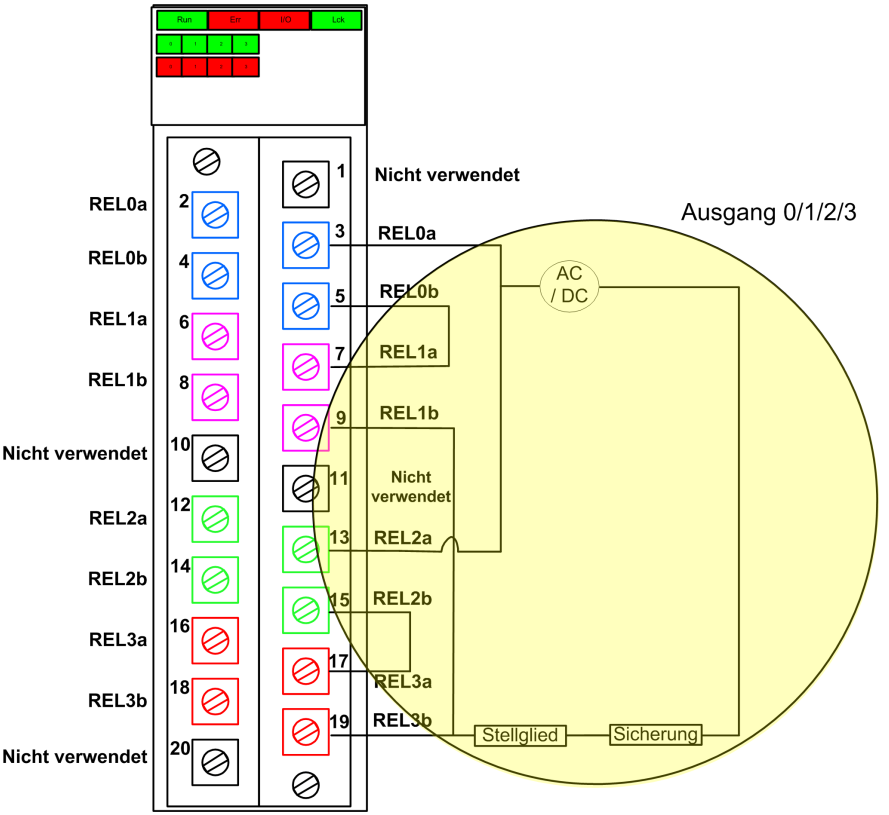
Verdrahtung C

Diese Verdrahtungsdarstellung bezieht sich auf Anwendung_4, Anwendung_5, Anwendung_7 und Anwendung_8:



Verdrahtung D

Diese Verdrahtungsdarstellung bezieht sich auf Anwendung_6:



BMXSRA0405 - Datenstruktur

Einführung

Der gerätespezifische abgeleitete Datentyp (Device Derived Data Type, DDDT) `T_U_DIS_SIS_OUT_4` ist die Schnittstelle zwischen dem Relaisausgangsmodul BMXSRA0405 und der Anwendung, die auf der CPU läuft. Der DDDT `T_U_DIS_SIS_OUT_4` umfasst die Datentypen `T_SAFE_COM_DBG_OUT` und `T_U_DIS_SIS_CH_ROUT`.

All diese Strukturen werden im Folgenden beschrieben.

DDDT-Struktur T_U_DIS_SIS_OUT_4

Die DDDT-Struktur T_U_DIS_SIS_OUT_4 umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
MOD_HEALTH[1]	BOOL	• 1: Das Modul funktioniert ordnungsgemäß. • 0: Das Modul funktioniert nicht ordnungsgemäß.	RO
SAFE_COM_STS[1]	BOOL	• 1: Die Modulkommunikation ist gültig. • 0: Die Modulkommunikation ist nicht gültig.	RO
CONF_LOCKED	BOOL	• 1: Die Modulkonfiguration ist gesperrt. • 0: Die Modulkonfiguration ist nicht gesperrt.	RO
APPLI	UINT	Relaisanwendungskonfiguration: 1, 2, 3, 4, 5, 6 oder 7	RO
TIME_PERIOD	UINT	Timer-Zeitraum für die automatische Relaisüberwachung (in Minuten)	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Debug-Struktur für sichere Kommunikation	RO
CH_OUT	ARRAY[0 bis 3] von T_U_DIS_SIS_CH_ROUT	Array der Kanalstruktur	–
S_TO	UINT	Sicherheitstimeout, der den Wechsel des Moduls in den Fehlerausweichzustand auslöst.	RO
MUID[2]	ARRAY[0 bis 3] von DWORD	Eindeutige Modul-ID (automatisch von Control Expert zugewiesen)	RO
RESERVED_1	ARRAY[0 bis 7] von INT	–	–
RESERVED_2	ARRAY[0 bis 6] von INT	–	–

1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. MOD_HEALTH und SAFE_COM_STS sind auf 0 gesetzt.

2. Dieser automatisch generierte Wert kann geändert werden, indem im Hauptmenü von Control Expert der Befehl **Generieren > IDs erneuern & Alles generieren** ausgeführt wird.

Struktur T_SAFE_COM_DBG_OUT

Die Struktur T_SAFE_COM_DBG_OUT umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
S_COM_EST	BOOL	• 1: Die Kommunikation mit dem Modul wurde hergestellt. • 0: Die Kommunikation mit dem Modul wurde nicht hergestellt oder ist fehlerhaft.	RO
M_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Das Modul wird mit dem NTP-Server synchronisiert. • 0: Das Modul wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CPU_NTP_SYNC	BOOL	Mit einer CPU-Firmware bis V3.10: • 1: Die CPU wird mit dem NTP-Server synchronisiert. • 0: Die CPU wird nicht mit dem NTP-Server synchronisiert. **HINWEIS:** Mit einer CPU-Firmware ab V3.20 ist der Wert stets 1.	RO
CHECKSUM	BYTE	Prüfsumme des Kommunikations-Frame	RO
COM_DELAY	UINT	Kommunikationsverzögerung zwischen zwei Werten, wie vom Modul erhalten: • 1 bis 65534: Die Zeit in ms, seitdem die CPU die letzte Kommunikation vom Modul empfangen hat. • 65535: Die CPU hat keine Kommunikation vom Modul empfangen.	RO
COM_TO	UINT	Timeout-Wert für die Kommunikation vom Modul	R/W
STS_MS_IN	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der vom Modul empfangenen Daten	RO
S_NTP_MS	UINT	Sicherer Zeitwert für einen Sekundenbruchteil (bis zur nächsten ms) für den aktuellen Zyklus	RO
STS_S_IN	UDINT	Sicherer Zeitstempelwert (in Sekunden) der vom Modul empfangenen Daten	RO
S_NTP_S	UDINT	Sicherer Zeitwert (in Sekunden) für den aktuellen Zyklus	RO
CRC_IN	UDINT	CRC-Wert für die vom Modul empfangenen Daten	RO

Element	Datentyp	Beschreibung	Zugriff
STS_MS_OUT	UINT	Sicherer Zeitstempelwert für einen Sekundenbruchteil (bis zur nächsten ms) der an das Modul gesendeten Daten	RO
STS_S_OUT	UDINT	Sicherer Zeitstempelwert (in Sekunden) der an das Modul gesendeten Daten	RO
CRC_OUT	UDINT	CRC-Wert für die an das Modul gesendeten Daten	RO

Struktur T_U_DIS_SIS_CH_ROUT

Die Struktur T_U_DIS_SIS_CH_ROUT umfasst die folgenden Elemente:

Element	Datentyp	Beschreibung	Zugriff
CH_HEALTH[1]	BOOL	• 1: Der Kanal ist funktionsfähig. • 0: Auf dem Kanal wurde ein Fehler entdeckt. Er ist nicht funktionsfähig. **Formel**: CH_HEALTH = not (IC) and SAFE_COM_STS and not (module in Fallback state)	RO
VALUE	EBOOL	Sicherer Befehl des Ausgabekanals: • 1: Befehl, den Ausgang zu schließen (erregt) • 0: Befehl, den Ausgang zu öffnen (deaktiviert)	R/W
TRUE_VALUE[2]	BOOL	Rücklesewert des Ausgangsrelaiskanals: • 1: Der Ausgang ist geschlossen (erregt). • 0: Der Ausgang ist offen (deaktiviert).	RO
IC	BOOL	• 1: Das Modul hat einen ungültigen Kanal erkannt. • 0: Der Kanal wird intern vom Modul als funktionsfähig erklärt.	RO
CH_FBC	BOOL	Konfiguration der Fehlerausweicheinstellung für die Kanäle: • 1: Benutzerdefinierter Wert • 0: Letzten Wert halten	RO

Element	Datentyp	Beschreibung	Zugriff
CH_FBST	BOOL	Konfiguration des Fehlerausweichzustands der Kanäle bei Auswahl von „Benutzerdefinierter Wert“: • 1: Erregt • 0: Entregt	RO
1. Wenn die SAFE-Task auf der CPU sich nicht im RUN-Modus befindet, werden die Daten, die zwischen CPU und Modul ausgetauscht werden, nicht aktualisiert. CH_HEALTH ist auf 0 gesetzt. 2. Das Element TRUE_VALUE kann von BMX CRA oder BME CRA mit einem Zeitstempel versehen werden.			

M580-Sicherheitsspannungsversorgungen

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die M580-Sicherheitsspannungsversorgungen beschrieben.

M580-Sicherheitsspannungsversorgungen

Einführung

Die folgenden Spannungsversorgungen können für den M580-Sicherheits-PAC verwendet werden:

- BMXCPS4002S – redundante 100-240-VAC-Sicherheitsspannungsversorgung
- BMXCPS4022S – redundante 24/48-VDC-Sicherheitsspannungsversorgung für Hochspannung
- BMXCPS3522S – redundante 125-VDC-Sicherheitsspannungsversorgung für Hochspannung

⚠WARNUNG

VERLUST DER FÄHIGKEIT ZUR AUSFÜHRUNG VON SICHERHEITSFUNKTIONEN

Nutzen Sie nur die Spannungsversorgung BMXCPS4002S, BMXCPS4022S oder BMXCPS3522S in Racks mit M580-Sicherheitsmodul. Überprüfen Sie Ihre physische Installation und Ihr Projekt in Control Expert, um sicherzustellen, dass nur M580-Sicherheitsspannungsversorgungsmodule eingesetzt werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Funktionalität der Spannungsversorgung

Jedes M580-Sicherheitsspannungsversorgungsmodul wandelt VDC- oder VAC-Spannung in zwei Ausgangsspannungen um (24 VDC und 3,3 VDC), wie im Folgenden beschrieben:

Funktionen	**Spannungsversorgung**		
	BMXCPS4002S	**BMXCPS4022S**	**BMXCPS3522S**
Hauptnetz für die Eingangsspannung	100...240 VAC, 50...60 Hz	24 bis 48 VDC	100 bis 150 VDC
Beschränkung der Ausgangsspannung für Bauträgergruppe	40 VDC	40 VDC	40 VDC

Funktionen	Spannungsversorgung		
	BMXCPS4002S	**BMXCPS4022S**	**BMXCPS3522S**
Umgebungstemperatur für Spannungsbeschränkung	-25 bis +60 °C	-25 bis +60 °C	-25 bis +60 °C
Verdrahtung mit	• Wechselstromnetz mit Nullleiterverbindung zur Masse ODER • Wechselstromnetz mit isoliertem Nullleiter und Widerstand gegen die Masse, mit AC-Nullleiter vom Benutzer verschweißt	Ein Gleichstromnetz mit 24 bis 48 VDC	Ein Gleichstromnetz mit 125 VDC

Jede Spannungsversorgung erkennt Überspannung, Überlast und Kurzschlüsse auf den 3,3-VDC- und 24-VDC-Baugruppenträgerleitungen.

Wenn der obere Schwellenwert von 40 VDC erkannt wird, geht das Modul wie folgt vor:

- Es wird ein Reset durchgeführt, sodass die Module, die von der Spannungsversorgung Spannung empfangen, neu initialisiert werden.
- Abhängig davon, wo der Schwellenwert erkannt wurde, gilt Folgendes:
  - Auf der 24-VDC-Baugruppenträgerleitung: Der PAC wird heruntergefahren.
  - Auf der 3,3-VDC-Baugruppenträgerleitung: Der PAC-Betrieb wird eingestellt, aber der PAC steht weiterhin unter Spannung.

Unter *Diagnose für die 24-VDC- und 3,3-VDC-Baugruppenträgerspannungen*, Seite 135 finden Sie Informationen dazu, wie Sie in diesen Fällen vorgehen.

Redundante Spannungsversorgungsmodule

BMXCPS4002S, BMXCPS4022S und BMXCPS3522S sind redundante Spannungsversorgungsmodule. In einem redundanten Ethernet-Rack können zwei dieser Module installiert werden – eines als Master, eines als Slave. Die möglichen Konfigurationen lauten wie folgt:

Konfiguration	Funktionen		
	Verwaltung der Redundanz (Leistungskontrolle und LED-Diagnose)	**Bereitstellung von Daten für die Anwendung**	**Überwachung und Speicherung der Spannungsversorgungsdaten**
2 Spannungsversorgungen im Hauptrack	✓	✓	✓
2 Spannungsversorgungen im Erweiterungsrack	✓	X	✓
1 Spannungsversorgung in einem Legacy-Rack	X	X	✓
✓ = Unterstützt X = Nicht unterstützt			

Weitere Informationen zu redundanten Spannungsversorgungen finden Sie in der *Beschreibung der Modicon X80-Spannungsversorgungsmodule* (siehe Modicon X80, Racks und Spannungsversorgungen, Hardware-Referenzhandbuch).

Diagnose des M580-Sicherheitsspannungsversorgungsmoduls

Diagnose für die 24-VDC- und 3,3-VDC-Baugruppenträgerspannungen

Die Sicherheitsspannungsversorgungen BMXCPS4002S, BMXCPS4022S und BMXCPS3522S verfügen über eine automatische Erkennung von Überspannung, Überlastung und Kurzschlüssen, die an den 24-VDC- oder 3,3-VDC-Baugruppenträgerspannungen auftreten können.

Wenn die Spannungsversorgung eines dieser Probleme an der 24-VDC-Spannung entdeckt, geschieht Folgendes:

- Die Leistungsumwandlungsfunktion wird für die gesamte Bauträgergruppe deaktiviert.
- Es wird für alle Module im Rack ein RESET-Befehl ausgegeben.
- Die LED **OK** der Spannungsversorgung wird ausgeschaltet.
- Der gesamte PAC wird ausgeschaltet.

Wenn die Spannungsversorgung eines dieser Probleme an der 3,3-VDC-Spannung entdeckt, geschieht Folgendes:

- Die Leistungsumwandlungsfunktion wird für die 3,3-VDC-Bauträgergruppe deaktiviert.
- Es wird für alle Module im Rack ein RESET-Befehl ausgegeben.
- Die LED **OK** der Spannungsversorgung wird ausgeschaltet.
- Der Betrieb des gesamten PAC-Programms wird angehalten. Einige PAC-Schaltkreise werden jedoch ggf. immer noch mit Spannung versorgt.

Führen Sie in beiden Fällen die folgenden Schritte aus, um das Problem zu beheben:

1. Schalten Sie die Primärstromquelle aus.
2. Überprüfen Sie die Kompatibilität des geschätzten Verbrauchs der PAC-Spannungsversorgung und die Kapazität des M580-Sicherheitsspannungsversorgungsmoduls in Bezug auf die 24-VDC- und 3,3-VDC-Baugruppenträgerleitungen.
3. Beheben Sie die Ursache des Problems.
4. Warten Sie nach dem Abschalten 1 Minute.
5. Schließen Sie die Primärquelle wieder an, um das M580-Sicherheitsspannungsversorgungsmodul neu zu starten.

Diagnose der Alarmrelaiskontakte

Die Sicherheitsspannungsversorgungen BMXCPS4002S, BMXCPS4022S und BMXCPS3522S verfügen über einen zweistiftigen Alarmrelaiskontakt, über den Sie die folgenden Informationen erfassen können:

- Das Relais ist aktiviert (d. h. geschlossen):
  - Die 24-VDC- und 3,3-VDC-Baugruppenträgerspannungen sind beide OK.
  - RESET ist nicht aktiv.
  - Wenn die Spannungsversorgung sich im lokalen Hauptrack befindet:

    - Die CPU ist funktionsfähig.

    - Die CPU befindet sich im RUN-Modus.
- Wenn das Relais deaktiviert ist (d. h. offen):
  - Eine oder beide der 24-VDC- und 3,3-VDC-Baugruppenträgerspannungen sind nicht OK.
  - RESET ist aktiv.
  - Wenn die Spannungsversorgung sich im lokalen Hauptrack befindet:

    - Die CPU ist nicht funktionsfähig.

    - Die CPU befindet sich im STOP-Modus.

M580-Sicherheits-DDTs

Einführung

Die M580-Sicherheitsspannungsversorgungsmodule verfügen über zwei Sätze abgeleiteter Datentypen (Derived Data Types (DDT):

- PWS_DIAG_DDT_V2 für die Diagnose
- PWS_CMD_DDT für Befehle

PWS_DIAG_DDT_V 2

Byte-Offset	Name	Typ: '-00006-78911-0').	Kommentar
0	Reserviert	BYTE	–
1	Reserviert	BYTE	–
2	PwsMajorVersion	BYTE	Spannungsversorgung, große Firmwareversion
3	PwsMinorVersion	BYTE	Spannungsversorgung, kleine Firmwareversion
4	Modell	BYTE	Modellkennung Modellkennung: • BMXCPS4002S = 01 • BMXCPS4022S = 02 • BMXCPS3522S = 03
5	Status	BYTE	Zustand der Spannungsversorgung
6	I33BacPos	UINT	Strommessung auf 3,3-VDC-Baugruppenträgerleitung in nomineller Rolle (Hersteller)
8	V33Buck	UINT	Spannungsmessung auf 3,3-VDC-Abwärtsregler
10	I24Bac	UINT	Strommessung auf 24-VDC-Baugruppenträgerleitung
12	V24Int	UINT	Spannungsmessung auf 24 VDC Int.
14	Temperatur	INT	Messung der Umgebungstemperatur
16	OperTimeMasterSincePO	UDINT	Betriebszeit als Master seit letztem Einschalten
20	OperTimeSlaveSincePO	UDINT	Betriebszeit als Slave seit letztem Einschalten

Byte-Offset	Name	Typ: '-00006-78911-0').	Kommentar
24	OperTimeMaster	UDINT	Betriebszeit als Master seit Herstellung
28	OperTimeSlave	UDINT	Betriebszeit als Slave seit Herstellung
32	Work	UDINT	Durchgeführte Arbeit seit Herstellung
36	RemainingLTPC	UINT	Verbleibende Lebenszeit in Prozent
38	NbPowerOn	UINT	Anzahl der Einschaltvorgänge seit Herstellung
40	NbVoltageLowFail	UINT	Anzahl der Fehler auf Primärspannung durch Erreichen des unteren Schwellenwerts
42	NbVoltageHighFail	UINT	Anzahl der Fehler auf Primärspannung durch Erreichen des oberen Schwellenwerts
44	Reserviert	UDINT	–
48	Reserviert	UDINT	–
52	RemainingLTMO	UINT	Verbleibende Lebenszeit in Monaten
54	Reserviert	BYTE	–
63	Reserviert	BYTE	–

PWS_CMD_DDT

Byte-Offset	Name	Typ: '-00006789-110').	Kommentar
0	Reserviert	BYTE	–
1	Code	BYTE	Befehlscode: • 1 = Austauschen • 3 = Zurücksetzen
2	PwsTarget	BYTE	Spannungsversorgungsziel: 1 für links, 2 für rechts, 3 für beide Spannungsversorgungsziel: • 1 = Links • 2 = Rechts
3	Reserviert	BYTE	–
15	Reserviert	BYTE	–

Prüfung eines M580-Sicherheitssystems

Inhalt dieses Kapitels

Einführung

In diesem Kapitel wird erläutert, mit welchen Berechnungen Sie Ihr M580-Sicherheitssystem überprüfen können.

Architekturen des M580-Sicherheitsmoduls

Einführung

In diesem Abschnitt werden die internen Architekturen der Sicherheitsmodule erläutert.

Architektur von M580-Sicherheits-CPU und -Koprozessor

Einführung

Die CPUs BME•58•040S und der Koprozessor BMEP58CPROS3 agieren als Prozessorpaar und sind von der TÜV Rheinland Group für die Verwendung in M580-Sicherheitslösungen gemäß Sicherheitsintegritäts-Level 3 (SIL3) zertifiziert.

Gemeinsam stellen CPU und Koprozessor die folgenden SIL3-Sicherheitsfunktionen bereit:

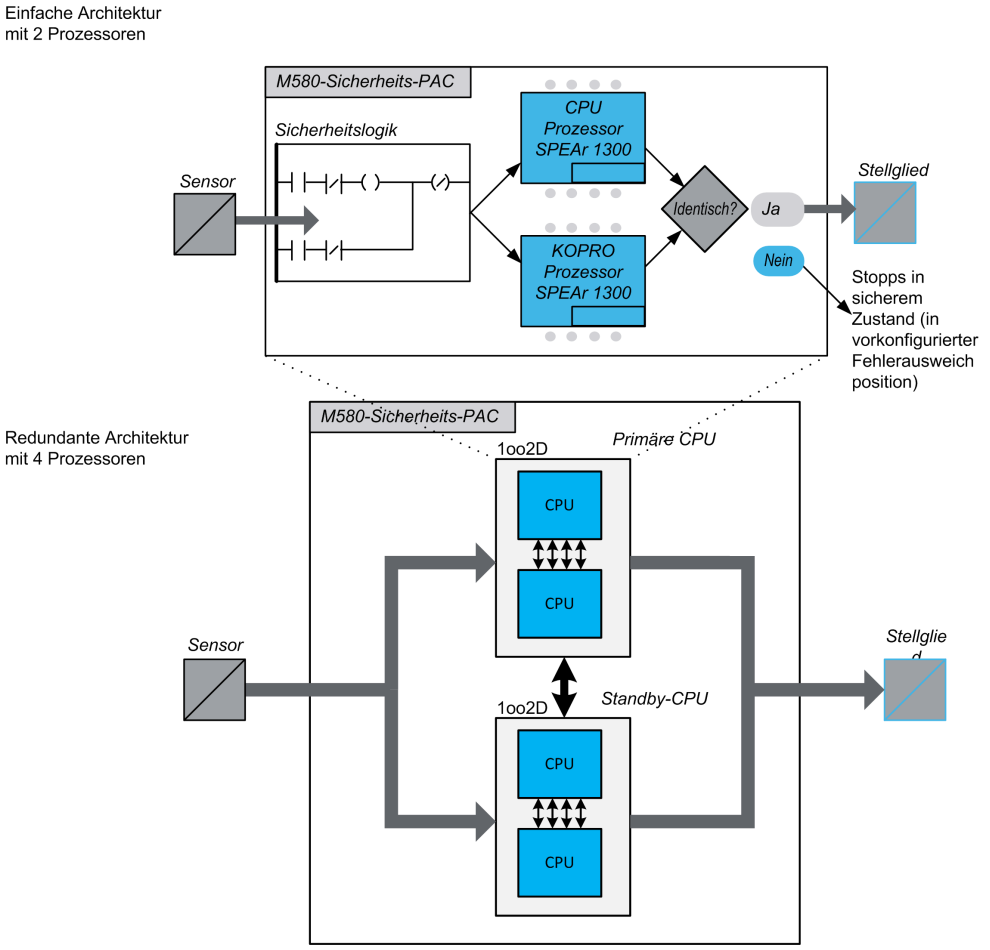
- Unabhängige, doppelte Ausführung des Sicherheitstask-Codes
- Vergleich der Ergebnisse der doppelten Codeausführung
- Regelmäßige Selbsttests
- Unterstützung einer a 1oo2D-Architektur („one out of two“) mit Diagnose

HINWEIS: Zusätzlich zur Sicherheitsfunktion stellen die CPUs BMEP58•040S vergleichbare Funktionen wie äquivalente nicht-sicherheitsorientierte Standalone-M580-CPUs und die CPUs BMEH58•040S vergleichbare Funktionen wie äquivalente nicht-sicherheitsorientierte Hot Standby-M580-CPUs bereit. In den folgenden zwei Handbüchern finden Sie Informationen zu den nicht-sicherheitsorientierten Funktionen dieser Sicherheits-CPUs: *Modicon M580 – Hardware, Referenzhandbuch* und *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen*.

Beschreibung der internen CPU- und Koprozessor-Architektur

Die Sicherheits-CPU und der Koprozessor für M580 umfassen jeweils einen Prozessor vom Typ SPEAr 1300. Jeder Prozessor führt die Sicherheitslogik in seinem eigenen Speicherbereich aus und vergleicht die Ergebnisse der Ausführung am Ende der Sicherheitstask.

Die folgende Abbildung zeigt die interne Architektur der M580-Sicherheits-CPU in einer einfachen und einer redundanten Konfiguration:



Doppelte Codeerstellung und -ausführung

Die zwei Prozessoren im M580-Sicherheits-PAC sorgen für eine doppelte Erstellung und Ausführung des Codes. Dies bietet die folgenden Vorteile hinsichtlich der Fehlererkennung:

- Es werden unabhängig voneinander zwei ausführbare Codeprogramme generiert. Die Verwendung zweier unabhängiger Code-Compiler hilft bei der Erkennung systematischer Fehler bei der Codeerstellung.

- Die zwei generierten Codeprogramme werden von zwei separaten Prozessoren ausgeführt. Daher kann die CPU sowohl systematische Fehler bei der Codeausführung als auch zufällige Fehler im PAC erkennen.
- Beide Prozessoren nutzen einen eigenen, unabhängigen Speicherbereich. Daher kann der PAC zufällige Fehler im RAM erkennen, sodass nicht bei jedem Zyklus ein vollständiger RAM-Test erforderlich ist.

1oo2D-Architektur

In einer 1oo2D-Architektur („one out of two with Diagnostic“) mit Diagnose führen zwei unabhängige Kanäle die Sicherheitslogik aus. Bei Auftreten eines Fehler in einem Kanal wechselt das System in den sicheren Zustand.

Einfache Architektur

Die einfache Architektur mit M580-Sicherheits-PACs basiert auf einer 1oo2D-Architektur mit zwei Prozessoren, die selbst in einer nicht-redundanten Konfiguration Konformität mit dem Sicherheitsintegritäts-Level SIL3 gewährleistet.

Redundante Architektur

Die redundante Architektur mit M580-Sicherheits-PACs bietet maximale Systemverfügbarkeit und Prozesszeit dank kompletter Redundanz (Vierfach-Struktur, d. h. vier CPUs) für Steuerung, Spannungsversorgung und Kommunikation.

Eine der CPUs (Prozessorpaar) agiert als primäre CPU und unterstützt die Anwendung durch Ausführung der Programmlogik und Steuerung der E/A. Die primäre CPU (Prozessorpaar) aktualisiert die sekundäre CPU (Prozessorpaar), sodass diese stets bereit ist, die E/A-Steuerung zu übernehmen.

Das System überwacht sich selbst kontinuierlich. Sollte die Steuerung durch die primäre CPU ausfallen, schaltet das System zur sekundären CPU um. In diesem eingeschränkten Modus behält das System das SIL3-Status. Wenn sowohl die primäre als auch die sekundäre CPU ausfällt, geht das System in den Fail-Safe-Modus über.

Mit der redundanten M580-Sicherheits-PAC-Architektur, d. h. einer Vierfach-Architektur (4 Prozessoren) lassen sich Systemverfügbarkeit und Konformität mit dem Sicherheitsintegritäts-Level SIL3 verbessern.

Watchdog

Ein Hardware- und ein Firmware-Watchdog überprüfen die PAC-Aktivität und die Zeit, die erforderlich ist, um die Sicherheitsprogrammlogik auszuführen.

HINWEIS: Konfigurieren Sie den Software-Watchdog (im Dialogfeld **Eigenschaften der SAFE-Task**) für die folgenden Elemente:

- Ausführungszeit der Anwendung
- Filterung erkannter E/A-Kommunikationsfehler
- Prozesssicherheitsdauer

Weitere Informationen erhalten Sie unter *Prozesssicherheitsdauer*, Seite 156.

Speicherprüfung

Die Integrität des statischen Speichers wird über eine zyklische Redundanzprüfung (Cyclic Redundancy Check, CRC) und die doppelte Codeausführung getestet. Die Integrität des Inhalts des dynamischen Speichers wird durch die doppelte Codeausführung, einen regelmäßigen Speichertest und einen ECC-Mechanismus (Error Correcting Code, Fehlerkorrekturcode) getestet, mit dem die häufigsten Instanzen beschädigter interner Daten erkannt und korrigiert werden. Bei einem Kaltstart werden diese Tests neu initialisiert und komplett ausgeführt, bevor die CPU in den STOP- oder RUN-Betrieb wechselt.

Überwachung der Überspannung

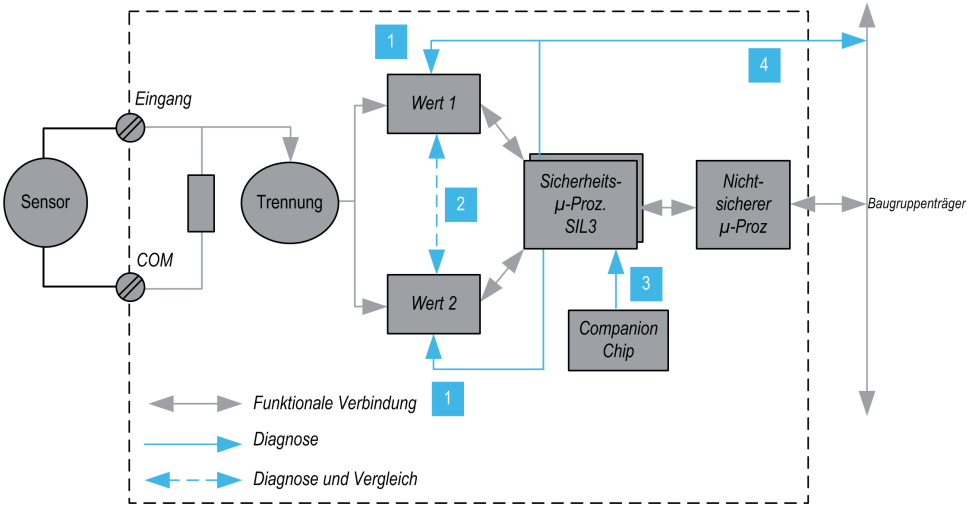
Die CPU empfängt ihre Spannung über die Baugruppenträgerleitung von ihrem dedizierten M580-Sicherheitsspannungsversorgungsmodul. Das Spannungsversorgungsmodul stellt regulierte 24 VDC mit einer absoluten Höchstspannung im Bereich 0 bis 36 VDC bereit.

Integriert in die CPU ist eine Funktion zur Überprüfung der internen Spannungsversorgungen. Wenn eine Unter- oder Überspannung erkannt wird, wird der PAC heruntergefahren.

Sicherheitsarchitektur für das analoge Eingangsmodul BMXSAI0410

Architektur mit Sicherheitsfunktionen

Die interne Architektur des Moduls BMXSAI0410 führt seine Sicherheitsfunktionen wie folgt aus:



1 Die Messgeräte werden regelmäßig überwacht, um sicherzustellen, dass sie ohne erkannten Fehler zehn analoge Werte zwischen 4 und 20 mA erfassen. Gleichzeitig wird die Linearität der Messphasen überprüft.

2 Jeder Eingangswert wird von zwei identischen Schaltkreisen erfasst. Die Messwerte werden vom Sicherheitsprozessor verglichen. Wenn sich die Werte unterscheiden, wird dieser Kanal als nicht gültig betrachtet. Zwischen den beiden Werten darf eine maximale Diskrepanz von 0,35 % bestehen.

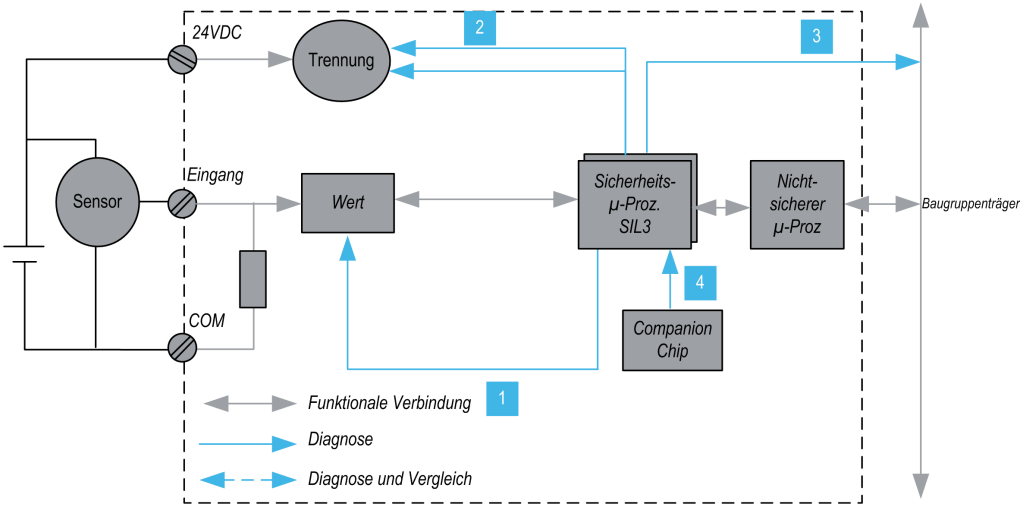
3 Der Companion Chip versorgt den Sicherheitsprozessor, diagnostiziert ihn ständig und überwacht die Baugruppenträgerspannung.

4 Die Versorgungsspannung des Baugruppenträgers wird überwacht, um Unter- oder Überspannung zu entdecken.

Sicherheitsarchitektur für das digitale Eingangsmodul BMXSDI1602

Architektur mit Sicherheitsfunktionen

Die interne Architektur des Moduls BMXSDI1602 führt die Sicherheitsfunktionen wie folgt aus:



1 Die Messgeräte werden ständig überwacht, um sicherzustellen, dass sie 1 und 0 messen können.

2 Die externe 24-VDC-Spannungsversorgung wird ständig vom Sicherheitsprozessor überwacht. Jeder Eingangswert wird von zwei identischen Schaltkreisen erfasst. Die Werte werden vom Sicherheitsprozessor verglichen. Wenn sich die Werte unterscheiden, wird dieser Kanal als nicht gültig betrachtet.

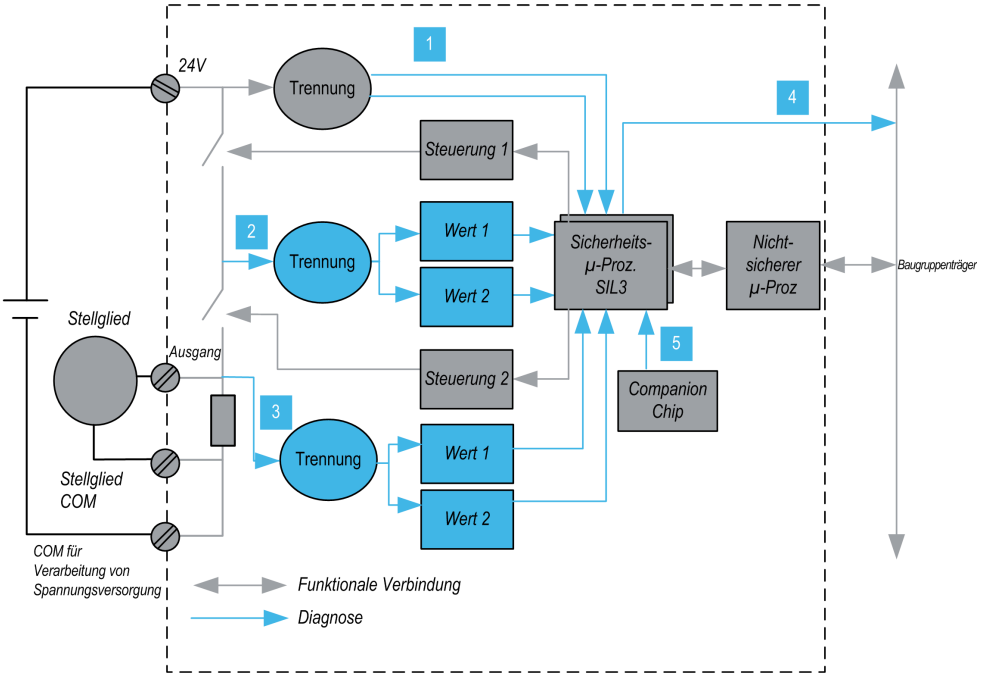
3 Die Versorgungsspannung des Baugruppenträgers wird überwacht, um Unter- oder Überspannung zu entdecken.

4 Der Companion Chip versorgt den Sicherheitsprozessor, diagnostiziert ihn ständig und überwacht die Baugruppenträgerspannung.

Sicherheitsarchitektur für das digitale Ausgangsmodul BMXSDO0802

Architektur mit Sicherheitsfunktionen

Die interne Architektur des Moduls BMXSDO0802 führt die Sicherheitsfunktionen wie folgt aus:



1 Die externe 24-VDC-Spannungsversorgung wird ständig vom Sicherheitsprozessor überwacht.

2 Jeder Ausgang besteht aus zwei seriellen Switches zwischen der externen 24-VDC-Spannungsversorgung und der Masse. Der Mittelpunktwert (2) wird redundant gelesen und an den Sicherheitsprozessor gesendet. Die Mittelpunktmesswerte werden vom Sicherheitsprozessor verglichen. Wenn sich die Werte von den erwarteten Werten unterscheiden, wird dieser Kanal als nicht gültig betrachtet.

3 Der Tiefpunktwert (3) wird ebenfalls überwacht, um eine externe Verdrahtungsdiagnose durchzuführen.

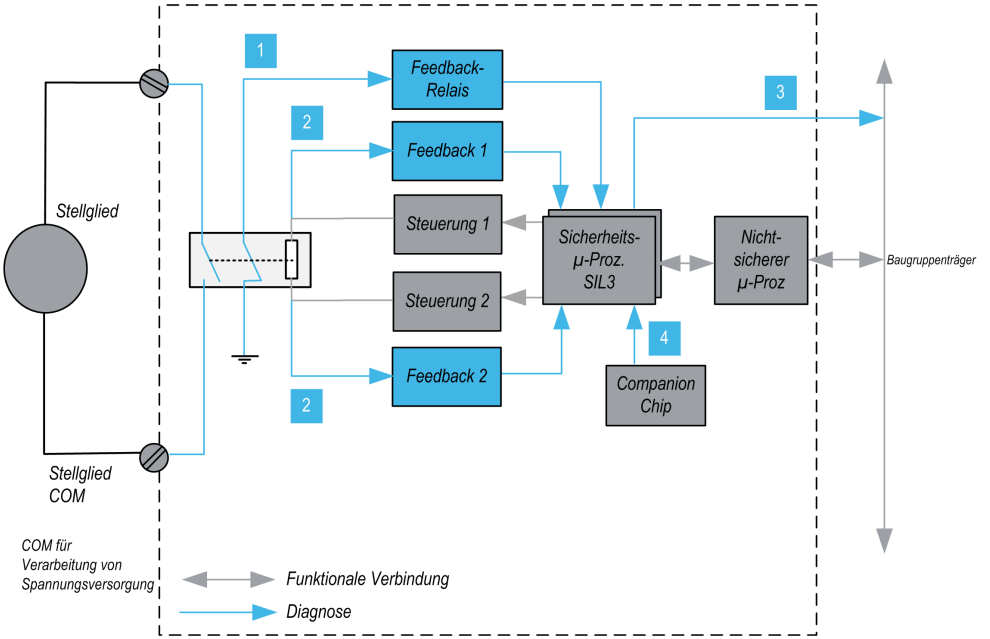
4 Die Versorgungsspannung des Baugruppenträgers wird überwacht, um Unter- oder Überspannung zu entdecken.

5 Der Companion Chip versorgt den Sicherheitsprozessor, diagnostiziert ihn ständig und überwacht die Baugruppenträgerspannung.

Sicherheitsarchitektur für das digitale Relaisausgangsmodul BMXSRA0405

Architektur mit Sicherheitsfunktionen

Die interne Architektur des Moduls BMXSRA0405 führt die Sicherheitsfunktionen wie folgt aus:



1 Der Zustand des Relais wird ständig vom Sicherheitsprozessor überwacht. Er liest den Zustand eines NC-Kontakts, der mechanisch mit dem NO-Kontakt verbunden ist, der wiederum mit dem Stellglied verbunden ist.

2 Der Zustand des Relaisbefehls wird ständig überwacht. Jeder Eingangswert wird von zwei identischen Schaltkreisen empfangen. Die Messwerte werden vom Sicherheitsprozessor verglichen. Wenn sich die Werte unterscheiden, wird dieser Kanal als nicht gültig betrachtet.

3 Die Versorgungsspannung des Baugruppenträgers wird überwacht, um Unter- oder Überspannung zu entdecken.

4 Der Companion Chip versorgt den Sicherheitsprozessor, diagnostiziert ihn ständig und überwacht die Baugruppenträgerspannung.

SIL- und MTTF-Werte des M580-Sicherheitsmoduls

Einführung

In diesem Abschnitt werden die SIL- und MTTF-Werte erläutert, die Sie für die Berechnungen Ihres M580-Sicherheitsmoduls nutzen können.

Berechnung des Sicherheitsintegritäts-Levels

Klassifizierung der Produkte von Schneider Electric

Der M580-Sicherheits-PAC kann aus Folgendem bestehen:

- Sicherheitsmodule, die Sicherheitsfunktionen ausführen können, u. a.:
  - CPU und Koprozessor
  - E/A-Module
  - Spannungsversorgung
- Nicht-störende Module, Seite 29, die keine Sicherheitsfunktionen ausführen, Ihnen aber die Möglichkeit geben, Ihrem Sicherheitsprojekt nicht-sichere Elemente hinzuzufügen.

  HINWEIS:

  - Da nicht-störende Module nicht Teil der Sicherheitsschleife sind, werden sie auch nicht bei der Berechnung des Sicherheitsintegritäts-Levels berücksichtigt.
  - Ein Fehler in einem nicht-störenden Modul wirkt sich nicht negativ auf die Ausführung der Sicherheitsfunktionen aus.
  - Die Spannungsversorgungen BMXCPS4002S, BMXCPS4022S und BMXCPS3522S sind zertifiziert. Da sie eine vernachlässigbare Rate gefährlicher Fehler haben (< 1 % des SIL3-Ziels), wird die Spannungsversorgung nicht für die Berechnung von Sicherheitsintegritäts-Level und Sicherheitsschleife berücksichtigt. Als Folge daraus werden für die Spannungsversorgungsmodule die PFH- und PFD-Werte nicht bereitgestellt.

PFD/PFH-Werte für M580-Sicherheitsmodule

Schneider Electric bietet folgende Sicherheitsmodule an, die für den Einsatz in Sicherheitsanwendungen zertifiziert sind. Die Sicherheitsmodule werden mit den entsprechenden Werten für Ausfallwahrscheinlichkeiten, Seite 152 (PFD/PFH) für verschiedene Prüfabstände, Seite 155 (PTI) aufgeführt. Diese PFD/PFH-Werte tragen zur globalen PFD/PFH der gesamten Sicherheitsschleife, Seite 17 bei.

Die nachstehenden Tabellen zeigen die Sicherheitsmodule mit den entsprechenden PDF/PFH-Werten für SIL2- und SIL3-Anwendungen, wo anwendbar:

Produkttyp	**Produktreferenz**	**SIL**	**PTI = 1 Jahr**	
			PFD_G	**PFH_G**
CPU und Koprozessor	BME•58•040S & BMEP58CPROS3	SIL3[1]	4.38E-07	1.00E-10
Analogeingang	BMXSAI0410	SIL3[2]	5.76E-06	1.31E-09
Digitaleingang	BMXSDI1602	SIL3[2]	6.81E-06	1.56E-09
Digitalausgang	BMXSDO0802	SIL3[1]	5.75E-06	1.31E-09
Digitales Relaisausgangsmodul	BMXSRA0405	SIL2 [3]	5.85E-06	1.68E-09
		SIL3[4]	5.84E-06	1.34E-09
		SIL3[5]	–	1.35E-09
Spannungsversorgung	BMXCPS4002S, BMXCPS4022S und BMXCPS3522S	SIL3	–	–

1. 1 Ausgang bei 80 °C
2. 1 Eingang bei 80 °C
3. 1 Relais pro Ausgang bei 80 °C
4. 2 Relais pro Ausgang bei 80 °C
5. 4 Relais pro Ausgang bei 80 °C

Produkttyp	**Produktreferenz**	**SIL**	**PTI = 5 Jahre**	
			PFD_G	**PFH_G**
CPU und Koprozessor	BME•58•040S und BMEP58CPROS3	SIL3[1]	2.20E-06	1.01E-10
Analogeingang	BMXSAI0410	SIL3[2]	2.88E-05	1.31E-09
Digitaleingang	BMXSDI1602	SIL3[2]	3.41E-05	1.56E-09
Digitalausgang	BMXSDO0802	SIL3[1]	2.88E-05	1.31E-09
Digitales Relaisausgangsmodul	BMXSRA0405	SIL2[3]	2.92E-05	1.68E-09
		SIL3[4]	2.92E-05	1.34E-09
		SIL3[5]	–	1.35E-09

Produkttyp	Produktreferenz	SIL	PTI = 5 Jahre	
			PFD_G	PFH_G
Spannungsversorgung	BMXCPS4002S, BMXCPS4022S und BMXCPS3522S	SIL3	–	–
1. 1 Ausgang bei 80 °C 2. 1 Eingang bei 80 °C 3. 1 Relais pro Ausgang bei 80 °C 4. 2 Relais pro Ausgang bei 80 °C 5. 4 Relais pro Ausgang bei 80 °C				

Produkttyp	Produktreferenz	SIL	PTI = 10 Jahre	
			PFD_G	PFH_G
CPU und Koprozessor	BME•58•040S und BMEP58CPROS3	SIL3[1]	4.44E-06	1.02E-10
Analogeingang	BMXSAI0410	SIL3[2]	5.76E-05	1.31E-09
Digitaleingang	BMXSDI1602	SIL3[2]	6.81E-05	1.56E-09
Digitalausgang	BMXSDO0802	SIL3[1]	5.75E-05	1.31E-09
Digitales Relaisausgangsmodul	BMXSRA0405	SIL2[3]	5.84E-05	1.68E-09
		SIL3[4]	5.84E-05	1.34E-09
		SIL3[5]	–	1.35E-09
Spannungsversorgung	BMXCPS4002S, BMXCPS4022S und BMXCPS3522S	SIL3	–	–
1. 1 Ausgang bei 80 °C 2. 1 Eingang bei 80 °C 3. 1 Relais pro Ausgang bei 80 °C 4. 2 Relais pro Ausgang bei 80 °C 5. 4 Relais pro Ausgang bei 80 °C				

Produkttyp	Produktreferenz	SIL	PTI = 20 Jahre	
			PFD_G	PFH_G
CPU und Koprozessor	BME•58•040S und BMEP58CPROS3	SIL3[1]	9.00E-06	1.04E-10
Analogeingang	BMXSAI0410	SIL3[2]	1.15E-04	1.31E-09
Digitaleingang	BMXSDI1602	SIL3[2]	1.36E-04	1.56E-09

Produkttyp	Produktreferenz	SIL	PTI = 20 Jahre	
			PFD_G	PFH_G
Digitalausgang	BMXSDO0802	SIL3[1]	1.15E-04	1.31E-09
Digitales Relaisausgangsmodul	BMXSRA0405	SIL2[3]	1.17E-04	1.68E-09
		SIL3[4]	1.17E-04	1.34E-09
		SIL3[5]	–	1.35E-09
Spannungsversorgung	BMXCPS4002S, BMXCPS4022S und BMXCPS3522S	SIL3	–	–

1. 1 Ausgang bei 80 °C
2. 1 Eingang bei 80 °C
3. 1 Relais pro Ausgang bei 80 °C
4. 2 Relais pro Ausgang bei 80 °C
5. 4 Relais pro Ausgang bei 80 °C

Ausfallwahrscheinlichkeit von SIL3-Anwendungen

Für SIL3-Anwendungen definiert die Norm IEC 61508 die folgenden Ausfallwahrscheinlichkeiten bei Anforderung (PFD) und Ausfallwahrscheinlichkeiten pro Stunde (PFH) für jede Sicherheitsschleife, abhängig vom Betriebsmodus:

- PFD ≥ 10^{-4} bis < 10^{-3} für einen Betriebsmodus mit niedrigem Anforderungsniveau
- PFH ≥ 10^{-8} bis < 10^{-7} für einen Betriebsmodus mit hohem Anforderungsniveau

Die M580-Sicherheitssteuerung ist für die Verwendung in Systemen mit niedrigem und hohem Anforderungsniveau zertifiziert.

Beispielberechnung des Sicherheitsintegritäts-Levels

Diese Beispielberechnung zeigt Ihnen, wie Sie Folgendes festlegen:

- Den Risikobeitrag der Sicherheitsmodule von Schneider Electric zu Ihrer Sicherheitsanwendung
- Das verbleibende Risiko der anderen Geräte in der Sicherheitsschleife (z. B. Sensoren und Aktoren), das für Ihre Sicherheitsanwendung, ein bestimmtes Sicherheitsintegritäts-Level und einen Betriebsmodus eine Rolle spielt.

  HINWEIS: Wenn Sie den Risikobeitrag der Sensoren und Aktoren zu Ihrer Sicherheitsanwendung berechnen möchten, wenden Sie sich an die Hersteller dieser Geräte, um die PFD/PFH-Werte für den entsprechenden Prüfabstand zu erhalten.

Die folgenden Sicherheitsmodule von Schneider Electric sind Teil dieser Beispielberechnung:

- 1: CPU BMEP584040S
- 1: Koprozessor BMEP58CPROS3
- 1: Analogeingang BMXSAI0410
- 1: Digitalausgang BMXSDO0802
- 1: Spannungsversorgung BMXCPS4002S

Für die folgende Berechnung werden PFH_G-Werte für einen Betriebsmodus mit hohem Anforderungsniveau für eine SIL3-Sicherheitsschleife mit einem PTI von 20 Jahren angewendet. Der maximal zulässige PFH-Wert für diese Sicherheitsanwendung beträgt 10^{-7} (oder 1.0E-7):

Sicherheitsmodul		**Beitrag (wissenschaftliche Schreibweise)**	**Verbleibender Beitrag für Sensoren und Aktoren**
CPU und Koprozessor		7.01E-10	–
Analogeingang		1.31E-09	
Digitalausgang		1.31E-09	
Spannungsversorgung		–	
Gesamt	Numerisch	**2.72E-09**	**97.28E-09**
	% max.	**2,72 %**	**97,28 %**
Hinweis 1: Der Relaisausgang verwendet vier Relais, um einen Ausgang zu unterstützen.			

Werte für das M580-Sicherheitsmodul für Maschinen

Schneider Electric stellt die folgenden Sicherheitsmodule zur Verfügung, die gemäß dem ISO13849-1-Standard für die Verwendung in Sicherheitsmaschinenanwendungen zertifiziert sind. In der folgenden Tabelle werden die Sicherheitsmodule und, wo zutreffend, ihre Werte, Kategorien und Performance Level aufgeführt.

Produkttyp	**Produktreferenz**	**Konfiguration**	**Kategorie**	**Performance Level**	**MTTF (Jahre)**	**DCav**
CPU und Koprozessor	BME•58•040S & BMEP58CPROS3	Ohne Bedeutung	4	e	235	Hoch (> 99 %)
Analogeingang	BMXSAI0410	mit 1 Kanal	2	d	255	99,66 %
		mit 2 Kanälen	4	e	255	99,66 %
Digitaleingang	BMXSDI1602	mit 1 Kanal	2	d	231	99,69 %
		mit 2 Kanälen	4	e	231	99,69 %

Produkttyp	Produktreferenz	Konfiguration	Kategorie	Performance Level	MTTF (Jahre)	DCav
Digitalausgang	BMXSDO0802	Ohne Bedeutung	4	e	253	99,63 %
Digitales Relaisausgangsmodul	BMXSRA0405	mit 1 Kanal	2	c	156	99,77 %
		mit 2 Kanälen	4	e	156	99,77 %

Werte für M580-Sicherheitsmodule für die Bahn

Schneider Electric bietet die folgenden zertifizierten Sicherheitsmodule für den Schienenverkehrssektor gemäß den Cenelec-Normen EN50126, EN50128, EN50129. In der nachstehenden Tabelle werden die Sicherheitsmodule und ihre Zuverlässigkeitswerte aufgeführt:

Produkttyp	Produktreferenz	SIL	TFFR (PTI = 20 Jahre)
CPU und Koprozessor	BME•58•040S und BMEP58CPROS3	SIL4	1.04E-10
Analogeingang	BMXSAI0410	SIL4	1.31E-09
Digitaleingang	BMXSDI1602	SIL4	1.56E-09
Digitalausgang	BMXSDO0802	SIL4	1.31E-09
Digitales Relaisausgangsmodul	BMXSRA0405	SIL3 [1]	1.68E-09
		SIL4[2]	1.34E-09
		SIL4[3]	1.35E-09
Spannungsversorgung	BMXCPS4002S, BMXCPS4022S und BMXCPS3522S	SIL4	–

HINWEIS: SIL-Werte sind bei 80 °C

1. 1 Relais pro Ausgang bei 80 °C
2. 2 Relais pro Ausgang bei 80 °C
3. 4 Relais pro Ausgang bei 80 °C

Die Summe der TFFR-Werte eines Eingangsmoduls, der CPU und des Koprozessors, der Spannungsversorgung und eines Ausgangsmoduls liegt immer unter 3,5E-09/h, was unter dem zugewiesenen Budget von 40 % liegt, das als maximale Restfehlerstromrate für eine SIL4-Sicherheitsfunktion vorgesehen ist und somit die Integration anderer Produkte in die Sicherheitsschleife ermöglicht.

TFFR pro Stunde und Funktion	SIL-Attribut
$10^{-9} \leq TFFR \leq 10^{-8}$	4
$10^{-8} \leq TFFR \leq 10^{-7}$	3
$10^{-7} \leq TFFR \leq 10^{-6}$	2
$10^{-60} \leq TFFR \leq 10^{-5}$	1

Beschreibung der Sicherheitszeiten

Die M580-Sicherheitssteuerung verfügt über eine minimale PAC-Zykluszeit von 10 ms. Dies ist für die Verarbeitung der Signale der E/A-Module, die Ausführung der Programmlogik und die Einstellung der Ausgänge erforderlich. Um die maximale PAC-Antwortzeit zu berechnen, müssen Sie die maximale Antwortzeit der verwendeten Sensoren und Aktoren kennen. Darüber hinaus ist die maximale Antwortzeit des PAC von der für den Prozess erforderlichen Prozesssicherheitszeit (PST, Process Safety Time), Seite 156 abhängig.

Prüfabstand (PTI)

Der Prüftext ist ein periodischer Test, den Sie durchführen müssen, um Fehler in einem sicherheitsbezogenen System zu erkennen, damit das System bei Bedarf in einen ähnlichen neuen Zustand oder so nahe wie möglich an diesem Zustand zurückgesetzt werden kann. Das zeitliche Intervall zwischen zwei Prüftests wird als Prüfabstand (Proof Test Interval, PTI) bezeichnet.

Der Prüfabstand ist vom angestrebten Sicherheitsintegritäts-Level, von den Sensoren, den Aktoren und der PAC-Anwendung abhängig. Das M580-Sicherheitssystem ist für die Verwendung in einer SIL3-Anwendung gemäß IEC 61508 und einem Prüfabstand von 20 Jahren geeignet.

Leistungs- und Zeitberechnungen für das M580-Sicherheitssystem

Einführung

In diesem Abschnitt wird erläutert, wie Sie die PAC-Reaktionszeit, die Systemreaktionszeit und die Prozesssicherheitsdauer für Ihr M580-Sicherheitssystem berechnen.

Prozesssicherheitsdauer

Beschreibung der Prozesssicherheitsdauer

Die Prozesssicherheitsdauer (Process Safety Time, PST) ist ein wesentliches Element eines Prozesses, der von einer Sicherheitsschleife ausgeführt wird. Sie wird als der Zeitraum zwischen dem Auftreten eines Fehlers in Equipment Under Control (EUC) (Gesteuertes Gerät) und dem Auftreten eines gefährlichen Ereignisses definiert, auch wenn die Sicherheitsfunktion nicht ausgeführt wird (d. h. wenn der sichere Zustand nicht erreicht wird).

HINWEIS: Die Prozesssicherheitsdauer ist von Ihrem individuellen Sicherheitsprozess abhängig. Sie müssen sicherstellen, dass Ihr sicherheitsbezogenes System seine Sicherheitsfunktionen innerhalb der Prozesssicherheitsdauer ausführen kann.

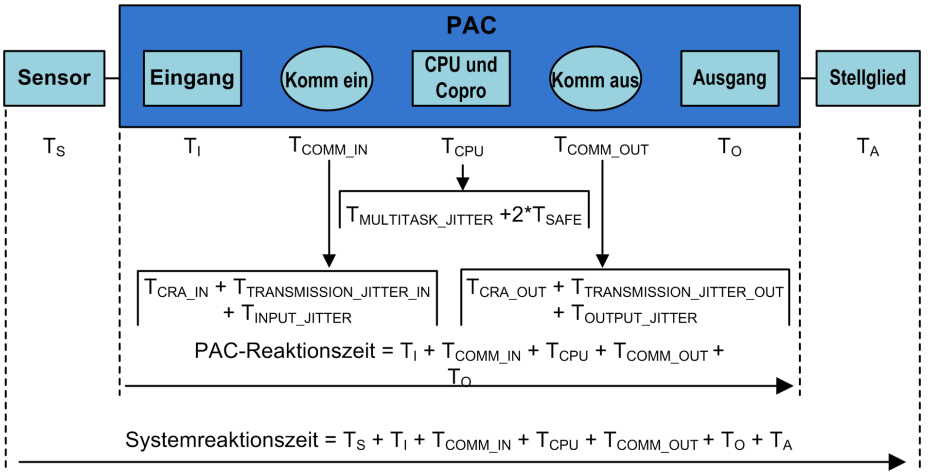
Beschreibung der Systemreaktionszeit

Die Systemreaktionszeit ist die Summe der PAC-Reaktionszeit plus die Reaktionszeit des ausgewählten Sensors (T_S) und Stellglieds (T_A).

HINWEIS: T_S und T_A sind vom Gerät abhängig.

Stellen Sie für jede Sicherheitsschleife sicher, dass die Systemreaktionszeit unter der Prozesssicherheitsdauer liegt.

Die Systemreaktionszeit wird im Folgenden erläutert:



Folgende Komponenten können zur Systemreaktionszeit gehören:

Komponente	**Beschreibung**	**Geschätzter Worst-Case-Wert**
T_S	Vom ausgewählten Sensor benötigte Zeit, um auf ein Prozessereignis zu reagieren.	Gerätespezifisch.
T_I	Vom Eingangsmodul maximal benötigte Zeit, um ein Sensorereignis zu erfassen und zu bestätigen . Sie umfasst Folgendes: • Eine Abtastperiode des Eingangsmoduls • Mehrere Abtastperioden des Eingangsmoduls zur Filterung	6 ms
T_{COMM_IN}	Verzögerung der Eingangskommunikation. Ihre Komponenten werden unter *Antwortzeit der Anwendung* (ART) im *Modicon M580 Standalone Systemplanungshandbuch für häufig verwendete Architekturen* beschrieben und umfassen Folgendes (die Zahlenangaben beziehen sich auf die Berechnung der ART (Antwortzeit der Anwendung - Application Response Time) im genannten Kapitel): • T_{CRA_IN}: CRA_Drop_Process (2) + CRA Input RPI (3) • T_{JITTER_IN}: Network_In_Time (4) + Network_In_Jitter (5) + CPU_In_Jitter (6)	–
T_{CPU}	Die Reaktionszeit von CPU und Koprozessor. Sie entspricht der Summe der von anstehenden Tasks mit höherer Priorität (FAST-Task) verursachten Verzögerung plus zwei Abfragezeiten der SAFE-Task - die erste entspricht einer gescheiterten, die zweite einer erfolgreichen Abfrage: $T_{MULTITASK\_JITTER}$ +2* T_{SAFE}.	

Komponente	Beschreibung	Geschätzter Worst-Case-Wert
$T_{MULTITASK\_JITTER}$	Durch die Ausführung anstehender Tasks mit höherer Priorität verursachte maximale Verzögerung. In diesem Fall handelt es sich um die FAST-Task. $T_{MULTITASK\_JITTER} = T_{FAST}$.	–
T_{SAFE}	Der für die SAFE-Task konfigurierte Zeitraum.	–
T_{FAST}	Dieser Wert wird berücksichtigt, da die Ausführung der FAST-Task höhere Priorität als die SAFE-Task besitzt. **HINWEIS:** Um die Formel zu vereinfachen, wird angenommen, dass sich keine Systemtask in einem Überlaufzustand befindet. Deshalb entspricht dieser Wert dem konfigurierten Zeitraum der FAST-Task – oder 0, falls die FAST-Task nicht konfiguriert ist.	–
T_{COMM_OUT}	Verzögerung der Ausgangskommunikation. Ihre Komponenten werden unter *Antwortzeit der Anwendung* (ART) im *Modicon M580 Standalone Systemplanungshandbuch für häufig verwendete Architekturen* beschrieben und umfassen Folgendes (die Zahlenangaben beziehen sich auf die Berechnung der ART (Antwortzeit der Anwendung - Application Response Time) im genannten Kapitel): • T_{CRA_OUT}: CRA_Drop_Process (12) • T_{JITTER_IN}: CPU_Out_Jitter (9) + Network_Out_Time (10) + Network_Out_Jitter (11)	–
T_O	Entspricht der Summe der folgenden Zeiten: • Verzögerung vom Lesen bis zum Anwenden des CPU-Ausgangswerts (0 bis 3 ms). • Vom Sicherheitsausgangsmodul benötigte Zeit, um den physischen Ausgang zu ändern, d. h. um die Änderung vom X-RAM zum physischen Ausgang umzusetzen (0 bis 3 ms).	6 ms
T_A	Reaktionszeit für das ausgewählte Stellglied.	Gerätespezifisch.

Beschreibung der PAC-Reaktionszeit

Für E/A-Module im lokalen Hauptrack (in der sich auch die CPU befindet) entspricht die PAC-Reaktionszeit der Summe der zugehörigen Reaktionszeiten für das ausgewählte Eingangsmodul (T_I) und Ausgangsmodul (T_O) plus die Reaktionszeit von CPU und Koprozessor (T_{CPU}):

PAC-Reaktionszeit (lokal) = $T_{CPU} + T_I + T_O$

Wenn sich das E/A-Modul in einem dezentralen Rack befindet, umfass die PAC-Reaktionszeit außerdem Eingangskommunikationsverzögerung (T_{COMM_IN}) und Ausgangskommunikationsverzögerung (T_{COMM_OUT}):

PAC-Reaktionszeit (dezentral) = $T_{CPU} + T_{COMM\_IN} + T_I + T_{COMM\_OUT} + T_O$

Beschreibung der Reaktionszeit von CPU und Koprozessor

Die Reaktionszeit von CPU und Koprozessor wird direkt von der Dauer der SAFE-Task und der FAST-Task beeinflusst. Stellen Sie sicher, dass die Sicherheitslogik innerhalb des Zeitraums der SAFE-Task ausgeführt wird.

Da ein Signal genau zu Beginn des Ausführungszyklus auftreten kann, nachdem die Signale schon verarbeitet wurden, sind ggf. zwei SAFE-Taskzyklen notwendig, um auf das Signal zu reagieren.

Da die FAST-Task eine höhere Priorität als die SAFE-Task hat, müssen Sie bei der Schätzung des Jitters außerdem die Zeit für die Ausführung der FAST-Task berücksichtigen.

Dies führt zu folgender Berechnung für die längste Reaktionszeit (Worst Case):

Reaktionszeit von CPU und Koprozessor= $2 \times T_{SAFE} + T_{FAST}$

HINWEIS: Wenn Sie die sichere Peer-to-Peer-Kommunikation, Seite 187 einsetzen, um die Sicherheitsfunktion auszuführen, wird die CPU-Reaktionszeit anders berechnet.

Beschreibung der Zeit für Eingangsmodule

Die Höchstzeit (Worst Case) für das digitale Sicherheitseingangsmodul und das analoge Sicherheitseingangsmodul T_I beträgt 6 ms..

Beschreibung der Zeit für Ausgangsmodule

Die Höchstzeit T_O für das digitale Sicherheitsausgangsmodul beträgt geschätzte 6 ms.

Das für das digitale Ausgangsmodul, Seite 109 und das digitale Relaisausgangsmodul, Seite 127 zu konfigurierende Rückfall-Sicherheitstimeout S_TO . Je nach konfigurierter Dauer der SAFE-Task (T_{SAFE}), muss der Wert für S_TO wie folgt konfiugriert werden:

- Wenn $(2,5 * T_{SAFE}) \leq 40$ ms, ist S_TO auf mindestens 40 ms einzustellen.
- Wenn $(2,5 * T_{SAFE}) > 40$ ms, ist S_TO auf mindestens $(2,5 * T_{SAFE})$ ms einzustellen.

HINWEIS
GEFAHR EINES UNBEABSICHTIGTEN GERÄTEBETRIEBS Setze Sie das Rückfall-Sicherheitstimeout (S_TO) für ein Sicherheitsausgangsmodul mindestens auf einen Wert, der 40 ms bzw. (2,5 * T_{SAFE}) überschreitet, je nachdem, welcher Wert größer ist. Hierbei gilt, dass T_{SAFE} der konfigurierten Dauer der SAFE-Task entspricht. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Bei Hot Standby-Anwendungen ist die Auswirkung der für einen Austausch, Seite 161 benötigten zusätzlichen Zeit (T_{SWAP}) und der für eine Umschaltung, Seite 162 benötigten zusätzlichen Zeit T_{SWITCH} auf den Parameter des Rückfall-Sicherheitstimeouts (S_TO) zu berücksichtigen.

Berechnung der Systemreaktionszeit

Wenn Sie die erforderliche Prozesssicherheitsdauer (PST) und die maximale Reaktionszeit von Sensoren und Stellgliedern kennen, können Sie die maximale Systemreaktionszeit (SRT) berechnen, die für Ihren Prozess tolerierbar ist.

Die maximale Systemreaktionszeit (Worst Case) kann wie folgt berechnet werden:

Für Systeme mit E/A in dezentralen Stationen:

Max. SRT = $T_S + T_I + 2 \times T_{CRA} + T_{RPI} + 2 \times T_{SAFE} + T_{FAST} + T_O + T_A$.

Oder:

Max. SRT = 16 ms + $T_S + 2.5 \times T_{SAFE} + T_{FAST} + T_A$.

Für System mit lokalem E/A:

Max. SRT = $T_S + T_I + 2.5 \times T_{SAFE} + T_{FAST} + T_O + T_A$.

Oder:

Max. SRT = 15 ms + $T_S + 2.5 \times T_{SAFE} + T_{FAST} + T_A$.

HINWEIS: Bei Hot Standby-PACs müssen für die Berechnung der maximalen Sicherheitsreaktionszeit die zusätzlichen Komponenten für die obigen Berechnungen berücksichtigt werden:

- Bei Auftreten eines unerwarteten Ereignisses und einer Umschaltung könnte die maximale Sicherheitsreaktionszeit durch Hinzufügen der Komponenten, Seite 162 T_{SWITCH} zu den obigen Berechnungen erhöht werden.

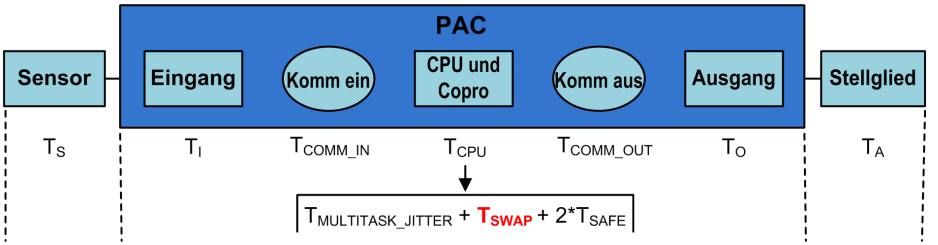
- Wenn der Systembediener einen Austausch durchführt, können die maximale Sicherheitsreaktionszeit durch Hinzufügen einer Komponenten, Seite 161 T_{SWAP} zu den obigen Berechnungen erhöht werden.

Systemreaktionszeit bei einem Austausch

Bei einem Austausch handelt es sich um eine vom Bediener ausgelöste Aktion in einem Hot Standby-System, die den Austausch der Rollen des primären und des Standby-PAC bewirkt. Ein Austausch nimmt zusätzliche Zeit in Anspruch, da während des Vorgangs keine Informationen verloren gehen dürfen und sämtliche Systemausgänge sicher ihr Timeout erreichen müssen.

Die zusätzliche Austauschzeit-Komponente wird der Zeit T_{CPU} im Anschluss an die reguläre Komponente T_{JITTER} hinzugefügt, wie nachstehend gezeigt:

Die T_{SWAP}-Zeitkomponente wird der Zeit T_{CPU} im Anschluss an die reguläre Komponente T_{JITTER} hinzugefügt. Diese Abfolge wird nachstehend dargestellt. Mit Ausnahme der Einbeziehung der Austauschkomponenten ist die Beschreibung der Systemreaktionszeit dieselbe wie oben, Seite 156:



Die Zeitkomponente T_{SWAP} entspricht der Summe von Folgendem:

$T_{ADDITIONAL\_JITTER}$ + $T_{TRANSFER}$

Die austauschspezifischen Komponenten werden beschrieben wie folgt:

Komponente	Beschreibung	Geschätzter Worst-Case-Wert
$T_{ADDITIONAL\_JITTER}$	Vom Multitask-System beim Neustart der Task auf dem neuen PAC verursachter Jitter. Folglich gilt: $T_{ADDITIONAL\_JITTER} = T_{SAFE}$.	–
$T_{TRANSFER}$	Bei der Diagnose der MAST-Task akzeptiert der PAC den Austauschbefehl und beginnt mit der Übertragung aller neuesten Daten für jede Task.	Sie nachstehende Formel.

$T_{TRANSFER}$ kann berechnet werden wie folgt:

$K3 \times (MAST_{KB} + 2 \times SAFE_{KB} + FAST_{KB}) + K4 \times (MAST_{DFB} + 2 \times SAFE_{DFB} + FAST_{DFB}) / 1000$

Hierbei gilt:

- $TASK_{KB}$ = Größe (in kByte) der für TASK zwischen primärem und Standby-PAC ausgetauschten Daten.
- $MAST_{DFB}$ = Anzahl der in der TASK deklarierten DFBs.
- K3 und K4 sind Konstanten mit Werten, die von dem in der Anwendung eingesetzten spezifischen CPU-Modul wie folgt vorgegeben werden:

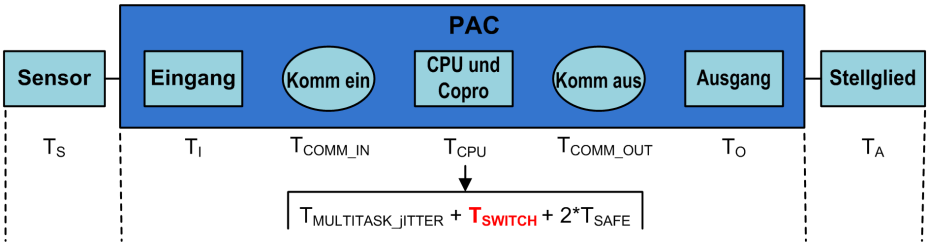
Koeffizient	BMEH582040S	BMEH584040S oder BMEH586040S
K3	46,4 µs/kB	14,8 µs/kB
K4	34,5 µs/DFB-Instanz	11,0 µs/DFB-Instanz

Wenn der Systembediener einen Austausch durchführen möchten, ohne dass die Sicherheitsmodulausgänge in ihren Fehlerausweichzustand wechseln, setzen Sie den Parameter des Rückfall-Sicherheitstimeouts der Sicherheitsausgangsmodule (S_TO) mindestens auf einen Wert größer als: $T_{MULTITASK\_JITTER} + T_{SWAP} + T_{SAFE}$.

Systemreaktionszeit bei einer Umschaltung

Eine Umschaltung findet statt, wenn der Standby-PAC in einem Hot Standby-System aufgrund eines unerwarteten Ereignisses, z. B. beim plötzlichen Betriebsausfall der Hardware im primären PAC, zum primären PAC wird. Ziel der Umschaltung ist die unterbrechungsfreie Übernahme des Betriebs durch den neuen primären PAC, der den Betrieb ab dem Punkt wiederaufnimmt, an dem der alte primäre PAC den Betrieb eingestellt hat. Unter Umständen kann es jedoch zu einer erneuten Ausführung des letzten Zyklus kommen. Systemziel ist eine schnellstmögliche Wiederherstellung des Betriebs.

Die T_{SWITCH}-Zeitkomponente wird der Zeit T_{CPU} im Anschluss an die reguläre Komponente T_{JITTER} hinzugefügt. Diese Abfolge wird nachstehend dargestellt. Mit Ausnahme der Einbeziehung der Umschaltungskomponenten ist die Beschreibung der Systemreaktionszeit dieselbe wie oben, Seite 156:



Die Zeitkomponente T_{SWITCH} entspricht der Summe von Folgendem:

$T_{DETECT} + T_{ADDITIONAL\_JITTER}$

Die umschaltungsspezifischen Komponenten werden beschrieben wie folgt:

Komponente	Beschreibung	Geschätzter Worst-Case-Wert
T_{DETECT}	Zeit, die der Standby-PAC zur Erkennung und Bestätigung des Betriebsausfalls des primären PAC benötigt.	15 ms
$T_{ADDITIONAL\_JITTER}$	Vom Multitask-System beim Neustart der Task auf dem neuen PAC verursachter Jitter. Folglich gilt: $T_{ADDITIONAL\_JITTER} = T_{SAFE}$.	–

Im Gegensatz zu einem Austausch wird für zusätzliche Zeit für eine Datenübertragung benötigt.

Damit das System auf ein unerwartetes Ereignis reagieren und eine Umschaltung durchführen kann, ohne dass die Sicherheitsmodulausgänge in ihren Fehlerausweichzustand wechseln, setzen Sie den Parameter des Rückfall-Sicherheitstimeouts der Sicherheitsausgangsmodule (S_TO) mindestens auf einen Wert größer als: $T_{JITTER} + T_{SWITCH} + T_{SAFE}$.

Konfiguration der maximalen Zeiträume für SAFE- und FAST-Task auf der CPU

Der M580-Sicherheits-PAC kann die SAFE- und FAST-Task nur periodisch ausführen (d. h. für diese Tasks wird keine zyklische Ausführung unterstützt).

Die Einstellung **Periode** für die SAFE-Task und der höchste zulässige Wert für den **Watchdog** der CPU werden auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften der SAFE-Task** konfiguriert. Die Einstellungen für das **Rückfall-Timeout** des digitalen Ausgangs werden auf der Registerkarte **Konfiguration** für das Ausgangsmodul, Seite 103 konfiguriert.

Ebenso werden die Einstellung **Periode** für die FAST-Task und der höchste zulässige Wert für den **Watchdog** der CPU auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften der FAST-Task** konfiguriert.

HINWEIS:

- Die zulässige Dauer der SAFE-Task beträgt 10 bis 255 ms, Standardwert 20 ms.
- Die zulässige Dauer der FAST-Task beträgt 1 bis 255 ms, Standardwert 5 ms.
- Die zulässige Dauer der Watchdog-Einstellungen beträgt 10 bis 500 ms, Standardwert 250 ms.
- Die zulässige Dauer des Rückfall-Timeouts beträgt 0 bis 65535 ms, Standardwert 500 ms.

Stellen Sie sicher, dass die Watchdog-Dauer länger ist als die für die SAFE-Task.

Überprüfen Sie bei der Bereitstellung Ihres Projekts die Einstellung für die Dauer der SAFE-Task Ihrer CPU. Zu diesem Zeitpunkt stellt Control Expert Safety die Echtzeitwerte des PAC bereit.

Diese Informationen finden Sie in Control Expert Safety auf der Registerkarte **Task** unter **Extras > SPS-Fenster**.

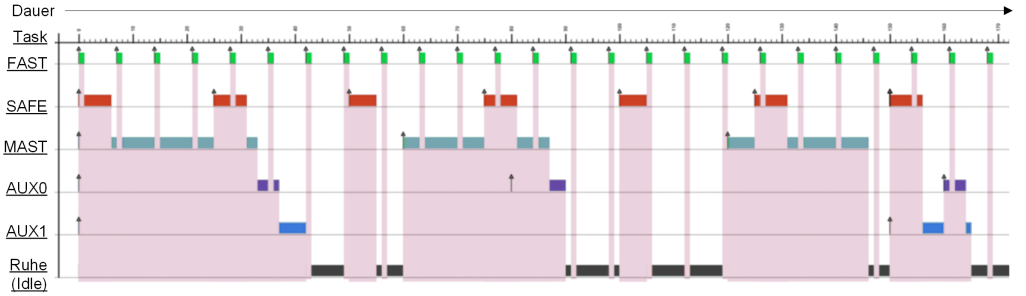
⚠WARNUNG

RISIKO DES ÜBERSCHREITENS DER PROZESSSICHERHEITSDAUER

Legen Sie die Höchstdauer der SAFE-Task der CPU immer unter Berücksichtigung der Prozesssicherheitsdauer fest. Der Zeitraum der SAFE-Task auf der CPU muss geringer sein als die Prozesssicherheitsdauer Ihres Projekts.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Die folgende Zeichnung erläutert die Ausführung der einzelnen Tasks in einem Multitasking-System und zeigt die Bevorrechtung der CPU-Ressourcen in Abhängigkeit der Taskpriorität:



FAST			SAFE			MAST			AUX0			AUX1			RUHE (IDLE)
Periode 7 ms	Ausf. 1 ms	Bandbreite 14 %	Periode 25 ms	Ausf. 5 ms	Bandbreite 20%	Periode 60 ms	Ausf. 18 ms	Bandbreite 30%	Periode 80 ms	Ausf. 3 ms	Bandbreite 4%	Periode 150 ms	Ausf. 5 ms	Bandbreite 3%	Freie Bandbreite 29 %

HINWEIS: Wenn die MAST-Task nicht im zyklischen Modus ausgeführt wird und um eine optimale CPU-Leistung zu gewährleisten, empfiehlt Schneider Electric, dass 20 % der CPU-Bandbreite ungenutzt bleiben.

Berechnung der Auswirkungen der Task-Ausführungszeiträume auf die CPU-Bandbreite

Jede konfigurierte Task nimmt einen Teil der CPU-Verarbeitungszeit oder -Bandbreite ein. Der geschätzte Prozentsatz der CPU-Bandbreite, die eine Task benötigt, ist das Ergebnis (oder der Quotient) der von einer Task benötigten Zeit (E_{TASK}) dividiert durch die

konfigurierte Ausführungsdauer für diese Task (T_{TASK}). Dies kann wie folgt dargestellt werden:

Task-Bandbreite = E_{TASK} / T_{TASK}.

Das bedeutet, dass der Gesamtprozentsatz der von einer Anwendung benötigten CPU-Bandbreite der Summe der benötigten CPU-Bandbreiten-Prozentsätze für alle Tasks entspricht.

HINWEIS: Wenn die MAST-Task nicht im zyklischen Modus ausgeführt wird und um eine optimale CPU-Leistung zu gewährleisten, empfiehlt Schneider Electric, dass der Prozentsatz der von einer Anwendung ingesamt beanspruchten CPU-Bandbreite 80 % nicht überschreitet.

In der folgenden Tabelle werden zwei Anwendungen aufgeführt sowie die Auswirkungen von Tasks mit hoher Priorität (FAST und SAFE) auf die Auslastung der CPU-Bandbreite:

Nr.	FAST			SAFE			MAST			AUX0			Ge-sa-mt
	Pro	Ausf	BB%	Pro	Ausf	BB%	Pro	Ausf	BB%	Pro	Ausf	BB%	
1	5 ms	1 ms	20 %	20 ms	5 ms	25%	50 ms	18 ms	35%	200 ms	30 ms	15%	96%
2	7 ms	1 ms	14%	25 ms	5 ms	20 %	60 ms	18 ms	30%	200 ms	30 ms	15%	79%

Pro = Taskzeitraum (T_{TASK})

Ausf = Für die Task benötigte Ausführungszeit (E_{TASK})

BB% = Bandbreite der Task

Auswirkungen der CIP Safety-Kommunikation auf die Reaktionszeit des Sicherheitssystems

Einführung

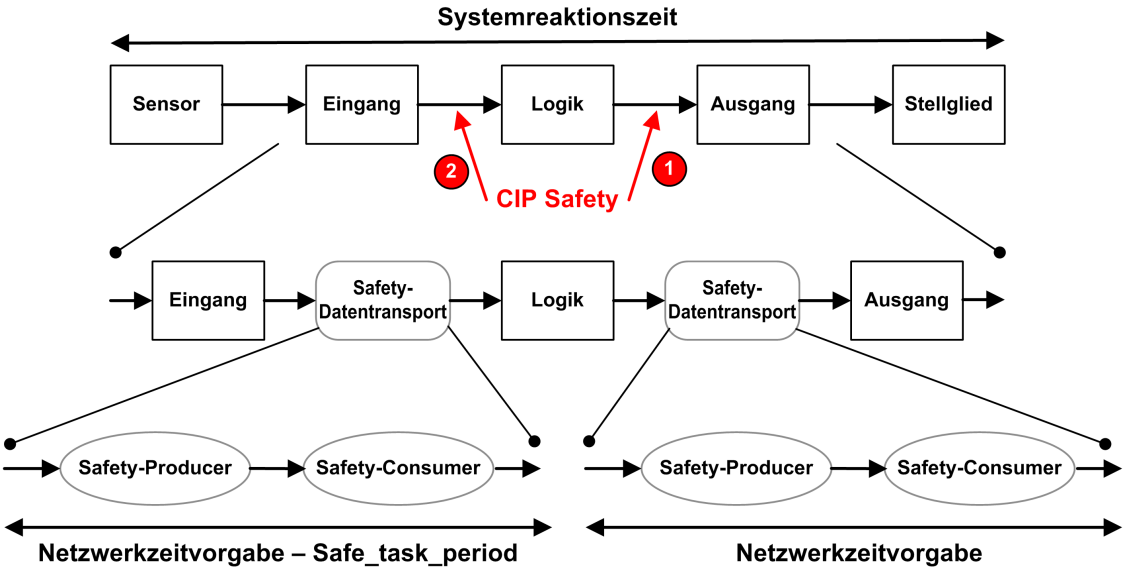
Die von der CIP Safety-Kommunikation beanspruchte Zeit, als *Netzwerkzeitvorgabe* bezeichnet, wird der *Systemreaktionszeit*, Seite 156 als fester Bestandteil hinzugefügt. Die Netzwerkzeitvorgabe entspricht dem maximalen Zeitraum (ungüngstigster Fall), der mit der Erfassung der Daten durch den Sicherheitsdaten-Producer beginnt und mit Erkennung eines sicheren Zustands durch die Consumer-Anwendung endet. Dazu gehören ebenfalls Fehler, die während der Produktion und des Verbrauchs auftreten.

Wenn die CIP Safety-Kommunikation zwischen einem Eingang und der Logik erfolgt, ersetzen Sie die Begriffsvariable TCOMM_IN in der Berechnung der Prozesssicherheitszeit, Seite 156 durch die *Netzwerkzeitvorgabe - Periode_der_SAFE_Task*. Wenn die CIP Safety-Kommunikation zwischen der Logik und einem Ausgang erfolgt, ersetzen Sie die Variable

TCOMM_OUT in der Berechnung der Prozesssicherheitszeit durch die *Netzwerkzeitvorgabe*.

Die Standardmessungen der Netzwerkzeitvorgabe fallen je nach der Rolle der M580-Sicherheits-CPU als Producer oder Consumer unterschiedlich aus.

Die verschiedenen Elemente der Netzwerkzeitvorgabe und deren Positionierung im Kontext der Systemreaktionszeit werden in folgendem Diagramm ausgewiesen:



1 CIP Safety-CPU als Producer

2 CIP Safety-CPU als Cosumer

Berechnung der Netzwerkzeitvorgabe

Die Netzwerkzeitvorgabe kann anhand der folgenden Formel berechnet werden:

Netzwerkzeitvorgabe = Netzwerkzeitvorgabe-Multiplikator * 128 µs > (EPI * Timeout-Multiplikator + Sicherheitsnachrichtenzeit(max) + Zeitkoord_Nachrichtenzeit(max) + Verbindungskorrektur_Konstante*128 µs)

Hierbei gilt:

- **Sicherheitsnachrichtenzeit(max)** entspricht der tatsächlichen Zeit aus den vom Sicherheitsdaten-Producer erfassten Daten bis zum Zeitpunkt der Übergabe der Sicherheitsdaten zur Nutzung an die Consumer-Anwendung.

- **Zeitkoord_Nachrichtenzeit(max)** entspricht der maximalen Zeit, die u. U. zur Übertragung der Informationen zur Zeitkoordinierung vom Consumer an den Producer benötigt wird.
- **Timeout-Multiplikator** ist ein in der Verarbeitung des CIP Safety-Protokolls verwendeter Parameter, der die Anzahl der ggf. verlorenen Nachrichten festlegt, bevor ein Verbindungsfehler signalisiert wird. Der Timeout-Multiplikator 1 bedeutet, dass keine Nachricht verloren wurde.
- **Verbindungskorrektur_Konstante** ist ein Wert in Inkrementen zu je 128 µs, der vom Zeitstempel abgezogen wird, um dem schlimmstmöglichen Fehler aufgrund einer Zeitverschiebung, dem asynchronen Typ der Producer- und Consumer-Uhren und der zur Übermittlung der Zeitkoordinierungsnachricht vom Consumer an den Producer benötigten Mindestzeit Rechnung zu tragen.
- **EPI** entspricht dem erwarteten Paketintervall und basiert auf der konfigurierten Periode der SAFE-Task.
- **Netzwerkzeitvorgabe-Multiplikator** und **Timeout-Multiplikator** sind CIP-Kommunikationsparameter, die für den SafetyOpen-Verbindungsframe vom Typ 2, Seite 381 konfiguriert werden.

Standardwerte der Netzwerkzeitvorgabe

Die Standardberechnung des Netzwerkzeitvorgabe ist von der Rolle der CIP Safety-CPU als Consumer (Fall 2 im vorhergehenden Diagramm) oder Producer (Fall 1) abhängig.

CPU als Consumer (Fall 2):

- Timeout-Multiplikator = 2
- EPI = Periode der SAFE-Task / 2
- Sicherheitsnachrichtenzeit(max) = Periode der SAFE-Task + 20 ms (ungünstigster Fall)
- Zeitkoord_Nachrichtenzeit(max) = Periode der SAFE-Task + 20 ms (ungünstigster Fall)
- Verbindungskorrektur_Konstante = 0 ms

Netzwerkzeitvorgabe = 1,5 * Minimale Netzwerkzeitvorgabe = 1,5 * (3 * Periode der SAFE-Task + 40 ms) = 4,5 * Periode der SAFE-Task + 60 ms

CPU als Producer (Fall 1):

- Timeout-Multiplikator = 2
- EPI = Periode der SAFE-Task
- Sicherheitsnachrichtenzeit(max) = Periode der SAFE-Task + 20 ms (ungünstigster Fall)
- Zeitkoord_Nachrichtenzeit(max) = Periode der SAFE-Task + 20 ms (ungünstigster Fall)
- Verbindungskorrektur_Konstante = 0 ms

Netzwerkzeitvorgabe = 1,5 * Minimale Netzwerkzeitvorgabe = 1,5 * (4 * Periode der SAFE-Task + 40 ms) = 6 * Periode der SAFE-Task + 60 ms

Sicherheitsbibliothek

Inhalt dieses Kapitels

Sicherheitsbibliothek

Einführung in die Sicherheitsbibliothek

Bei der Installation von Control Expert Safety wird automatisch eine Sicherheitsbibliothek mit elementaren Funktionen (EFs), elementaren Funktionsbausteinen (EFBs) und abgeleiteten Funktionsbausteinen (DFBs) integriert. Diese EFs, EFBs und DFBs werden durch das Präfix „S_“ markiert und sind für die Verwendung von Code-Sections vorgesehen, die von der SAFE-Task verwaltet werden.

HINWEIS: Außerdem wird eine zusätzliche Sammlung von EFs, EFBs und DFBs installiert. Dies ist dieselbe Sammlung von Datenobjekten, die auch nicht-sichere M580-PACs verwenden. Diese EFs, EFBs und DFBs können nur in Code-Sections genutzt werden, die von Prozess-Namespace-Tasks verwaltet werden (MAST, FAST, AUX0 und AUX1).

Eine Beschreibung der in der M580-Sicherheitsbibliothek enthaltenen Bausteine finden Sie im Dokument zur *Sicherheitsbausteinbibliothek von Control Expert*.

Zertifizierte Sicherheitsfunktionen und Funktionsbausteine

⚠WARNUNG

UNERWARTETES VERHALTEN DER ANWENDUNG

- Verwenden Sie in Ihrer Anwendung niemals V1.00 des abgeleiteten Funktionsbausteins S_GUARD_LOCKING.
- Aktualisieren Sie ab Unity Pro 13.0 XLS in Ihrer Anwendung den Funktionsbaustein S_GUARD_LOCKING mit V1.01 oder höher und generieren Sie die Anwendung neu.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

HINWEIS:

Unity Pro ist die vorherige Bezeichnung von Control Expert bis Version 13.1.

Dabei handelt es sich um einen Untersatz von EFs und Funktionsbausteinen, die in der Sicherheitslogik eingesetzt werden können. Sie werden in der Sicherheitsbibliothek bereitgestellt:

Familie	Gruppe oder Name	Typ	Beschreibung
Logische Funktionen	S_AND_*, S_OR_*, S_XOR_*, S_NOT_*, S_SHL_*, S_SHR_*, S_ROR_*, S_ROL_*	EF	Abhängig vom Typ, z. B. S_AND mit 2 bis 32 Eingängen (Inline-Code)
Logische Funktionen	S_RS, S_SR, S_F_TRIG, S_R_TRIG	EFB	–
Mathematik	S_ADD_*, S_MUL_*, S_SUB_*, S_DIV_*, S_ABS_*, S_SIGN_*, S_NEG_*, S_MOVE, S_SQRT_REAL	EF	Vom Typ abhängige Fehlerbehandlung (z. B. Überlauf) berücksichtigen (Inline-Code)
Vergleich	S_GT_*, S_GE_*, S_LT_*, S_LE_*, S_NE_*, S_EQ_*	EF	Abhängig vom Typ (Inline-Code)
Statistik	S_LIMIT_*, S_MAX_*, S_MIN_*, S_MUX_*, S_SEL	EF	Abhängig vom Typ (Inline-Code)
Typ-zu-Typ	S_BIT_TO*, S_BOOL_TO_*, S_BYTE_TO_*, S_DINT_TO_*, S_DWORD_TO_*, S_INT_TO_*, S_REAL_TO_*, S_TIME_TO_*, S_UDINT_TO_*, S_UINT_TO_*, S_WORD_TO_*	EF	Abhängig vom Typ (Inline-Code)
Zeitgeber und Zähler	S_CTU_*, S_CTD_*, S_CTUD_*	EFB	Abhängig vom Typ
Zeitgeber und Zähler	S_TON, S_TOF, S_TP	EFB	–
Peer-to-Peer	S_RD_ETH_MX, S_WR_ETH_MX, S_RD_ETH_MX2, S_WR_ETH_MX2	DFB	Funktionen für die Ausführung einer sicheren Peer-to-Peer-Kommunikation
Aktorverbindung	S_EDM, S_ENABLE_SWITCH, S_ESPE, S_OUTCONTROL, S_GUARD_LOCKING, S_GUARD_MONITORING, S_MODE_SELECTOR	DFB	Funktionsbausteine für die Maschinensicherheit mit Verbindung zu Aktoren
Sensorverbindung	S_EQUIVALENT, S_ANTIVALENT, S_EMERGENCYSTOP, S_TWO_HAND_CONTROL_TYPE_II, S_TWO_HAND_CONTROL_TYPE_III, S_MUTING_SEQ, S_MUTING_PAR, S_AI_COMP	DFB	Funktionsbausteine für die Maschinensicherheit mit Verbindung zu Sensoren
System	S_SYST_STAT_MX, S_SYST_TIME_MX, S_SYST_CLOCK_MX, S_SYST_RESET_TASK_BIT_MX, S_SYST_READ_TASK_BIT_MX	EFB	Systemfunktionsbausteine

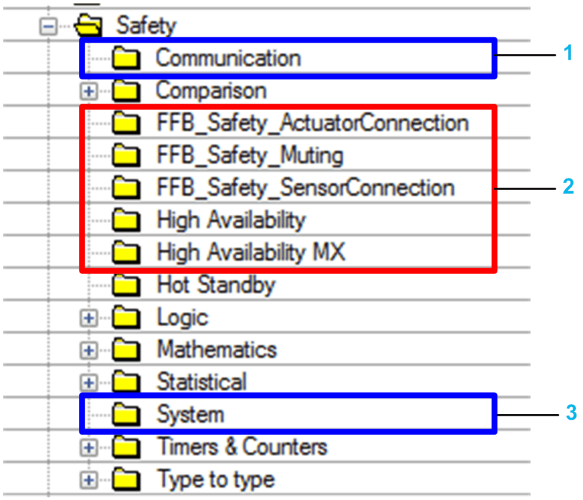
Nicht-zertifizierte Sicherheitsfunktionen und Funktionsbausteine

Dabei handelt es sich um einen Untersatz von abgeleiteten Funktionsbausteinen (DFBs), die in der Sicherheitslogik eingesetzt werden können. Diese Funktionsbausteine sind nicht zertifiziert. Sie haben den Zweck, Ihnen Beispiele für Sicherheitsfunktionsbausteine bereitzustellen, die Sie anpassen und individuell verwenden können. Diese Funktionsbausteine lassen sich in Ihre Anwendung kopieren. Ändern Sie sie dann so ab, dass sie Ihren Anforderungen entsprechen.

Familie	Gruppe oder Name	Typ	Beschreibung
High Availability MX	S_DIHA, S_AIHA	DFB	Funktion für hohe Verfügbarkeit gemäß SIL2 oder SIL3 für digitale Eingangsmodule (Inline-Code)
Sensorverbindung	AI_COMP	DFB	Funktionsbausteine für die Maschinensicherheit mit Verbindung zu Sensoren

Anzeigen der Sicherheitsbibliothek in Control Expert

Auf die Sicherheitsbibliothek können Sie nur über die SAFE-Task zugreifen. Wenn Sie die Sicherheitsbibliothek im **FBD-Editor** öffnen, werden die Gruppen der EFs, EFBs und DFBs angezeigt. Einige dieser Gruppen enthalten Sicherheitsversionen von Funktionen und Bausteinen, die in nicht-sicheren Tasks verwendet werden. Andere Gruppen (siehe unten) enthalten Funktionen und Bausteine, die nur für die SAFE-Task eingesetzt werden können:



1 Bausteine zum Lesen und Schreiben von Sicherheitsdatenwerten.

2 Bausteine für sicherheitsspezifische Aufgaben.

3 Bausteine zum Lesen und Schreiben von Werten des Sicherheitssystems.

Ein Beispiel dafür, wie einige der Sicherheitsbausteine implementiert werden, finden Sie im Konfigurationsbeispiel für die PAC-zu-PAC-Kommunikation, Seite 189, inklusive S_RD_ETH_MX und S_WR_ETH_MX.

Eine Beschreibung der verfügbaren Sicherheitsfunktionen und -bausteine finden Sie auch in der Sicherheitsbausteinbibliothek von *Control Expert*™Institute.

Datentrennung in einem M580-Sicherheitssystem

Inhalt dieses Kapitels

Einführung

In diesem Kapitel wird die Trennung der Daten in einem M580-Sicherheitssystem erläutert.

Datentrennung in einem M580-Sicherheitsprojekt

Datentrennung und -umfang

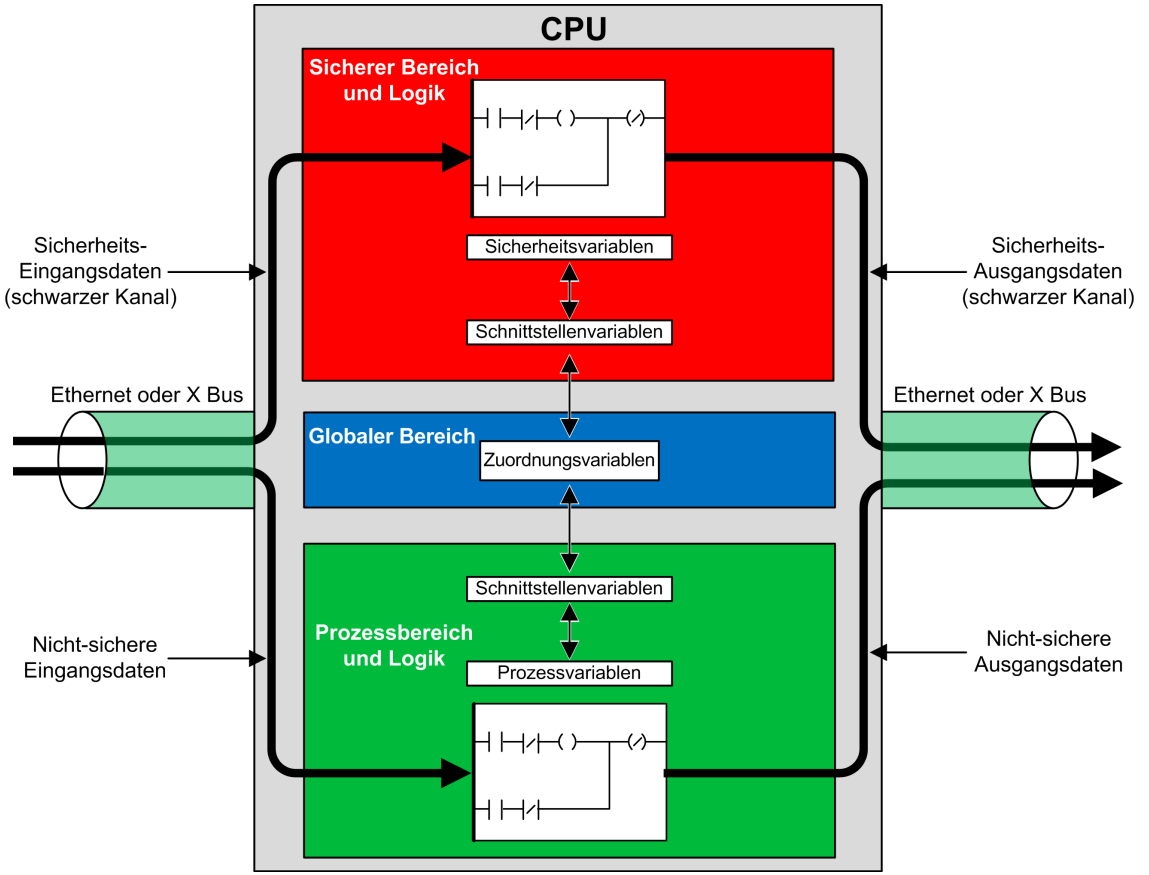
Ein M580-Sicherheitsprojekt umfasst ein Sicherheitsprogramm und ein Prozessprogramm (nicht-sicheres Programm). Control Expert isoliert die vom Sicherheitsprogramm verwendete Logik und Daten von Daten und Logik des Prozessprogramms. Dies geschieht, indem Control Expert die beiden Bereiche des Projekts in eigenen Namespaces (Bereichen) gespeichert werden: *safe* oder *process*.

Aus diesem Grund ist der Umfang einer Sicherheitsvariablen auf den Sicherheitsbereich begrenzt und der Umfang einer Prozessvariablen auf den Prozessbereich. Dies wird deutlich, wenn Sie Ihrer Anwendung Programmlogik hinzufügen:

- Wenn Sie in der SAFE-Task eine EF oder einen EFB konfigurieren, werden nur Variablen angezeigt, die im Sicherheitsbereich erstellt wurden. Variablen, die im Prozessbereich erstellt wurden, werden nicht angezeigt.
- Wenn Sie in einer nicht-sicheren Task (MAST, FAST, AUX0 oder AUX1) eine EF oder einen EFB konfigurieren, werden nur Variablen angezeigt, die im Prozessbereich erstellt wurden. Variablen, die im Sicherheitsbereich erstellt wurden, werden nicht angezeigt.

Um die Kommunikation zwischen dem Sicherheits- und dem Prozessbereich zu ermöglichen, verfügt Control Expert auch über den Bereich *global*. Der globale Bereich dient als Durchgang für die Datenübertragung zwischen Sicherheits- und Prozessbereich. Dies geschieht, indem in beiden Bereichen Schnittstellenvariablen deklariert werden, die dann mit Zuordnungsvariablen verbunden werden, die im globalen Bereich deklariert sind.

Diese Datentrennung in der M580-Sicherheits-CPU und dem Coprozessor wird im Folgenden grafisch dargestellt:



Eigenschaften der Bereiche

Die drei Datenbereiche eines M580-Sicherheitsprojekts verfügt über die folgenden Eigenschaften:

Bereich	Unterstützte Variablentypen	Bereich	Externer Zugriff
Global	Nur nicht lokalisierte Variablen. **HINWEIS:** Lokalisierte Variablen können für die Zuweisung einer Sicherheits- oder Prozess-Schnittstellenvariablen nicht verwendet werden.	Zugriff möglich auf: • Sicherheitsvariablen über Namespace-Adressierung • Prozessvariablen über Namespace-Adressierung • Andere globale Variablen	Der Zugriff auf Variablen aus allen drei Bereichen geschieht über HMI-, SCADA- oder FactoryCast-Anwendungen. (Siehe Hinweis unten.)
Safe	Nur nicht lokalisierte Variablen.	Kann nur auf andere Sicherheitsvariablen zugreifen.	
Prozess	Beides: • Lokalisierte Variablen • Nicht lokalisierte Variablen	Kann nur auf andere Prozessvariablen zugreifen.	

Wenn ein externes Anzeigeprogramm versucht, eine Prozessvariable zu lesen, ist das Adressierungsformat davon abhängig, ob die Einstellung **Nutzung des Prozess-Namespace** im Bereich **Umfang > Allgemein** im Fenster **Tools > Projekteinstellungen...** ausgewählt ist. Folgendes gilt für die Einstellung **Nutzung des Prozess-Namespace**:

- Ist die Option ausgewählt, kann das Bedienerfenster die Variablen des Prozessbereichs nur unter Verwendung des folgenden Formats lesen: „PROCESS.<Variablenname>”.
- Ist die Option nicht ausgewählt, dann kann das Bedienerfenster die Prozessbereichsvariablen nur durch Verwendung des folgenden Formats ohne PROCESS-Präfix lesen: „<Variablenname>“. Stellen Sie in diesem Fall sicher, dass alle Prozessvariablen eindeutige Namen haben und nicht mit dem Namen einer globalen Variablen übereinstimmen.

  HINWEIS: Wenn die Einstellung **Nutzung des Prozess-Namespace** nicht ausgewählt ist, stellen Sie sicher, dass alle Prozessvariablen eindeutige Namen haben und nicht mit dem Namen einer globalen Variablen übereinstimmen. Wenn ein Variablenname sowohl im globalen Bereich als auch im Prozessbereich enthalten ist, gibt Control Expert bei der Generierung des Projekts einen Fehler aus.

Übertragung von Daten zwischen Namespace-Bereichen

Einführung

Der M580-Sicherheits-PAC verfügt über drei Dateneditoren:

- **Sicherheitsdateneditor** zur Verwaltung von Daten im sicheren Namespace
- **Prozessdateneditor** zur Verwaltung von Daten im Prozess-Namespace
- **Globaler Dateneditor** zur Verwaltung globaler Variablen und Datentypen, die in der gesamten Anwendung genutzt werden

Sowohl der **Sicherheitsdateneditor** als auch der **Prozessdateneditor** enthalten die Registerkarte **Schnittstelle**. Auf der Registerkarte **Schnittstelle** können Sie nicht lokalisierte Variablen im Prozess-Namespace erstellen. Auf der Registerkarte **Schnittstelle** werden zwei Gruppen nicht lokalisierter Variablen angezeigt:

- <Eingänge>: Eine in dieser Gruppe erstellte Variable kann mit einer globalen Pass-Through-Variablen verbunden werden und von ihr Daten erhalten. Dies geschieht im **Globalen Dateneditor**.
- <Ausgänge>: Eine in dieser Gruppe erstellte Variable kann mit einer globalen Pass-Through-Variablen verbunden werden und ihr Daten senden. Dies geschieht im **Globalen Dateneditor**.

  HINWEIS: Eine Variable, die auf einer der Registerkarten **Schnittstelle** erstellt wurde, muss folgende Bedingungen erfüllen:

  - Es muss eine Variable der Kategorie EDT oder DDT sein.
  - Sie muss denselben Datentyp wie die globale Variable aufweisen, mit der sie verbunden ist.
  - Es darf keine Variable sein, die mit einem extrahierten Bit einer lokalisierten Variablen verbunden ist (z. B. %MW10.1).

Nicht lokalisierte Variablen, die auf der Registerkarte **Schnittstelle** des **Sicherheitsdateneditors** und des **Prozessdateneditors** erstellt wurden, können wie folgt verbunden werden:

Eine Prozessvariable in dieser Gruppe im Prozessdateneditor ...	**Kann mit einer Sicherheitsvariablen in dieser Gruppe im Prozessdateneditor verbunden werden ...**
<Eingänge>	<Ausgänge>
<Ausgänge>	<Eingänge>

Mit diesen drei Dateneditoren können Sie die Übertragung der Daten zwischen dem sicheren Namespace und dem Prozess-Namespace konfigurieren.

Übertragen von Daten zwischen Namespaces

Der Prozess der Übertragung von Daten vom sicheren Namespace zum Prozess-Namespace und derjenige in umgekehrter Richtung sind Spiegelbilder voneinander. Das nachstehende Beispiel illustriert die Übertragung von Daten vom Prozessbereich zum sicheren Bereich:

Element	Beschreibung
1	Öffnen Sie den **Prozessdateneditor**, klicken Sie auf die Programmregisterkarte **Schnittstelle** und erstellen Sie eine neue Variable im Teil **<Ausgänge>** des Dateneditors.
2	Öffnen Sie den **Sicherheitsdateneditor**, klicken Sie auf die Programmregisterkarte **Schnittstelle** und erstellen Sie eine neue Variable mit demselben Typ wie die Schritt 1 im Teil **<Eingänge>** des Dateneditors erstellte Variable. Doppelklicken Sie dann in das Feld **Effekti-Parameter**. Daraufhin wird das Dialogfeld **Datenumfangseditor: Variablenauswahl** geöffnet.
3	Wählen Sie im Dropdown-Menü in der oberen rechten Ecke des Dialogfelds den Ziel-Namespace **PROCESS** aus. Daraufhin werden die Variablen im ausgewählten Namespace PROCESS im Teil <Ausgänge> angezeigt.
4	Wählen Sie in Schritt 1 erstellte Prozessvariable aus, um sie der in Schritt 2 erstellten sicheren Variablen zuzuordnen, und klicken Sie dann auf **OK**. Die ausgewählte Zielvariable wird im Feld **Effektiv-Parameter** angezeigt.
5	**Speichern** Sie die vorgenommenen Änderungen.

Nachdem Sie das bearbeitete Anwendungsprogramm kompiliert, heruntergeladen und ausgeführt haben, wird der Wert wie folgt übertragen:

- Die in den **<Ausgängen>** erstellten Daten auf der Registerkarte **Schnittstelle** werden am Ende der entsprechenden Taskausführung veröffentlicht.
- Die in den **<Eingängen>** erstellten Daten auf der Registerkarte **Schnittstelle** werden am Anfang der entsprechenden Taskausführung abonniert.

Kommunikation im M580-Sicherheitssystem

Inhalt dieses Kapitels

Einführung

In diesem Kapitel wird die Kommunikation im M580-Sicherheitssystem erläutert.

Zeitsynchronisierung

Einführung

PAC mit einer CPU-Firmware bis V3.10:	Der NTP-Dienst muss konfiguriert werden, um eine sichere Kommunikation zu ermöglichen. Sowohl für die sicheren Sender als auch für die sicheren Empfänger muss über die NTP-Dienste eine Zeitsynchronisierung durchgeführt werden.
PAC mit einer CPU-Firmware ab V3.20:	Die sichere Zeitsynchronisierung basiert auf einer internen und „monotonen“ Zeituhr. Für die sichere Kommunikation ist keine NTP-Zeitsynchronisierung erforderlich: • Die Sicherheits-CPU teilt ihre sichere Zeit mit allen lokalen und dezentralen E/A. • Das dezentrale E/A-Kopf-Kommunikationsmodul BM•CRA31210 benötigt eine Firmware ab Version 2.60. • Für eine Peer-to-Peer-Kommunikation teilen die CPUs ihre Sicherheitszeit.

Konfiguration der Zeitsynchronisation mit einer CPU-Firmware bis V3.10

Einführung

Wenn Sie E/A-Sicherheitsmodule in einer RIO-Station installieren, muss die aktuelle Uhrzeit für den PAC konfiguriert werden. Das kann in drei Konfigurationen mit einer CPU-Firmware bis Version 3.10 durchgeführt werden:

1. **Dezentraler NTP-Server mit CPU als NTP-Client**: Konfigurieren Sie ein Gerät im Steuerungsnetzwerk als NTP-Server und dann die Sicherheits-CPU als NTP-Client.
2. **Lokaler NTP-Server**: Konfigurieren Sie die Sicherheits-CPU als NTP-Server für Geräte im Ethernet-RIO-Netzwerk.
3. **Dezentraler NTP-Server mit eNOC oder eNOP**: Konfigurieren Sie ein Gerät im Steuerungsnetzwerk als NTP-Server und anschließend ein Modul - entweder ein BMENOP0300- oder ein BMENOC0301/11 -Kommunikationsmodul - im lokalen Hauptrack und aktivieren Sie die Option **CPU-Zeitaktualisierung > CPU-Zeit mit diesem Modul aktualisieren** im zugehörigen DTM. Bei der Einrichtung einer RIO-Station mit Sicherheitsgeräten müssen Sie die Sicherheits-CPU wie in Fall 2 oben beschrieben als NTP-Server konfigurieren.

In beiden Konfigurationen muss zudem Folgendes durchgeführt werden:

- Aktivieren Sie den NTP-Dienst.
- Stellen Sie den NTP-Abfragezeitraum auf 20 s ein.

Wenn die Sicherheits-CPU weder als NTP-Server noch als NTP-Client konfiguriert wird, wie oben beschrieben, dann werden die Zeiteinstellungen der dezentralen E/A-Sicherheitsmodule und der CPU nicht synchronisiert und die Kommunikation über Black Channel funktioniert nicht ordnungsgemäß. Die Ein- und Ausgänge der E/A-Sicherheitsmodule in RIO-Stationen gehen in den sicheren (entregten) Zustand bzw. in den Fehlerausweichzustand über.

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Wenn Sie E/A-Sicherheitsmodule in einer RIO-Station installieren, muss für den PAC mit einer Firmware bis Version 3.10 die aktuelle Zeit konfiguriert werden. Aktivieren Sie den NTP-Dienst für Ihr M580-System und konfigurieren Sie die Sicherheits-CPU als NTP-Server oder -Client.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Schneider Electric empfiehlt, zwei NTP-Quellen zu konfigurieren. Diese können auf redundante Weise konfiguriert werden, wobei eine als Primär- und die andere als Standby-Zeitserver fungiert. Beide Server sollten jedoch zeitsynchronisiert sein. Jede Zeitanpassung von 2 s oder mehr in einem NTP-Abfragezeitraum führt dazu, dass die CPU und die E/A-Sicherheitsmodule nicht synchronisiert werden und vom NTP-Zeitserver abweichen.

Ändern der NTP-Zeiteinstellungen während des Betriebs

⚠VORSICHT

GEFAHR EINER ABSCHALTUNG DES SICHERHEITSSYSTEMS

Wenn Sie Control Expert V13 bzw. V13.1 oder eine CPU-Firmware bis 2.70 verwenden, nehmen Sie keine Änderung an den Zeiteinstellungen im NTP-Server oder in der CPU vor.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Eine Zeitänderung während des Betriebs kann den Verlust der Kommunikation und die Abschaltung des Sicherheitssystems zur Folge haben.

Eine betriebsbegleitende Zeitänderung kann zur Desynchronisation der Uhrzeit mit der Referenzuhr führen. Darüber hinaus kann sie den Verlust der Sicherheitskommunikation verursachen, was den Übergang der E/A in den entsprechenden Fehlerausweichzustand bzw. in den sicheren Zustand auslöst. Überwachen Sie Ihr System auf jegliche Desynchronisation. Sollte eine Desynchronisation auftreten, stellen Sie die Synchroniation

wieder her, um einen Kommunikationsverlust zu vermeiden. Halten Sie sich bei Auftreten einer derartigen Desynchronisation an das nachstehende Verfahren, Seite 182 zur erneuten Synchronisation des Systems.

Wenn Sie Control Expert ab V14 und die CPU-Firmware 2.80, 2.90 oder 3.10 verwenden: Die Zeiteinstellung kann im NTP-Server oder in der CPU während des Betriebs ohne negative Auswirkungen geändert werden. Führen Sie diesen Vorgang direkt im Anschluss an eine Zeitänderung durch. Halten Sie sich dazu an das nachstehend beschriebene Verfahren.

Informationen zur Konfiguration des NTP-Dienstes für eine M580-CPU finden Sie unter *Registerkarte „NTP“* im *Modicon M580 Hardware-Referenzhandbuch* .

Vorgehensweise zur vder NTP-Zeiteinstellungen

Wenn die Spannungsversorgung der CPU aus- und wiedereingeschaltet oder die CPU zurückgesetzt wird und sie usprünglich eine Zeiteinstellung von einem externen NTP-Server erhalten hat, halten Sie sich an das nachstehend beschriebene Verfahren, um die CPU-Zeit zu synchronisieren.

⚠VORSICHT

GEFAHR EINES BETRIEBSUNFÄHIGEN GERÄTS

Wenn die optionale Funktion **CPU-Zeit mit diesem Modul aktualisieren** für ein Modul BMENOP0300 oder BMENOC0301/11 zur Aktualisierung der PAC-Zeit verwendet wird, muss die Sicherheitszeit, sobald die Zeit vom externen NTP-Server verfügbar wird (d. h. sobald %SW152 von 0 zu 1 übergeht), über %SW128 mit dem externen NTP-Server synchronisiert werden. Halten Sie sich zur Synchronisation der NTP-Zeit an das nachstehend beschriebene Verfahren.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Das folgende Verfahren gilt, wenn sich die SAFE-Task im RUN-Zustand befindet und Control Expert ab V14.0 sowie die CPU-Firmware V2.80, V2.90 oder V3.10 zum Einsatz kommen:

Schritt	Aktion
1	Vergewissern Sie sich, dass die Uhrzeit der CPU bzw. des externen NTP-Servers gültig, funktionstüchtig und stabil ist.
2	Wenn die Konfiguration eine oder mehrere eRIO-Stationen umfasst, warten Sie 2 NTP-Abfragezeiträume, nachdem der NTP-Dienst wieder funktionsfähig ist bzw. nach der Zeitänderung (die die Desynchronisation ausgelöst hat), damit der neue Referenzzeitwert an alle CRA-Module gesendet werden kann.

Schritt	Aktion
3	Synchronisieren Sie die Systemzeit der Referenzuhr mithilfe des Systemworts %SW128: • Setzen Sie %SW128 auf 16#1AE5 für mindestens 500 ms. • Setzen Sie anschließend %SW128 auf #E51A für mindestens 500 ms.
4	Vergewissern Sie sich, dass die Zeit synchronisiert wurde, indem Sie überprüfen, ob die Parameterwerte für CPU_NTP_SYNC und M_NTP_SYNC im sicheren E/A-DDDT „True“ entsprechen (1).

Wenn diese Synchronisationssequenz nicht ordnungsgemäß ausgeführt wurde, wiederholen Sie sie.

HINWEIS

GEFAHR EINER ABSCHALTUNG DES SICHERHEITSSYSTEMS

- Bei Verwendung von Control Expert ab V14.0 und einer CPU-Firmware ab V2.80 sollten Sie zur Durchführung einer Änderung der PAC-Zeit diese Änderung berücksichtigen, indem Sie den zuvor beschriebenen Synchronisationsvorgang durchführen.
- Wenn Sie den Synchronisationsvorgang nicht durchführen, können die Sicherheits-E/A bei einer Uhrabweichung für die Dauer des Timeouts für eine Kommunikationsverzögerung in den sicheren Zustand bzw. in den entsprechenden Fehlerausweichzustand übergehen.

Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.

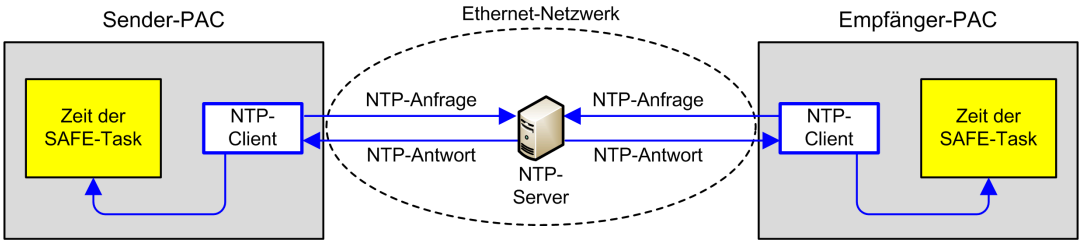
Während Schritt 3 des Zeitsynchronisationsprozesses werden bestimmte Diagnosefunktionen der sicheren Kommunikation für eine Dauer von 500 ms deaktiviert. Schneider Electric empfiehlt maximal eine Zeitänderung und Zeitsynchronisation pro Tag.

NTP-Dienst für Peer-to-Peer-Kommunikation

Für die sichere Ethernet-PAC-zu-PAC-Kommunikation ist eine Synchronisation der Zeitbasis des Sender- und Empfänger-PAC erforderlich.

HINWEIS: Schneider Electric empfiehlt in jedem PAC – entweder die Sicherheits-CPU oder ein Kommunikationsmodul BMENOP0300 bzw. BMENOC0301/11 – die Konfiguration eines NTP-Clients sowie die Konfiguration eines anderen Netzwerkgeräts als NTP-Server.

Die folgende Abbildung zeigt das Synchronisationsprinzip der Zeitbasis des Sender- und Empfänger-PAC:



Konfigurieren Sie in Control Expert für jeden Client die NTP-Dienstparameter wie folgt:

- Wählen Sie **NTP-Client** aus.
- Setzen Sie **IP-Adresse für primären NTP-Server** auf die IP-Adresse des dezentralen NTP-Servers.
- Schneider Electric empfiehlt, den Wert für den **Abfragezeitraum** auf 20 Sekunden zu setzen.

NTP-Server-Zeitkonsistenz und Systembits

NTP-Server-Zeitkonsistenz:

- Wenn die NTP-Serverzeit mit der internen PAC-Zeit übereinstimmt, die von der EF `S_SYST_CLOCK` angezeigt wird, d. es ist ein Unterschied von weniger als 2 Sekunden vorhanden, wird der Zeitwert im EF `S_SYST_CLOCK` mit der zuletzt empfangenen NTP-Serverzeit aktualisiert, mit einer Flanke von 1ms/s als Filter.

- Wenn die empfangene NTP-Serverzeit von der internen PAC-Zeit abweicht, die vom EF `S_SYST_CLOCK` angezeigt wird, d. h. es sind mehr als 2 Sekunden Unterschied gegeben, geschieht Folgendes:
  - Die zuletzt empfangene NTP-Serverzeit wird vom PAC ignoriert.
  - Der vom EF `S_SYST_CLOCK` angezeigte Zeitwert wird intern aktualisiert.
  - Der `status`-Parameter von `S_SYST_CLOCK` wird auf 0 gesetzt.
  - Der Ausgangsparameter `SYNCHRO_NTP` der DFBs `S_RD_ETH_MX` und `S_WR_ETH_MX` wird auf 0 gesetzt, um auf den Fehler hinzuweisen.

  In diesem Fall können Sie die interne PAC-Zeit wie folgt zurücksetzen:
  - Initialisieren Sie die Anwendung durch einen Kaltstart neu.
  - Laden Sie die Anwendung herunter.
  - Starten Sie den PAC neu.
  - Halten Sie sich an die Vorgehensweise zur Änderung der NTP-Zeiteinstellungen, Seite 182.

    HINWEIS: Wenn die NTP-Synchronisation auf einem der zwei PACs verloren geht (`SYNCHRO_NTP`-Parameter auf 0 gesetzt), kann die Zeitbasis vom Sender- wie auch vom Empfänger-PAC desynchronisiert sein. In diesem Fall ist die sichere Peer-to-Peer-Kommunikation möglicherweise nicht mehr funktionsfähig (der DFB `S_RD_ETH_MX`, Ausgangsparameter `health`, wird auf 0 gesetzt).

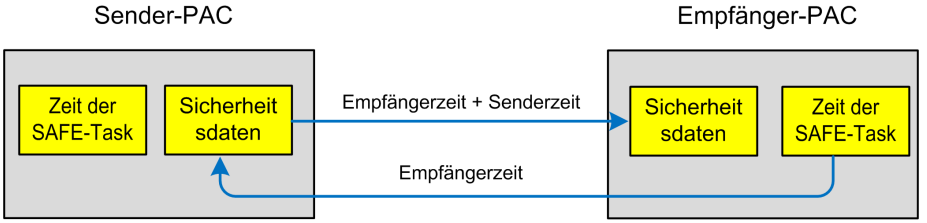
Zeitsynchronisierung für eine CPU-Firmware ab V3.20

Zeitsynchronisierung für die Peer-to-Peer-Kommunikation

HINWEIS: Mit einer CPU-Firmware ab Version 3.20 wird der NTP-Dienst nicht für die Zeitsynchronisierung verwendet.

Für die sichere Ethernet-PAC-zu-PAC-Kommunikation müssen Sender- und Empfänger-PAC eine gemeinsame Sicherheitszeit teilen.

Die folgende Abbildung zeigt das Prinzip des Teilens der Zeit zwischen Sender- und Empfänger-PAC:



Konfigurieren Sie in Control Expert Folgendes:

- eine Kommunikation Sender-zu-Empfänger für die Datenübertragung
- eine Kommunikation Empfänger-zu-Sender für die Übertragung der Sicherheitszeit

Zeitkonsistenz

Von der CPU wird eine interne Sicherheitszeit (NTP-abhängig) an die zugehörigen lokalen und dezentralen E/A-Sicherheitsmodule ausgegeben.

Peer-to-Peer-Kommunikation

Einführung

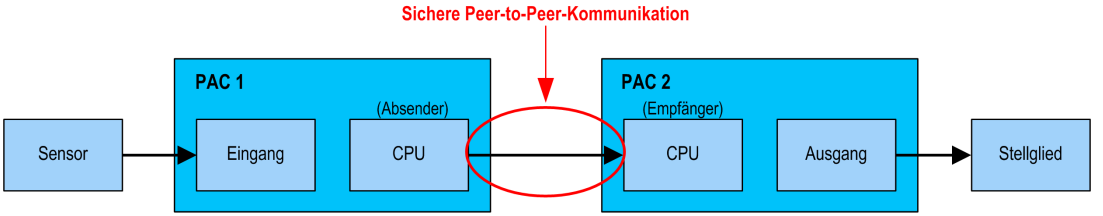
In diesem Abschnitt wird die Peer-to-Peer-Kommunikation zwischen M580-Sicherheits-PACs erläutert.

Peer-to-Peer-Kommunikation

Einführung

Es lassen sich zwei M580-Sicherheits-PACs für die sichere Peer-to-Peer-Kommunikation über Ethernet konfigurieren. Die Konfiguration basiert auf der Modbus-TCP-Scanner-Kommunikation, integriert in einen schwarzen Kanal.

Die sichere Peer-to-Peer-Kommunikation funktioniert wie folgt:



Die Kommunikation wird von zwei grundlegenden Funktionsbausteinen aus der M580-Safety Block-Bibliothek durchgeführt, die die Sicherheitsschleife auf SIL3-Ebene verwaltet. Das Protokoll erkennt Übertragungsfehler (Auslassungen, Einführungen, falsche Reihenfolgen, Verzögerungen, falsche Adressierungen, maskierte Bits) und verwaltet die Neuübertragungen.

Diese sichere Peer-to-Peer-Kommunikation ist nur zwischen folgenden PACs möglich:

- zwei M580-Sicherheits-PACs, bei mit einer CPU-Firmware bis Version 3.10
- zwei M580-Sicherheits-PACs, bei mit einer CPU-Firmware ab Version 3.20

HINWEIS: Darüber hinaus ist die sichere Peer-to-Peer-kommunikation zwischen einer Modicon Quantum-Sicherheits-SPS und einer M580-Sicherheits-SPS mit einer CPU-Firmware bis Version 3.10 möglich.

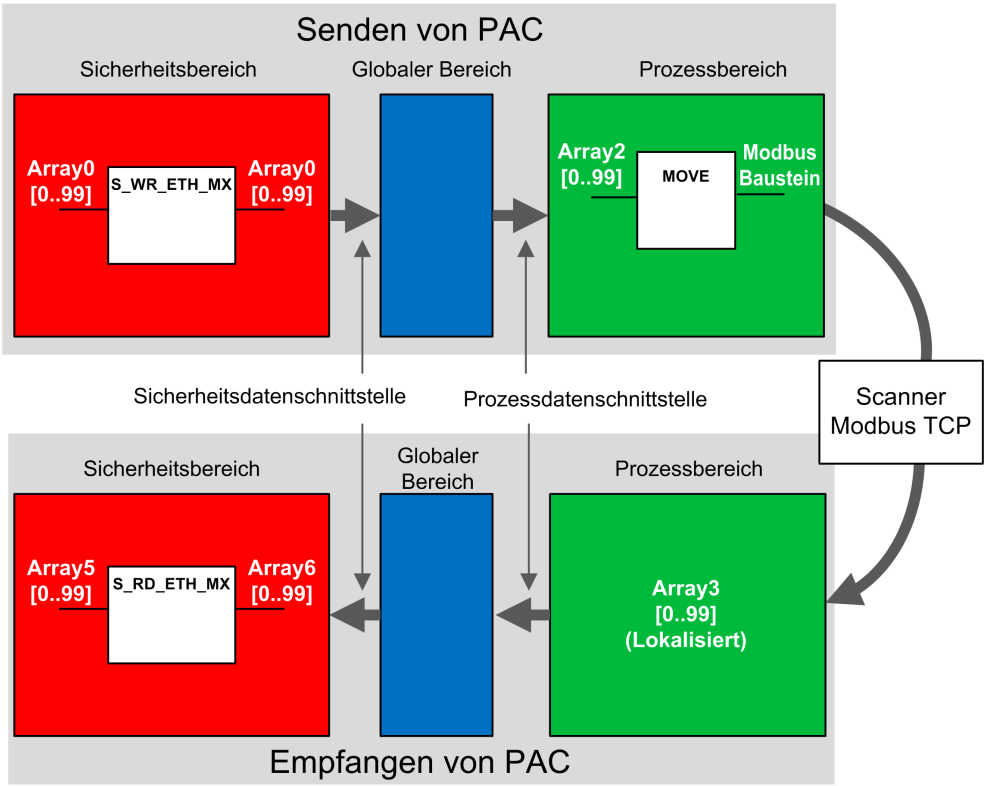
Peer-to-Peer-Architektur mit einer CPU-Firmware bis V3.10

Architekturentwicklung

Wenn eine CPU-Firmware bis Version 3.10 verwendet wird, basiert die Lösungsarchitektur auf folgenden Komponenten:

- NTP-Dienst für zeitbasierte Synchronisierung
- Ausführung von zwei DFBs (`S_WR_ETH_MX` und `MOVE`) im Sender-PAC und eines DFB (`S_RD_ETH_MX`) im Empfänger-PAC
- Scannen über Modbus-TCP für den Datentransport

Die folgende Abbildung zeigt einen Überblick des Prozesses, der für die Durchführung der sicheren Peer-to-Peer-Kommunikation erforderlich ist:



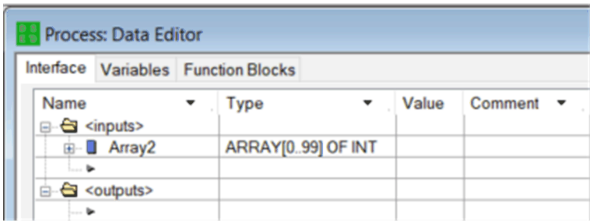
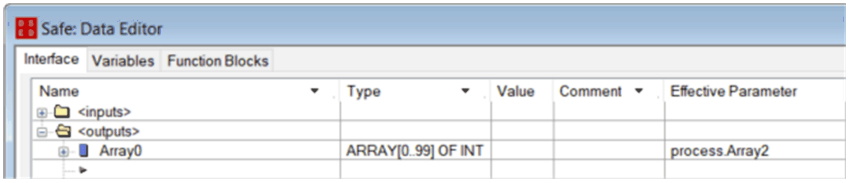
In obiger Abbildung erstellt Control Expert automatisch - und verbirgt für eine externe Ansicht - die Arrays 1 und 4 in den globalen Bereichen der Peer-PACs. Vom Standpunkt des

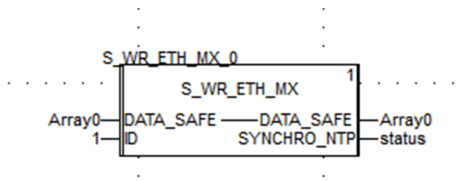
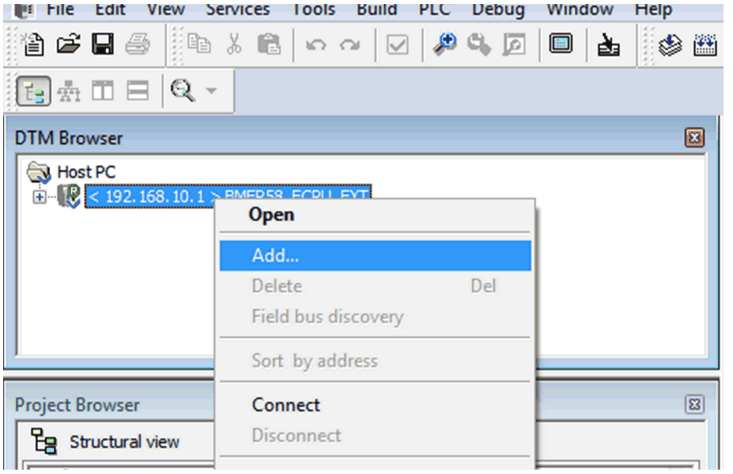
Benutzer aus werden Verbindungen von Array 0 zu Array 2 und von Array 3 zu Array 5 erstellt.

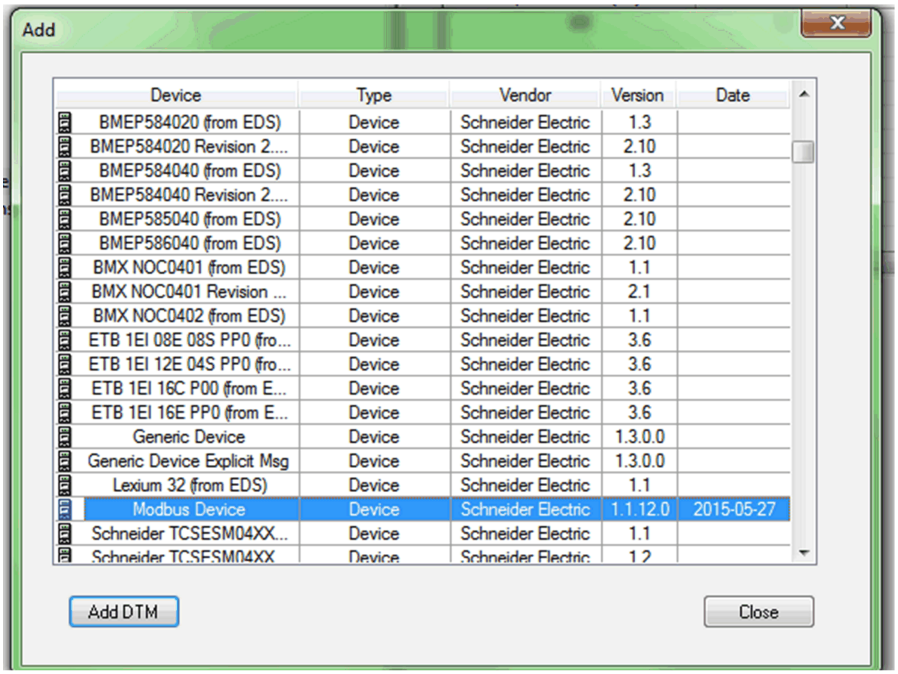
HINWEIS: Im Ethernet-Netzwerk können Sie sichere und nicht-sichere Daten kombinieren, ohne dass die Integritätsebene der sicheren Daten beeinträchtigt wird. Im Ethernet-Netzwerk gibt es bei Verwendung der sicheren Peer-to-Peer-Kommunikation keine Einschränkungen.

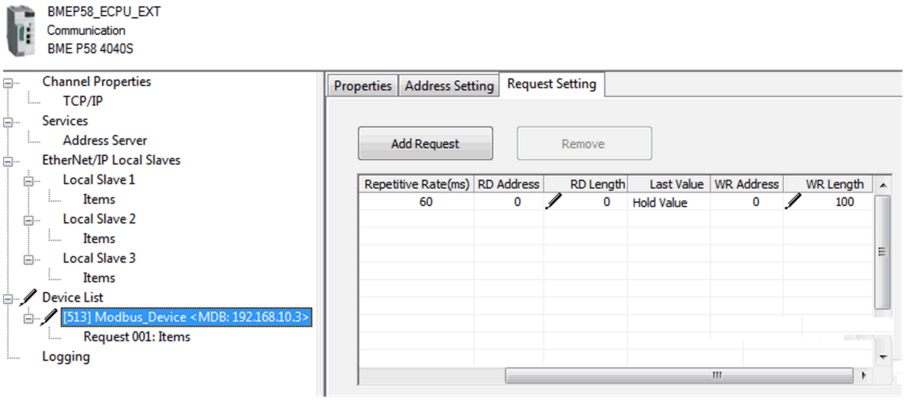
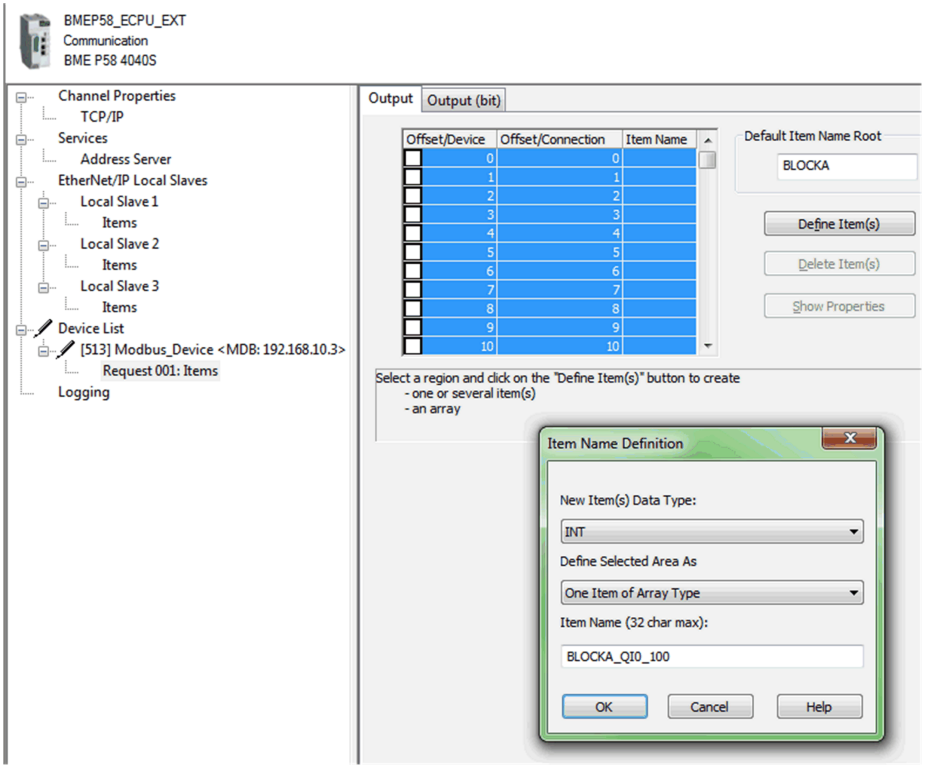
Konfigurationsdetails für die Peer-to-Peer-Datenübertragung

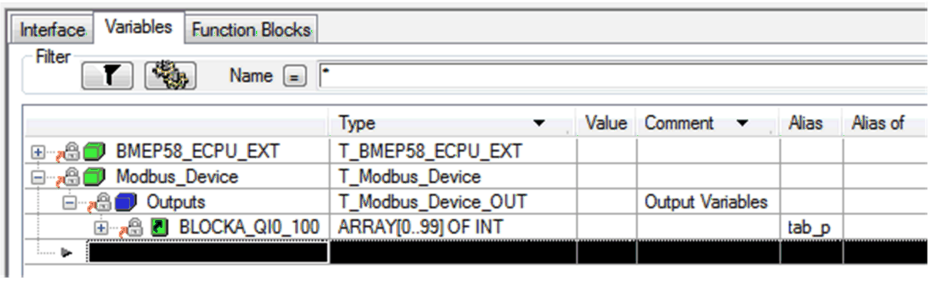
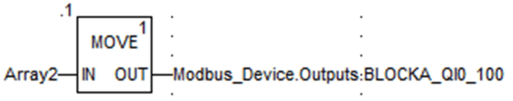
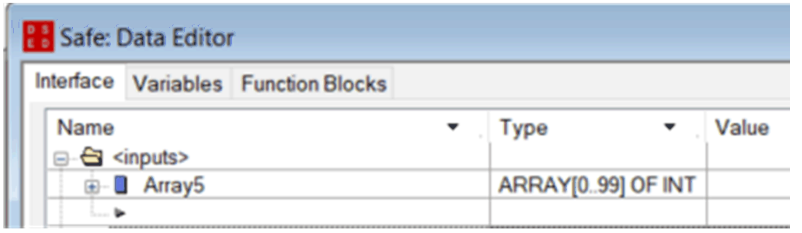
Das nachfolgende Beispiel zeigt die Konfiguration einer Peer-to-Peer-Übertragung von Daten zwischen zwei Sicherheits-PACs mit einer CPU-Firmware bis Version 3.10 und Control Expert bis Version 14.1:

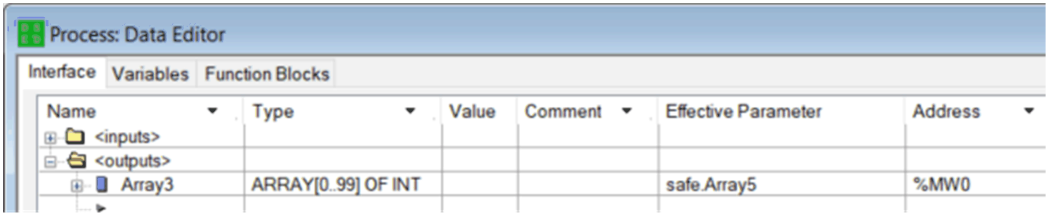
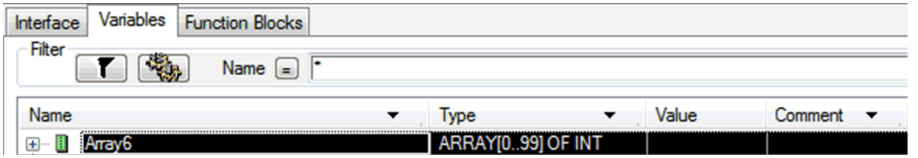
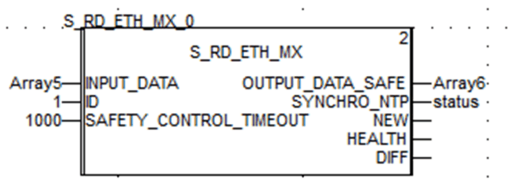
Element	Beschreibung
1	Nutzen Sie im Sender-PAC den **Prozessdateneditor**, um im Bereich **Schnittstelle** ein Array mit 100 Ganzzahlen zu erstellen. In diesem Beispiel lautet der Name des Arrays Array2: 
2	Erstellen Sie im Sender-PAC ein weiteres Array mit 100 Ganzzahlen als Ausgang. Dies geschieht auf der Registerkarte **Schnittstelle** im **Sicherheitsdateneditor**. Verbinden Sie das Array mit dem in Schritt 1 erstellten Array des Prozessbereichs. Dies geschieht in der Spalte **Effektiv-Parameter**. In diesem Beispiel lautet der Name des Arrays Array0:  **HINWEIS:** Die Ganzzahlvariablen von Index 0 bis 90 des Arrays enthalten die Sicherheitsvariablenwerte, die mit dem Empfänger-PAC ausgetauscht werden sollen. Der verbleibende Bereich ist für automatisch erstellte Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Diagnosedaten werden vom Empfänger-PAC genutzt, um festzustellen, ob die übertragenen Daten sicher sind.

Element	Beschreibung
3	Konfigurieren Sie auf dem Sender-PAC den DFB `S_WR_ETH_MX` in einer Section der SAFE-Task. Verbinden Sie den DFB mit Array0: 
4	Wählen Sie im **DTM-Browser** des Sender-PAC die CPU (in diesem Beispiel) oder ein NOC-Kommunikationsmodul aus (falls vorhanden). Klicken Sie dann auf **Hinzufügen...**, um einen Modbus-Scanner zu erstellen, der Daten vom Sender-PAC über Modbus-TCP an den Empfänger-PAC sendet: 

Element	Beschreibung
5	Wählen Sie **Modbus-Gerät** und klicken Sie auf **DTM hinzufügen**, um den Modbus-Scanner hinzuzufügen: 
6	Öffnen Sie das neu hinzugefügte Modbus-Gerät und fügen Sie einen Request hinzu. Gehen Sie dann auf der Registerkarte **Request-Einstellungen** wie folgt vor: • Legen Sie den Wert in der Spalte **WR-Länge** auf 100 fest. Dies bezieht sich auf die Länge der zu schreibenden Daten. • Legen Sie den Wert in der Spalte **WR-Adresse** fest. Dabei handelt es sich um die Adresse, an die der Empfänger-PAC die erhaltenen Daten schreibt (in diesem Beispiel auf 0, sodass der Sender-PAC beim Wert %MW0 in der Tabelle des Empfänger-PAC mit dem Schreiben beginnt).

Element	Beschreibung
	
7	Wählen Sie den Knoten **Request 001: Elemente**. Definieren Sie auf der Registerkarte **Ausgang** den Arraytyp INT (d. h. ≥100 Ganzzahlen). Dabei handelt es sich um die Tabelle des Sender-PAC, die in den Empfänger-PAC geschrieben wird: 

Element	Beschreibung
8	Sobald Sie die Konfiguration generiert und gespeichert haben, wird der Baustein (in diesem Beispiel BLOCKA_QI0_100) automatisch als Prozessvariable erstellt: 
9	Verwenden Sie im Sender-PAC in einer Prozesscode-Section einen DFB vom Typ `MOVE`, um den Inhalt von Array2 in das oben definierte Array in der Modbus-Gerätestruktur zu kopieren: 
10	Nutzen Sie im Empfänger-PAC den **Safe: Dateneditor**, um im Bereich **Schnittstelle** ein Array mit 100 Ganzzahlen (Array5) zu erstellen. 

Element	Beschreibung
11	Erstellen Sie im Empfänger-PAC im **Prozessdateneditor** ein Array Array3 mit 100 Ganzzahlen in der Section <Ausgänge> der Registerkarte **Schnittstelle**. Verbinden Sie dieses Array mit dem Array des Datenbereichs (Array5, erstellt in Schritt 10). Dies geschieht in der Spalte **Effektiv-Parameter**. Die vom Sender-PAC gesendeten Daten werden über den Modbus-Scanner in dieses Array geschrieben, vorausgesetzt, dass sich diese Variable an der Adresse befindet, die im Scanner des Sender-PAC definiert ist (in diesem Beispiel %MW0): 
12	Nutzen Sie im Empfänger-PAC den **Sicherheitsdateneditor**, um ein Array mit 100 Ganzzahlen (Array6) zu erstellen: 
13	Instanziieren Sie im Empfänger-PAC in einer Code-Section der SAFE-Task den DFB `S_RD_ETH_MX` mit dem in Schritt 10 erstellten Array (Array5) als Eingangsparameter und mit dem in Schritt 12 erstellten Array (Array6) als Ausgangsparameter: 

Schwarzer Kanal/Peer-to-Peer

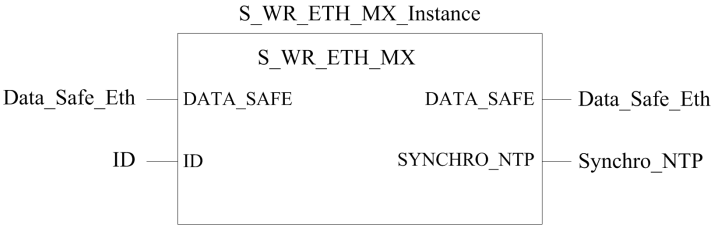
Jede Peer-to-Peer-Datenübertragung besteht aus *Benutzersicherheitsdaten*, in denen der anwendungsbezogene Inhalt übertragen wird, sowie *reservierten Daten*. Die *reservierten Daten* werden vom Sicherheits-PAC genutzt, um die Zuverlässigkeit der Übertragung sicherzustellen, damit die SIL3-Anforderungen erfüllt werden. Die *reservierten Daten* bestehen aus den folgenden Elementen:

- Eine CRC, die vom Sender-PAC aus den zu übertragenden Daten berechnet wird. Der Empfänger-PAC prüft die CRC, bevor er die übertragenen Daten nutzt.
- Eine Kommunikationskennung, die Teil der CRC-Berechnung ist, um Masquerading und Insertion-Angriffe während der Übertragung von Sicherheitsdaten zu vermeiden.
- Ein Zeitstempel mit der Zeit der Übertragung in ms. Diese gestempelte Zeit basiert auf dem Zeitwert des NTP-Diensts und wird genutzt, um Sender- und Empfänger-PAC zu synchronisieren. Der die Daten sendende Sender-PAC fügt den an den Empfänger-PAC gesendeten Daten einen Zeitwert hinzu. Der Empfänger-PAC vergleicht den empfangenen Zeitstempel mit seinem eigenen Zeitwert und geht damit wie folgt vor:
  - Er prüft das Alter der Daten.
  - Er weist doppelte Übertragungen zurück.
  - Er legt die chronologische Reihenfolge der empfangenen Übertragungen fest.
  - Er bestimmt die vergangene Zeit zwischen dem Empfang der einzelnen Datenübertragungen.

Konfiguration des DFB `S_WR_ETH_MX` in der Programmlogik des Sender-PAC

Darstellung

DFB-Darstellung:



Eine ausführliche Beschreibung dieses DFB finden Sie hier: *EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek*.

Beschreibung

Der DFB `S_WR_ETH_MX` gilt für PACs mit einer CPU-Firmware bis Version 3.10. Dieser DFB berechnet Daten (reservierte Daten mit CRC und Zeitstempel), die der Empfänger braucht, um Fehler zu prüfen und zu verwalten, die während der sicheren Peer-to-Peer-Kommunikation auftreten.

Der DFB S_WR_ETH_MX muss bei jedem Zyklus im Sender-PAC aufgerufen werden. Innerhalb des Zyklus muss er in der Logik ausgeführt werden, nachdem an den zu sendenden Daten alle erforderlichen Änderungen vorgenommen wurden. Das heißt, dass während des Zyklus die zu sendenden Daten nach der Ausführung des DFB nicht geändert werden dürfen, da andernfalls die im reservierten Datenbereich verwendeten CRC-Informationen nicht korrekt sind und die sichere Peer-to-Peer-Kommunikation fehlschlägt.

Sie müssen dem Parameter ID einen eindeutigen Wert zuweisen, mit dem die sichere Peer-to-Peer-Kommunikation zwischen Sender und Empfänger identifiziert wird.

⚠WARNUNG

SICHERHEITSFUNKTIONEN KÖNNEN NICHT MEHR AUSGEFÜHRT WERDEN

Der Wert des Parameters ID muss eindeutig und im Netzwerk für ein Sender/Empfänger-Paar festgelegt sein.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Beschreibung des Arrays DATA_SAFE

Verwenden Sie die Registerkarte **Schnittstelle** sowohl im **Sicherheitsdateneditor** als auch im **Prozessdateneditor** in , um die Verbindung zwischen den Prozessvariablen und den Sicherheitsvariablen herzustellen.Control Expert

Die Verbindung von Sicherheits- und Prozessvariablen auf diese Weise ermöglicht das Folgende:

- Übertragung des Werts von Sicherheitsvariablen auf Prozessvariablen über verbundenen globale Variablen.
- Senden der variablen Werte des Prozessbereichs der sendenden PAC zum Prozessbereich der empfangenden PAC mittels expliziter Nachrichtenübertragung über Modbus TCP.

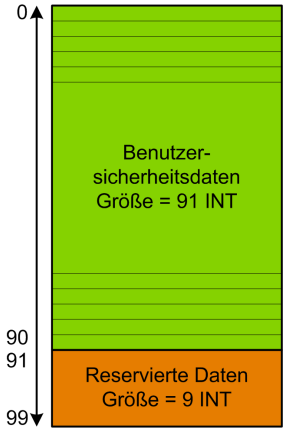
Das Array DATA_SAFE besteht aus zwei Bereichen:

- Die Zone **Benutzersicherheitsdaten** enthält die Daten des Sicherheitsspeicherbereichs der PAC. Dieser Bereich startet bei Index 0 und endet bei Index 90.

- Die Zone **Reservierte Daten** ist für automatisch erstelle Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Daten werden von der empfangenden PAC verwendet, um zu bestimmen, ob die in der Zone **Benutzersicherheitsdaten** enthaltenen Daten sicher sind. Dieser Bereich startet bei Index 91 und endet bei Index 99.

  HINWEIS: Führen Sie in der Zone **Reservierte Daten** keinen Schreibvorgang durch.

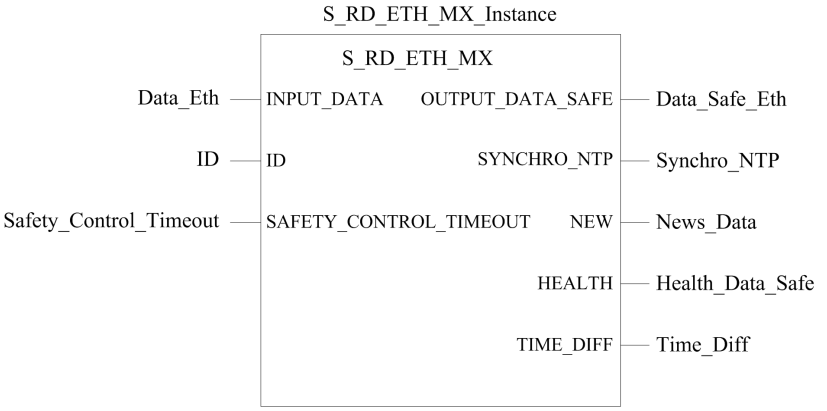
Darstellung der Struktur des Arrays `DATA_SAFE` (Array[0..99] of INT):



Konfiguration des DFB S_RD_ETH_MX in der Programmlogik des Empfänger-PAC

Darstellung

DFB-Darstellung:



Eine ausführliche Beschreibung dieses DFB finden Sie hier: *EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek*.

Beschreibung

Der DFB S_RD_ETH_MX gilt für PACs mit einer CPU-Firmware bis Version 3.10. Er kopiert die im Prozessbereich empfangenen Daten in den Sicherheitsbereich und prüft deren Genauigkeit.

⚠WARNUNG

SICHERHEITSFUNKTIONEN KÖNNEN NICHT MEHR AUSGEFÜHRT WERDEN

- Der DFB `S_RD_ETH_MX` muss in jedem Zyklus in der Programmlogik des Empfänger-PAC aufgerufen werden. Er muss ausgeführt werden, bevor die Daten im Zyklus genutzt werden.
- Der Wert des Parameters `ID` muss eindeutig und im Netzwerk für ein Sender/Empfänger-Paar festgelegt sein.
- Sie müssen den Wert des `HEALTH`-Bits des DFB `S_RD_ETH_MX` in jedem Zyklus testen, bevor Sie sichere Daten zur Verwaltung der Sicherheitsfunktion nutzen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Der Funktionsbaustein `S_RD_ETH_MX` geht wie folgt vor:

- Er kopiert die im Register `INPUT_DATA` empfangenen Daten in das Register `OUTPUT_DATA_SAFE`, falls diese die folgenden Tests bestehen:
  - Er überprüft die CRC des zuletzt empfangenen Datenpakets, mittels E/A-Scanner über Ethernet (Modbus TCP). Wenn die CRC nicht korrekt ist, werden die Daten als unsicher betrachtet und nicht in das Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs geschrieben.
  - Der Funktionsbaustein überprüft die letzten empfangenen Daten, um zu bestimmen, ob diese aktueller sind als die Daten, die bereits im Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs geschrieben sind (durch Vergleich des Zeitstempels). Wenn die zuletzt empfangenen Daten nicht aktueller sind, werden sie nicht in das Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs kopiert.
- Er prüft das Alter der Daten im Sicherheitsspeicherbereich. Wenn die Daten älter sind als der maximal konfigurierbare Wert, der im Eingangsregister `SAFETY_CONTROL_TIMEOUT` eingestellt wurde, werden die Daten als unsicher deklariert und das `HEALTH`-Bit wird auf 0 gesetzt.

  HINWEIS: Das Datenalter ist der Zeitunterschied zwischen dem Zeitpunkt, zu dem die Daten auf dem Sender-PAC berechnet wurden, und dem Zeitpunkt, zu dem die Daten im Empfänger-PAC geprüft werden. Die Zeitbasisreferenz wird regelmäßig mit der Zeit aktualisiert, die von einem NTP-Server empfangen wird.

  Wenn das `HEALTH`-Bit auf 0 gesetzt wird, werden die im Array `OUTPUT_DATA_SAFE` verfügbaren Daten als unsicher betrachtet. Reagieren Sie in diesem Fall angemessen.

Beschreibung der Arrays `INPUT_DATA` und `OUTPUT_DATA_SAFE`

Das Array `INPUT_DATA` besteht aus Daten aus dem Prozessdatenspeicherbereich. Das Array `OUTPUT_DATA_SAFE` besteht aus Sicherheitsvariablen. Verwenden Sie die

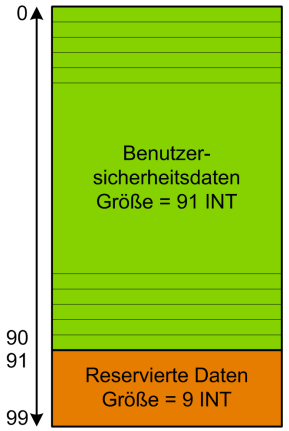
Registerkarten **Sicherheitsdateneditor** und **Prozessdateneditor** in , um die Verbindung zwischen den Prozessvariablen und den Sicherheitsvariablen herzustellen.Control Expert

Die Arrays `INPUT_DATA` und `OUTPUT_DATA_SAFE` bestehen aus zwei Bereichen:

- Der Bereich für **Benutzersicherheitsdaten** enthält die Benutzerdaten. Dieser Bereich startet bei Index 0 und endet bei Index 90.
- Die Zone **Reservierte Daten** ist für automatisch erstelle Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Daten werden von der empfangenden PAC verwendet, um zu bestimmen, ob die in der Zone **Benutzersicherheitsdaten** enthaltenen Daten sicher sind. Dieser Bereich startet bei Index 91 und endet bei Index 99.

  HINWEIS: Das Ausführen eines Schreibvorgangs im Bereich **Reservierte Daten** wird nicht empfohlen, da auf diese Weise automatisch erstellte Diagnosedaten überschrieben werden.

Darstellung der Struktur der Arrays `INPUT_DATA` und `OUTPUT_DATA_SAFE` (Array[0..99] of INT):



Berechnung des Werts SAFETY_CONTROL_TIMEOUT

Berücksichtigen Sie beim Berechnen des Werts `SAFETY_CONTROL_TIMEOUT` das Folgende:

- Minimalwert: `SAFETY_CONTROL_TIMEOUT` > T1
- Empfohlener Wert: `SAFETY_CONTROL_TIMEOUT` > 2 * T1

T1 = CPU_{Sender} MAST-Zykluszeit + CPU_{Sender} SAFE-Zykluszeit + Wiederholungsrate (Repetitive_rate) + Netzwerkübertragungszeit + $CPU_{Empfänger}$ MAST-Zykluszeit + $CPU_{Empfänger}$ SAFE-Zykluszeit

Hierbei gilt:

- *CPU_{Sender} MAST-Zykluszeit* ist die MAST-Zykluszeit der Sender-PAC.
- *CPU_{Sender} SAFE-Zykluszeit* ist die SAFE-Zykluszeit der Sender-PAC.
- *Wiederholungsrate* (Repetitive_rate) ist die Zeit für die Schreibanfrage des E/A-Abfragegeräts vom Sender-PAC zum Empfänger-PAC.
- *Netzwerkübertragungszeit* ist die auf dem Ethernet-Netzwerk verwendete Zeit für die Datenübertragung vom Sender-PAC zum Empfänger-PAC.
- *$CPU_{Empfänger}$ MAST-Zykluszeit* ist die MAST-Zykluszeit des Empfänger-PAC.
- *$CPU_{Empfänger}$ SAFE-Zykluszeit* ist die SAFE-Zykluszeit des Empfänger-PAC.

Beachten Sie, dass der für Parameter `SAFETY_CONTROL_TIMEOUT` definierte Wert einen direkten Effekt auf die Stabilität und Verfügbarkeit der sicheren Peer-to-Peer-Kommunikation hat. Wenn der Parameterwert `SAFETY_CONTROL_TIMEOUT` sehr viel größer als T1 ist, kann die Übertragung verschiedene Verzögerungen (wie Netzwerkverzögerungen) oder korrupte Datenübertragungen tolerieren.

Sie tragen die Verantwortung für die Konfiguration Ihres Ethernet-Netzwerks, sodass die Last während der Datenübertragung keine übermäßigen Verzögerungen auf dem Netzwerk verursacht, da dies zu einem Ablauf des Timeouts führen kann. Ziehen Sie ein dediziertes Ethernet-Netzwerk für sichere Peer-to-Peer-Protokolle in Betracht, um Ihre sichere Peer-to-Peer-Kommunikation vor übermäßigen Verzögerungen durch die gleichzeitige Übertragung nicht-sicherer Daten auf demselben Netzwerk zu schützen.

Bei der Inbetriebnahme Ihres Projekts müssen Sie die Leistung der sicheren Peer-to-Peer-Kommunikation schätzen, indem Sie die Werte im Ausgangsparameter `TIME_DIFF` überprüfen und die Marge mithilfe des im Parameter `SAFETY_CONTROL_TIMEOUT` definierten Werts prüfen.

Informationen zum `HEALTH`-Bit

Wenn der Wert des `HEALTH` -Bit dem Folgenden entspricht:

- 1: Die Integrität der Daten ist korrekt (CRC) und das Alter der Daten ist kleiner als der im Eingangsregister `SAFTETY_CONTROL_TIMEOUT` festgelegte Wert.

  HINWEIS: Das Alter der Daten ist die Zeit zwischen:

  - Dem Start des Zyklus, wenn die Daten im Sender-PAC berechnet werden.
  - Dem Start des Zyklus, wenn die Daten im Empfänger-PAC überprüft werden.
- 0: Neue gültige Daten werden im erforderlichen Zeitintervall nicht empfangen (Der Timer läuft ab und das `HEALTH`-Bit wird auf 0 gesetzt).

  HINWEIS: Wenn das `HEALTH`-Bit auf 0 gesetzt wird, werden die Daten im Ausgangsarray `OUTPUT_DATA_SAFE` als unsicher betrachtet. Reagieren Sie angemessen.

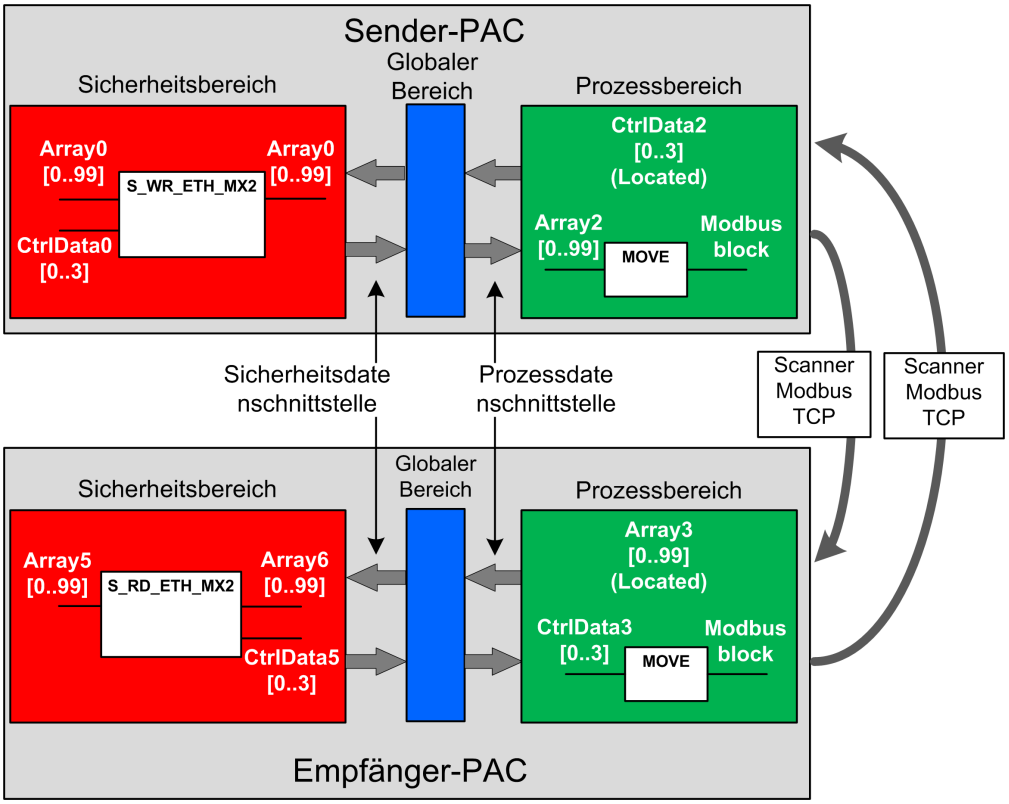
Peer-to-Peer-Architektur mit einer CPU-Firmware ab V3.20

Architekturentwicklung

Wenn eine CPU-Firmware ab Version 3.20 verwendet wird, basiert die Lösungsarchitektur auf folgenden Komponenten:

- Ausführung von zwei DFBs (`S_WR_ETH_MX2` und `MOVE`) im Sender-PAC und einem DFBs (`S_RD_ETH_MX2` und `MOVE`) im Empfänger-PAC
- Abfrage per Modbus TCP für den sicheren Datentransport vom Sender zum Empfänger
- Abfrage per Modbus TCP für den Steuerungsdatentransport vom Empfänger zum Sender

Die folgende Abbildung bietet einen Überblick über den Prozess der für die Durchführung der sicheren Peer-to-Peer-Kommunikation erforderlich ist:

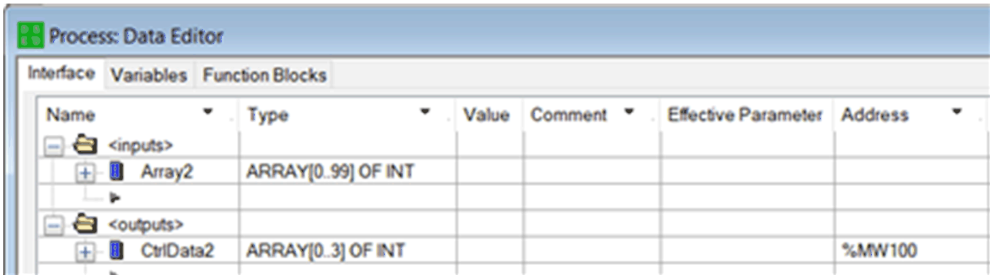


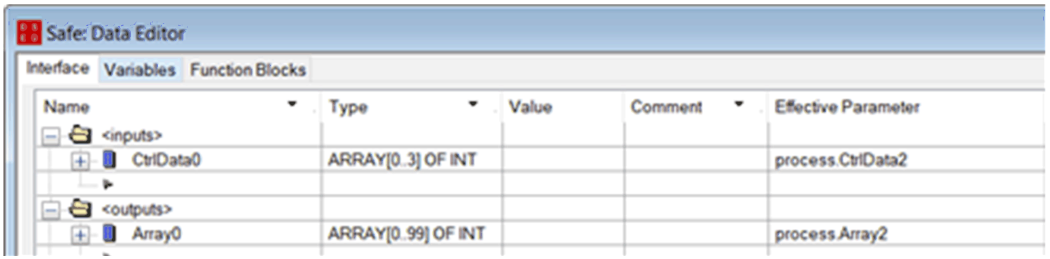
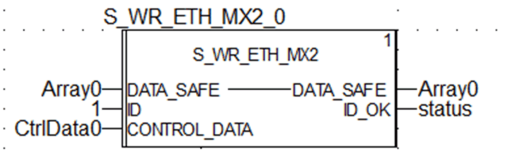
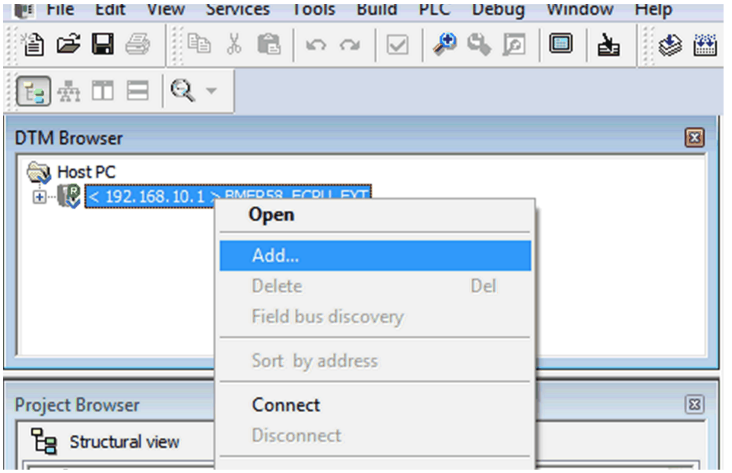
In der obigen Abbildung erstellt Control Expert automatisch Array1 und Array4 in den globalen Bereichen der Peer-PACs (und verbirgt diese für eine externe Ansicht). Vom Standpunkt des Benutzer aus werden Verbindungen von Array0 zu Array2 und von Array3 zu Array5 erstellt.

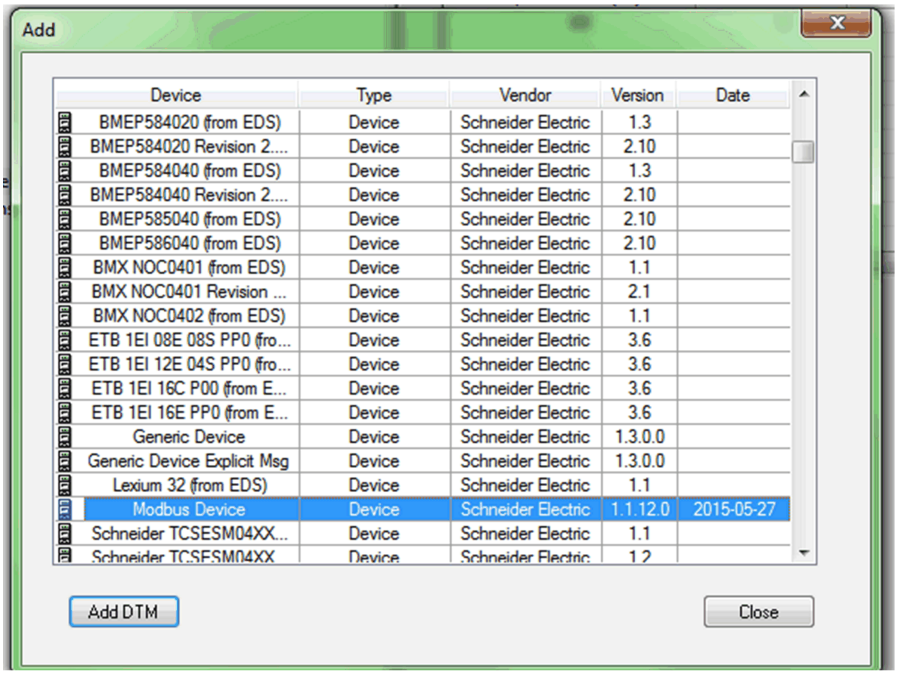
HINWEIS: Im Ethernet-Netzwerk können Sie sichere und nicht-sichere Daten kombinieren, ohne dass die Integritätsebene der sicheren Daten beeinträchtigt wird. Im Ethernet-Netzwerk gibt es bei Verwendung der sicheren Peer-to-Peer-Kommunikation keine Einschränkungen.

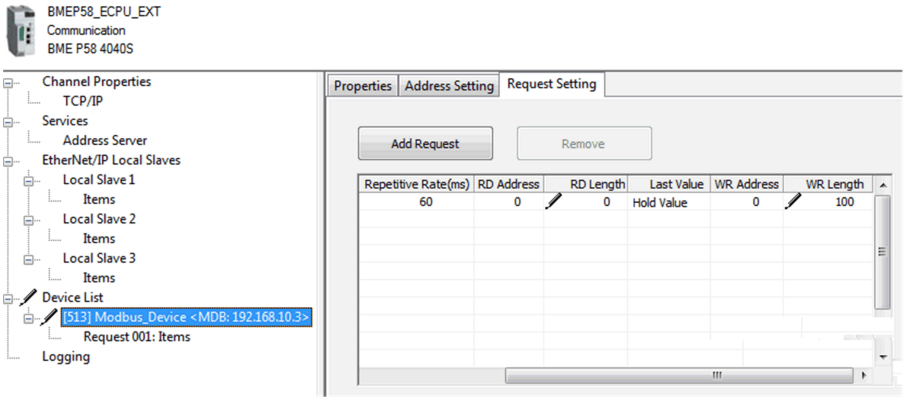
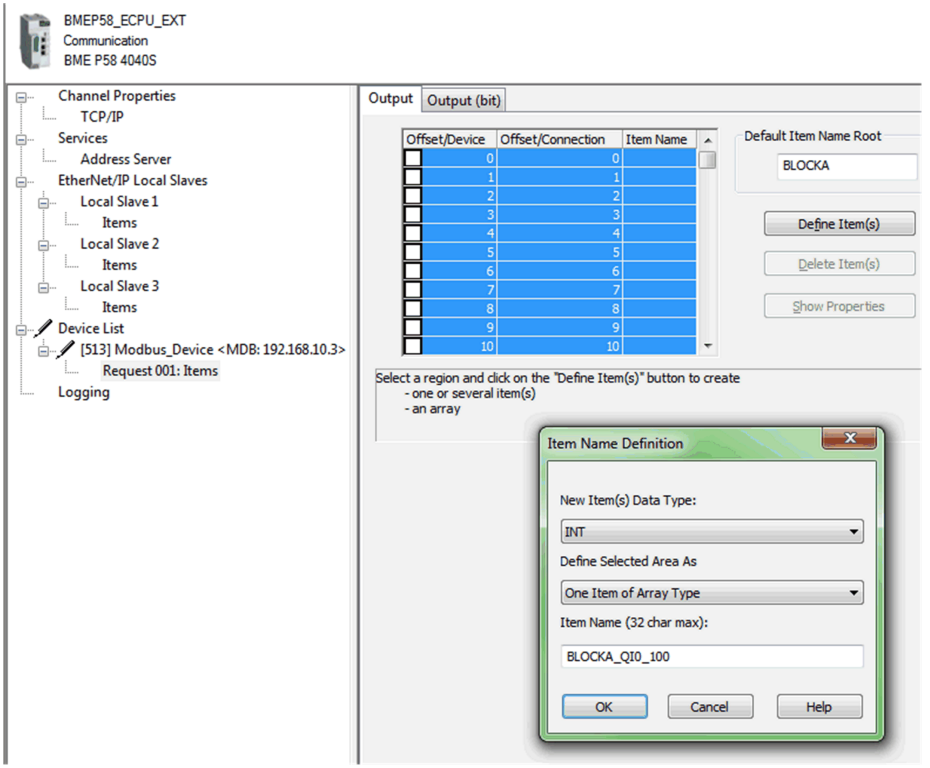
Konfigurationsdetails für die Peer-to-Peer-Datenübertragung

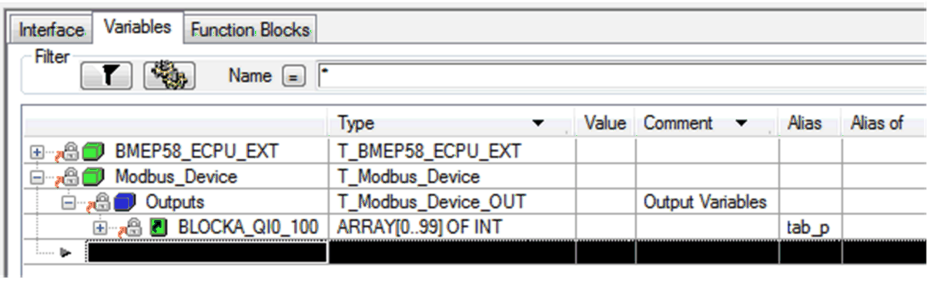
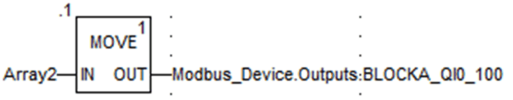
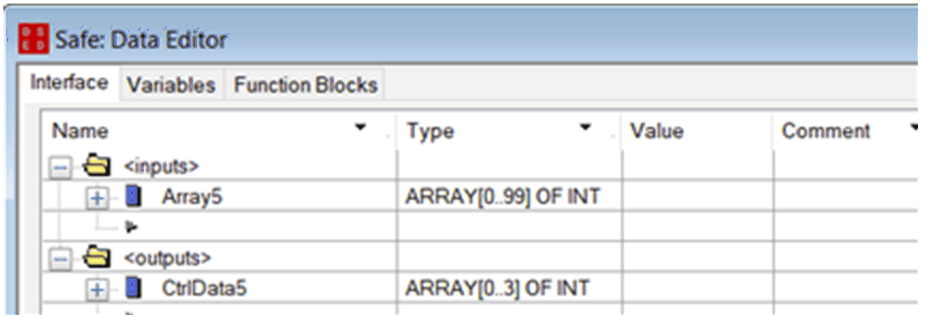
Das nachfolgende Beispiel zeigt die Konfiguration einer Peer-to-Peer-Übertragung von Daten zwischen zwei Sicherheits-PACs mit einer Firmware ab Version 3.20 und Control Expert 15.0 oder später:

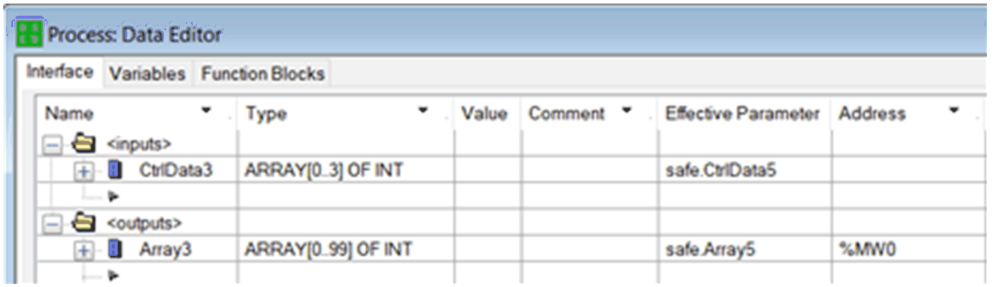
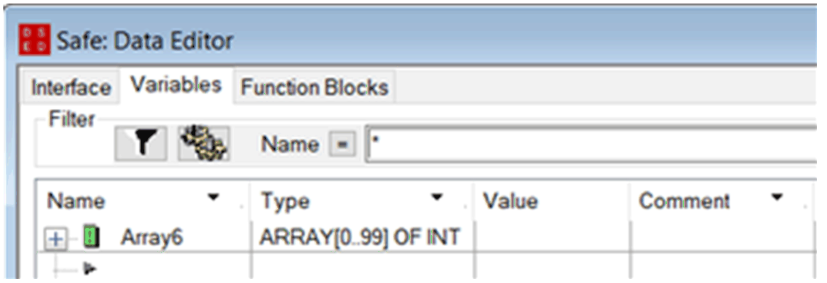
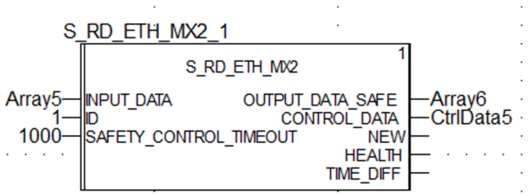
Element	Beschreibung
1	Nutzen Sie im Sender-PAC den **Prozessdateneditor**, um im Bereich „Schnittstelle“ ein Array mit 100 Ganzzahlen (Array2) zu erstellen. Erstellen Sie im selben **Prozessdateneditor** ein Array mit 4 Ganzzahlen (CtrlData2) als Ausgang im Bereich **Schnittstelle**. Die Steuerungsdaten vom Empfänger-PAC werden über den Modbus-Scanner in das Array CtrlData2 geschrieben, vorausgesetzt, das Array CtrlData2 befindet sich an der Adresse, die im Scanner des Sender-PAC definiert ist (in diesem Beispiel %MW100 - siehe Schritt 14): 
2	Verwenden Sie im Sender-PAC den **Sicherheitsdateneditor**, um ein anderes Array mit 100 Ganzzahlen (Array0) als Ausgang im Bereich **Schnittstelle** zu erstellen, und verknüpfen Sie dieses in der Spalte **Effektiv-Parameter** mit den in Schritt 1 oben erstellten process.Array2-Daten. Erstellen Sie im selben **Sicherheitsdateneditor** ein Array mit 4 Ganzzahlen (CtrlData0) als Eingang im Sicherheitsbereich **Schnittstelle** und verknüpfen Sie dieses in der Spalte **Effektiv-Parameter** mit den in Schritt 1 oben erstellten process.CtrlData2-Daten.

Ele-ment	Beschreibung
	 **HINWEIS:** Die Ganzzahlvariablen von Index 0 bis 90 des Arrays enthalten die Sicherheitsvariablenwerte, die Sie mit dem Empfänger-PAC austauschen möchten. Der verbleibende Bereich ist für automatisch erstellte Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Diagnosedaten werden vom Empfänger-PAC genutzt, um festzustellen, ob die übertragenen Daten sicher sind.
3	Konfigurieren Sie auf dem Sender-PAC den DFB `S_WR_ETH_MX2` in einer Section der SAFE-Task. Verbinden Sie den DFB mit Array0 und CtrlData0. 
4	Wählen Sie im **DTM-Browser** des Sender-PAC die CPU (in diesem Beispiel) oder ein NOC-Kommunikationsmodul aus (falls vorhanden). Klicken Sie dann auf **Hinzufügen...**, um einen Modbus-Scanner zu erstellen, der Daten vom Sender-PAC über Modbus-TCP an den Empfänger-PAC sendet: 

Element	Beschreibung
5	Wählen Sie **Modbus-Gerät** und klicken Sie auf **DTM hinzufügen**, um den Modbus-Scanner hinzuzufügen: 
6	Öffnen Sie das neu hinzugefügte Modbus-Gerät. Gehen Sie auf der Registerkarte **Request-Einstellungen** wie folgt vor: • Legen Sie den Wert in der Spalte **WR-Länge** auf 100 fest. Dies bezieht sich auf die Länge der zu schreibenden Daten. • Legen Sie den Wert in der Spalte **WR-Adresse** fest. Dabei handelt es sich um die Adresse, an die der Empfänger-PAC die erhaltenen Daten schreibt (in diesem Beispiel auf 0, sodass der Sender-PAC beim Wert %MW0 in der Tabelle des Empfänger-PAC mit dem Schreiben beginnt).

Element	Beschreibung
	
7	Wählen Sie den Knoten **Request 001: Elemente**. Definieren Sie auf der Registerkarte **Ausgang** den Arraytyp INT (d. h. ≥100 Ganzzahlen). Dabei handelt es sich um die Tabelle des Sender-PAC, die in den Empfänger-PAC geschrieben wird: 

Element	Beschreibung
8	Nachdem Sie die Konfiguration generiert und gespeichert haben, wird der Baustein (in diesem Beispiel BLOCKA_QI0_100) automatisch als Prozessvariable erstellt: 
9	Verwenden Sie auf dem Sender-PAC in einer Prozess-Code-Section einen DFB vom Typ `MOVE`, um die Inhalte des Arrays „tab_p“ in das oben definierte Array in der Modbus-Gerätestruktur zu kopieren: 
10	Nutzen Sie im Empfänger-PAC den **Sicherheitsdateneditor**, um ein Array mit 100 Ganzzahlen (Array5) im Bereich **Schnittstelle** zu erstellen. Erstellen Sie im selben **Sicherheitsdateneditor** ein Array mit 4 Ganzzahlen (CtrlData5) als Ausgang im Bereich **Schnittstelle**. 
11	Nutzen Sie im Empfänger-PAC den **Prozessdateneditor**, um ein Array mit 100 Ganzzahlen (Array3) als Ausgang im Bereich **Schnittstelle** zu erstellen. Verbinden Sie das Array Array3 mit dem Array Array5 (erstellt in Schritt 10). Dies geschieht in der Spalte **Effektiv-Parameter**. Die Steuerungsdaten vom Sender-PAC werden über den Modbus-Scanner in das Array Array3 geschrieben, vorausgesetzt, das Array Array3 befindet sich an der Adresse, die im Scanner des Sender-PAC definiert ist (in diesem Beispiel %MW0). Erstellen Sie im selben **Prozessdateneditor** ein Array mit 4 Ganzzahlen (CtrlData3) als Eingang im Bereich **Schnittstelle**. Verbinden Sie das Array CtrlData3 mit dem Array CtrlData5 (erstellt in Schritt 10). Dies geschieht in der Spalte **Effektiv-Parameter**.

Ele-ment	Beschreibung
	
12	Nutzen Sie im Empfänger-PAC den **Sicherheitsdateneditor**, um ein Array mit 100 Ganzzahlen (Array6) zu erstellen: 
13	Instanziieren Sie im Empfänger-PAC in einer Code-Section der SAFE-Task den DFB `S_RD_ETH_MX2` mit dem in Schritt 10 erstellten Array (Array5) als Eingangsparameter und mit den in Schritt 10 (CtrlData5) und in Schritt 12 (Array6) erstellten Arrays als Ausgangsparameter: 
14	Wiederholen Sie im Empfänger-PAC die Schritte 4 bis 9, um eine Kommunikation mit 4 Ganzzahlen zu konfigurieren und das Array CtrlData2 vom Empfänger- an den Sender-PAC zu senden. In diesem Beispiel müssen die CtrlData an der Adresse %MW100 in den Sender-PAC geschrieben werden.

Schwarzer Kanal/Peer-to-Peer

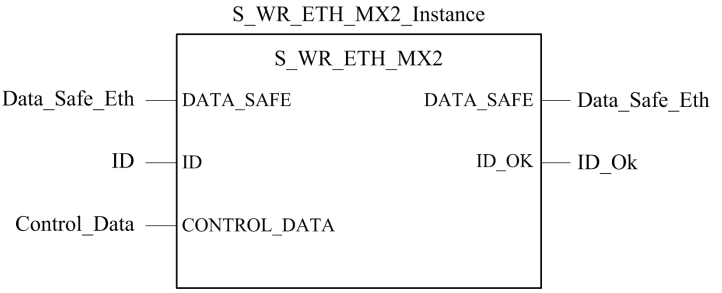
Jede Peer-to-Peer-Datenübertragung besteht aus *Benutzersicherheitsdaten*, in denen der anwendungsbezogene Inhalt übertragen wird, sowie *reservierten Daten*. Die *reservierten Daten* werden vom Sicherheits-PAC genutzt, um die Zuverlässigkeit der Übertragung sicherzustellen, damit die SIL3-Anforderungen erfüllt werden. Die *reservierten Daten* bestehen aus den folgenden Elementen:

- Eine CRC, die vom Sender-PAC aus den zu übertragenden Daten berechnet wird. Der Empfänger-PAC prüft die CRC, bevor er die übertragenen Daten nutzt.
- Eine Kommunikationskennung, die Teil der CRC-Berechnung ist, um Masquerading und Insertion-Angriffe während der Übertragung von Sicherheitsdaten zu vermeiden.
- Ein Zeitstempel mit der Zeit der Übertragung in ms. Mit einer CPU-Firmware ab Version 3.20 entspricht diese Stempelzeit dem von der Empfänger-CPU bereitgestellten sicheren Zeitwert. Der die Daten sendende Sender-PAC fügt den an den Empfänger-PAC gesendeten Daten einen Zeitwert hinzu. Der Empfänger-PAC vergleicht den empfangenen Zeitstempel mit seinem eigenen Zeitwert und geht damit wie folgt vor:
  - Er prüft das Alter der Daten.
  - Er weist doppelte Übertragungen zurück.
  - Er legt die chronologische Reihenfolge der empfangenen Übertragungen fest.
  - Er bestimmt die vergangene Zeit zwischen dem Empfang der einzelnen Datenübertragungen.

Konfiguration des DFB S_WR_ETH_MX2 in der Programmlogik des Sender-PAC

Darstellung

DFB-Darstellung:



Eine ausführliche Beschreibung dieses DFB finden Sie hier: *EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek*.

Beschreibung

Der DFB S_RD_ETH_MX2 gilt für PACs mit einer CPU-Firmware ab Version 3.20. Dieser DFB berechnet Daten (reservierte Daten mit CRC und Zeitstempel), die der Empfänger braucht, um Fehler zu prüfen und zu verwalten, die während der sicheren Peer-to-Peer-Kommunikation auftreten.

Der DFB `S_WR_ETH_MX2` muss bei jedem Zyklus im Sender-PAC aufgerufen werden. Innerhalb des Zyklus muss er in der Logik ausgeführt werden, nachdem an den zu sendenden Daten alle erforderlichen Änderungen vorgenommen wurden. Das heißt, dass während des Zyklus die zu sendenden Daten nach der Ausführung des DFB nicht geändert werden dürfen, da andernfalls die im reservierten Datenbereich verwendeten CRC-Informationen nicht korrekt sind und die sichere Peer-to-Peer-Kommunikation fehlschlägt.

Sie müssen dem Parameter `ID` einen eindeutigen Wert zuweisen, mit dem die sichere Peer-to-Peer-Kommunikation zwischen Sender und Empfänger identifiziert wird.

⚠WARNUNG

SICHERHEITSFUNKTIONEN KÖNNEN NICHT MEHR AUSGEFÜHRT WERDEN

Der Wert des Parameters `ID` muss eindeutig und im Netzwerk für ein Sender/Empfänger-Paar festgelegt sein.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Beschreibung des Arrays `DATA_SAFE`

Verwenden Sie die Registerkarte **Schnittstelle** sowohl im **Sicherheitsdateneditor** als auch im **Prozessdateneditor** in , um die Verbindung zwischen den Prozessvariablen und den Sicherheitsvariablen herzustellen.Control Expert

Die Verbindung von Sicherheits- und Prozessvariablen auf diese Weise ermöglicht das Folgende:

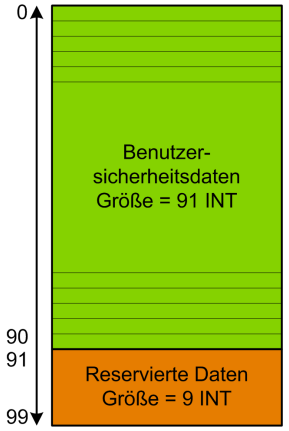
- Übertragung des Werts von Sicherheitsvariablen auf Prozessvariablen über verbundenen globale Variablen.
- Senden der variablen Werte des Prozessbereichs der sendenden PAC zum Prozessbereich der empfangenden PAC mittels expliziter Nachrichtenübertragung über Modbus TCP.

Das Array `DATA_SAFE` besteht aus zwei Bereichen:

- Die Zone **Benutzersicherheitsdaten** enthält die Daten des Sicherheitsspeicherbereichs der PAC. Dieser Bereich startet bei Index 0 und endet bei Index 90.
- Die Zone **Reservierte Daten** ist für automatisch erstelle Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Daten werden von der empfangenden PAC verwendet, um zu bestimmen, ob die in der Zone **Benutzersicherheitsdaten** enthaltenen Daten sicher sind. Dieser Bereich startet bei Index 91 und endet bei Index 99.

  HINWEIS: Führen Sie in der Zone **Reservierte Daten** keinen Schreibvorgang durch.

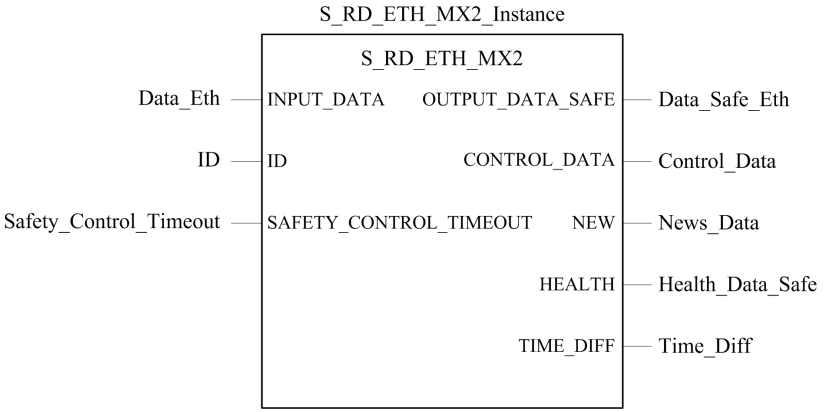
Darstellung der Struktur des Arrays `DATA_SAFE` (Array[0..99] of INT):



Konfigurieren des DFB S_RD_ETH_MX2 in der Programmlogik des Empfänger-PAC

Darstellung

DFB-Darstellung:



Eine ausführliche Beschreibung dieses DFB finden Sie hier: *EcoStruxure™ Control Expert – Sicherheit, Bausteinbibliothek*.

Beschreibung

Der DFB S_RD_ETH_MX2 gilt für PACs mit einer CPU-Firmware ab Version 3.20. Er kopiert die im Prozessbereich empfangenen Daten in den Sicherheitsbereich und prüft deren Genauigkeit.

⚠WARNUNG

VERLUST DER FÄHIGKEIT ZUR AUSFÜHRUNG VON SICHERHEITSFUNKTIONEN

- Der DFB `S_RD_ETH_MX2` muss in jedem Zyklus in der Programmlogik des Empfänger-PAC aufgerufen werden. Er muss ausgeführt werden, bevor die Daten im Zyklus genutzt werden.
- Der Wert des Parameters `ID` muss eindeutig und im Netzwerk für ein Sender/Empfänger-Paar festgelegt sein.
- Sie müssen den Wert des `HEALTH`-Bits des DFB `S_RD_ETH_MX2` in jedem Zyklus testen, bevor Sie sichere Daten zur Verwaltung der Sicherheitsfunktion nutzen.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Der Funktionsbaustein `S_RD_ETH_MX2` geht wie folgt vor:

- Er kopiert die im Register `INPUT_DATA` empfangenen Daten in das Register `OUTPUT_DATA_SAFE`, falls diese die folgenden Tests bestehen:
  - Er überprüft die CRC des zuletzt empfangenen Datenpakets, mittels E/A-Scanner über Ethernet (Modbus TCP). Wenn die CRC nicht korrekt ist, werden die Daten als unsicher betrachtet und nicht in das Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs geschrieben.
  - Der Funktionsbaustein überprüft die letzten empfangenen Daten, um zu bestimmen, ob diese aktueller sind als die Daten, die bereits im Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs geschrieben sind (durch Vergleich des Zeitstempels). Wenn die zuletzt empfangenen Daten nicht aktueller sind, werden sie nicht in das Register `OUTPUT_DATA_SAFE` des Sicherheitsspeicherbereichs kopiert.
- Er prüft das Alter der Daten im Sicherheitsspeicherbereich. Wenn die Daten älter sind als der maximal konfigurierbare Wert, der im Eingangsregister `SAFETY_CONTROL_TIMEOUT` eingestellt wurde, werden die Daten als unsicher deklariert und das `HEALTH`-Bit wird auf 0 gesetzt.

  HINWEIS: Das Datenalter ist der Zeitunterschied zwischen dem Zeitpunkt, zu dem die Daten auf dem Sender-PAC berechnet wurden, und dem Zeitpunkt, zu dem die Daten im Empfänger-PAC geprüft werden.

  Wenn das `HEALTH`-Bit auf 0 gesetzt wird, werden die im Array `OUTPUT_DATA_SAFE` verfügbaren Daten als unsicher betrachtet. Reagieren Sie in diesem Fall angemessen.

Beschreibung der Arrays `INPUT_DATA` und `OUTPUT_DATA_SAFE`

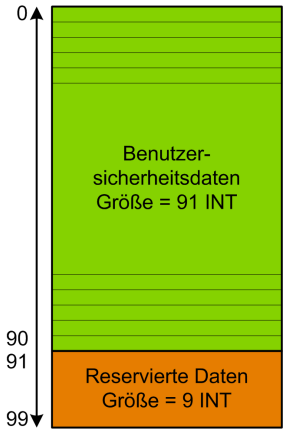
Das Array `INPUT_DATA` besteht aus Daten aus dem Prozessdatenspeicherbereich. Das Array `OUTPUT_DATA_SAFE` besteht aus Sicherheitsvariablen. Verwenden Sie die Registerkarten **Sicherheitsdateneditor** und **Prozessdateneditor** in Control Expert, um die Verbindung zwischen den Prozessvariablen und den Sicherheitsvariablen herzustellen.

Die Arrays INPUT_DATA und OUTPUT_DATA_SAFE bestehen aus zwei Bereichen:

- Der Bereich für **Benutzersicherheitsdaten** enthält die Benutzerdaten. Dieser Bereich startet bei Index 0 und endet bei Index 90.
- Die Zone **Reservierte Daten** ist für automatisch erstellte Diagnosedaten reserviert und verwendet die CRC und den Zeitstempel. Diese Daten werden vom empfangenden PAC verwendet, um zu bestimmen, ob die in der Zone **Benutzersicherheitsdaten** enthaltenen Daten sicher sind. Dieser Bereich startet bei Index 91 und endet bei Index 99.

  HINWEIS: Das Ausführen eines Schreibvorgangs im Bereich **Reservierte Daten** wird nicht empfohlen, da auf diese Weise automatisch erstellte Diagnosedaten überschrieben werden.

Darstellung der Struktur der Arrays INPUT_DATA und OUTPUT_DATA_SAFE (Array[0..99] of INT):



Beschreibung des Arrays CONTROL_DATA

Das Array CONTROL_DATA muss mit Variablen im globalen Bereich verknüpft werden (definiert über die Sicherheitsdatenschnittstelle). Anschließend müssen die globalen Variablen mit lokalisierten Variablen (definiert über die Prozessdatenschnittstelle) im Prozessbereich verknüpft werden, damit die Daten vom E/A-Scanner an den entsprechenden Sender übertragen werden.

Berechnung des Werts SAFETY_CONTROL_TIMEOUT

Berücksichtigen Sie beim Berechnen des Werts SAFETY_CONTROL_TIMEOUT das Folgende:

- Minimalwert: SAFETY_CONTROL_TIMEOUT >2 * T1
- Empfohlener Wert: SAFETY_CONTROL_TIMEOUT > 3 * T1

T1 = CPU_{Sender} MAST-Zykluszeit + CPU_{Sender} SAFE-Zykluszeit + Wiederholungsrate + Netzwerkübertragungszeit + $CPU_{Empfänger}$ MAST-Zykluszeit + $CPU_{Empfänger}$ SAFE-Zykluszeit

Hierbei gilt:

- *CPU_{Sender} MAST-Zykluszeit* ist die MAST-Zykluszeit des Sender-PAC.
- *CPU_{Sender} SAFE-Zykluszeit* ist die SAFE-Zykluszeit des Sender-PAC.
- *Wiederholungsrate* ist die Zeit für die Schreibanfrage des E/A-Abfragegeräts vom Sender-PAC zum Empfänger-PAC.
- *Netzwerkübertragungszeit* ist die im Ethernet-Netzwerk verwendete Zeit für die Datenübertragung vom Sender-PAC zum Empfänger-PAC.
- *$CPU_{Empfänger}$ MAST-Zykluszeit* ist die MAST-Zykluszeit des Empfänger-PAC.
- *$CPU_{Empfänger}$ SAFE-Zykluszeit* ist die SAFE-Zykluszeit des Empfänger-PAC.

Beachten Sie, dass der für den Parameter SAFETY_CONTROL_TIMEOUT definierte Wert eine direkte Wirkung auf die Stabilität und Verfügbarkeit der sicheren Peer-to-Peer-Kommunikation hat. Wenn der Parameterwert SAFETY_CONTROL_TIMEOUT sehr viel größer als T1 ist, kann die Übertragung verschiedene Verzögerungen (wie Netzwerkverzögerungen) oder beschädigte Datenübertragungen tolerieren.

Sie tragen die Verantwortung für die Konfiguration Ihres Ethernet-Netzwerks, damit die Last während der Datenübertragung keine übermäßigen Verzögerungen auf dem Netzwerk verursacht, da dies zu einem Ablauf des Timeouts führen kann. Ziehen Sie ein dediziertes Ethernet-Netzwerk für sichere Peer-to-Peer-Protokolle in Betracht, um Ihre sichere Peer-to-Peer-Kommunikation vor übermäßigen Verzögerungen durch die gleichzeitige Übertragung nicht-sicherer Daten auf demselben Netzwerk zu schützen.

Bei der Inbetriebnahme Ihres Projekts müssen Sie die Leistung der sicheren Peer-to-Peer-Kommunikation schätzen, indem Sie die Werte im Ausgangsparameter TIME_DIFF überprüfen und die Marge mithilfe des im Parameter SAFETY_CONTROL_TIMEOUT definierten Werts prüfen.

Informationen zum HEALTH-Bit

Wenn der Wert des HEALTH -Bit dem Folgenden entspricht:

- 1: Die Integrität der Daten ist korrekt (CRC) und das Alter der Daten ist kleiner als der im Eingangsregister SAFTETY_CONTROL_TIMEOUT eingestellte Wert.

  HINWEIS: Das Alter der Daten ist die Zeit zwischen:

  - Dem Start des Zyklus, wenn die Daten im Sender-PAC berechnet werden.
  - Dem Start des Zyklus, wenn die Daten im Empfänger-PAC überprüft werden.

- 0: Neue gültige Daten werden im erforderlichen Zeitintervall nicht empfangen (der Timer läuft ab und das `HEALTH`-Bit wird auf 0 gesetzt).

  HINWEIS: Wenn das `HEALTH`-Bit auf 0 gesetzt wird, werden die Daten im Ausgangsarray `OUTPUT_DATA_SAFE` als unsicher betrachtet. Reagieren Sie angemessen.

M580-Kommunikation über schwarze Kanäle

Schwarzer Kanal

Ein schwarzer Kanal ist ein Mechanismus zur Verschlüsselung und Prüfung übertragener Sicherheitsdaten:

- Nur Sicherheitsgeräte von Schneider Electric können die Daten verschlüsseln und entschlüsseln, die über den schwarzen Kanal in einem M580-Sicherheitssystem gesendet werden.
- Der Zustand der Übertragungen wird für jede gesendete Nachricht vom sendenden und empfangenen Sicherheitsmodul überprüft.

Durch Verwendung eines schwarzen Kanals wird es möglich, Sicherheitsdaten über zwischengeschaltete nicht-sichere Geräte zu senden, z. B. Baugruppenträger, Ethernet-Verbindungen oder Kommunikationsadapter. Da Übertragungen über schwarze Kanäle verschlüsselt sind, können die zwischengeschalteten Geräte den Inhalt nicht unerkannt lesen oder verändern.

Übertragungen über einen schwarzen Kanal funktionieren unabhängig vom verwendeten Kommunikationsprotokoll:

- X Bus ist das Protokoll für Baugruppenträger-Übertragungen zwischen Sicherheitsgeräten in demselben Rack (z. B. von CPU zu lokalem E/A oder von dezentralem Kommunikationsadapter (CRA) zu lokalem E/A).
- Ethernet/IP ist das Protokoll für Datenübertragungen zwischen Racks (z. B. von der CPU zu einem CRA-Modul).

E/A-Sicherheitsmodule und die CPU können Kommunikation über schwarze Kanäle senden und empfangen. Bei jeder Übertragung fügt das übertragende Gerät (CPU oder E/A) der Nachricht die folgenden Informationen hinzu:

- Ein CRC-Tag zur Aktivierung eines Nachrichteninhaltstests.
- Einen Zeitstempel zur Aktivierung eines Tests der Nachrichtenpünktlichkeit.
- Weitere Informationen – einschließlich Anwendungsversion und E/A-Konfiguration –, mit denen das E/A-Modul bei der Übertragung identifiziert wird.

Mit einer CPU-Firmware bis Version 3.10 muss die CPU bei Verwendung von E/A-Sicherheitsmodulen in einem dezentralen Rack entweder als NTP-Client oder NTP-Server konfiguriert werden.

Wenn keine dieser Konfigurationen implementiert wird, werden die Zeiteinstellungen der E/A-Sicherheitsmodule und der CPU nicht synchronisiert. Die Kommunikation über schwarze Kanäle funktioniert dann nicht. Die Ein- und Ausgänge der E/A-Sicherheitsmodule in RIO-Stationen gehen in den sicheren (entregten) Zustand bzw. in den Fehlerausweichzustand über.

⚠VORSICHT

GEFAHR EINES UNBEABSICHTIGTEN BETRIEBS

Wenn Sie E/A-Sicherheitsmodule in einer RIO-Station installieren, muss für den PAC mit einer CPU-Firmware bis Version 3.10 die aktuelle Zeit konfiguriert werden. Aktivieren Sie den NTP-Dienst für Ihr M580-System und konfigurieren Sie die Sicherheits-CPU als NTP-Server oder -Client.

Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.

Das Empfängergerät (E/A oder CPU) verschlüsselt die Nachricht und testet die Übereinstimmung des Inhalts. Die folgenden Probleme können erkannt werden:

Problem	Beschreibung
Übertragungsfehler	Es ist ein Fehler in der Nachrichtenadresse oder -weiterleitung aufgetreten.
Wiederholungen	Die Nachricht wurde mehrfach gesendet.
Gelöschte Daten	Ein Teil der Nachricht oder die ganze Nachricht fehlt.
Eingefügte Daten	Der Nachricht wurden zusätzliche Daten hinzugefügt.
Datenreihenfolge falsch	Die Reihenfolge der Nachricht wurde geändert.
Beschädigte Daten	In der Nachricht wurde mindestens ein Bitfehler erkannt.
Verzögerungen	Die Lieferzeit der Nachricht ist zu lang.
Masquerading	Die Nachrichtenquelle darf keine Daten senden.

Wenn diese Fehler entdeckt werden, wird der Kanal als fehlerhaft angesehen. Es werden die entsprechenden Sicherheitsfunktionen ausgeführt:

- Wenn die CPU erkennt, dass eine Übertragung von einem Eingangsmodul fehlerhaft ist, setzt die CPU die Eingangswerte dieses Moduls in den sicheren (entregten) Zustand bzw. in den Fehlerausweichzustand.
- Wenn ein Ausgangsmodul erkennt, dass eine Übertragung von der CPU fehlerhaft ist, wird die Ausgänge in den vorkonfigurierten Fehlerausweichzustand gesetzt.

Die Ausgänge gehen automatisch in den von der CPU angeforderten Zustand über, sobald die Kommunikation zwischen CPU und Ausgangsmodul ordnungsgemäß wiederhergestellt wurde.

HINWEIS

UNVERWARTETE ÄNDERUNG DES AUSGANGSZUSTANDS BEI WIEDERHERSTELLUNG DER KOMMUNIKATION

Die Programmlogik muss den Funktionsfähigkeitsstatus der Ausgangskanäle überwachen und die Sicherheitsfunktion durch Setzen der Ausgangsbefehle in den sicheren Zustand entsprechend aktivieren.

Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.

Kommunikation zwischen M580-CPU und E/A-Sicherheitsmodul

Einführung

In diesem Abschnitt wird die Kommunikation zwischen M580-Sicherheits-CPU und E/A-Sicherheitsmodulen erläutert.

Kommunikation zwischen M580 -Sicherheits-PAC und den E/A

Kommunikation zwischen PAC und E/A

Die M580-Sicherheits-CPU und der -Koprozessor steuern gemeinsam den gesamten Datenaustausch des Baugruppenträgers, während die Sicherheits-E/A auf die Befehle der CPU und des Koprozessors reagieren. E/A-Sicherheitsmodule können in einem X Bus-Rack vom Typ BMXXBP•••• oder in einem Ethernet-Rack vom Typ BMEXBP•••• untergebracht werden.

Die Kommunikation zwischen dem Sicherheits-PAC und den E/A-Sicherheitsmodulen im lokalen Hauptrack erfolgt über die Bauträgergruppe.

Die Kommunikation zwischen dem Sicherheits-PAC und den in einer RIO-Station installierten E/A-Sicherheitsmodulen erfolgt über ein Adaptermodul in der RIO-Station:

- Ein Adapter vom Typ BMECRA31210 für ein Ethernet-Rack
- Ein Adapter vom Typ BMXCRA31210 für ein X-Bus-Rack

  HINWEIS: Mit einer CPU-Firmware ab Version 3.20 benötigt das Adaptermodul BM•CRA31210 eine Firmware ab Version 2.60.

  HINWEIS: Ein Adapter vom Typ BMXCRA31200 kann nicht genutzt werden, um die E/A-Sicherheitsmodule mit dem M580-Sicherheits-PAC zu verbinden.

Die Kommunikation zwischen dem Sicherheits-PAC und den E/A-Sicherheitsmodulen im lokalen Hauptrack und in einer RIO-Station verläuft über einen Black Channel, Seite 216.

Wie die Zeiteinstellungen der CPU und der E/A-Sicherheitsmodule synchronisiert werden, ist von der Version der CPU-Firmware abhängig:

- Bei PACs mit einer CPU-Firmware bis V3.10 muss der NTP-Dienst konfiguriert werden.

  HINWEIS: Wenn Sie E/A-Sicherheitsmodule in einem lokalen Rack (oder in einer Erweiterung des lokalen Racks) installieren, muss der NTP-Dienst nicht aktiviert werden.

- Bei PACs mit einer CPU-Firmware ab V3.20 basiert die sichere Zeitsynchronisation auf einer internen und „monotonen“ Zeituhr.

Detaillierte Informationen finden Sie im Kapitel *Zeitsynchronisation*, Seite 180.

Optional können Sie Glasfaser-Repeater-Module vom Typ BMXNRP0200 oder BMXNRP0201 einsetzen, um die physische Verbindung zwischen CPU und Koprozessor im lokalen Rack und dem Adapter in der RIO-Station zu verstärken. Glasfaser-Repeater-Module sorgen für eine verbesserte Störfestigkeit des RIO-Netzwerks und unterstützen längere Kabelstrecken. Gleichzeitig bleiben der volle Dynamikbereich des Netzwerks und das Sicherheitsintegritäts-Level gewährleistet.

Das Kommunikationsprotokoll zwischen E/A-Sicherheitsmodul und PAC gewährleistet den Datenaustausch. Dadurch können beide Geräte die Genauigkeit der empfangenen Daten prüfen, beschädigte Daten und Betriebsstörungen des übertragenden Moduls erkennen. Dementsprechend kann eine Sicherheitsschleife nicht-störende, Seite 29 RIO-Adapter und einen Baugruppenträger umfassen.

Spannungsversorgung für das E/A-Sicherheitsmodul

Das E/A-Sicherheitsmodul erhält über den Baugruppenträger 24-VDC- und 3,3-VDC-Spannung vom M580-Sicherheitsspannungsversorgungsmodul, Seite 131. Das Sicherheitsspannungsversorgungsmodul überwacht die bereitgestellte Spannung, damit 36 VDC nicht überschritten werden.

Spannung für nicht-sichere Funktionen:

Jedes E/A-Sicherheitsmodul wendet 5-VDC-Spannung vom Baugruppenträger auf seine nicht-sicheren Funktionen an.

Externe Spannungsversorgung für das digitale E/A-Sicherheitsmodul:

Eine externe Spannungsversorgung von maximal 60 VDC ist für nicht-sichere Prozesse (Sensor, Aktor) erforderlich und kann eine geschützte Kleinspannungsversorgung (SELV/PELV) der Kategorie II sein. Die Spannungsversorgung für die nicht-sicheren Prozesse wird vom E/A-Sicherheitsmodul auf Über- und Unterspannung überwacht.

Diagnose eines M580-Sicherheitssystems

Inhalt dieses Kapitels

Einführung

Dieses Kapitel enthält Informationen zur Diagnose eines M580-Sicherheitssystems, die nach Bedarf anhand der Hardware-LED-Anzeigen (LED-Status) und der Systembits oder -wörter durchgeführt werden kann.

Diagnose von M580-Sicherheits-CPU und -Coprozessor

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für die Sicherheits-CPUs des BME•58•040S und für den Sicherheits-Coprozessor des BMEP58CPROS3 beschrieben.

Blockierendes Verhalten – Diagnose

Einführung

Blockierendes Verhalten, das während Ausführung des Sicherheits- oder Prozessprogramms auftritt, ergibt sich aus der Erkennung von Systemfehlern oder aus dem HALT-Zustand einer Task, in der der Fehler entdeckt wurde.

HINWEIS: Der M580-Sicherheits-PAC verfügt über zwei unabhängige HALT-Zustände:

- Der Prozess-HALT gilt für nicht-SAFE-Tasks (MAST, FAST, AUX0 und AUX1). Sobald eine Prozesstask in den HALT-Zustand übergeht, gehen alle anderen Prozesstasks ebenfalls in den HALT-Zustand über.
- Ein SAFE-HALT bezieht sich ausschließlich auf die SAFE-Task.

Eine Beschreibung der Zustände HALT und STOP finden Sie unter *M580-Sicherheits-PAC – Betriebszustände*, Seite 269.

Diagnose

Wenn die CPU ein blockierendes Verhalten erkennt, das zu einem Systemfehler führt, wird eine Beschreibung des erkannten Fehlers in Systemwort `%SW124` aufgeführt.

Wenn die CPU ein blockierendes Verhalten erkennt, das zu einem HALT-Zustand führt, wird eine Beschreibung des erkannten Fehlers in Systemwort `%SW125` aufgeführt.

Werte des Systemworts `%SW124` und die Beschreibung des entsprechenden blockierenden Verhaltens:

Wert von `%SW124` (hex.)	**Beschreibung des blockierenden Verhaltens**
5AF2	RAM-Fehler bei Speicherprüfung
5AFB	Fehler im Code der Sicherheitsfirmware
5AF6	Überlauf des Sicherheitswatchdogs in der CPU

Wert von %SW124 (hex.)	Beschreibung des blockierenden Verhaltens
5AFF	Überlauf des Sicherheitswatchdogs im Coprozessor
5B01	Coprozessor beim Start nicht erkannt

Werte des Systemworts %SW125 und die Beschreibung des entsprechenden blockierenden Verhaltens:

Wert von %SW125 (hex.)	Beschreibung des blockierenden Verhaltens
0•••	Ausführung einer unbekannten Funktion
0002	Signaturfunktion der SD-Karte (verwendet mit den Funktionen *SIG_CHECK* und *SIG_WRITE*)
2258	Ausführung der Anweisung HALT
2259	Ausführungsfluss anders als Referenzfluss
23••	Ausführung einer CALL-Funktion für ein nicht definiertes Unterprogramm
5AF3	Vergleichsfehler von CPU erkannt
5AF9	Anweisungsfehler beim Hochfahren oder während der Laufzeit
5AFA	Vergleichsfehler in CRC-Wert
5AFC	Vergleichsfehler vom Coprozessor erkannt
5AFD	Interner Fehler vom Coprozessor erkannt; Sub-Code in %SW126: 1 (unbekanntes Ergebnis), 2 (CRC-Anwendung), 7 (falscher Aktivitätszähler)
5AFE	Coprozessor-Synchronisierungsfehler erkannt – nur CPU; Sub-Code in %SW126: 3 (Diagnose), 4 (UL Ende), 5 (Vergleich), 6 (BC aus), 8 (HALT bei UL), 9 HALT während Vergleich), 10 (HALT bei BC aus).
81F4	SFC-Knoten falsch
82F4	SFC-Code nicht abrufbar
83F4	SFC-Arbeitsbereich nicht zugänglich
84F4	Zu viele SFC-Initialschritte
85F4	Zu viele aktive SFC-Schritte
86F4	SFC-Sequenzcode falsch
87F4	SFC-Codebeschreibung falsch
88F4	SFC-Referenztabelle falsch
89F4	Interner SFC-Indexberechnungsfehler
8AF4	SFC-Schrittzustand nicht verfügbar
8BF4	SFC-Speicher wegen Änderung nach Download zu klein

Wert von %SW125 (hex.)	Beschreibung des blockierenden Verhaltens
8CF4	Transitions-/Aktionsbereich nicht zugänglich
8DF4	SFC-Arbeitsbereich zu klein
8EF4	Version des SFC-Codes älter als Interpretierer
8FF4	Version des SFC-Codes jünger als Interpretierer
90F4	Fehlerhafte Beschreibung eines SFC-Objekts: NULL-Zeiger
91F4	Aktionsbezeichner nicht zulässig
92F4	Fehlerhafte Definition der Zeit für einen Aktionsbezeichner
93F4	Makroschritt in der Liste der aktiven Schritte für die Deaktivierung nicht gefunden
94F4	Überlauf in der Aktionstabelle
95F4	Überlauf in der Schrittaktivierungs-/-deaktivierungstabelle
9690	Fehler in der CRC-Prüfsumme der Anwendung
DE87	Berechnung hat Gleitkommafehler erkannt
DEB0	Task-Watchdog-Überlauf (%S11 und %S19 sind festgelegt)
DEF0	Division durch 0
DEF1	Fehler bei der Zeichenfolgeübertragung
DEF2	Kapazität überschritten
DEF3	Index-Überlauf
DEF4	Inkonsistente Taskdauer
DEF7	SFC-Ausführungsfehler
DEFE	SFC-Schritte nicht definiert

Neustarten der Anwendung

Nach Auftreten eines blockierenden Verhaltens müssen die gestoppten Tasks initialisiert werden. Ein HALT kann aus verschiedenen Gründen auftreten:

- Wenn er aufgrund einer Prozesstask (MAST, FAST, AUX0 oder AUX1) auftritt, geschieht die Initialisierung über den Control Expert-Befehl **SPS > Init** oder durch Setzen des Bits %S0 auf 1.
- Wenn er aufgrund einer SAFE-Task auftritt, geschieht die Initialisierung über den Control Expert-Befehl **SPS > Sicherheit init.**.

Bei der Initialisierung verhält sich die Anwendung folgendermaßen:

- Die Daten nehmen ihre Initialwerte an.

- Die Tasks werden am Ende des Zyklus gestoppt.
- Das Abbild der Eingänge wird aktualisiert.
- Die Ausgänge werden in die Fehlerposition gesetzt.

Mit dem RUN-Befehl kann die Anwendung bzw. können die Tasks dann neu gestartet werden.

Nicht blockierendes Verhalten – Diagnose

Einführung

Das System wechselt in ein nicht blockierendes Verhalten, wenn es auf dem Baugruppenträger-Bus (X Bus oder Ethernet) des Racks einen Ein-/Ausgangsfehler erkennt oder durch die Ausführung einer Anweisung, die von einem Anwenderprogramm bearbeitet werden kann und keine Änderung des CPU-Zustands bewirkt.

Im Folgenden werden einige der Systembits und -wörter beschrieben, mit denen Sie den Zustand des Sicherheitssystems und seiner Komponentenmodule diagnostizieren können.

HINWEIS: Die verfügbaren Systembits und -wörter enthalten nicht alle Informationen zum Zustand der Sicherheitsmodule. Schneider Electric empfiehlt, die DDDT-Struktur der Sicherheits-CPU und E/A-Sicherheitsmodule zu verwenden, um den Zustand des M580-Sicherheitssystems zu diagnostizieren.

Informationen zum M580-Sicherheits-CPU-DDDT finden Sie unter *Eigenständige DDT-Datenstruktur für M580-CPUs* im *Hardware-Referenzhandbuch für Modicon M580*.

Informationen zu den M580-E/A-Sicherheitsmodul-DDDTs finden Sie in den folgenden Abschnitten:

- BMXSAI0410-Datenstruktur, Seite 60 für das analoge Sicherheitseingangsmodul
- BMXSDI1602-Datenstruktur, Seite 94 für das digitale Sicherheitseingangsmodul
- BMXSDO0802-Datenstruktur, Seite 109 für das digitale Sicherheitsausgangsmodul
- BMXSRA0405-Datenstruktur, Seite 126 für das digitale Sicherheitsrelaisausgangsmodul

HINWEIS: Weitere Diagnostik geschieht über Ethernet-Geräte und explizite Nachrichtenübertragung. Dafür stehen folgende Möglichkeiten zur Verfügung:

- Funktionsbaustein READ_VAR (siehe EcoStruxure™ Control Expert, Kommunikation, Bausteinbibliothek) für Modbus-TCP-Geräte
- Funktionsbaustein DATA_EXCH (siehe Modicon M580, Hardware, Referenzhandbuch), mit Festlegung des CIP-Protokolls im ADDM-Baustein, für Ethernet/IP-Geräte

Verhalten in Verbindung mit der E/A-Diagnose

Ein E/A-spezifisches, nicht blockierendes Verhalten kann anhand folgender Anzeigen diagnostiziert werden:

- LED-Muster CPU-**I/O**: permanent EIN
- LED-Muster **I/O**-Modul: permanent EIN
- Systembits (Fehlertyp):
  - `%S10` auf 0: Globaler E/A-Fehler auf einem der Module im lokalen oder dezentralen Ethernet- oder X-Bus-Rack
  - `%S16` auf 0: E/A-Fehler in der aktuellen Task auf einem X-Bus-Rack
  - `%S40` bis `%S47` auf 0: E/A-Fehler auf einem X-Bus-Rack auf Adresse 0 bis 7
  - `%S117` auf 0: RIO-Fehler auf einem dezentralen X-Bus-Rack
  - `%S119` auf 0: E/A-Fehler auf einem lokalen X-Bus-Rack

    HINWEIS: Diese Bits (`%S10`, `%S16`, `%S40`...`%S47`, `%S117` und `%S119`) melden viele – allerdings nicht alle – der möglichen erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.
- Systembits und -wörter in Verbindung mit dem fehlerhaften Kanal (E/A-Kanalnummer und Fehlertyp) oder Informationen im I/O des Device DDT-Moduls (für im Device DDT-Adressierungsmodus konfigurierte Module):
  - Bit `%Ir.m.c.ERR` auf 1 gesetzt. Kanalfehler (impliziter Austausch).
  - Wort `%MWr.m.c.2`: Der Wert des Worts verweist auf den Typ des im angegebenen Kanal erkannten Fehlers und ist vom E/A-Modul abhängig (impliziter Austausch).

Verhalten in Verbindung mit der Ausführung der Diagnoseprogramms

Ein nicht blockierendes Verhalten in Verbindung mit der Programmausführung kann anhand folgender Systembits und -wörter diagnostiziert werden:

- Systembits (Fehlertyp):
  - %S15 auf 1 gesetzt: Fehler bei der Bearbeitung der Zeichenfolgen.
  - %S18 auf 1 gesetzt: Kapazitätsüberlauf, Fehler in Bezug auf Gleitkomma oder Division durch 0.

    (Siehe *Systembits für die Ausführung der SAFE-Task*, Seite 411.)

    Wenn %S18 auf 1 gesetzt ist, enthält %SW17 eine Beschreibung des verursachenden Ereignisses, Seite 414.
  - %S20 auf 1 gesetzt: Index-Überlauf.

    HINWEIS: Wenn das konfigurierbare Systembit %S78 im Programm festgelegt ist, wechselt die SAFE-Task in den HALT-Zustand, wenn das Systembit %S18 auf 1 gesetzt wird.
- Systemwort (Art des erkannten Fehlers):
  - %SW125 (siehe Modicon M580, Hardware, Referenzhandbuch) (immer aktualisiert)

LED-Diagnose der M580-Sicherheits-CPU

CPU-LEDs

Mit den LEDs an der Vorderseite der CPU (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) lässt sich der Zustand des PAC wie nachstehend beschrieben diagnostizieren.

Informationen zur Diagnose redundanzbezogener LEDs, einschließlich **[A]**, **[B]**, **[PRIM]**, **[STBY]** und **[REMOTE RUN]**, finden Sie im *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen* im Kapitel LED-Diagnose für M580 Hot Standby-CPUs.

HINWEIS: LEDs sind keine zuverlässigen Indikatoren und garantieren nicht die Bereitstellung präziser Informationen. Sie sollten LEDs deshalb nur zu allgemeinen Diagnosezwecken bei der Inbetriebnahme und Fehlersuche heranziehen.

⚠ WARNUNG
GEFAHR EINER UNPRÄZISEN SYSTEMDIAGNOSE Setzen Sie LEDs nicht als Betriebsindikatoren ein. **Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.**

PAC-Zustand	Namen und Farben der LEDs:							
	RUN	ERR	IO[1]	ETH MS	ETH NS	DL	SRUN	SMOD
	Grün	Rot	Rot	Grün/Rot	Grün/Rot	Grün	Grün	Grün
Spannung AUS								
Spannung EIN • Selbsttest								
Nicht konfiguriert					 Kein Kabel ange-schlossen und mit einem anderen aktiven Gerät verbun-den  Andern-falls			
Konfiguriert: • Kein externer Fehler erkannt							–	–
• Externer Fehler erkannt				–	–		–	–
• Kein Ethernet-Link, inkl. Ethernet-Baugrup-penträger							–	–
• Doppelte IP-Adresse			–				–	–

PAC-Zustand	Namen und Farben der LEDs:							
	RUN	ERR	IO[1]	ETH MS	ETH NS	DL	SRUN	SMOD
	Grün	Rot	Rot	Grün/Rot	Grün/Rot	Grün	Grün	Grün
• STOP-Zustand			 Fehler in E/A-Modul, Kanal oder Konfiguration erkannt  Kein Fehler an konfiguriertem Ein-/Ausgang erkannt		 Nicht angeschlossen  Verbunden  Kein Kabel		 SAFE-Task wird ausgeführt ODER  SAFE-Task wurde angehalten	 Sicherheitsmodus ODER  Wartungsmodus
• RUN-Zustand			–		 Nicht angeschlossen  Verbunden  Kein Kabel		 SAFE-Task wird ausgeführt ODER  SAFE-Task wurde angehalten	 Sicherheitsmodus ODER  Wartungsmodus
HALT-Zustand (behebbarer Fehler erkannt)			–				 SAFE-Task wird ausgeführt	 Sicherheitsmodus

PAC-Zustand	Namen und Farben der LEDs:							
	RUN	ERR	IO[1]	ETH MS	ETH NS	DL	SRUN	SMOD
	Grün	Rot	Rot	Grün/Rot	Grün/Rot	Grün	Grün	Grün
							 SAFE-Task wurde angehalten	 Wartungsmodus
SAFE-Zustand (nicht behebbarer Fehler erkannt)								
Aktualisierung des Betriebssystems								

1. Nicht alle Fehler eines E/A-Sicherheitsmoduls werden über die LEDs gemeldet. Wenn Sie weitere Informationen benötigen, überprüfen Sie die DDDTs der E/A-Sicherheitsmodule.

Legende:

Symbol	Beschreibung	Symbol	Beschreibung	Symbol	Beschreibung
	Leuchten Grün		Leuchten Rot		AUS
	Blinken Grün (500 ms EIN, 500 ms AUS)		Blinken Rot (500 ms EIN, 500 ms AUS)	–	Nicht zutreffend

LED-Diagnose des M580-Sicherheits-Coprozessors

LEDs des Coprozessors

Mit den LEDs auf der Vorderseite des Coprozessors (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) lässt sich der Zustand des PAC wie folgt diagnostizieren.

Zustand des Coprozessors	**Namen und Farben der LEDs:**			
	SRUN	**ERR**	**SMOD**	**DL**
	Grün	**Rot**	**Grün**	**Grün**
Spannung AUS				
WAIT-Zustand (Warten auf Firmware-Download von der CPU)				
Nicht konfiguriert (keine Anwendung)				
Konfiguriert und im Sicherheitsmodus ausgeführt: • SAFE-Task wurde angehalten				
• SAFE-Task wird ausgeführt				
Konfiguriert und im Wartungsmodus ausgeführt: • SAFE-Task wurde angehalten				
• SAFE-Task wird ausgeführt				
SAFE-Task in HALT (behebbarer Fehler erkannt)				
SAFE-Zustand (nicht behebbarer Fehler erkannt)				

Legende:

Symbol	**Beschreibung**	**Symbol**	**Beschreibung**	**Symbol**	**Beschreibung**
	Leuchten Grün		Leuchten Rot		AUS

Symbol	Beschreibung		Symbol	Beschreibung		Symbol	Beschreibung
	Blinken Grün (500 ms EIN, 500 ms AUS)			Blinken Rot (500 ms EIN, 500 ms AUS)			

LED für den Speicherkartenzugriff

Einführung

Die grüne LED für den Speicherkartenzugriff befindet sich unterhalb der Schutzabdeckung des SD-Speicherkartensteckplatzes und verweist auf den Zugriff auf die Speicherkarte durch die CPU, wenn eine Speicherkarte eingesteckt ist. Die LED ist bei geöffneter Abdeckung sichtbar.

Zugewiesene LED-Status

Alleine zeigen die LEDs für den **Speicherkartenzugriff** diese Status an:

LED-Status	Beschreibung
EIN	Die Speicherkarte wird erkannt, die CPU greift allerdings nicht auf die Karte zu.
blinkend	Die CPU greift auf die Speicherkarte zu.
Blinken	Die Speicherkarte wird nicht erkannt.
OFF	Die Speicherkarte kann aus dem CPU-Steckplatz entnommen werden oder die CPU erkennt die Speicherkarte nicht.

HINWEIS: Stellen Sie sicher, dass die LED ausgeschaltet ist, bevor Sie die Karte aus ihrem Steckplatz entnehmen.

Bedeutung der LED im Verbindung mit anderen LEDs

Die LED für die Zugriffskarte arbeitet mit der **BACKUP**-LED (siehe Modicon M580, Hardware, Referenzhandbuch) zusammen. Die kombinierten LED-Muster stellen folgende Diagnoseinformationen bereit:

Speicherkartenstatus	Zustand	CPU-Status	LED für den Speicherkartenzugriff	BACKUP-LED
Keine Speicherkarte in Steckplatz	—	Keine Konfiguration		
Speicherkarte nicht OK	—	Keine Konfiguration		
Speicherkarte ohne Projekt	—	Keine Konfiguration		
Speicherkarte mit einem nicht kompatiblen Projekt	—	Keine Konfiguration		
Speicherkarte mit einem kompatiblen Projekt	Bei der Wiederherstellung des Projekts aus der Speicherkarte im CPU RAM wird ein Fehler erkannt.	Keine Konfiguration	Während der Übertragung:  Übertragungsende: 	Während der Übertragung:  Übertragungsende: 
	Bei der Wiederherstellung des Projekts aus der Speicherkarte im CPU RAM wird kein Fehler erkannt.	—	Während der Übertragung:  Übertragungsende: 	Während der Übertragung:  Übertragungsende: 
– Kein besonderer Zustand bzw. CPU-Status				

Diese Legende zeigt die verschiedenen LED-Muster:

Symbol	Bedeutung	Symbol	Bedeutung
	Aus		Leuchten Rot
	Leuchten Grün		Blinken Grün

M580 – Diagnose der Sicherheitsspannungsversorgung

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für die M580-Sicherheitsspannungsversorgungen beschrieben.

Spannungsversorgung und LED-Diagnose

LEDs der Spannungsversorgung

Die Sicherheitsspannungsversorgungen BMXCPS4002S, BMXCPS4022S und BMXCPS3522S verfügen auf der Vorderseite über die folgenden Diagnose-LEDs:

- **OK**: Betriebszustand
- **ACT**: Aktivität
- **RD**: Redundanz (für Bauweisen mit redundanter Spannungsversorgung)

Die LEDs der M580-Sicherheitsspannungsversorgung übermitteln die folgenden Diagnose-Informationen:

LED	Beschreibung
OK	• EIN (grün) bedeutet, dass alle der folgenden Punkte zutreffen: ◦ Die 24-VDC-Spannung des Baugruppenträgers ist OK. ◦ Die 3,3-VDC-Spannung des Baugruppenträgers ist OK. ◦ Die Taste RESET wurde nicht aktiviert. • Blinken bedeutet, dass einer der folgenden Punkte zutrifft: ◦ Der 24-VDC-Strom des Baugruppenträgers ist derzeit nicht OK. ◦ Der 3,3-VDC-Strom des Baugruppenträgers ist derzeit nicht OK und die Taste RESET wurde nicht aktiviert. • OFF bedeutet, dass mindestens einer der folgenden Punkte zutrifft: ◦ Die 24-VDC-Spannung des Baugruppenträgers ist nicht OK. ◦ Die 3,3-VDC-Spannung des Baugruppenträgers ist nicht OK. ◦ Die Taste RESET wurde aktiviert.
ACT	• EIN (grün) bedeutet, dass die Spannungsversorgung das System mit Spannung versorgt. Bei einer Bauweise mit redundanter Spannungsversorgung ist das Modul das primäre Modul. • AUS bedeutet, dass die Spannungsversorgung das System nicht mit Spannung versorgt. Bei einer Bauweise mit redundanter Spannungsversorgung ist das Modul das Standby-Modul.
RD	• EIN (grün) bedeutet, dass die Kommunikation zwischen den zwei Spannungsversorgungsmodulen OK ist. • Blinken bedeutet, dass einer der folgenden Punkte zutrifft: ◦ Der 24-VDC-Strom des Baugruppenträgers ist derzeit nicht OK. ◦ Der 3,3-VDC-Strom des Baugruppenträgers ist derzeit nicht OK. • OFF bedeutet, dass mindestens einer der folgenden Punkte zutrifft: ◦ Die Kommunikation zwischen den zwei Spannungsversorgungsmodulen ist nicht OK. ◦ Es werden automatische Tests durchgeführt.

Diagnose des analogen Eingangsmoduls BMXSAI0410

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für das analoge Sicherheitseingangsmodul BMXSAI0410 beschrieben.

DDDT-Diagnose für BMXSAI0410

Einführung

Das analoge Sicherheitseingangsmodul BMXSAI0410 verfügt über die folgenden Diagnosetools und nutzt die DDT-Gerätelemente vom Typ T_U_ANA_SIS_IN_4, Seite 61:

- Eingangsdiagnose
- Erkennung eines internen Fehlers
- Diagnose der Kanalverdrahtung

Eingangsdiagnose

Die mit den jeweiligen Kanälen verbundenen Sensoren werden auf ihre Fähigkeit überwacht, zehn analoge Eingangswerte zwischen 4 und 20 mA genau messen zu können. Wenn die Eingangsmessungen nicht erfolgreich sind, wird das Bit CH_HEALTH in der DDDT-Struktur T_U_ANA_SIS_CH_IN, Seite 63 auf 0 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Erkennung eines internen Fehlers

Das Modul verarbeitet den Eingangswert über zwei separate, parallele Schaltkreise. Die zwei Werte werden verglichen, um festzustellen, ob im Modulprozess ein interner Fehler aufgetreten ist. Wenn sich die verglichenen Werte unterscheiden, wird das Bit IC in der DDDT-Struktur T_U_ANA_SIS_CH_IN auf 1 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Die Architekturdarstellung, Seite 144 für das analoge Sicherheitseingangsmodul BMXSAI0410 hilft bei der visuellen Darstellung dieses Prozesses.

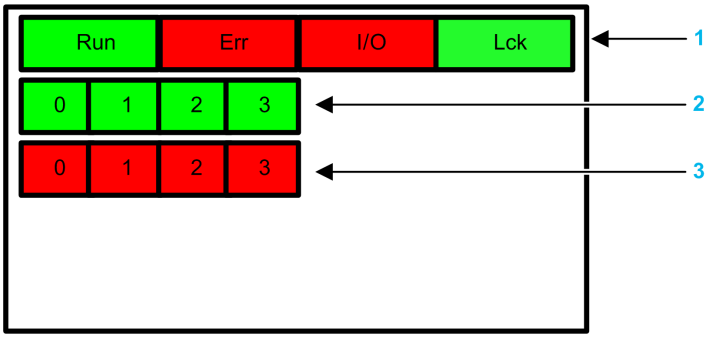
Diagnose der Kanalverdrahtung

Die Verdrahtung des Sensors mit dem Eingangskanal wird ständig auf getrennte Drähte geprüft. Dies wird erkannt, wenn der gemessene Strom unter 3,75 mA oder über 20,75 mA beträgt. In diesem Fall wird das Bit `OOR` in der DDDT-Struktur `T_U_ANA_SIS_CH_IN` auf 1 gesetzt.

LED-Diagnose des analogen Eingangsmoduls BMXSAI0410

LED-Panel

Das analoge Eingangsmodul BMXSAI0410 verfügt auf der Vorderseite über die folgenden LED-Panels:



1 Modulzustand-LEDs

2 Kanalzustand-LEDs

3 Kanalfehler-LEDs

HINWEIS:

- Die Kanalfehler-LEDs sind optional und funktionieren nur, wenn das Modul entsprechend konfiguriert wird. Wenn ein Kanalfehler erkannt wird, leuchtet die entsprechende LED, bis das Problem gelöst wird.
- Da das Eingangsmodul nur vier Kanäle hat, werden die LEDs 4 bis 7 nicht verwendet. Sie leuchten niemals.

Moduldiagnose

Nutzen Sie die vier LEDs oben auf dem LED-Panel, um den Zustand des analogen Eingangsmoduls BMXSAI0410 zu diagnostizieren:

Modul-LEDs				**Modulzustand**	**Empfohlene Reaktion**
Run	**Err**	**E/A**	**LCK**		
Blinken[1]	Blinken[1]	Blinken[1]	Blinken[1]	Automatischer Test beim Hochfahren	–
Blinken[1]	EIN	AUS	Blinken[1]	Der automatische Test beim Hochfahren hat einen internen Fehler auf den Eingangskanälen erkannt.	Tauschen Sie das Modul aus.
AUS	EIN	AUS	AUS	Es wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
AUS	Blinken[1]	AUS	X	Es ist kein E/A-Modul konfiguriert.	Konfigurieren Sie das Modul über die CPU.
X	X	EIN	X	Am Eingangskanal wurde ein externer Fehler erkannt.	Siehe *Kanaldiagnose*, Seite 240 (unten).
EIN	Blinken[1]	X	X	Es besteht keine Kommunikation zwischen CPU und E/A-Modul.	Überprüfen Sie Folgendes: • Die CPU ist eine M580-Sicherheits-CPU, die funktionsfähig ist. • Der Baugruppenträger ist funktionsfähig (falls sich das E/A-Modul im Hauptrack befindet). • Das Kabel zwischen CPU und E/A-Modul ist funktionsfähig und ordnungsgemäß angeschlossen (falls sich das E/A-Modul in einem erweiterten oder dezentralen Rack befindet).
EIN	Flackern[2]	X	AUS	Die Kommunikation ist nicht sicher. Die Konfiguration ist entsperrt.	Führen Sie mit den DDDT-Variablen, Seite 60 ein Debugging der E/A-Modulinstanz durch.
EIN	Flackern[2]	X	EIN	Die Kommunikation ist nicht sicher. Die Konfiguration ist gesperrt.	Überprüfen Sie Folgendes:

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
					• Die gesperrte Konfiguration im Modul entspricht der in der CPU-Anwendung gespeicherten Konfiguration, die über Control Expert vorgenommen wurde. • Führen Sie mit den DDDT-Variablen, Seite 60 ein Debugging der E/A-Modulinstanz durch.
EIN	EIN	AUS	X	Es wurde ein interner Fehler des Eingangskanals erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
EIN	AUS	AUS	AUS	Die Kommunikation mit der CPU ist OK und die Konfiguration ist entsperrt.	–
EIN	AUS	AUS	EIN	Die Kommunikation mit der CPU ist OK und die Konfiguration ist gesperrt.	–
X gibt an, dass der LED-Zustand EIN oder AUS sein kann. 1. Blinken: 500 ms EIN/500 ms AUS 2. Flackern: 50 ms EIN/50 ms AUS					

Kanaldiagnose

Nutzen Sie alle LEDs auf dem analogen Eingangsmodul BMXSAI0410, um den Kanalzustand zu diagnostizieren:

Modul-LEDs				Kanal-LEDs		Kanalzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 3)**	**Erkannter Fehler (LED 0 bis 3)**		
EIN	AUS	Aus	X	EIN	AUS	Der Eingangsstrom des Kanals liegt im Bereich von 4 bis 20 mA.	–
EIN	AUS	EIN	X	AUS	AUS	Der Eingangsstrom des Kanals liegt außerhalb des Bereichs von 4 bis 20 mA.	Stellen Sie sicher, dass die externe Spannungsversorgung, die externe Verkabelung

Modul-LEDs				Kanal-LEDs		Kanalzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 3)**	**Erkannter Fehler (LED 0 bis 3)**		
							und der Sensor funktionsfähig sind.
EIN	EIN	AUS	X	AUS	EIN	Der Kanal ist nicht funktionsfähig.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
X gibt an, dass der LED-Zustand EIN oder AUS sein kann.							

Diagnose des digitalen Eingangsmoduls BMXSDI1602

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für das digitale Sicherheitseingangsmodul BMXSDI1602 beschrieben.

DDDT-Diagnose für BMXSDI1602

Einführung

Das digitale Sicherheitseingangsmodul BMXSDI1602 verfügt über die folgenden Diagnosetools und nutzt die DDT-Gerätelemente vom Typ T_U_DIS_SIS_IN_16, Seite 94:

- Eingangsdiagnose
- Erkennung eines internen Fehlers
- Diagnose der Kanalverdrahtung
- Diagnose von Über- und Unterspannung

Eingangsdiagnose

Jeder Eingangskanal wird zu Beginn jedes Zyklus (oder Scans) auf Funktionsfähigkeit und Effektivität geprüft. Jeder Kanal wird in den erregten Zustand forciert. Es wird getestet, ob der erregte Zustand erreicht wurde. Dann wird der Kanal in den deaktivierten Zustand forciert. Es wird getestet, ob der deaktivierte Zustand erreicht wurde.

Wenn der Kanal nicht erfolgreich zwischen erregtem und deaktiviertem Zustand wechseln kann, wird das Bit CH_HEALTH in der DDDT-Struktur T_U_DIS_SIS_CH_IN, Seite 96 auf 0 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Erkennung eines internen Fehlers

In jedem Zyklus führt das Modul eine Eingangsdiagnosesequenz durch. Das Modul verarbeitet den Eingangswert über zwei separate, identische Schaltkreise. Die zwei Werte werden verglichen, um festzustellen, ob im internen Modulprozess ein interner Fehler aufgetreten ist. Wenn sich die verglichenen Werte unterscheiden, wird das Bit IC in der

DDDT-Struktur T_U_DIS_SIS_CH_IN auf 1 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Die Architekturdarstellung, Seite 145 für das digitale BMXSDI1602-Sicherheitseingangsmodul hilft bei der visuellen Darstellung dieses Prozesses.

Diagnose der Kanalverdrahtung

Die Verdrahtung des Sensors mit dem Eingangskanal kann ständig auf die folgenden Probleme überprüft werden:

- Getrennter Draht (offene Stromkreise)
- Kurzschluss an 24 VDC
- Kurzschluss an 0 VDC
- Querschluss zwischen zwei parallelen Kanälen

Die Verfügbarkeit dieser Diagnose ist von der Spannungsquelle der spezifischen Verdrahtung, Seite 72 abhängig sowie davon, ob die Diagnosefunktion auf der Konfigurationsseite des Moduls aktiviert ist.

Wenn einer dieser Fehler entdeckt wird, setzt die DDDT-Struktur T_U_DIS_SIS_CH_IN das entsprechende Bit auf 1:

- Das Bit OC wird auf 1 gesetzt, wenn ein offener (getrennter) Draht oder ein Masseschluss an 0 VDC erkannt wird.
- Das Bit SC wird auf 1 gesetzt, wenn ein Kurzschluss an 24 VDC oder ein Querschluss zwischen zwei Kanälen erkannt wird.

Diagnose von Über- und Unterspannung

Das Modul führt ständig Tests auf Über- und Unterspannung aus. Es gelten die folgenden Schwellenwerte:

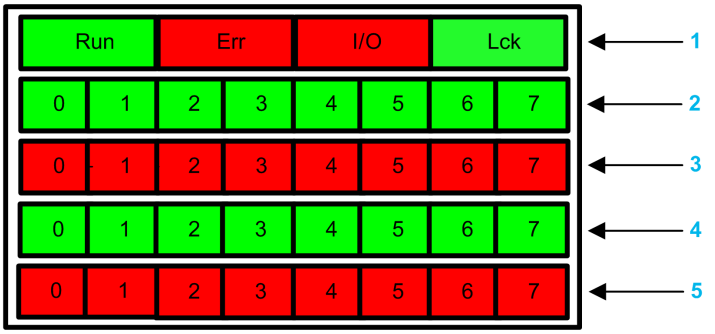
- Unterspannungsschwelle = 18,6 VDC
- Überspannungsschwelle = 33 VDC

Wenn Über- oder Unterspannung erkannt wird, setzt das Modul das Bit PP_STS des Geräte-DDT vom Typ T_U_DIS_SIS_IN_16 auf 0.

LED-Diagnose des digitalen Eingangsmoduls BMXSDI1602

LED-Panel

Das digitale Eingangsmodul BMXSDI1602 verfügt auf der Vorderseite über die folgenden LED-Panels:



1 Modulzustand-LEDs

2 Kanalstatus-LEDs für Rang A

3 Kanalfehler-LEDs für Rang A

4 Kanalstatus-LEDs für Rang B

5 Kanalfehler-LEDs für Rang B

HINWEIS: Wenn ein Kanalfehler erkannt wird, leuchtet die entsprechende LED, bis das Problem gelöst wird.

Moduldiagnose

Nutzen Sie die vier LEDs oben auf dem LED-Panel, um den Zustand des digitalen Eingangsmoduls BMXSDI1602 zu diagnostizieren:

Modul-LEDs				**Modulzustand**	**Empfohlene Reaktion**
Run	**Err**	**E/A**	**LCK**		
Blinkend	Blinken[1]	Blinken[1]	Blinken[1]	Automatischer Test beim Hochfahren	–
Blinkend	EIN	AUS	Blinken[1]	Der automatische Test beim Hochfahren hat einen internen Fehler auf den Eingangskanälen erkannt.	Tauschen Sie das Modul aus.

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
Blinkend	EIN	EIN	Blinken[1]	• Der automatische Modultest beim Hochfahren hat einen internen Fehler auf den Eingangskanälen erkannt. • Die externe 24-VDC-Spannungsversorgung liegt außerhalb des Bereichs.	Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung des Vorstellglieds funktionsfähig ist. Schließen Sie die 24-VDC-Spannungsversorgung an.
AUS	EIN	AUS	AUS	Es wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
AUS	Blinken[1]	AUS	X	Es ist kein E/A-Modul konfiguriert.	Konfigurieren Sie das Modul über die CPU.
X	XX	EIN	X	• Die externe 24-VDC-Spannungsversorgung liegt außerhalb des Bereichs. • Am Eingangskanal wurde ein externer Fehler erkannt.	• Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung des Vorstellglieds funktionsfähig ist. • Siehe *Kanaldiagnose*, Seite 246.
EIN	Blinken[1]	X	X	Es besteht keine Kommunikation zwischen CPU und Modul.	Überprüfen Sie Folgendes: • Die CPU ist eine M580-Sicherheits-CPU, die funktionsfähig ist. • Der Baugruppenträger ist funktionsfähig (falls sich das E/A-Modul im Hauptrack befindet). • Das Kabel zwischen CPU und E/A-Modul ist funktionsfähig und ordnungsgemäß angeschlossen (falls sich das E/A-Modul in einem erweiterten oder dezentralen Rack befindet).
EIN	Flackern[2]	X	AUS	Die Kommunikation ist nicht sicher. Die Konfiguration ist entsperrt.	Führen Sie mit den DDDT-Variablen, Seite 94 ein Debugging der E/A-Modulinstanz durch.

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
EIN	Flackern[2]	X	EIN	Die Kommunikation ist nicht sicher. Die Konfiguration ist gesperrt.	• Stellen Sie sicher, dass die gesperrte Konfiguration im Modul der in der CPU-Anwendung gespeicherten Konfiguration entspricht, die über Control Expert vorgenommen wurde. • Führen Sie mit den DDDT-Variablen, Seite 94 ein Debugging der E/A-Modulinstanz durch.
EIN	EIN	AUS	X	Es wurde ein interner Fehler des Eingangskanals erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
EIN	AUS	AUS	AUS	Die Kommunikation mit der CPU ist OK und die Konfiguration ist entsperrt.	–
EIN	AUS	AUS	EIN	Die Kommunikation mit der CPU ist OK und die Konfiguration ist gesperrt.	–
X gibt an, dass der LED-Zustand EIN oder AUS sein kann. 1. Blinken: 500 ms EIN/500 ms AUS 2. Flackern: 50 ms EIN/50 ms AUS					

Kanaldiagnose

Nutzen Sie alle LEDs auf dem digitalen Eingangsmodul BMXSDI1602, um den Kanalzustand zu diagnostizieren:

Modul-LEDs				Kanal-LEDs		Kanalzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 7, Rang A/B)**	**Erkannter Fehler (LED 0 bis 7, Rang A/B)**		
EIN	AUS	AUS	X	EIN	AUS	Eingangszustand EIN	–
EIN	AUS	AUS	X	AUS	AUS	Eingangszustand AUS	–
EIN	EIN	AUS	X	AUS	EIN	Eingangszustand AUS Am Kanal wurde ein interner Fehler erkannt.	Ersetzen Sie das Modul, falls das Problem bestehen bleibt.

Modul-LEDs				**Kanal-LEDs**		**Kanalzustand**	**Empfohlene Reaktion**
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 7, Rang A/B)**	**Erkannter Fehler (LED 0 bis 7, Rang A/B)**		
EIN	EIN	EIN	X	AUS	EIN	Die externe 24-VDC-Spannungsversorgung liegt außerhalb des Bereichs.	Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung des Vorstellglieds funktionsfähig ist.
EIN	AUS	EIN	X	X	Blinken[1]	Der Eingang befindet sich in einem der folgenden Zustände: • Ein offener Schaltkreis • Ein Kurzschluss an 0 VDC	Stellen Sie sicher, dass die Verkabelung ordnungsgemäß angeschlossen und funktionsfähig ist.
EIN	AUS	EIN	X	X	Flackern[2]	Der Eingang befindet sich in einem der folgenden Zustände: • Ein Kurzschluss an 24 VDC • Ein Kurzschluss an 0 VDC	Stellen Sie sicher, dass die Verkabelung ordnungsgemäß angeschlossen und funktionsfähig ist.
X gibt an, dass der LED-Zustand EIN oder AUS sein kann.							

Diagnose des digitalen Ausgangsmoduls BMXSDO0802

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für das digitale Sicherheitsausgangsmodul BMXSDO0802 beschrieben.

DDDT-Diagnose für BMXSDO0802

Einführung

Das digitale Sicherheitsausgangsmodul BMXSDO0802 verfügt über die folgenden Diagnosetools und nutzt die DDT-Gerätelemente vom Typ `T_U_DIS_SIS_OUT_8, Seite 109`:

- Ausgangsdiagnose
- Erkennung eines internen Fehlers
- Diagnose der Kanalverdrahtung
- Diagnose von Über- und Unterspannung

Ausgangsdiagnose

Jeder Ausgangskanal wird zu Beginn jedes Zyklus (oder Scans) auf Funktionsfähigkeit und Effektivität geprüft. Bei diesem Test werden die Ausgangskontaktzustände gewechselt (von EIN zu AUS oder von AUS zu EIN). Dies geschieht in so kurzen Zeiträumen, dass das Stellglied nicht reagiert (unter 1 ms). Wenn der Kanal nicht erfolgreich zwischen erregtem und deaktiviertem Zustand wechseln kann, wird das Bit `CH_HEALTH` in der DDDT-Struktur `T_U_DIS_SIS_CH_OUT, Seite 111` auf 0 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Erkennung eines internen Fehlers

Das Modul verarbeitet den Ausgangswert über zwei separate, identische Schaltkreise. Jeder Schaltkreis liest die Mittelpunktspannung des Kanals. Die zwei Werte werden verglichen. Wenn es sich bei den Werten nicht um die erwarteten Werte handelt, wird ein interner Fehler ausgegeben, indem das Bit `IC` in der DDDT-Struktur `T_U_DIS_SIS_CH_OUT` auf 1 gesetzt wird, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

Die Architekturdarstellung, Seite 146 für das digitale Sicherheitsausgangsmodul BMXSDO0802 hilft bei der visuellen Darstellung dieses Prozesses.

Diagnose der Kanalverdrahtung

Die Verdrahtung des Stellglieds mit dem Ausgangskanal kann ständig auf die folgenden Probleme überprüft werden:

- Getrennter Draht (offene Stromkreise)
- Kurzschluss an 24 VDC
- Kurzschluss an 0 VDC
- Querschluss zwischen zwei parallelen Kanälen
- Kanalüberlast

HINWEIS: Eine Kanalüberlast wird nur erkannt, wenn der Ausgang erregt ist.

Die Verfügbarkeit dieser Diagnose ist davon abhängig, ob die Diagnosefunktion auf der Konfigurationsseite des Moduls aktiviert ist.

Wenn einer dieser Fehler entdeckt wird, setzt die DDDT-Struktur `T_U_DIS_SIS_CH_OUT` das entsprechende Bit auf 1:

- Das Bit `OC` wird auf 1 gesetzt, wenn ein offener (getrennter) Draht erkannt wird.
- Das Bit `SC` wird auf 1 gesetzt, wenn ein Kurzschluss an 24 VDC oder ein Querschluss zwischen zwei Kanälen erkannt wird.
- Das Bit OL wird auf 1 gesetzt, wenn ein Masseschluss an 0 VDC oder eine Kanalüberlast erkannt wird.

Diagnose von Über- und Unterspannung

Das Modul führt ständig Tests auf Über- und Unterspannung aus. Es gelten die folgenden Schwellenwerte:

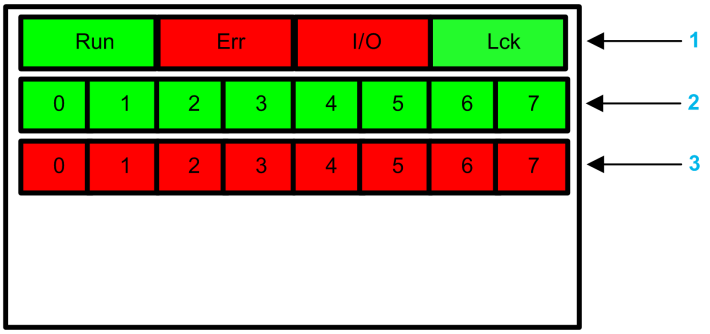
- Unterspannungsschwelle = 18 VDC
- Überspannungsschwelle = 31,8 VDC

Wenn Über- oder Unterspannung erkannt wird, setzt das Modul das Bit `PP_STS` des Geräte-DDT vom Typ `T_U_DIS_SIS_OUT_8` auf 0.

LED-Diagnose des digitalen Ausgangsmoduls BMXSDO0802

LED-Panel

Das digitale Ausgangsmodul BMXSDO0802 verfügt auf der Vorderseite über das folgende LED-Panel:



1 Modulzustand-LEDs

2 Kanalzustand-LEDs

3 Kanalfehler-LEDs

HINWEIS: Wenn ein Kanalfehler erkannt wird, leuchtet die entsprechende LED, bis das Problem gelöst wird.

Moduldiagnose

Nutzen Sie die vier LEDs oben auf dem LED-Panel, um den Zustand des digitalen Ausgangsmoduls BMXSDO0802 zu diagnostizieren:

Modul-LEDs				**Modulzustand**	**Empfohlene Reaktion**
Run	**Err**	**E/A**	**LCK**		
Blinken[1]	Blinken[1]	Blinken[1]	Blinken[1]	Automatischer Test beim Hochfahren	–
Blinken[1]	EIN	AUS	Blinken[1]	Der automatische Test beim Hochfahren hat einen internen Fehler auf den Ausgangskanälen erkannt.	Tauschen Sie das Modul aus.

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
Blinken[1]	EIN	EIN	Blinken[1]	• Der automatische Modultest beim Hochfahren hat einen internen Fehler auf den Ausgangskanälen erkannt. • Die externe 24-VDC-Spannungsversorgung liegt außerhalb des Bereichs.	Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung des Vorstellglieds funktionsfähig ist. Schließen Sie die 24-VDC-Spannungsversorgung an.
AUS	EIN	AUS	AUS	Es wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
AUS	Blinken[1]	AUS	X	Es ist kein E/A-Modul konfiguriert.	Konfigurieren Sie das Modul über die CPU.
X	X	EIN	X	• Die externe 24-VDC-Spannungsversorgung liegt außerhalb des Bereichs. • Am Ausgangskanal wurde ein externer Fehler erkannt.	• Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung des Vorstellglieds funktionsfähig ist. • Siehe *Kanaldiagnose*, Seite 252 (unten).
EIN	Blinken[1]	X	X	Es besteht keine Kommunikation zwischen CPU und Modul. Das Modul befindet sich im Fehlerausweichzustand (oder in RESET, falls das Modul nie ordnungsgemäß funktioniert hat).	Überprüfen Sie Folgendes: • Die CPU ist eine M580-Sicherheits-CPU, die funktionsfähig ist. • Der Baugruppenträger ist funktionsfähig (falls sich das E/A-Modul im Hauptrack befindet). • Das Kabel zwischen CPU und E/A-Modul ist funktionsfähig und ordnungsgemäß angeschlossen (falls sich das E/A-Modul in einem erweiterten oder dezentralen Rack befindet).
EIN	Flackern[2]	X	AUS	Die Kommunikation ist nicht sicher. Die Konfiguration ist entsperrt. Das Modul	Überprüfen Sie die verfügbaren DDDT-Variablen, um ein Debugging der sicheren Kommunikation sicherzustellen.

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
				befindet sich im Fehlerausweichzu-stand (oder in RESET, falls das Modul nie ordnungsgemäß funktioniert hat).	
EIN	Flackern[2]	X	EIN	Die Kommunikation ist nicht sicher. Die Konfiguration ist gesperrt. Das Modul befindet sich im Fehlerausweichzu-stand.	• Stellen Sie sicher, dass die gesperrte Konfiguration im Modul der in der CPU-Anwendung gespeicherten Konfiguration entspricht, die über Control Expert vorgenommen wurde. • Führen Sie mit den DDDT-Variablen, Seite 109 ein Debugging der E/A-Modulinstanz durch.
EIN	EIN	AUS	X	Am Ausgangskanal wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
EIN	AUS	AUS	AUS	Die Kommunikation mit der CPU ist sicher und die Konfiguration ist entsperrt.	–
EIN	AUS	AUS	EIN	Die Kommunikation mit der CPU ist sicher und die Konfiguration ist gesperrt.	–
X gibt an, dass der LED-Zustand EIN oder AUS sein kann. 1. Blinken: 500 ms EIN/500 ms AUS 2. Flackern: 50 ms EIN/50 ms AUS					

Kanaldiagnose

Nutzen Sie alle LEDs auf dem digitalen Ausgangsmodul BMXSDO0802, um den Kanalzustand zu diagnostizieren:

Modul-LEDs				Kanal-LEDs		Kanalzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 7)**	**Erkannter Fehler (LED 0 bis 7)**		
EIN	AUS	AUS	X	EIN	AUS	Ausgangszustand EIN	–
EIN	AUS	AUS	X	AUS	AUS	Ausgangszustand AUS	–
EIN	EIN	AUS	X	AUS	EIN	Ausgangszustand AUS Am Ausgangskanal wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
EIN	EIN	EIN	X	AUS	EIN	Die externe 24-VDC-Spannungsversorgung des Vorstellglieds liegt außerhalb des Bereichs.	Stellen Sie sicher, dass die externe 24-VDC-Spannungsversorgung funktionsfähig ist.
EIN	AUS	EIN	X	AUS	Blinken[1]	Der Ausgang befindet sich in einem der folgenden Zustände: • Ein offener Schaltkreis • Ein Kurzschluss an 0 VDC • Eine Spannungsüberlast	Stellen Sie sicher, dass die Verkabelung ordnungsgemäß angeschlossen und funktionsfähig ist.
EIN	AUS	EIN	X	EIN	Flackern[2]	Der Ausgang befindet sich in einem der folgenden Zustände: • Ein Kurzschluss an 24 VDC • Ein Kurzschluss an einem anderen aktiven Ausgangskanal	Stellen Sie sicher, dass die Verkabelung ordnungsgemäß angeschlossen und funktionsfähig ist.

X gibt an, dass der LED-Zustand EIN oder AUS sein kann.

1. Blinken: 500 ms EIN/500 ms AUS

2. Flackern: 50 ms EIN/50 ms AUS

Diagnose des digitalen Relaisausgangsmoduls BMXSRA0405

Einführung

In diesem Abschnitt werden die verfügbare Diagnosetools für das digitale Sicherheitsrelaisausgangsmodul BMXSRA0405 beschrieben.

DDDT-Diagnose für BMXSRA0405

Einführung

Das digitale Sicherheitsrelaisausgangsmodul BMXSRA0405 verfügt über die folgenden Diagnosetools und nutzt die DDT-Gerätelemente vom Typ `T_U_DIS_SIS_OUT_4, Seite 127`:

- Ausgangskontaktdiagnose
- Erkennung eines internen Fehlers

Ausgangskontaktdiagnose

Abhängig von der für das Modul konfigurierten Anwendungsnummer kann das Modul automatisch testen, ob es seine Ausgangskontaktzustände (von EIN zu AUS oder von AUS zu EIN) so schnell wechseln kann, dass die Stellglieder darauf nicht reagieren. Wenn die Kanäle nicht erfolgreich zwischen erregtem und deaktiviertem Zustand wechseln können, wird das Bit `CH_HEALTH` in der DDDT-Struktur `T_U_DIS_SIS_CH_ROUT, Seite 129` auf 0 gesetzt, um darauf hinzuweisen, dass es nicht funktionsfähig ist.

HINWEIS: Die Anwendungen Nummer 2, 4, 6 und 8 führen diesen Signaltest automatisch durch. Die Anwendungen Nummer 1, 3, 5 und 7 tun dies nicht, sodass täglich ein manueller Wechsel des Ausgangskanalzustands erfolgen muss, um die Funktionsfähigkeit zu testen.

Ausgangsbefehlsdiagnose (Erkennung eines internen Fehlers)

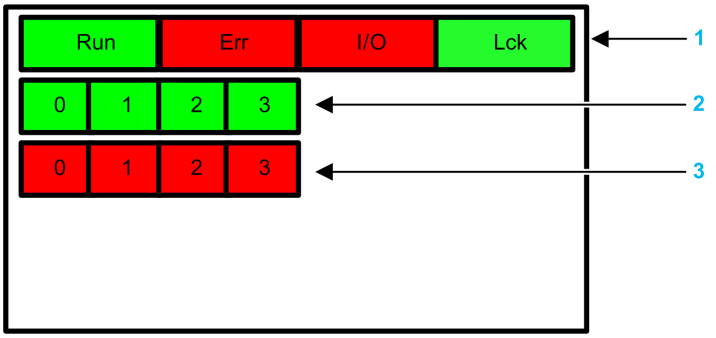
Der Relaisbefehl wird über zwei separate, parallele Schaltkreise verarbeitet. Die Werte der Schaltkreise werden verglichen. Wenn sich die verglichenen Werte unterscheiden, wird festgelegt, dass der Kanal nicht funktionsfähig ist. Das Bit `IC` in der DDDT-Struktur `T_U_DIS_SIS_CH_ROUT` wird auf 1 gesetzt.

Die Architekturdarstellung, Seite 148 für das digitale Sicherheitsrelaisausgangsmodul BMXSRA0405 hilft bei der visuellen Darstellung dieses Prozesses.

LED-Diagnose des digitalen Relaisausgangsmoduls BMXSRA0405

LED-Panel

Das digitale Relaisausgangsmodul BMXSRA0405 verfügt auf der Vorderseite über die folgenden LED-Panels:



1 Modulzustand-LEDs

2 Kanalzustand-LEDs

3 Kanalfehler-LEDs

HINWEIS:

- Wenn ein Kanalfehler erkannt wird, leuchtet die entsprechende LED, bis das Problem gelöst wird.
- Da das Relaisausgangsmodul nur vier Kanäle hat, werden die LEDs 4 bis 7 nicht verwendet. Sie leuchten niemals.

Moduldiagnose

Nutzen Sie die vier LEDs oben auf dem LED-Panel, um den Zustand des digitalen Relaisausgangsmoduls BMXSRA0405 zu diagnostizieren:

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
Blinken[1]	Blinken[1]	Blinken[1]	Blinken[1]	Automatischer Test beim Hochfahren	–
Blinken[1]	EIN	Blinken[1]	Blinken[1]	Der automatische Test beim Hochfahren hat einen internen Fehler auf den Ausgangskanälen erkannt.	–
AUS	EIN	AUS	AUS	Es wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
AUS	Blinken[1]	AUS	X	Es ist kein E/A-Modul konfiguriert.	Konfigurieren Sie das Modul über die CPU.
EIN	Blinken[1]	AUS	X	Keine Kommunikation zwischen CPU und Modul. Das Modul befindet sich im Fehlerausweichzu-stand.	Überprüfen Sie Folgendes: • Die CPU ist eine M580-Sicherheits-CPU, die funktionsfähig ist. • Der Baugruppenträger ist funktionsfähig (falls sich das E/A-Modul im Hauptrack befindet). • Das Kabel zwischen CPU und E/A-Modul ist funktionsfähig und ordnungsgemäß angeschlossen (falls sich das E/A-Modul in einem erweiterten oder dezentralen Rack befindet).
EIN	Flackern[2]	AUS	AUS	Es besteht keine Kommunikation zwischen CPU und Modul. Das Modul befindet sich im Fehlerausweichzustand (oder in RESET, falls das Modul nie ordnungsgemäß funktioniert hat).	Führen Sie mit den DDDT-Variablen, Seite 126 ein Debugging der E/A-Modulinstanz durch.
EIN	Flackern[2]	AUS	EIN	Die Kommunikation ist nicht sicher. Die Konfiguration ist gesperrt. Das Modul befindet sich im Fehlerausweichzustand (oder in RESET, falls das Modul nie ordnungsgemäß funktioniert hat).	• Stellen Sie sicher, dass die gesperrte Konfiguration im Modul der in der CPU-Anwendung gespeicherten Konfiguration entspricht, die über Control Expert. vorgenommen wurde.

Modul-LEDs				Modulzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**		
					• Führen Sie mit den DDDT-Variablen, Seite 126 ein Debugging der E/A-Modulinstanz durch.
EIN	EIN	AUS	X	Am Ausgangskanal wurde ein interner Fehler erkannt.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
EIN	AUS	AUS	AUS	Die Kommunikation mit der CPU ist sicher und die Konfiguration ist entsperrt.	–
EIN	AUS	AUS	EIN	Die Kommunikation mit der CPU ist sicher und die Konfiguration ist gesperrt.	–
X gibt an, dass der LED-Zustand EIN oder AUS sein kann. 1. Blinken: 500 ms EIN/500 ms AUS 2. Flackern: 50 ms EIN/50 ms AUS					

Kanaldiagnose

Nutzen Sie alle LEDs auf dem digitalen Relaisausgangsmodul BMXSRA0405, um den Kanalzustand zu diagnostizieren:

Modul-LEDs				Kanal-LEDs		Kanalzustand	Empfohlene Reaktion
Run	**Err**	**E/A**	**LCK**	**Kanalzustand (LED 0 bis 3)**	**Erkannter Fehler (LED 0 bis 3)**		
EIN	AUS	AUS	X	EIN	AUS	Das Ausgangsrelais ist geschlossen.	–
EIN	AUS	AUS	X	AUS	AUS	Das Ausgangsrelais ist offen.	–
EIN	EIN	AUS	X	AUS	EIN	Das Ausgangsrelais ist nicht funktionsfähig.	Tauschen Sie das Modul aus, falls sich der Fehler nicht beheben lässt.
X gibt an, dass der LED-Zustand EIN oder AUS sein kann.							

Bedienung eines M580-Sicherheitssystems

Inhalt dieses Kapitels

Einführung

Dieses Kapitel enthält Informationen zur Bedienung eines M580-Sicherheitssystems.

Prozess-, sicherheitsspezifische und globale Datenbereiche in Control Expert

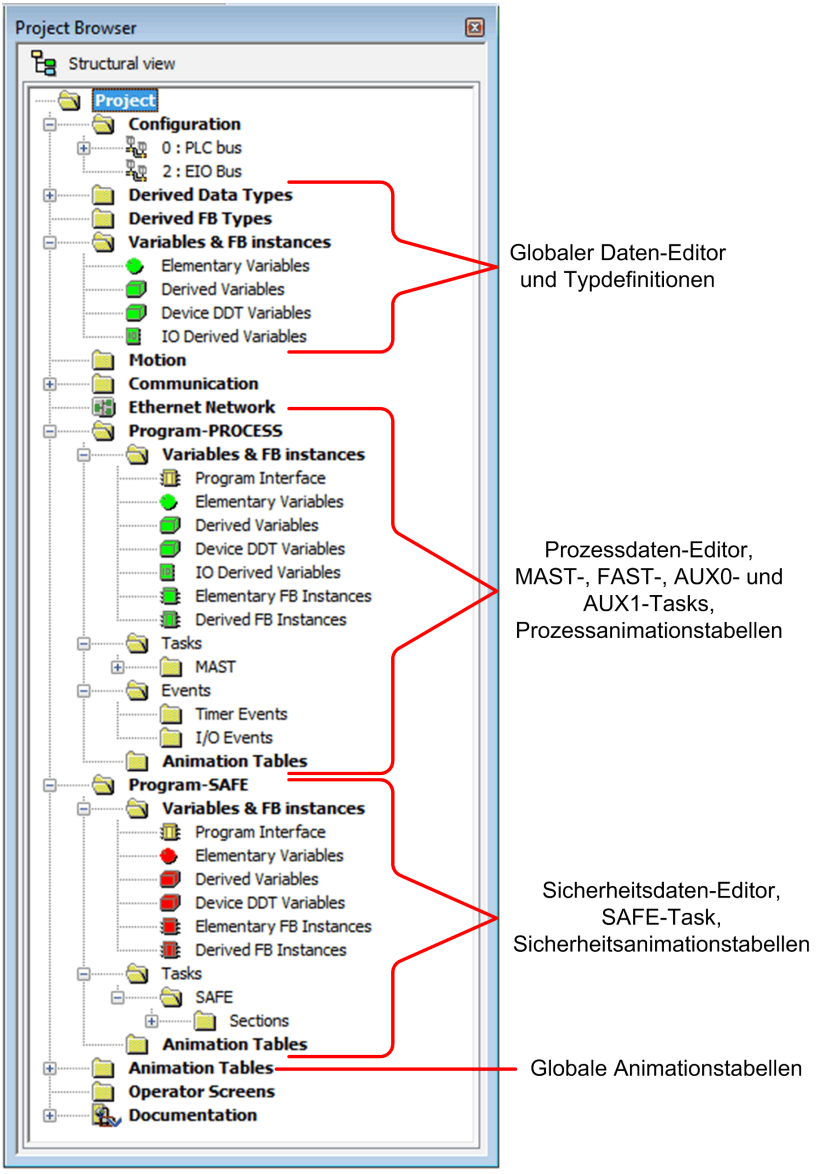
Einführung

In diesem Abschnitt wird die Untergliederung der Datenbereiche in einem M580-Control Expert-Sicherheitsprojekt beschrieben.

Datentrennung in Control Expert

Datenbereiche in Control Expert

Die **Strukturansicht** im **Projekt-Browser** zeigt die Datentrennung in Control Expert. an. Wie nachstehend dargestellt verfügt jeder Datenbereich über seinen eigenen Dateneditor sowie über eine Reihe von Animationstabellen:



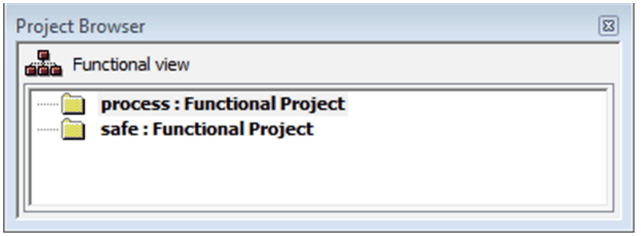
Eine Analyse des **Projekt-Browsers** ergibt Folgendes:

- Der sichere Bereich enthält einen Sicherheitsdaten-Editor, Sicherheitslogik und Funktionsbausteininstanzen, die von der SAFE-Task verwendet werden. Dabei ist allerdings auch Folgendes zu berücksichtigen:
  - E/A-Ereignisse, Timer-Ereignisse und Subroutinen werden in einem Sicherheitsprogramm nicht unterstützt.
  - IODDT-Variablen werden von der SAFE-Task nicht unterstützt und sind nicht im sicheren Bereich enthalten.
  - Rote Symbole verweisen auf die SAFE-Bereiche des Programms.
- Der Prozessbereich enthält einen Prozessdaten-Editor, Prozesslogik und Funktionsbausteininstanzen, die von den nicht-sicheren Tasks (d. h. MAST, FAST, AUX0 und AUX1) verwendet werden.
- Der globale Bereich enthält einen globalen Daten-Editor, abgeleitete Daten und Funktionsbausteintypen, die über Instanzen im Prozess- und Sicherheitsprogramm verfügen.

  HINWEIS: Der in diesem Kapitel verwendete Begriff *Globale Daten* bezieht sich auf den anwendungsspezifischen – oder globalen – Bereich der Datenobjekte in einem Sicherheitsprojekt. Er bezieht sich nicht auf den Dienst „Globale Daten“, der von zahlreichen Ethernet-Modulen von Schneider Electric unterstützt wird.

Projekt-Browser in der Funktionsansicht

In der **Funktionsansicht** im **Projekt-Browser** von Control Expert. werden für ein M580-Sicherheitssystem zwei funktionale Projekte angezeigt – ein Projekt für den Prozess-Namespace und ein Projekt für den sicheren Namespace.



Die Verwaltung jedes funktionalen Projekts in einem M580-Sicherheitssystem ist identisch mit der Verwaltung eines Projekts in der Funktionsansicht eines nicht-sicheren M580-Systems, mit Ausnahme von Animationstabellen und Code-Sections.

Auswirkungen auf die Strukturansicht:

Wenn Sie einem funktionalen Projekt eine Code-Section oder Animationstabelle hinzufügen, wird diese mit dem Namespace verknüpft, der dem funktionalen Projekt zugeordnet ist. Hinzufügen einer Code-Section oder Animationstabelle:

- Zu **Prozess: Funktionales Projekt** – Die Section/Tabelle wird dem Prozess-Namespace des Projekts in der Strukturansicht hinzugefügt.
- Zu **Sicher: Funktionales Projekt** – Die Section/Tabelle wird dem sicheren Namespace des Projekts in der Strukturansicht hinzugefügt.

Verfügbarkeit der Sprachen- und Task-Auswahl:

Bei der Erstellung einer neuen Code-Section für ein funktionales Projekt (durch Auswahl von **Erstellen > Neue Section...**) ist die verfügbare Auswahl der **Sprache** und **Task** vom jeweiligen funktionalen Projekt abhängig:

Bei der Erstellung einer neuen Code-Section für ein funktionales Projekt (durch Auswahl von **Erstellen > Neue Section...**) ist die verfügbare Auswahl der **Sprache** und **Task** vom zugeordneten funktionalen Projekt abhängig:

Funktionales Projekt	**Verfügbare Sprachen und Tasks**	
	Sprachen[1]	**Tasks**[2]
Prozess: Funktionales Projekt	• IL • FBD • LD • LL984-Segment • SFC • ST	• MAST • FAST • AUX0 • AUX1
Sicher: Funktionales Projekt	• FBD • LD	• SAFE

1. Ausgewählt auf der Registerkarte **Allgemein** im Dialogfeld „Neue Section“

2. Ausgewählt auf der Registerkarte **Lokalisierung** im Dialogfeld „Neue Section“ Die MAST-Task ist standardmäßig verfügbar. Andere Sections stehen nur nach deren Erstellung im Prozessprogramm zur Verfügung.

Farbcodierung der Symbole

Damit Sie die Prozess- und Sicherheitsbereiche des Projekts besser auseinanderhalten können, werden die Sicherheitsbereiche der Anwendung mit roten Symbolen markiert.

Betriebsarten, Betriebszustände und Tasks

Einführung

In diesem Abschnitt werden die vom M580-Sicherheits-PAC unterstützten Betriebsarten, Betriebszustände und Tasks beschrieben.

Betriebsarten des M580-Sicherheits-PAC

Zwei Betriebsarten

Der M580-Sicherheits-PAC verfügt über zwei Betriebsarten:

- Sicherheitsmodus: Die für Sicherheitsoperationen verwendete Standard-Betriebsart.
- Wartungsmodus: Optionale Betriebsart, die vorübergehend für das Debugging und die Änderung des Anwendungsprogramms bzw. für die Änderung der Konfiguration aktiviert werden kann.

Für den Wechsel zwischen den Betriebsarten kann ausschließlich das Softwaretool Control Expert Safety verwendet werden.

HINWEIS: Die Betriebsarteneinstellung für einen Hot Standby-Sicherheits-PAC - Sicherheits- oder Wartungsmodus wird bei der Übertragung einer Anwendung vom primären in den Standby-PAC nicht berücksichtigt. Bei einer Umschaltung, d. h. wenn ein Sicherheits-PAC von Standby zu Primär wechselt, wird die Betriebsart automatisch auf den Sicherheitsmodus eingestellt.

Der Sicherheitsmodus und dessen Beschränkungen

Der Sicherheitsmodus ist die Standard-Betriebsart des Sicherheits-PAC. Wenn der Sicherheits-PAC mit gültiger Anwendung eingeschaltet wird, wird automatisch der Sicherheitsmodus aktiviert. Der Sicherheitsmodus ermöglicht die Steuerung der Ausführung der Sicherheitsfunktion. Im Sicherheitsmodus können Sie ein Projekt hoch- und herunterladen, ausführen und anhalten.

Wenn sich der M580-Sicherheits-PAC im Sicherheitsmodus befindet, sind folgende Funktionen **nicht** verfügbar:

- Herunterladen einer geänderten Konfiguration von Control Expert in den PAC
- Bearbeiten und/oder Forcieren der Werte der Sicherheitsvariablen und der Zustände der Sicherheits-E/A

- Debuggen der Anwendungslogik mithilfe von Haltepunkten, Überwachungspunkten und einer schrittweisen Codeausführung
- Verwenden von Animationstabellen oder UMAS-Requests (z. B. von einer HMI) zum Schreiben der Sicherheitsvariablen und Sicherheits-E/A
- Ändern der Konfigurationseinstellungen für Sicherheitsmodule per CCOTF (Hinweis: Die Verwendung von CCOTF für nicht störende Module wird unterstützt.)
- Durchführen einer Online-Änderung der Sicherheitsanwendung
- Verwenden der Animation von Verbindungen (Link-Animation)

  HINWEIS: Im Sicherheitsmodus sind alle Sicherheitsvariablen und Sicherheits-E/A-Zustände schreibgeschützt. Der Wert einer Sicherheitsvariablen kann nicht direkt bearbeitet werden.

Sie können allerdings eine globale Variable erstellen und diese zur Übergabe eines Werts zwischen einer verbundenen (nicht-sicheren) Prozessvariablen und einer verbundenen Sicherheitsvariablen über die Registerkarten des Prozessdateneditors und des Sicherheitsdateneditors verwenden. Nach der Herstellung einer Verbindung erfolgt die Übertragung folgendermaßen:

- Zu Beginn jeder SAFE-Task werden die nicht-sicheren Variablenwerte in die sicheren Variablen kopiert.
- Am Ende der SAFE-Task werden die sicheren Ausgangsvariablenwerte in die nicht-sicheren Variablen kopiert.

Funktionsweise des Wartungsmodus

Der Wartungsmodus lässt sich mit dem Normalbetrieb einer nicht-sicheren M580-CPU vergleichen. Er dient ausschließlich dem Debugging und der Feineinstellung der SAFE-Anwendungstask. Der Wartungsmodus ist eine temporäre Betriebsart, da der Sicherheits-PAC automatisch in den Sicherheitsmodus übergeht, sobald die Kommunikation zwischen Control Expert und dem PAC unterbrochen oder ein Befehl zur Verbindungstrennung ausgegeben wird. Im Wartungsmodus können Personen mit entsprechender Berechtigung die Sicherheitsvariablen und Sicherheits-E/A, die für eine Bearbeitung konfiguriert wurden, sowohl lesen als auch schreiben.

Im Wartungsmodus wird der Code der SAFE-Task zweimal ausgeführt, die Ergebnisse werden jedoch nicht miteinander verglichen.

Wenn sich der M580-Sicherheits-PAC im Wartungsmodus befindet, sind folgende Funktionen verfügbar:

- Herunterladen einer geänderten Konfiguration von Control Expert in den PAC
- Bearbeiten und/oder Forcieren der Werte der Sicherheitsvariablen und der Zustände der Sicherheits-E/A
- Debuggen der Anwendungslogik mithilfe von Haltepunkten, Überwachungspunkten und einer schrittweisen Codeausführung

- Verwenden von Animationstabellen oder UMAS-Requests (z. B. von einer HMI) zum Schreiben der Sicherheitsvariablen und Sicherheits-E/A
- Ändern der Konfiguration per CCOTF
- Durchführen einer Online-Änderung der Sicherheitsanwendung
- Verwenden der Animation von Verbindungen (Link-Animation)

Im Wartungsmodus ist der SIL-Level der Sicherheits-SPS nicht gewährleistet.

⚠WARNUNG

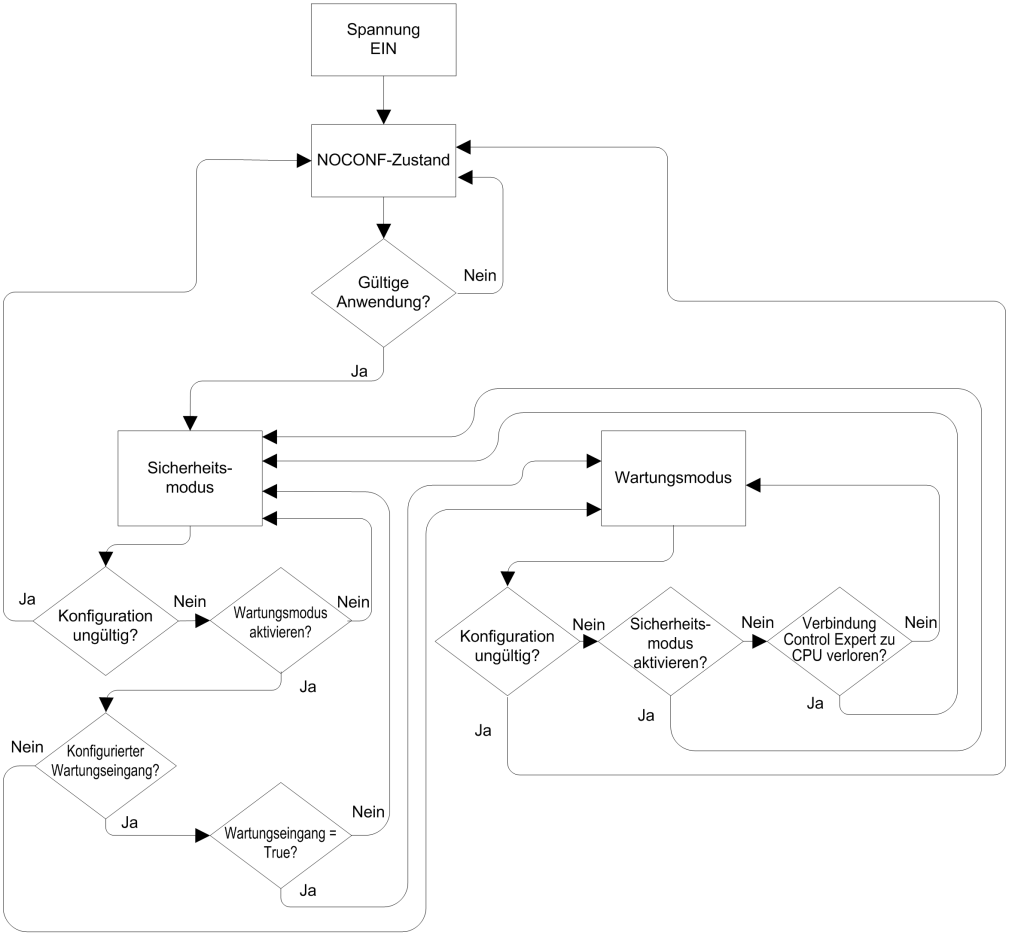
VERLUST DES SICHERHEITS-INTEGRITÄTSLEVELS

Wenn die Sicherheits-SPS im Wartungsmodus läuft, müssen angemessene Maßnahmen zur Gewährleistung des sicheren Systemzustands ergriffen werden.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Übergänge zwischen den Betriebsarten

Das nachstehende Diagramm zeigt, wann der Sicherheits- und der Wartungsmodus aktiviert werden und wann der M580-Sicherheits-PAC von einem in den anderen Modus wechselt.



Umschaltung zwischen Sicherheits- und Wartungsmodus:

- Es kann mit aktivierter Forcierung vom Wartungs- in den Sicherheitsmodus geschaltet werden. In diesem Fall bleibt der forcierte Variablenwert bzw. E/A-Zustand auch nach dem Übergang forciert, bis ein Übergang vom Sicherheits- in den Wartungsmodus erfolgt.

- Der Übergang vom Wartungs- in den Sicherheitsmodus kann auf folgende Weise erfolgen:
  - Manuell über einen Menü- oder Symbolleistenbefehl in Control Expert.
  - Automatisch über den Sicherheits-PAC bei Verlust der Kommunikation zwischen Control Expert und PAC für ca. 50 Sekunden.
- Wenn die Wartungseingangsfunktion konfiguriert ist, übernimmt sie die Kontrolle der Übergänge vom Sicherheits- in den Wartungsmodus. Die Wartungseingangsfunktion wird Control Expert in auf der Registerkarte **Konfiguration** konfiguriert. Dazu stehen folgende Möglichkeiten zur Auswahl:
  - Auswahl der Einstellung **Wartungseingang** und
  - Eingabe der topologischen Adresse eines Eingangsbits (%I) für ein (nicht störendes) digitales Eingangsmodul im lokalen Rack

  Wenn der Wartungseingang konfiguriert wurde, wird beim Übergang vom Sicherheits- in den Wartungsmodus der Zustand des angegebenen Eingangsbits (%I) berücksichtigt. Wenn das Bit auf 0 (False) gesetzt wird, wird der PAC im Sicherheitsmodus gesperrt. Wenn das Bit auf 1 (True) gesetzt wird, kann ein Übergang in den Wartungsmodus erfolgen.

Umschaltung zwischen Sicherheits- und Wartungsmodus in Control Expert

In folgenden Fällen ist eine Umschaltung vom Wartungs- in den Sicherheitsmodus für den Sicherheits-PAC nicht möglich:

- Der PAC befindet sich im Debug-Modus.
- In einer SAFE-Task-Section ist ein Haltepunkt aktiviert.
- In einer SAFE-Task-Section ist ein Überwachungspunkt aktiviert.

Wenn der Debug-Modus nicht aktiv, kein SAFE-Task-Haltepunkt aktiviert und kein SAFE-Task-Überwachungspunkt eingestellt ist, können Sie einen Übergang zwischen dem Sicherheits- und dem Wartungsmodus manuell aktivieren. Gehen Sie dazu vor wie folgt:

- Gehen Sie vor wie folgt, um vom Sicherheits- in den Wartungsmodus umzuschalten:
  - Wählen Sie **SPS > Wartung** aus.
  - Klicken Sie auf die Schaltfläche  in der Symbolleiste.
- Gehen Sie vor wie folgt, um vom Wartungs- in den Sicherheitsmodus umzuschalten:
  - Wählen Sie **SPS > Sicherheit** aus.
  - Klicken Sie auf die Schaltfläche  in der Symbolleiste.

HINWEIS: Das Aktivieren und Beenden des Sicherheitsmodus werden als Ereignisse im SYSLOG-Server in der CPU gespeichert.

Identifizierung der Betriebsart

Sie können die aktuelle Betriebsart eines M580-Sicherheits-PAC über die **SMOD**-LEDs der CPU und des Koprozessors oder in Control Expert identifizieren.

Status der **SMOD**-LEDs von CPU und Koprozessor:

- *Blinkend*: Der PAC befindet sich im Wartungsmodus.
- *Permanent leuchtend*: Der PAC befindet sich im Sicherheitsmodus.

Wenn Control Expert mit dem PAC verbunden ist, identifiziert die Software die Betriebsart des M580-Sicherheits-PAC über:

- Die Systemwörter %SW12 (Koprozessor) und %SW13 (CPU), Seite 414 geben Aufschluss über die Betriebsart des PAC:
  - Wenn %SW12 den Wert 16#A501 (hex.) und %SW13 den Wert 16#501A (hex.) aufweist, dann befindet sich der PAC im Wartungsmodus.
  - Wenn eines der oder beide Systemwörter den Wert 16#5AFE (hex.) aufweisen, dann befindet sich der PAC im Sicherheitsmodus.
- Auf den Unterregisterkarten **Task** und **Informationen** der CPU-Registerkarte **Animation** wird die jeweilige Betriebsart des PAC angegeben.
- In der Taskleiste am unteren Rand des Control Expert-Hauptfensters wird die Betriebsart als WARTUNG oder SICHERHEIT ausgewiesen.

Betriebszustände des M580-Sicherheits-PA

Betriebszustände

Nachstehend werden die verschiedenen Betriebszustände des M580-Sicherheits-PAC beschrieben.

HINWEIS: Eine Beschreibung der Beziehung zwischen den Betriebszuständen des M580-Sicherheits-PAC und den Betriebsarten des M580-Hot Standby-PAC finden Sie im Dokument *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen* sowie in den Kapiteln *Hot Standby-Systemstatus* und *Hot Standby-Statuszuordnungen und -übergänge*.

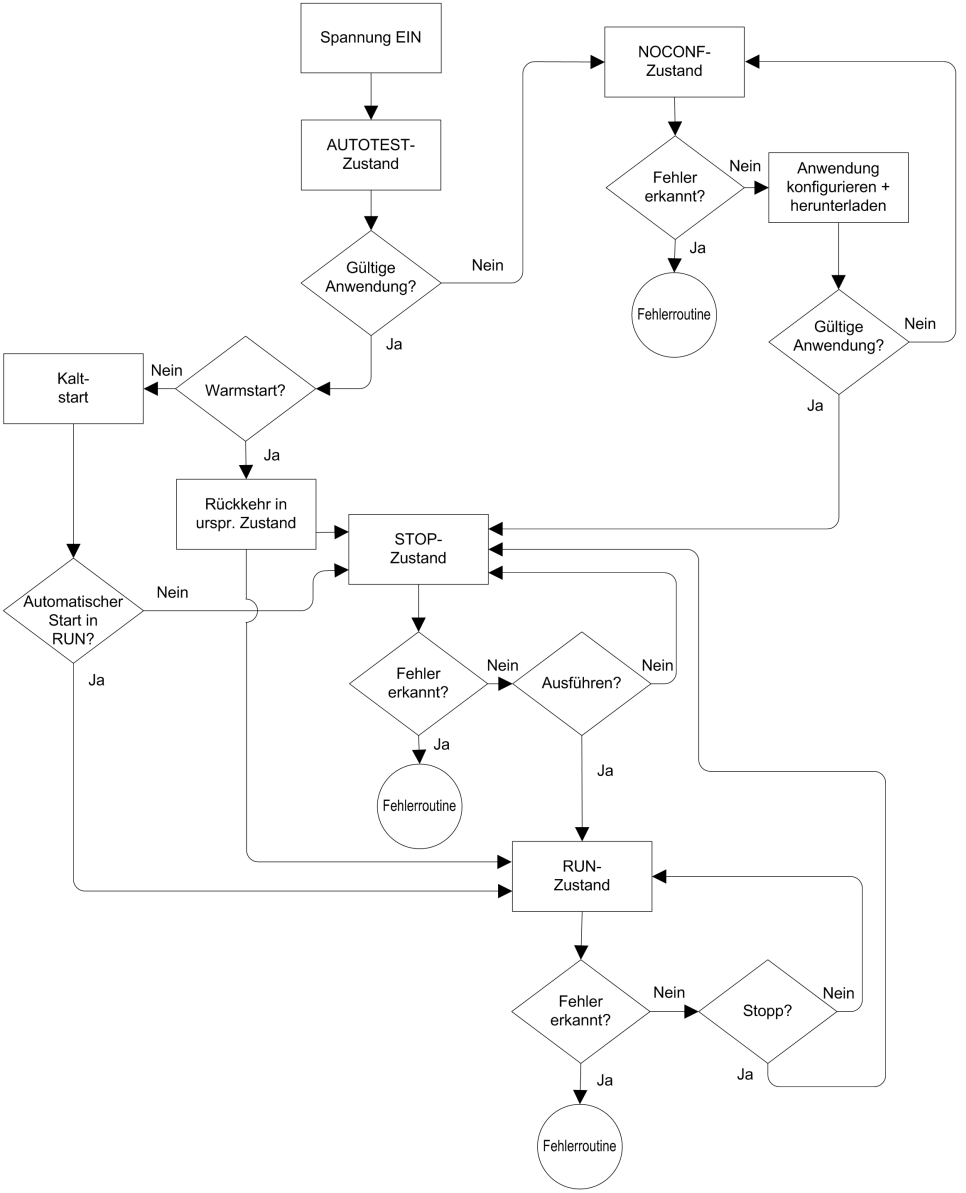
Betriebszustand	Gilt für ...	Beschreibung
AUTOTEST	PAC	Die CPU führt interne Selbsttests durch. **HINWEIS:** Wenn Erweiterungsracks mit dem lokalen Hauptrack verbunden sind und nicht verwendete Anschlüsse am Rack-Erweiterungsmodul nicht mit Leitungsabschlüssen versehen wurden, verbleibt die CPU auch nach Abschluss der Selbsttestphase im AUTOTEST-Modus.
NOCONF	PAC	Das Anwendungsprogramm ist nicht gültig.
STOP	PAC oder Task	Der PAC verfügt über eine gültige Anwendung und es wurde kein Fehler erkannt, der Betrieb wurde jedoch aufgrund folgender Ursache unterbrochen: • Beim Start ist die Option **Automatischer Start in RUN** nicht aktiviert (Sicherheitsmodus, Seite 264). • Die Ausführung wurde durch einen STOP-Befehl abgebrochen (sicherer Modus, Seite 264 oder Wartungsmodus, Seite 265). • Im Wartungsmodus wurden Haltepunkte eingestellt, dann wurde die Verbindung zwischen Control Expert und der CPU für mehr als 50 Sekunden getrennt. Die CPU liest die jeder Task zugeordneten Eingänge, aktualisiert jedoch nicht die Ausgänge, die in ihren Fehlerausweichzustand übergehen. Die CPU kann neu gestartet werden, sobald Sie bereit sind. **HINWEIS:** Die Ausgabe eines STOP-Befehls in Control Expert bewirkt den Stopp aller Tasks. Das STOP-Ereignis wird im SYSLOG-Server der CPU aufgezeichnet.
HALT	Task	Der M580-Sicherheits-PAC verfügt über zwei unabhängige HALT-Zustände: • Der Prozess-HALT gilt für nicht-SAFE-Tasks (MAST, FAST, AUX0 und AUX1). Sobald eine Prozesstask in den HALT-Zustand übergeht, gehen ebenfalls alle anderen Prozesstasks in den HALT-Zustand über. Die SAFE-Task wird von einem Prozess-HALT nicht beeinflusst. • Ein SAFE-HALT bezieht sich ausschließlich auf die SAFE-Task. Prozesstasks werden von einem SAFE-HALT nicht beeinflusst. In beiden Fällen wird der Task-Betrieb angehalten, da ein unerwarteteter Blockierzustand angetroffen wird, der einen nicht behebbaren, Seite 225 Zustand ergibt. Die CPU liest die jeder angehaltenen Task zugeordneten Eingänge, aktualisiert jedoch nicht die Ausgänge, die in ihren Fehlerausweichzustand übergehen.
RUN	PAC oder Task	Wenn eine gültige Anwendung vorhanden ist und kein Fehler erkannt wird, liest die CPU die jeder Task zugeordneten Eingänge, führt den jeder Task zugeordneten Code aus und aktualisiert die zugeordneten Ausgänge. • Im Sicherheitsmodus, Seite 264: Die Sicherheitsfunktion wird ausgeführt und sämtliche Einschränkungen werden angewendet.

Betriebszustand	Gilt für ...	Beschreibung
		• Im Wartungsmodus, Seite 265: Der PAC verhält sich wie jede Nicht-Sicherheits-CPU. Der Code der SAFE-Task wird zweimal ausgeführt, die Ergebnisse werden jedoch nicht miteinander verglichen. **HINWEIS:** Die Ausgabe eines RUN-Befehls in Control Expert bewirkt den Start aller Tasks. Das RUN-Ereignis wird im SYSLOG-Server der CPU aufgezeichnet.
WAIT	PAC	Die CPU befindet sich in einem Übergangszustand und sichert die Daten, wenn ein Spannungsausfall erkannt wird. Die CPU startet nur dann wieder, wenn die Spannung wiederhergestellt wird und die Versorgungsreserve aufgefüllt wurde. Da WAIT ein Übergangszustand ist, wird er unter Umständen nicht erkannt. Die CPU führt einen Warmstart, Seite 278 durch, um den WAIT-Zustand zu verlassen.
ERROR	PAC	Die CPU wird aufgrund eines nicht behebbaren, Seite 222 Hardware- oder Systemfehlers gestoppt. Der ERROR-Zustand löst die Sicherheitsfunktion, Seite 16 aus. Wenn das System bereit zum Neustart ist, führen Sie einen Kaltstart, Seite 278 der CPU aus (Aus- und Wiedereinschalten oder RESET), um den ERROR-Zustand zu verlassen.
OS DOWNLOAD	PAC	Es wird gerade eine CPU- oder COPRO-Firmware heruntergeladen.

Unter *M580-CPU - LED-Diagnose*, Seite 227 und *M580-Sicherheitscoprozessor - LED-Diagnose*, Seite 227 finden Sie Informationen zu den Betriebszuständen des PAC.

Übergänge zwischen Betriebszuständen

Die Übergänge zwischen den verschiedenen Zuständen eines M580-Sicherheits-PAC werden nachstehend beschrieben:



Unter *Fehlerverwaltung*, Seite 273 finden Sie Informationen zur Fehlerverwaltung durch das Sicherheitssystem.

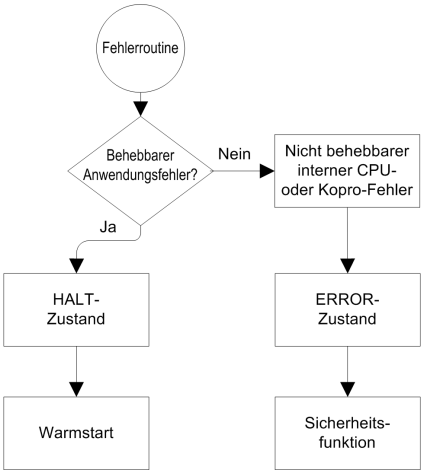
Fehlerverwaltung

Der M580-Sicherheits-PAC verwaltet folgende CPU-spezifischen Fehler:

- Behebbare Anwendungsfehler: Diese Ereignisse bewirken den Übergang der zugeordneten Task(s) in den HALT-Zustand.

  HINWEIS: Da die MAST-, FAST- und AUX-Task im gleichen Speicherbereich ausgeführt werden, bewirkt ein Ereignis, das den Übergang einer dieser Tasks in den HALT-Zustand auslöst, ebenfalls den Übergang der anderen nicht-sicheren Tasks in den HALT-Zustand. Die SAFE-Task hingegen wird in einem separaten Speicherbereich ausgeführt, d. h. die nicht-sicheren Tasks werden vom Übergang der SAFE-Task in den HALT-Zustand nicht beeinflusst.
- Nicht behebbare Anwendungsfehler: Interne CPU- oder Coprozessor-Fehler. Diese Ereignisse bewirken den Übergang des PAC in den ERROR-Zustand. Die Sicherheitsfunktion wird auf den betroffenen Teil der Sicherheitsregelung angewendet.

Nachstehend wird die Logik des Fehlerverarbeitungsprozesses beschrieben:



Nachstehend werden die Auswirkungen einer Fehlererkennung für die einzelnen Tasks beschrieben:

Typ des erkannten Fehlers	Task-Zustand			
	FAST	**SAFE**	**MAST**	**AUX**
Watchdog-Überlauf der FAST-Task	HALT	RUN[1]	HALT	HALT
Watchdog-Überlauf der SAFE-Task	RUN	HALT[2]	RUN	RUN

Typ des erkannten Fehlers	Task-Zustand			
	FAST	**SAFE**	**MAST**	**AUX**
Watchdog-Überlauf der MAST-Task	HALT	RUN	HALT	HALT
Watchdog-Überlauf der AUX-Task	HALT	RUN	HALT	HALT
Doppelte CPU-Codeausführung	RUN	HALT[2]	RUN	RUN
Überlauf des Sicherheits-Watchdogs[3]	ERROR	ERROR[2]	ERROR	ERROR
CPU-interner Fehler	ERROR	ERROR[2]	ERROR	ERROR

1. Da die FAST-Task eine höhere Priorität aufweist als die SAFE-Task, kann eine Verzögerung der FAST-Task den Übergang der SAFE-Task in den HALT- oder ERROR-Zustand an Stelle des RUN-Zustands auslösen.

2. Beim Wechsel der SAFE-Task in den ERROR- und HALT-Zustand werden die sicheren Ausgänge in den benutzerdefinierten Zustand (Fehlerausweichmodus oder Halten des Werts) gesetzt.

3. Der sicherheitsbezogene Watchdog wird auf einen Wert gesetzt, der dem 1,5-Fachen des Watchdogs der SAFE-Task entspricht.

Sicherheitsstatus-Anzeige der Taskleiste

Wenn Control Expert mit dem M580-Sicherheits-PAC verbunden ist, umfasst die Taskleiste ein Feld, in dem die kombinierten Betriebszustände der SAFE-Task und der Prozesstasks (MAST, FAST, AUX0, AUX1) angegeben werden:

Zustand der Prozesstask(s)	**Zustand der SAFE-Task**	**Meldung**
STOP (alle Prozesstasks im STOP-Zustand)	STOP	STOP
STOP (alle Prozesstasks im STOP-Zustand)	RUN	RUN
STOP (alle Prozesstasks im STOP-Zustand)	HALT	SAFE HALT
RUN (mindestens eine Prozesstask im RUN-Zustand)	STOP	RUN
RUN (mindestens eine Prozesstask im RUN-Zustand)	RUN	RUN
RUN (mindestens eine Prozesstask im RUN-Zustand)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

Anlaufsequenzen

Einführung

In folgenden Situationen kann der M580-Sicherheits-PAC die Anlaufsequenz auslösen:

- Bei der Erstinbetriebnahme
- Im Anschluss an eine Unterbrechung der Spannungsversorgung

Je nach Typ der Task und Kontext der Spannungsunterbrechung führt der M580-Sicherheits-PAC bei Wiederherstellung der Spannungsversorgung entweder einen Kaltstart, Seite 278 oder einen Warmstart, Seite 278 aus.

Erstinbetriebnahme

Bei der Erstinbetriebnahme führt der M580-Sicherheits-PAC einen Kaltstart aus. Sämtliche Tasks, einschließlich der SAFE-Task und der nicht-sicheren Tasks (MAST, FAST, AUX0, AUX1), wechseln in den STOP-Zustand, außer die Option **Automatischer Start in RUN** ist aktiviert. In diesem Fall gehen alle Tasks in den RUN-Zustand über.

Anlauf nach einer Unterbrechung der Stromversorgung

Der M580-Sicherheits-PAC stellt eine Spannungsreserve bereit, die bei einem Spannungsausfall alle Module im Rack für bis zu 10 ms weiter mit Spannung versorgt. Sobald die Spannungsreserve aufgebraucht ist, schaltet der M580-Sicherheits-PAC das System aus und wieder ein.

Vor dem Herunterfahren des Systems speichert die Sicherheits-CPU die folgenden Daten, die den Betriebskontext beim Spannungsausfall definieren:

- Datum und Uhrzeit des Spannungsausfalls (gespeichert in %SW54...%SW58)
- Zustand jeder Task
- Zustand der Ereignis-Timer
- Werte der aktiven Zähler
- Signatur der Anwendung
- Anwendungsdaten (aktuelle Werte der Anwendungsvariablen)
- Prüfsumme der Anwendung

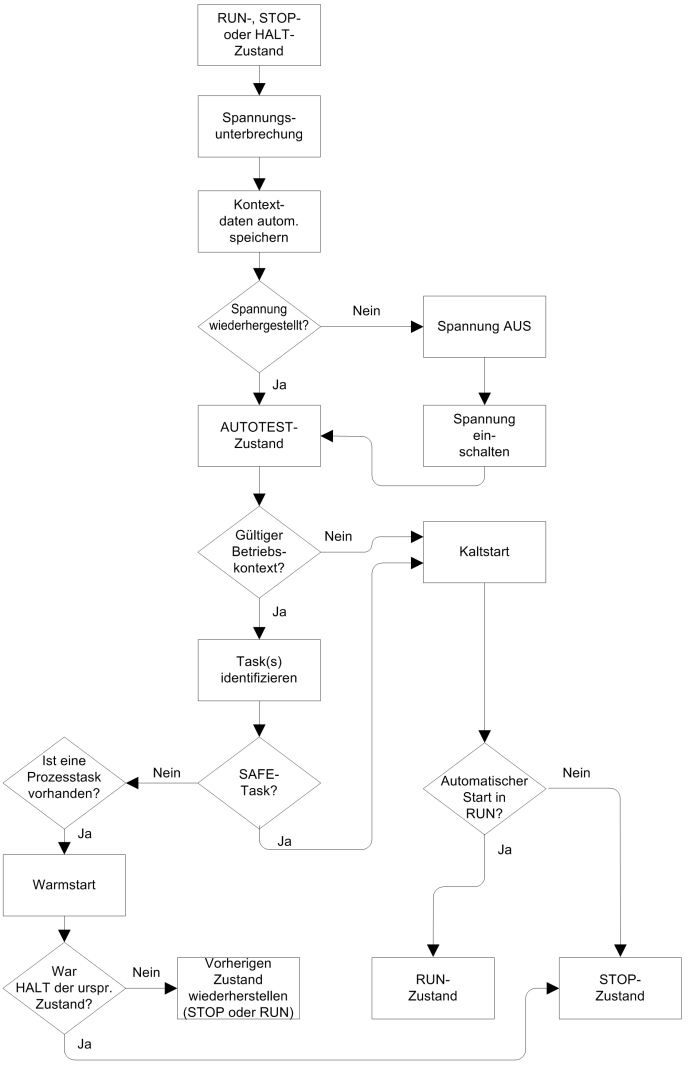
Nach dem Herunterfahren kann der Systemanlauf entweder automatisch (wenn die Spannungsversorgung vor Abschluss des Herunterfahrens wiederhergestellt wurde) oder manuell (wenn nicht) erfolgen.

Im Anschluss daran führt der M580-Sicherheits-PAC Selbsttests durch und prüft die Gültigkeit der Betriebskontextdaten, die beim Spannungsausfall gespeichert wurden:

- Die Prüfsumme der Anwendung wird geprüft.
- Die SD-Speicherkarte wird gelesen, um sicherzustellen, dass sie eine gültige Anwendung enthält.
- Wenn die Anwendung auf der SD-Speicherkarte gültig ist, werden die Signaturen geprüft, um sicherzustellen, dass sie identisch sind.
- Die gespeicherte Anwendungssignatur wird durch einen Vergleich mit der gesicherten Anwendungssignatur geprüft.

Wenn der Betriebskontext gültig ist, führen die nicht-sicheren Tasks einen Warmstart aus. Ist der Betriebskontext nicht gültig, dann führen die nicht-sicheren Tasks einen Kaltstart aus. In beiden Fällen führt die SAFE-Task einen Kaltstart aus.

Nachstehend wird die Anlaufsequenz nach einer Unterbrechung der Spannungsversorgung dargestellt:



Kaltstart

Bei einem Kaltstart gehen alle Tasks, einschließlich der SAFE-Task und der nicht-sicheren Tasks (MAST, FAST, AUX0, AUX1), in den STOP-Zustand über, außer die Option **Automatischer Start in RUN** ist aktiviert. In diesem Fall wechseln alle Tasks in den RUN-Zustand.

Bei einem Kaltstart werden folgende Vorgänge ausgeführt:

- Die Anwendungsdaten (einschließlich der internen Bits, E/A-Daten, internen Wörter usw.) den von der Anwendung definierten Initialwerten zugewiesen.
- Die Elementarfunktionen werden auf ihre Standardwerte eingestellt.
- Die elementaren Funktionsbausteine und deren Variablen werden auf ihre Standardwerte gesetzt.
- Die Systembits und -wörter werden auf ihre Standardwerte eingestellt.
- Alle forcierten Variablen werden durch Anwendung ihrer (initialisierten) Standardwerte initialisiert.

Ein Kaltstart kann für Daten, Variablen und Funktionen im Prozess-Namespace durch Auswahl von **SPS > Init** in Control Expert, Seite 294 oder durch Setzen des Systembits %S0 (COLDSTART) auf 1 durchgeführt werden. Das Systembit %S0 hat keinerlei Auswirkung auf die Daten und Funktionen, die dem sicheren Namespace angehören.

HINWEIS: Im Anschluss an einen Kaltstart kann die SAFE-Task erst nach dem Start der MAST-Task gestartet werden.

Warmstart

Ein Warmstart bewirkt den Übergang jeder Prozesstask – einschließllich der Tasks MAST, FAST, AUX0, AUX1 – in den Betriebszustand, in dem sich die Task zum Zeitpunkt der Unterbrechung der Spannungsversorgung befunden hat. Im Gegensatz dazu löst ein Warmstart den Übergang der SAFE-Task in den STOP-Zustand aus, außer die Option **Automatischer Start in RUN** wurde ausgewählt.

HINWEIS: Wenn sich eine Task zum Zeitpunkt des Spannungsausfalls im HALT-Zustand oder an einem Haltepunkt befunden hat, geht die Task nach dem Warmstart in den STOP-Zustand über.

Bei einem Warmstart werden folgende Vorgänge ausgeführt:

- Der zuletzt gehaltene Wert wird für die Variablen des Prozess-Namespace wiederhergestellt.
- Die Variablen des sicheren Namespace werden durch Anwendung ihrer (initialisierten) Standardwerte initialisiert.
- Alle forcierten Variablen werden durch Anwendung ihrer (initialisierten) Standardwerte initialisiert.

- Der zuletzt gehaltene Wert wird für die Anwendungsvariablen wiederhergestellt.
- %S1 (WARMSTART) wird auf 1 gesetzt.
- Die Verbindungen zwischen PAC und CPU werden zurückgesetzt.
- Die E/A-Module werden (sofern erforderlich) mit den gespeicherten Einstellungen neu konfiguriert.
- Die Ereignisse, die FAST-Task und die AUX-Tasks werden deaktiviert.
- Die MAST-Task wird ab Beginn des Zyklus neu gestartet.
- %S1 wird bei Abschluss der ersten Ausführung der MAST-Task auf 0 gesetzt.
- Die Ereignisse, die FAST-Task und die AUX-Tasks werden aktiviert.

Wenn eine Task bei Unterbrechung der Spannungsversorgung gerade ausgeführt wurde, wird die Ausführung der Task nach dem Warmstart zu Beginn der Task wieder aufgenommen.

⚠ WARNUNG
UNERWARTETER GERÄTEBETRIEB Sie müssen sicherstellen, dass die Auswahl der Option **Automatischer Start in RUN** mit dem ordnungsgemäßen Betrieb Ihres Systems vereinbar ist. Ist das nicht der Fall, dann muss diese Funktion deaktiviert werden. **Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.**

Tasks des M580-Sicherheits-PAC

Einführung

Ein M580-Sicherheits-PAC kann Einzeltask- und Multitask-Anwendungen ausführen. Im Gegensatz zu einer Einzeltask-Anwendung, in der ausschließlich die MAST-Task ausgeführt wird, wird in einer Multitask-Anwendung die Priorität jeder Task definiert.

Der M580-Sicherheits-PAC unterstützt folgende Tasks:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Eigenschaften der Tasks

Die vom M580-Sicherheits-PAC unterstützten Tasks weisen folgende Eigenschaften auf:

Name der Task	Prio-rität	Zeitmodell	Periode – Bereich	Standardzeit-raum	Watchdog-Bereich	Standard-Watchdog
FAST	1	Periodisch	1 bis 255 ms	5 ms	10 bis 500 ms[2]	100 ms[2]
SAFE	2	Periodisch	10 bis 255 ms	20 ms	10 bis 500 ms[2]	250 ms[2]
MAST[1]	3	Zyklisch[4] oder periodisch	1 bis 255 ms	20 ms	10 bis 1500 ms[2]	250 ms[2]
AUX0[3]	4	Periodisch	10 bis 2550 ms	100 ms	100 bis 5000 ms[2]	2000 ms[2]
AUX1[3]	5	Periodisch	10 bis 2550 ms	200 ms	100 bis 5000 ms[2]	2000 ms[2]

1. Die MAST-Task ist erforderlich und kann nicht deaktiviert werden.

2. Bei aktivierter CCOTF-Funktion (durch Auswahl von **Online-Änderung im RUN- oder STOP-Betrieb** auf der Registerkarte **Konfiguration** im Eigenschaftsfenster der CPU) beträgt die Mindesteinstellung für den **Watchdog** 64 ms.

3. Unterstützt von BMEP58•040S-Sicherheits-PACs im Standalone-Betrieb. Von BMEH58•040S-Sicherheits-PACs im Hot Standby-Betrieb nicht unterstützt.

4. BMEP58•040S-Sicherheits-PACs im Standalone-Betrieb unterstützen sowohl zyklische als auch periodische Modelle. BMEH58•040S-Sicherheits-PACs im Hot Standby-Betrieb unterstützen nur das periodische Modell.

Priorität der Tasks

Der M580-Sicherheits-PAC führt die ausstehenden Tasks nach deren Priorität aus. Während der Ausführung einer Task kann diese durch eine andere Task mit höherer relativer Priorität unterbrochen werden. Wenn beispielsweise die Ausführung des Codes einer periodischen Task geplant ist, wird durch diese Ausführung eine Task mit niedrigerer Priorität unterbrochen, bei einer Task mit höherer Priorität hingegen wird gewartet, bis deren Ausführung abgeschlossen ist.

Hinweise zur Konfiguration der Tasks

Alle nicht-sicheren Tasks (MAST, FAST, AUX0 und AUX1) werden im gleichen Speicherbereich, die SAFE-Task in ihrem eigenen, separaten Speicherbereich ausgeführt. Ergebnis:

- Wenn eine nicht-sichere Task den zugehörigen Watchdog überschreitet, wechseln alle nicht-sicheren Tasks in den HALT-Zustand, während die SAFE-Task weiterhin funktionsfähig bleibt.

- Wenn die SAFE-Task den zugehörigen Watchdog überschreitet, geht nur die SAFE-Task in den HALT-Zustand über. Alle nicht-sicheren Tasks bleiben funktionsfähig.

Bei der Erstellung und Konfiguration der Tasks für Ihre Anwendung sind folgende taskspezifischen Merkmale zu berücksichtigen:

SAFE-Task:

Konfigurieren Sie diese periodische Task für eine Ausführung von ausschließlich sicherheitsbezogenen Code-Sections für E/A-Sicherheitsmodule. Da die SAFE-Task eine niedrigere Priorität aufweist als die FAST-Task, kann die Ausführung der SAFE-Task durch die FAST-Task unterbrochen werden.

Legen Sie die maximale Ausführungszeit für die SAFE-Task durch Einstellung eines geeigneten Watchdog-Werts fest. Berücksichtigen Sie dabei die Zeit, die zur Ausführung des Codes und zum Lesen und Schreiben der sicheren Daten benötigt wird. Wenn die zur Ausführung der SAFE-Task erforderliche Zeit die Watchdog-Einstellung überschreitet, wechselt die SAFE-Task in den HALT-Zustand und das Systemwort %SW125 zeigt den Fehlercode 16#DEB0 an.

HINWEIS:

- Da die FAST-Task eine höhere Priorität aufweist als die SAFE-Task, können Sie in der Watchdog-Einstellung für die SAFE-Task unter Umständen eine Komponente zur Verzögerung der FAST-Task einbeziehen.
- Wenn der Überlauf der SAFE-Task-Ausführung dem „Sicherheits-Watchdog“ entspricht (d. h. dem 1,5-Fachen der Watchdog-Einstellung der SAFE-Task), wechseln CPU und Coprozessor in den ERROR-Zustand und die Sicherheitsfunktion wird angewendet.

MAST-Task:

Diese Task kann zyklisch oder periodisch konfiguriert werden. Bei einem Betrieb im zyklischen Modus muss durch Eingabe eines geeigneten MAST-Watchdog-Werts eine maximale Ausführungszeit festgelegt werden. Fügen Sie diesem Wert am Ende jedes Zyklus ein kleines Zeitintervall hinzu, um die Ausführung der Systemtasks mit niedrigerer Priorität zu ermöglichen. Da die AUX-Tasks eine niedrigere Priorität besitzen als die MAST-Task, kann es vorkommen, dass die AUX-Task nie ausgeführt werden, wenn dieses Zeitfenster nicht bereitgestellt wird. Ziehen Sie ein zusätzliches Zeitintervall von 10 % der Zyklusausführungszeit in Betracht, mit einem Mindestwert von 1 ms und einem Höchstwert von 10 ms.

Wenn die zur Ausführung einer zyklischen MAST-Task erforderliche Zeit die Watchdog-Einstellung überschreitet, wechseln die MAST-Task sowie alle anderen nicht-sicheren Tasks in den HALT-Zustand und das Systemwort %SW125 gibt den Fehlercode 16#DEB0 an.

Bei einem Betrieb im periodischen Modus kann die MAST-Task die zugehörige Dauer überschreiten. In diesem Fall wird die MAST-Task im zyklischen Modus ausgeführt und das Systembit %S11 wird gesetzt.

FAST-Task:

Aufgabe dieser periodischen Task ist die Ausführung eines Anwendungsteils mit hoher Priorität. Legen Sie durch Einstellung des FAST-Watchdog-Werts eine maximale Ausführungszeit fest. Da die FAST-Task die Ausführung aller anderen Tasks – einschließlich der SAFE-Task – unterbricht, sollte die Ausführungszeit der FAST-Task so kurz wie möglich eingestellt werden. Der Watchdog-Wert der FAST-Task sollte nicht viel größer sein als die FAST-Dauer.

Wenn die zur Ausführung der FAST-Task erforderliche Zeit die Watchdog-Einstellung überschreitet, wechseln die FAST-Task sowie alle anderen nicht-sicheren Tasks in den HALT-Zustand und das Systemwort %SW125 gibt den Fehlercode 16#DEB0 an.

AUX-Tasks:

AUX0 und AUX1 sind optionale periodische Tasks. Ihre Aufgabe ist die Ausführung eines Anwendungsteils mit niedrigerer Priorität. Die AUX-Tasks werden erst nach Abschluss der Ausführung der MAST-, der SAFE- und der FAST-Task ausgeführt.

Legen Sie die maximale Ausführungszeit für die AUX-Tasks durch Einstellung eines geeigneten Watchdog-Werts fest. Wenn die zur Ausführung der AUX-Tasks erforderliche Zeit die Watchdog-Einstellung überschreitet, wechseln die AUX-Tasks sowie alle anderen nicht-sicheren Tasks in den HALT-Zustand und das Systemwort %SW125 gibt den Fehlercode 16#DEB0 an.

Gestaltung eines M580-Sicherheitsprojekts

Generierung eines M580-Sicherheitsprojekts

Generieren eines M580-Sicherheitsprojekts

Das Menü **Generieren** in Control Expert für Sicherheitsanwendungen stellt drei verschiedene Generierungsbefehle sowie einen SAFE-Signatur-Befehl zur Auswahl:

Befehl	Beschreibung
Änderungen generieren	Es werden nur die Änderungen kompiliert, die seit dem vorherigen Generierungsbefehl am Anwendungsprogramm vorgenommen wurden, und dem zuvor generierten Anwendungsprogramm hinzugefügt.
Gesamtes Projekt neu generieren	Das gesamte Anwendungsprogramm wird neu kompiliert und dadurch das zuvor generierte Anwendungsprogramm ersetzt. **HINWEIS:** Bei M580-E/A-Sicherheitsmodulen wird über diesen Befehl kein neuer MUID-Wert (Module Unique Identifier) generiert. Stattdessen wird der zuvor generierte MUID-Wert beibehalten.
IDs erneuern & Alles generieren	Das gesamte Anwendungsprogramm wird neu kompiliert und dadurch das zuvor generierte Anwendungsprogramm ersetzt. **HINWEIS:** • Führen Sie diesen Befehl nur aus, wenn die E/A-Sicherheitsmodule nicht gesperrt, Seite 291 sind. • Bei M580-E/A-Sicherheitsmodulen wird über diesen Befehl ein neuer MUID-Wert (Module Unique Identifier) generiert und dadurch der vorhandene MUID-Wert ersetzt.
SAFE-Signatur aktualisieren	Mithilfe dieses Befehls können Sie manuell eine Signatur der SAFE-Quelle, Seite 283 für die Sicherheitsanwendung generieren. **HINWEIS:** Dieser Befehl ist nur aktiviert, wenn der Parameter **Allgemein > Generierungseinstellungen > Verwaltung der SAFE-Sicherheit** auf **Bei Benutzeraufforderung** eingestellt wird.

SAFE-Signatur

Einführung

M580-Sicherheits-PACs - sowohl in Standalone- als auch in Hot Standby-Installationen - umfassen einen Mechanismus zur Erzeugung eines algorithmusbasierten SHA256-Fingerprints der Sicherheitsanwendung: die Signatur der SAFE-Quelle (SourceSafeSignature). Bei der Übertragung einer Anwendung vom PC in den PAC vergleicht Control Expert die Signatur der SAFE-Quelle im PC mit der Signatur der SAFE-

Quelle im PAC, um zu ermitteln, ob die Sicherheitsanwendun im PC mit derjenigen im PAC übereinstimmt oder sich davon unterscheidet.

Die Funktion der SAFE-Signatur ist optional. Die Generierung einer SAFE-Quellsignatur kann je nach Größe der Sicherheitsanwendung ein zeitaufwändiger Prozess sein. Mithilfe der Optionen zur SAFE-Signaturverwaltung können Sie eine SAFE-Quellsignatur erzeugen, die einen algorithmusbasierten Wert für Ihre Sicherheitsanwendung erstellt:

- bei jeder Generierung oder
- nur dann, wenn Sie manuell eine Signatur der SAFE-Quelle erzeugen und diese zur neuesten Generierung hinzufügen möchten, oder
- überhaupt nicht

Aktionen, die eine Änderung der Signatur der SAFE-Quelle bewirken

Sowohl Änderungen an der Konfiguration als auch Änderungen von Variablenwerten können eine Änderung der SAFE-Quellsignatur zur Folge haben.

Konfigurationsänderungen: Folgende konfigurationsbezogene Aktionen bewirken eine Änderung der Signatur:

Gerät	Aktion
Sicherheits-CPU	Änderung der CPU-Referenz über **Prozessor ersetzen...**
	Änderung der CPU-Version über **Prozessor ersetzen...**
	Bearbeitung der Parameter auf der Konfigurationsregisterkarte der CPU **Konfiguration** oder **Hot Standby**
	Bearbeitung der Parameter auf einer beliebigen Registerkarte des Ethernet-Kommunikationskopfmoduls der CPU (**Sicherheit**, **IP-Konfig.**, **RSTP**, **SNMP**, **NTP**, **Service-Port**, **Sicherheit**...).
Sicherheitskoprozessor	Nicht zutreffend, da der Koprozessor nicht konfiguriert werden kann.
Anderes Sicherheitsmodul	**Hinzufügen**/**Löschen**/**Verschieben** eines Moduls: • Direkt (über einen Befehl) • Indirekt (z. B. Ersetzen eines Ethernet-Baugruppenträgers mit 8 Steckplätzen - mit einem Sicherheitsmodul in Steckplatz 7 - durch einen Ethernet-Baugruppenträger mit 4 Steckplätzen, wodurch ein Modul gelöscht wird)
	Bearbeitung der Sicherheitsmodulparameter auf der Registerkarte **Konfiguration** (z. B. **Kurzschlusserkennung an 24 V**, **Offene Draht-Erkennung**) und im linken Teilfenster des Editors (z. B. **Funktion**, **Fehlermodus**).
	Änderung der Modul-ID über den Befehl **IDs erneuern & Alles generieren**

Gerät	Aktion
	Änderung des Namens der Geräte-DDT-Instanz
CIP Safety-Modul	**Hinzufügen**/**Löschen** eines Moduls
	Änderung der Parameter des CIP Safety-Moduls im DTM-Editor des CIP Safety-Geräts oder in der **Geräteliste** im DTM-Editor des CPU-Masters
	Änderung des Namens der Geräte-DDT-Instanz
Sicherheitsspannungsversorgung	**Hinzufügen**/**Löschen** einer Sicherheitsspannungsversorgung
Anderes sicherheitsbezogenes Gerät	Änderung der topologischen Adresse eines Geräts, das ein Sicherheitsgerät unterstützt, z. B.: • Verschieben eines Racks mit einem Sicherheitsgerät • Verschieben eines Busses oder einer Station mit einem Sicherheitsgerät

Wertänderungen: Wenn nicht anders angegeben, werden die folgenden Elemente bei der Berechnung der Signatur der SAFE-Quelle berücksichtigt: Eine Änderung der folgenden Werte bewirkt eine Änderung der Signatur der SAFE-Quelle:

Typ	Elemente
Programm	SAFE-Task und zugehörige Code-Sections
Variablen	Alle Variablen des Sicherheitsbereichs und die zugehörigen Attribute
DDTs	Alle Attribute der Sicherheits-DDTs, außer Datums- und Versionsattribute
	Die Variablen innerhalb der DDTs, einschließlich der zugehörigen Attribute
	Die Sicherheits-DDTs, selbst wenn nicht in der Sicherheitsanwendung benutzt
DFBs	Alle Attribute der Sicherheits-DFBs, außer Datums- und Versionsattribute
	Die Variablen innerhalb der DFBs, einschließlich der zugehörigen Attribute
	Die Sicherheits-DFBs, selbst wenn nicht in der Sicherheitsanwendung benutzt
Einstellungen für den Sicherheitsbereich	Alle **Projekteinstellungen** für **Bereich** = sicher
Allgemeine Bereichseinstellungen	Folgende **Projekteinstellungen** für **Bereich** = allgemein/gemeinsam:
	Variablen • Führende Zahlen zulassen • Zeichensatz • Verwendung von EBOOL-Flanke zulässig • INT/DINT anstelle von ANY_BIT zulässig • Bit-Extraktion von INT, WORD und BYTE zulässig

Typ	Elemente
	• Direkt dargestellte Array-Variablen • Schnellabfrage zur Trenderstellung aktivieren • Referenzinitialisierung forcieren
	Programm > Sprachen > Allgemein • Prozeduren zulässig • Geschachtelte Kommentare zulässig • Mehrfachzuweisung zulässig [a:=b:=c] (ST/LD) • Leere Parameter bei informalem Aufruf zulässig (ST/IL) • Ausgangsverbindungen bei deaktivierten EF halten (EN=0) • Komplette Kommentare des Strukturelements anzeigen
	Programm > Sprachen > LD • Flankenerkennung in einem Zyklus für EBOOL
	Allgemein > Uhrzeit[1] • Benutzerdefinierte Zeitzone • Zeitzone • Zeitausgleich • Uhr automatisch an Sommer-/Winterzeit anpassen ◦ Alle START- und ENDE-Einstellungen für „Uhr automatisch an Sommer-/Winterzeit anpassen“
1. Diese Variablen werden nicht exportiert, eine Änderung ihrer Werte bewirkt jedoch eine Änderung der Teilsignatur der Konfiguration.	

Verwalten der Signatur der SAFE-Quelle

Die Signatur der SAFE-Quelle in Control Expert kann im Fenster **Extras > Projekteinstellungen** verwaltet werden. Wählen Sie dazu **Allgemein > Generierungseinstellungen** und dann eine der folgenden Einstellungen zur **Verwaltung der SAFE-Signatur** aus:

- **Automatisch** (Standard): Generiert eine neue SAFE-Quellsignatur bei jeder Ausführung des Befehls **Generieren**.
- **Bei Benutzeraufforderung**: Generiert eine neue SAFE-Quellsignatur bei Ausführung des Befehls **Generieren > SAFE-Signatur aktualisieren**.

  HINWEIS: Wenn Sie **Bei Benutzeraufforderung** auswählen generiert Control Expert bei jeder Generierung eine Signatur der SAFE-Quelle mit dem Wert 0. Wenn Sie den Befehl **Generieren > SAFE-Signatur aktualisieren** nicht ausführen, bedeutet das, dass Sie die SAFE-Signatur-Funktion nicht verwenden möchten.

Übertragen einer Anwendung vom PC in die SPS

Beim Download einer Anwendung vom PC in die SPS vergleicht Control Expert die Signatur der SAFE-Quelle in der heruntergeladenen Anwendung mit derjenigen im PAC. Control Expert verhält sich wie folgt:

Neue SAFE-Signatur	SAFE-Signatur des PAC	Anzeige in Control Expert
Beliebig	Keine Anwendung	Übertragungsbestätigung
Beliebig (außer 0)	0	Übertragungsbestätigung
0	0	Übertragungsbestätigung
0	Beliebig (außer 0)	Übertragungsbestätigung, gefolgt vom Hinweis „Hierdurch wird die SAFE-Signatur zurückgesetzt“ und einer neuen Übertragungsbestätigung
XXXX = YYYY[2]	YYYY	Übertragungsbestätigung
XXXX ≠ YYYY[3]	YYYY	Übertragungsbestätigung, gefolgt vom Hinweis „Hierdurch wird die SAFE-Signatur geändert“ und einer neuen Übertragungsbestätigung
1. Der Wert „0“ gibt an, dass keine Signatur der SAFE-Quelle automatisch oder manuell generiert wurde. 2. Die Sicherheitsanwendung im PC (XXXX) und diejenige im PAC (YYYY) sind IDENTISCH. 3. Die Sicherheitsanwendung im PC (XXXX) und diejenige im PAC (YYYY) sind VERSCHIEDEN.		

Anzeigen der Signatur der SAFE-Quelle

Sofern die Signatur der SAFE-Quelle verwendet wird, setzt sie sich aus einer Reihe hexadezimaler Werte zusammen und kann extrem lang ausfallen, was das Lesen und den Vergleich des Signaturwerts für den Benutzer äußerst schwierig gestaltet. Es besteht jedoch die Möglichkeit, die Signatur der SAFE-Quelle zu kopieren und zum Vergleich in einem geeigneten Texttool einzufügen. Der Wert der SAFE-Quellsignatur ist in Control Expert in folgenden Speicherpfaden zu finden:

- Registerkarte **Eigenschaften von Projekt > Identifikation**EcoStruxure™ Control Expert, Betriebsarten: Klicken Sie im **Projekt-Browser** mit der rechten Maustaste auf **Projekt** und wählen Sie **Eigenschaften** aus.
- Registerkarte **SPS-Fenster > Informationen**EcoStruxure™ Control Expert, Betriebsarten: Navigieren Sie im **Projekt-Browser** zu **Projekt > Konfiguration > SPS-Bus > <CPU>**, klicken Sie mit der rechten Maustaste und wählen Sie **Öffnen** und dann die Registerkarte **Animation** aus.
- Dialogfeld **PC < - - > SPS-Vergleich**EcoStruxure™ Control Expert, Betriebsarten: Wählen Sie diesen Befehl im Menü **SPS** aus.

- Dialogfeld **Projekt zur SPS übertragen**EcoStruxure™ Control Expert, Betriebsarten: Wählen Sie diesen Befehl im Menü **SPS** aus (oder im Dialogfeld **PC < - - > SPS-Vergleich**).

Vergleichen der Signatur der SAFE-Quelle mit der SAId

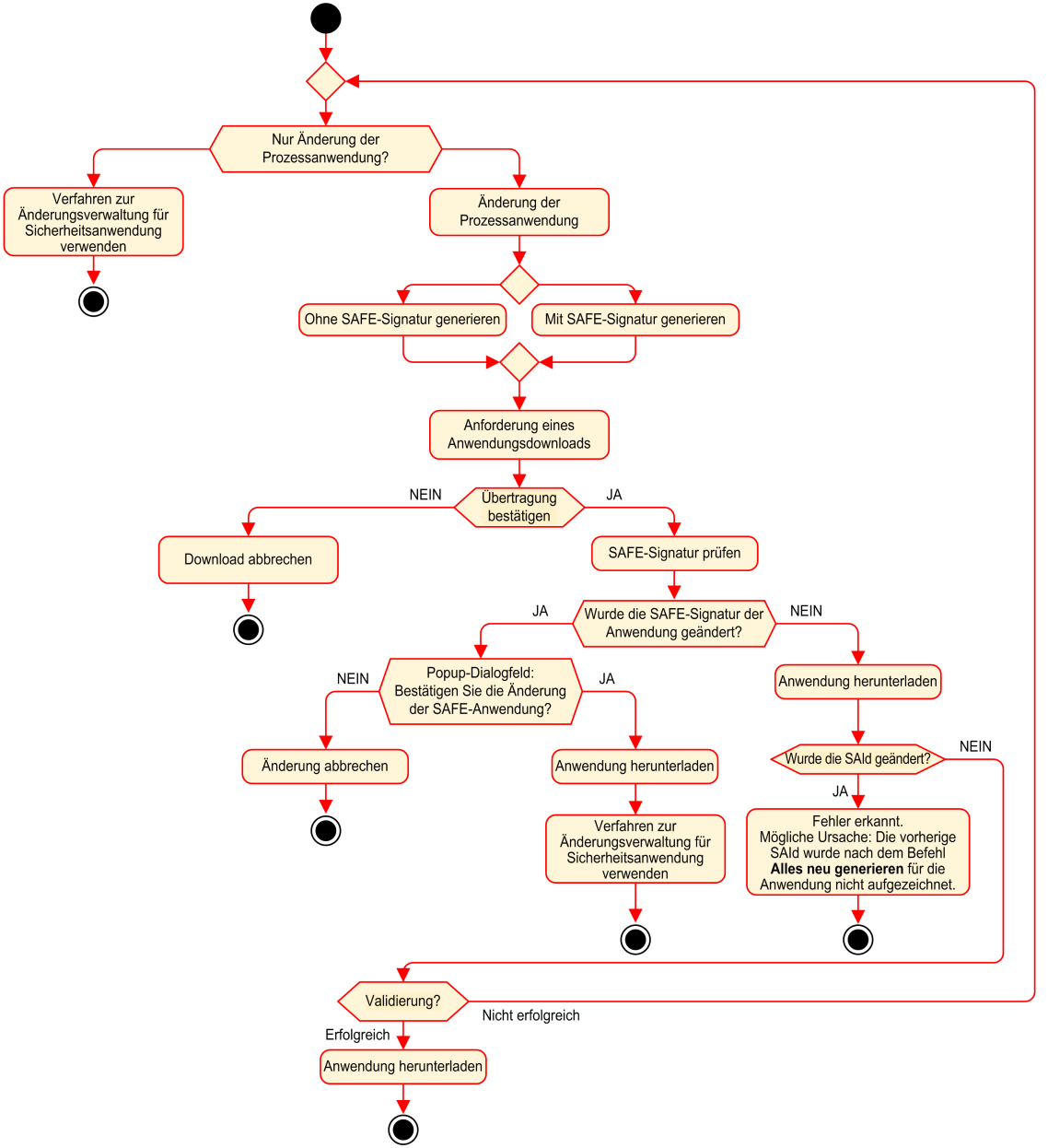
Die Signatur der SAFE-Quelle wurde eingeführt, um eine *Vorabkontrolle* zu ermöglichen und sicherzustellen, dass die Sicherheitsanwendung unverändert ist. Es wird empfohlen, diese Funktion bei jeder Änderung der Prozessanwendung, Seite 289 einzusetzen, um jede unbeabsichtigte Änderung der Sicherheitsanwendung zu vermeiden.

Die Signatur der SAFE-Quelle ist ein zuverlässiger Mechanismus, jedoch für Sicherheitsanwendungen nicht ausreichend, da derselbe Quellcode unterschiedlichen (ausführbaren) Binärcodes entsprechen kann, je nach Art der Generierung im Anschluss an die letztenÄnderung des Sicherheitscodes.

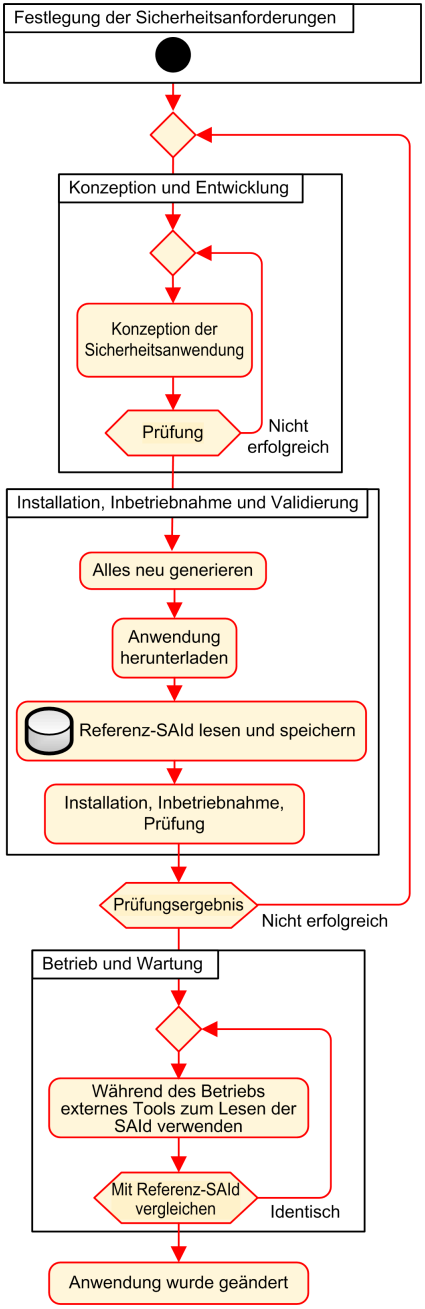
Die SAId, Seite 381 kann nur während des Betriebs bewertet werden. Ihre Berechnung wird doppelt ausgeführt und sowohl von der CPU als auch vom KOPRO mit dem von der Sicherheitsanwendung ausgeführten Binärcode verglichen. Da die SAId von sämtlichen Änderungen beeinflusst werden kann, einschließlich der ggf. über den Befehl **Alles neu generieren** nach einer Generierungsänderung bewirkten Änderungen, wird empfohlen, den Befehl **Alles neu generieren** zur Generierung einer Referenzversion der Sicherheitsanwendung heranzuziehen. Dieser Prozess, Seite 290 ermöglicht Ihnen die Verwendung jeder beliebigen Generierungsart(**Alles neu generieren**, **Änderungen generieren** online oder offline) für die Änderungen der Prozessanwendung, ohne dass eine Änderung an der SAId vorgenommen wird.

Die SAId ist die empfohlene Methode zur Gewährleistung, dass es sich bei der Sicherheitsanwendung um die validierte Anwendung handelt. Der SAId-Wert wird nicht automatisch von der Anwendung getestet. Aus diesem Grund sollte die SAId regelmäßig mit einem geeigneten Hilfsmittel (z. B. Control Expert oder ein HMI) durch Lesen des Ausgangs des Funktionsbausteins S_SYST_STAT_MX oder des Inhalts des Systemworts %SW169, Seite 414 geprüft werden.

Ändern der Prozessanwendung - Vereinfachtes Verfahren



SAId-Verwaltung



Sperre der Konfiguration der M580-E/A-Sicherheitsmodule

Sperre der Konfiguration der M580-E/A-Sicherheitsmodule

Sperren der Konfiguration der E/A-Sicherheitsmodule

Jedes E/A-Sicherheitsmodul ist an der Frontseite oben mit einer Taste zur Konfigurationssperre (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) ausgestattet. Aufgabe der Sperrfunktion ist die Verhinderung unbeabsichtigter Änderungen an der E/A-Modulkonfiguration. So kann die Sperre der aktuellen Konfiguration eines E/A-Moduls beispielsweise verhindern, dass dem Modul eine ungültige Konfiguration zugewiesen wird, oder ganz allgemein Konfigurationsfehler unterbinden.

Um den gewünschten Sicherheits-Integritätslevel (SIL) zu erreichen, sollte jedes E/A-Sicherheitsmodul nach der Konfiguration vor (Wieder-) Aufnahme des Betriebs gesperrt werden.

⚠WARNUNG

GEFAHR EINER UNBEABSICHTIGTEN BEEINTRÄCHTIGUNG DES PROJEKTSPEZIFISCHEN SICHERHEITS-INTEGRITÄTSLEVELS

Sie müssen jedes E/A-Sicherheitsmodul nach dessen Konfiguration und vor Beginn des Betriebs sperren.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Funktionsweise des Sperr- und Entsperrmechanismus:

- Um die Konfiguration eines E/A-Moduls zu sperren, drücken und halten Sie die Sperrtaste mehr als 3 Sekunden lang gedrückt und lassen Sie sie dann wieder los.
- Um die Konfiguration eines E/A-Moduls zu entsperren, drücken und halten Sie die Sperrtaste mehr als 3 Sekunden lang gedrückt und lassen Sie sie dann wieder los.

Situationen für die Sperre der Konfiguration von E/A-Sicherheitsmodulen

Das Verfahren zur Sperre der Konfiguration von SIL3-E/A-Sicherheitsmodulen fällt je nach Situation unterschiedlich aus. Folgende Situationen sind möglich:

- Erstkonfiguration der E/A-Module
- Schneller Geräteaustausch der E/A-Module
- Durchführung einer CCOTF-Änderung (Change Configuration On The Fly) der E/A-Module

Das Verfahren für jede dieser Situationen wird nachstehend beschrieben.

Erstkonfiguration der SIL3-E/A-Sicherheitsmodule:

Schritt	Aktion
1	Verbinden Sie Control Expert mit dem M580-Sicherheits-PAC.
2	Laden Sie das Projekt über den Befehl **Projekt von SPS übertragen** aus dem PAC in Control Expert.
3	Öffnen Sie im Control Expert-Fenster **SPS-Bus** alle SIL3-E/A-Sicherheitsprojekte und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert wurde.
4	Zeigen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul an und stellen Sie sicher, dass die Konfiguration jedes Moduls derjenigen in Schritt 3 oben entspricht.
5	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) für mehr als 3 Sekunden. Lassen Sie die Taste dann wieder los.
6	Überprüfen Sie in einer Animationstabelle die Gültigkeit des Sperrbit-Status (CONF_LOCKED) für jedes SIL3-E/A-Modul.

Schneller Geräteaustausch der SIL3-E/A-Sicherheitsmodule:

Schritt	Aktion
1	Ersetzen Sie das SIL3-E/A-Sicherheitsmodul durch ein neues.
2	Verbinden Sie Control Expert mit dem M580-Sicherheits-PAC im Wartungsmodus, Seite 265
3	Öffnen Sie im Control Expert-Fenster **SPS-Bus** alle SIL3-E/A-Sicherheitsprojekte und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert wurde.
4	Zeigen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul an und stellen Sie sicher, dass die Konfiguration jedes Moduls nicht geändert wurde und derjenigen in Schritt 3 oben entspricht.
5	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) für mehr als 3 Sekunden. Lassen Sie die Taste dann wieder los.
6	Überprüfen Sie in einer Animationstabelle die Gültigkeit des Sperrbit-Status (CONF_LOCKED) für jedes SIL3-E/A-Modul.

Durchführung einer CCOTF-Änderung, um ein neues SIL3-E/A-Sicherheitsmodul hinzuzufügen:

Schritt	Aktion
1	Verbinden Sie Control Expert mit dem M580-Sicherheits-PAC im Wartungsmodus, Seite 265
2	Fügen Sie in der Konfiguration ein neues SIL3-E/A-Sicherheitsmodul hinzu und bearbeiten Sie nach Bedarf die Moduleinstellungen
3	Führen Sie den Befehl **Generieren > Änderungen generieren** aus.
4	Öffnen Sie im Control Expert-Fenster **SPS-Bus** alle SIL3-E/A-Sicherheitsprojekte und vergewissern Sie sich, dass jedes Modul ordnungsgemäß konfiguriert wurde.
5	Zeigen Sie in einer Animationstabelle in Control Expert den DDDT für jedes SIL3-E/A-Sicherheitsmodul an und stellen Sie sicher, dass die Konfiguration jedes Moduls nicht geändert wurde und derjenigen in Schritt 3 oben entspricht.
6	Sperren Sie die Konfiguration jedes SIL3-E/A-Moduls durch Drücken und Gedrückthalten der Konfigurationssperrtaste (siehe Modicon M580, Sicherheitssystem - Planungshandbuch) für mehr als 3 Sekunden. Lassen Sie die Taste dann wieder los.
7	Überprüfen Sie in einer Animationstabelle die Gültigkeit des Sperrbit-Status (CONF_LOCKED) für jedes SIL3-E/A-Modul.
8	Setzen Sie den PAC über das Control Expert-Menü **SPS** in den Sicherheitsmodus, Seite 264.

Initialisierung der Daten in Control Expert

Initialisierung der Daten in Control Expert für den M580-Sicherheits-PAC

Zwei Initialisierungsbefehle

Das Menü **SPS** in Control Expert stellt zwei separate Befehle zur Dateninitialisierung bereit:

- Der Befehl **Init** initialisiert die Daten für den prozessspezifischen (oder nicht-sicheren) Namespace, die von der MAST-, der FAST-, der AUX0- und der AUX1-Task verwendet werden können. Sie können diesen Befehl ausführen, wenn der PAC im Sicherheits- oder Wartungsmodus läuft und sich im STOP-Zustand befindet. Dieser Befehl entspricht dem Setzen des Systembits %S0 (COLDSTART) auf 1.

  HINWEIS: Durch Setzen des Bits %S0 auf 1 werden nur die Daten im Prozess-Namespace initialisiert. Die Daten im sicheren Namespace sind hiervon nicht betroffen.

- Der Befehl **Init Safety** initialisiert nur die Daten für den sicheren Namespace, die ausschließlich von der SAFE-Task verwendet werden können. Sie können diesen Befehl nur dann ausführen, wenn die SAFE-Task im Wartungsmodus läuft und sich im STOP- oder HALT-Zustand befindet. Wenn der Befehl ausgeführt wird, während sich die SAFE-Task im HALT-Zustand befindet, wird die SAFE-Task im STOP-Zustand neu gestartet.

Sowohl der Befehl **Init** als auch der Befehl **Init Safety** lösen einen Kaltstart, Seite 278 aus.

Verwendung der Animationstabellen in Control Expert

Animationstabellen und Bedienerfenster

Einführung

Ein M580-Sicherheits-PAC unterstützt drei Arten von Animationstabellen, von denen jede einem der folgenden Datenbereich zugeordnet ist:

- Animationstabellen des Prozessbereichs enthalten ausschließlich Daten des Prozess-Namespace.
- Animationstabellen des Sicherheitsbereichs enthalten ausschließlich Daten des sicheren Namespace.
- Globale Animationstabellen können Daten für die gesamte Anwendung enthalten, einschließlich Daten, die für den sicheren und den prozessspezifischen Namespace erstellt wurden, sowie globale Variablen.

  HINWEIS: Die Datenvariablennamen in einer globalen Animationstabelle umfassen ein Präfix, das auf den Quell-Namespace verweist:

  - Eine Datenvariable des sicheren Namespace wird angezeigt als „SAFE. <varname>“.
  - Eine Datenvariable des Prozess-Namespace wird angezeigt als „PROCESS. <Variablenname>“.
  - Eine Datenvariable des globalen (oder anwendungsspezifischen) Namespace wird nur mit dem entsprechenden <Variablennamen> ohne Namespace-Präfix angezeigt.

Sowohl die prozess- als auch die sicherheitsbezogenen Daten eines M580-Sicherheits-PAC sind ebenfalls über externe Prozesse zugänglich (z. B. SCADA oder HMI).

Die Möglichkeit zur Erstellung und Änderung einer Animationstabelle sowie zur Ausführung der Funktionen einer Animationstabelle ist vom Namespace der betroffenen Variablen und von der Betriebsart des Sicherheitsprojekts abhängig.

Voraussetzungen für die Erstellung und Bearbeitung von Animationstabellen

Die Erstellung und Bearbeitung von Animationstabellen beinhaltet das Hinzufügen und Löschen von Datenvariablen. Die Möglichkeit zum Hinzufügen oder Löschen von Datenvariablen in einer Animationstabelle ist abhängig von folgenden Elementen:

- Namespace (sicher oder prozessspezifisch), in dem sich die Datenvariablen befinden.

- Betriebsart (Sicherheits- oder Wartungsmodus) des M580-Sicherheits-PAC.

Wenn Control Expert mit dem M580-Sicherheits-PAC verbunden ist, können Sie Animationstabellen erstellen und bearbeiten. Dazu stehen folgende Möglichkeiten zurm Auswahl:

- Das Hinzufügen oder Löschen von Variablen des Prozess-Namespace in einer prozessspezifischen oder globalen Animationstabelle wird unterstützt, wenn sich der M580-Sicherheits-PAC im Sicherheits- oder Wartungsmodus befindet.
- Das Hinzufügen oder Löschen von Variablen des sicheren Namespace in einer Sicherheits-Animationstabelle wird unterstützt, wenn sich der M580-Sicherheits-PAC im Wartungsmodus befindet.
- Das Hinzufügen oder Löschen von Variablen des sicheren Namespace in einer Sicherheits-Animationstabelle wird unterstützt, wenn sich der M580-Sicherheits-PAC im Sicherheitsmodus befindet, sofern in den Auslese-Informationen der Projekteinstellungen keine Animationstabellen enthalten sind.

  HINWEIS: Animationstabellen können durch Auswahl von **Tools > Projekteinstellungen...** von den Auslese-Informationen in Control Expert ausgeschlossen bzw. in diese aufgenommen werden. Dadurch wird das Fenster **Projekteinstellungen...** geöffnet, in dem Sie **Projekteinstellungen > Allgemein > SPS-integrierte Daten > Auslese-Information > Animationstabellen** auswählen.

Voraussetzungen für die Verwendung von Animationstabellen

Sie können Animationstabellen verwenden, um einen Variablenwert zu forcieren bzw. dessen Forcierung aufzuheben, einen einzelnen Variablenwert bzw. mehrere Variablenwerte zu ändern. Die Möglichkeit zur Nutzung dieser Funktionen ist vom Namespace abhängig, in dem sich die Variable befindet, sowie von der Betriebsart des M580-Sicherheits-PAC:

- Die prozessspezifischen oder globalen Variablenwerte können sowohl im Sicherheits- als auch im Wartungsmodus gelesen und geschrieben werden.
- Die Werte der Sicherheitsvariablen können im Wartungsmodus gelesen und geschrieben werden.
- Die Werte der Sicherheitsvariablen können im Sicherheitsmodus nur gelesen werden.

Prozess für die Erstellung von Animationstabellen im sicherheits- oder prozessspezifischen Namespace in Control Expert

Control Expert stellt zwei Verfahren für die Erstellung von Animationstabellen für den sicherheits- oder prozessspezifischen Namespace zur Auswahl:

- Klicken Sie im Fenster einer Sicherheits- oder Prozesscode-Section mit der rechten Maustaste in das Code-Fenster und wählen Sie dann eines der folgenden Elemente:
  - **Animationstabelle initialisieren**, um das Datenobjekt in einer vorhandenen Animationstabelle im Sicherheits- oder Prozess-Namespace hinzuzufügen.
  - **Neue Animationstabelle initialisieren**, um das Datenobjekt in einer neuen Animationstabelle im Sicherheits- oder Prozess-Namespace hinzuzufügen.

  In beiden Fällen werden alle Variablen in der Code-Section in der bereits vorhandenen bzw. neuen Animationstabelle hinzugefügt.
- Klicken Sie im **Projekt-Browser** entweder im Bereich der Prozess- oder der Sicherheitsdaten mit der rechten Maustaste auf den Ordner **Animationstabellen** und wählen Sie dann **Neue Animationstabelle** aus. Control Expert erstellt eine neue, leere Animationstabelle. Sie können dann einzelne Variablen aus dem mit der Tabelle verknüpften (sicherheits- oder prozessspezifischen) Namespace hinzufügen.

Prozess für die Erstellung globaler Animationstabellen

Erstellen Sie eine globale Animationstabelle im **Projekt-Browser** durch einen Rechtsklick auf den Ordner der globalen **Animationstabellen** und die anschließende Auswahl von **Neue Animationstabelle**. Sie können in der neuen Animationstabelle Variablen hinzufügen. Dazu stehen Ihnen folgende Möglichkeiten zur Auswahl:

- *Ziehen und Ablegen*: Sie können eine Variable aus einem Daten-Editor ziehen und in der globalen Animationstabelle ablegen. Da die Animationstabelle für die gesamte Anwendung gilt, können Sie die Variable aus dem **Sicherheitsdaten-Editor**, dem **Prozessdaten-Editor** oder dem **Globalen Daten-Editor** ziehen und ablegen.
- *Dialogfeld „Instanzauswahl“*: Sie können in eine Zeile in der Animationstabelle doppelklicken und dann auf die Schaltfläche mit den Auslassungspunkten klicken, um das Dialogfeld **Instanzauswahl** zu öffnen. Verwenden Sie die Filterliste im oberen rechten Bereich des Dialogfelds, um einen der folgenden Projektbereiche auszuwählen:
  - SAFE: Anzeige der dem Sicherheitsbereich zugeordneten Datenobjekte.
  - PROCESS: Anzeige der dem Prozessbereich zugeordneten Datenobjekte.
  - APPLICATION: Anzeige der anwendungsspezifischen Datenobjekte einer höheren Ebene.

  Wählen Sie ein Datenobjekt aus und klicken Sie dann auf **OK**, um das Element in der Animationstabelle hinzuzufügen.

HINWEIS: Die in einer globalen Animationstabelle hinzugefügten Datenobjekte:

- des Prozessbereichs weisen das Präfix „PROCESS“ im Variablennamen auf (z. B. PROCESS.variable_01.
- des Sicherheitsbereichs weisen das Präfix „SAFE“ im Variablennamen auf (z. B. SAFE.variable_02.
- des globalen Bereichs verfügen über kein Präfix im Variablennamen.

Anzeige der Daten in den Bedienerfenstern

Sie können Daten in einem Bedienerfenster – z. B. HMI, SCADA oder FactoryCast-Anwendung – auf dieselbe Weise anzeigen, wie Sie eine Verbindung zu Daten in einer Animationstabelle herstellen. Die zur Auswahl stehenden Datenvariablen sind die im Datenwörterbuch von Control Expert enthaltenen Variablen.

Sie können das Datenwörterbuch aktivieren, indem Sie das Fenster **Tools > Projekteinstellungen...** öffnen und dann in **Bereich > Allgemein** die Option **Allgemein > SPS-integrierte Daten > Datenwörterbuch** auswählen.

Das Datenwörterbuch stellt Datenvariablen in den Bedienerfenstern zur Verfügung:

- Die Variablen des sicheren Namespace umfassen das Präfix „SAFE“ und sind nur über das Format „SAFE.<Variablenname>“ zugänglich.
- Die Variablen des globalen oder anwendungsspezifischen Namespace umfassen kein Präfix und sind nur über den „<Variablennamen>“ ohne Präfix zugänglich.
- Die Einstellung **Nutzung des Prozess-Namespace** legt fest, wie ein Bedienerfenster auf die Variablen des Prozess-Namespace zugreifen kann.
  - Bei Auswahl von **Nutzung des Prozess-Namespace** kann das Bedienerfenster die Variablen des Prozessbereich nur über das Format „PROCESS.<Variablenname>“ lesen.
  - Bei Aufhebung der Auswahl von **Nutzung des Prozess-Namespace** kann das Bedienerfenster die Variablen des Prozessbereich nur über das Format „<Variablenname> ohne PROCESS-Präfix lesen.

    HINWEIS: Wenn zwei Variablen mit demselben Namen deklariert werden, ein im Prozess-Namespace und die andere im globalen Namespace, dann ist nur die Variable im globalen Namespace für eine HMI-, SCADA- oder Factory Cast-Anwendung zugänglich.

Im Dialogfeld **Instanzauswahl** können Sie auf die einzelnen Datenobjekte zugreifen.

⚠VORSICHT
UNERWARTETER VARIABLENWERT • Stellen Sie sicher, dass Ihre Anwendung über angemessene Projekteinstellungen verfügt. • Überprüfen Sie die Syntax für den Zugriff auf die Variablen in den verschiedenen Namespaces. **Die Nichtbeachtung dieser Anweisungen kann Verletzungen oder Sachschäden zur Folge haben.**

Beachten Sie Folgendes, um einen Zugriff auf die falsche Variable zu vermeiden:

- Verwenden Sie unterschiedliche Namen für die im prozessspezifischen und im globalen Namespace deklarierten Variablen.
- Wählen Sie **Nutzung des Prozess-Namespace** aus und verwenden Sie folgende Syntax für den Zugriff auf Variablen mit demselben Namen:
  - „PROCESS.<Variablenname>“ für die im Prozess-Namespace deklarierten Variablen
  - „<Variablenname>“ ohne Präfix für die im globalen Namespace deklarierten Variablen

Trend-Erfassungstool

Das Trend-Erfassungstool von Control Expert wird nicht für eine Verwendung mit einem M580-Sicherheitsprojekt unterstützt.

Hinzufügen von Code-Sections

Hinzufügen von Code zu einem M580-Sicherheitsprojekt

Arbeiten mit Tasks in Control Expert

Im Prozess-Namespace enthält Control Expert standardmäßig die MAST-Task. Die MAST-Task kann nicht entfernt werden. Sie können jedoch die Tasks FAST, AUX0 und AUX1 hinzufügen. Beachten Sie, dass die Erstellung einer Task im Prozessteil eines Sicherheitsprojekts der Erstellung einer Task in einem nicht-sicheren Projekt entspricht. Weitere Informationen finden Sie unter *Erstellen und Konfigurieren einer* im *Handbuch der Betriebsarten von EcoStruxure™ Control Expert*.

In den sicheren Namespace integriert Control Expert standardmäßig die SAFE-Task. Die SAFE-Task kann nicht entfernt und keine andere Task kann in der Section **Programmsicherheit** im **Projekt-Browser** von Control Expert hinzugefügt werden. Sie können der SAFE-Task zahlreiche Sections hinzufügen.

Konfigurieren der Eigenschaften der SAFE-Task

Die SAFE-Task unterstützt nur die periodische Task-Ausführung (die zyklische Ausführung wird nicht unterstützt). Die Einstellungen **Dauer** und **Watchdog** der SAFE-Task werden im Dialogfeld **Eigenschaften der SAFE-Task** festgelegt und unterstützen folgenden Wertebereich:

- Periode der SAFE-Task: 10...255 ms mit dem Standardwert 20 ms.
- Watchdog der SAFE-Task: 10...500 ms, in Schritten von 10 ms, mit einem Standardwert von 250 ms.

Stellen Sie die **Dauer** der SAFE-Task auf einen Mindestwert in Abhängigkeit von der Größe der Sicherheitsdaten und dem SPS-Modell ein. Die Mindestdauer der SAFE-Task kann anhand der nachstehenden Formeln berechnet werden:

- Für eine sichere E/A-Kommunikation erforderlicher absoluter Mindestwert:
  - 10 ms
- Für die Übertragung und den Vergleich der Sicherheitsdaten zwischen CPU und KOPRO benötigte Zeit (in ms):
  - (0,156 x Data_Safe_Size) + 2 ms (für BMEP584040S, BMEP586040S, BMEH584040S und BMEH586040S)
  - (0,273 x Data_Safe_Size) + 2 ms (für BMEP582040S und BMEH582040S)

  Hierbei gilt: Data_Safe_Size entspricht der Größe der Sicherheitsdaten in KByte.

- Zusätzliche Zeit (in ms), die von den Hot Standby-PACS für die Übertragung der Sicherheitsdaten vom primären in den Standby-PAC benötigt wird:
  - $(K1 \times Task_{kb} + K2 \times Task_{DFB}) / 500$

  Für diese Formel gilt Folgendes:
  - $Task_{DFB}$ = Anzahl der im sicheren Teil der Anwendung deklarierten DFBs.
  - $Task_{kb}$ = Größe (in KByte) der von der SAFE-Task zwischen primärem und Standby-PAC ausgetauschten Sicherheitsdaten.
  - K1 und K2 sind Konstanten mit Werten, die von dem in der Anwendung eingesetzten spezifischen CPU-Modul vorgegeben werden:

Koeffizient	BMEH582040S	BMEH584040S und BMEH586040S
K1	32,0	10,0
K2	23,6	7,4

HINWEIS:

- Der mit diesen Formeln berechnete Wert ist ein absoluter Mindestwert für die Dauer der SAFE-Task und gilt nur für eine erste Schätzung des Zeitlimits für den SAFE-Zyklus. Er berücksichtigt nicht den Zeitraum, der für die Ausführung des Benutzercodes, bzw. nicht die Marge, die für den beabsichtigten Betrieb des PAC-spezifischen Multitask-Systems erforderlich ist. Weitere Informationen finden Sie im Thema Hinweise zum Systemdurchsatz im SM580 Standalone-Systemplanungshandbuch für verwendete Architekturen .
- Standardmäßig sind Data_Safe_Size und $Size_{kbytes}$ identisch. Diese Werte können über das Menü **SPS > Speicherbedarf** und im Fenster **SPS > Hot Standby** angezeigt werden.

Berechnungsbeispiele

Typische Ergebnisse der Berechnung der minimalen SAFE-Task-Dauer

Minimale Dauer der SAFE-Task (ms)					
$Size_{kbytes}$[1]	Nb_{DFB_Inst}	BMEP582040S	BMEP584040S oder BMEP586040S	BMEH582040S	BMEH584040S oder BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29
200	10	57	33	70	37

Minimale Dauer der SAFE-Task (ms)					
$Size_{kbytes}$[1]	**Nb_{DFB_Inst}**	**BMEP582040S**	**BMEP584040S oder BMEP586040S**	**BMEH582040S**	**BMEH584040S oder BMEH586040S**
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179
1. Es wird angenommen, dass $Size_{kbytes}$ und Data_Safe_Size gleich sind.					

HINWEIS: Konfigurieren Sie den Watchdog der SAFE-Task mit einem Wert, der größer ist als die **Dauer** der SAFE-Task.

Informationen zu den Auswirkungen der Konfiguration der SAFE-Task auf die Prozesssicherheitszeit finden Sie unter *Prozesssicherheitszeit*, Seite 156.

Eine Beschreibung der Ausführungspriorität der SAFE-Task finden Sie unter *Tasks des M580-Sicherheits-PAC*, Seite 279.

Erstellen der Code-Sections

Klicken Sie mit der rechten Maustaste auf den Ordner **Section** für eine Task und wählen Sie dann die Option **Neue Section...** aus, um ein Konfigurationsfenster zu öffnen. Für die Sicherheits- und die Prozesstasks sind folgende Programmiersprachen verfügbar:

Sprache	Sicherheits-tasks	Prozesstasks			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
LL984-Segment	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓: verfügbar – : nicht verfügbar					

Mit Ausnahme dieser Einschränkungen in Bezug auf die Verfügbarkeit der Programmiersprachen für die SAFE-Task verhält sich das Konfigurationsfenster für neue Sections genauso wie für ein nicht-sicheres M580-Projekt. Weitere Informationen finden Sie unter *Dialogfeld „Eigenschaften“ für FBD-, KOP-, AWL- oder ST-Sections im Handbuch der Betriebsarten von EcoStruxure™ Control Expert*.

Hinzufügen von Daten in den Code-Sections

Da die SAFE-Task von den Prozesstasks getrennt ist, können nur die im **Sicherheitsdateneditor** verfügbaren Daten in einer Code-Section der SAFE-Task hinzugefügt werden. Dazu gehören folgende Daten:

- Im **Sicherheitsdateneditor** erstellte nicht-lokalisierte Sicherheitsvariablen (d. h. ohne %M- oder %MW-Adresse).
- Datenobjekte, die den Geräte-DDT-Strukturen des M580-Sicherheitsmoduls angehören.

Desgleichen umfassen die für die Code-Sections der nicht-sicheren Tasks verfügbaren Daten sämtliche Daten innerhalb des Bereichs des Prozess-Namespace. Dazu gehören alle Projektdaten außer:

- Daten, die ausschließlich für den SAFE-Namespace verfügbar sind (siehe oben)
- Im **globalen Dateneditor** erstellte Datenobjekte

Codeanalyse

Bei der Analyse oder Generierung eines Projekts gibt Control Expert in folgenden Fällen eine Fehlermeldung aus:

- Daten, die dem Prozess-Namespace angehören, werden in die SAFE-Task aufgenommen.
- Daten, die dem sicheren Namespace angehören, werden in eine Prozesstask (MAST, FAST, AUX0, AUX1) aufgenommen.
- Lokalisierte Bits (%M) oder Wörter (%MW) werden in eine Section der SAFE-Task aufgenommen.

Diagnose-Anforderung

Einführung

Die Diagnose-Anforderung ist nur für M580-Sicherheitsspannungsversorgungen verfügbar, die sich auf einem Hauptrack befinden. Verwendet wird der Funktionsbaustein PWS_DIAG. Ein Hauptrack hat eine Adresse von 0 und in Steckplatz 0 oder 1 eine CPU oder ein Kommunikationsadaptermodul (CRA). Ein Erweiterungsrack ist kein Hauptrack.

Die CPU kann Diagnose-Anforderungen von redundanten Spannungsversorgungen im lokalen Rack stellen und über einen Kommunikationsadapter (CRA) von redundanten Spannungsversorgungen in einem dezentralen Rack. Wenn die Master- und Slave-Spannungsversorgungen funktionsfähig sind, wechselt die Master-Spannungsversorgung in den Master-Diagnosemodus und die Slave-Spannungsversorgung wechselt in den Slave-Diagnosemodus. Die LEDs zeigen, dass der Test durchgeführt wird.

HINWEIS: Diese Anforderung wird nicht implementiert, wenn das System gerade hochgefahren wird.

Nachdem der Diagnosetest abgeschlossen ist, kehrt der Master in den normalen Betriebszustand zurück und der Slave kehrt in den normalen oder den Fehlerzustand zurück, abhängig vom Testergebnis. Die Testergebnisse werden im Spannungsversorgungsspeicher gespeichert.

Von der Diagnose-Anforderung ausgegebene Daten

Zu den von den Spannungsversorgungen an die CPU gesendeten Diagnosedaten gehören folgende:

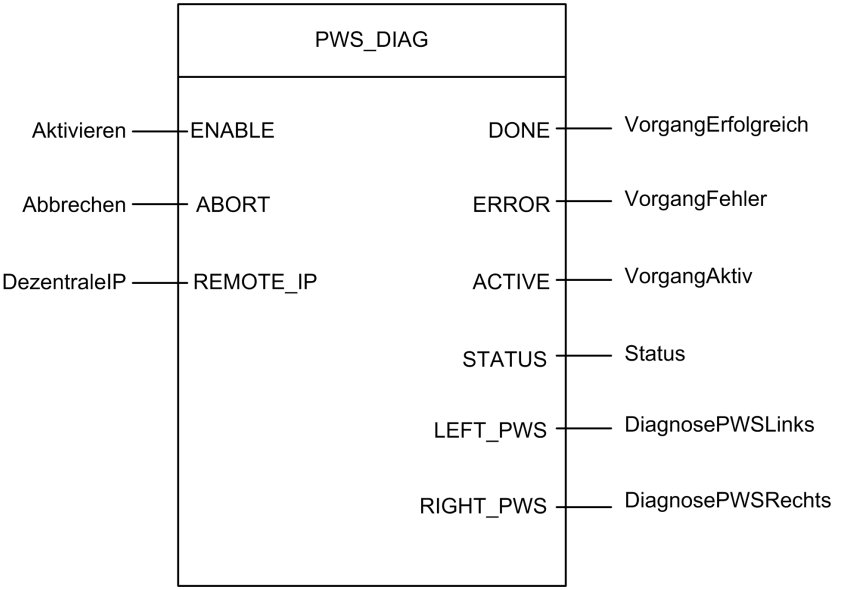
- Umgebungstemperatur der Spannungsversorgung
- Spannung und Strom auf der 3,3-V-Baugruppenträgerleitung
- Spannung und Strom auf der 24-VDC-Baugruppenträgerleitung
- Insgesamt kumulierte Energie der Spannungsversorgungen auf den 24-VDC- und 3,3-VDC-Baugruppenträgerleitungen seit Herstellung
- Betriebszeit als Master seit letztem Einschalten und seit Herstellung

- Gesamtbetriebszeit als Slave seit letztem Einschalten und seit Herstellung
- Verbleibende Lebenszeit in Prozent (LTPC): Zeit bis zur vorbeugenden Wartung zwischen 100 und 0 %

  HINWEIS: Kein Austausch bei 0 %.
- Anzahl der Einschaltvorgänge der Spannungsversorgung

  HINWEIS: Vom SCADA aus ist es möglich, die Anzahl der Einschaltvorgänge seit der Installation und alle anderen Diagnoseelemente zurückzusetzen.
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS4002S unter die Unterspannungsebene 1 gefallen ist (95 VAC).
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS4002S über die Übersapnnungsebene 2 angestiegen ist (195 VAC).
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS4022S unter die Unterspannungsebene 1 gefallen ist (20 VDC).
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS4022S über die Übersapnnungsebene 2 angestiegen ist (40 VAC).
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS3522S unter die Unterspannungsebene 1 gefallen ist (110 VDC).
- Anzahl der Fälle, in denen die Hauptspannung des BMXCPS3522S über die Übersapnnungsebene 2 angestiegen ist (140 VAC).
- Aktueller Status der Spannungsversorgung (Master, Slave, nicht in Betrieb)

Darstellung in FBD



Parameter

Eingangsparameter:

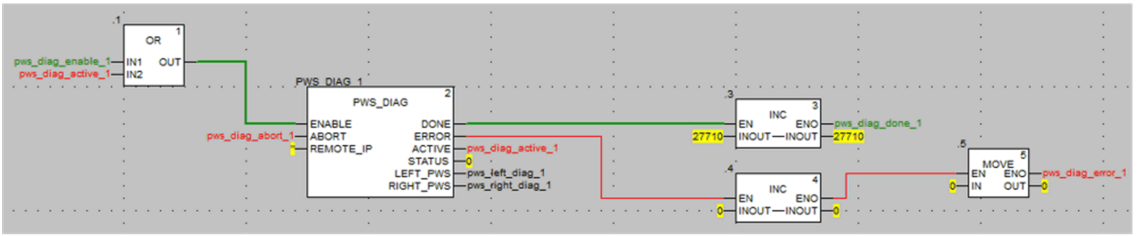
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine Variable an den Stift an, um die Spannungsversorgung im lokalen Rack anzusprechen.

Ausgangsparameter:

Parametername	Datentyp	Beschreibung
DONE	BOOL	EIN: Die Operation wurde erfolgreich abgeschlossen.
ERROR	BOOL	EIN: Die Operation wurde erfolglos abgebrochen.
EIN	BOOL	EIN: Die Operation ist aktiv.
STATUS	WORD	Bezeichner des erkannten Fehlers

Parametername	Datentyp	Beschreibung
LEFT_PWS	ANY	Diagnosedaten für die linke Spannungsversorgung. Verwenden Sie für die richtige Interpretation die Variable des Typs PWS_DIAG_DDT_V2, Seite 137.
RIGHT_PWS	ANY	Diagnosedaten für die rechte Spannungsversorgung. Verwenden Sie für die richtige Interpretation die Variable des Typs PWS_DIAG_DDT_V2.

Beispiel



pws_left_diag_1		PWS_DIAG_DDT	
pws_right_diag_1		PWS_DIAG_DDT	
PwsMajorVersion	153	BYTE	Power Supply major version
PwsMinorVersion	162	BYTE	Power Supply minor version
Model	0	BYTE	Power Supply Model identifier
State	12	BYTE	Power Supply state
I33BacPos	0	UINT	Measure current of 3V3 Bac in nominal role (producer)
V33Buck	0	UINT	Measure voltage of 3V3 Buck
I24Bac	0	UINT	Measure current of 24V Bac
V24Int	0	UINT	Measure voltage of 24V Int
Temperature	0	INT	Measure of Ambient Temperature
OperTimeMaster...	16935	DINT	Operating Time as Master since last Power ON
OperTimeSlaveSi...	2	DINT	Operating Time as Slave since last Power ON
OperTimeMaster	282128	DINT	Operating Time as Master since Manufacturing
OperTimeSlave	44	DINT	Operating Time as Slave Since Manufacturing
Work	0	DINT	Work supplied since Manufacturing
RemainingLTPC	0	UINT	Remaining Life Time in percent
NbPowerOn	0	UINT	Number of Power ON since Manufacturing
NbVoltageLowFail	0	UINT	Number of failure detected on Primary Voltage by Low Threshold
NbVoltageHighFail	0	UINT	Number of failure detected on Primary Voltage by High Threshold

Die Befehle „Swap“ und „Clear“

Einführung

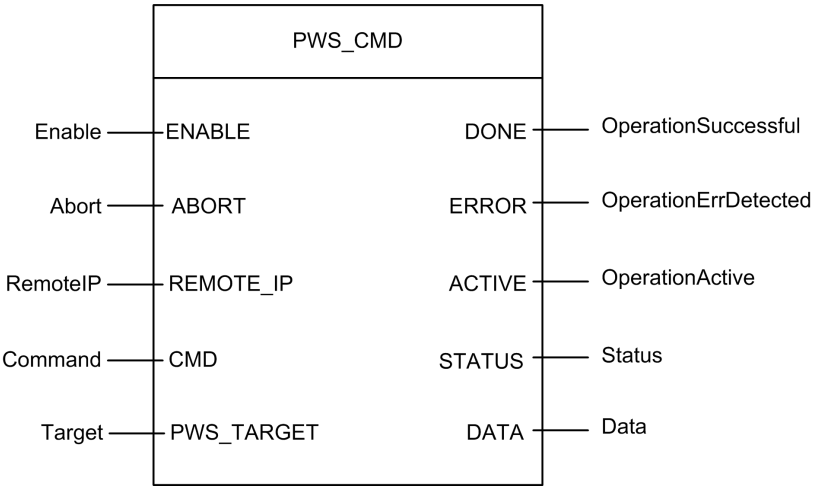
Der Funktionsbaustein PWS_CMD kann zur Ausgabe zweier Befehle genutzt werden:

- Austauschanforderung („swap“): Mit diesem Befehl wird festgelegt, dass die Spannungsversorgung als Master dient. Wenn beide Spannungsversorgungen funktionsfähig sind, wird die angegebene Spannungsversorgung zum Master, die andere zum Slave.
- Löschanforderung („clear“): Mit diesem Befehl werden die folgenden Zähler zurückgesetzt:
  - Anzahl der Fälle, in denen die Hauptspannung unter die Unterspannungsebene 1 gefallen ist
  - Anzahl der Fälle, in denen die Hauptspannung unter die Unterspannungsebene 2 gefallen ist
  - Anzahl der Einschaltvorgänge der Spannungsversorgung

Beide Anforderungen sind nur für Spannungsversorgungen im Hauptrack verfügbar. Ein Hauptrack hat eine Adresse von 0 und in Steckplatz 0 oder 1 eine CPU oder ein Kommunikationsadaptermodul (CRA). Ein Erweiterungsrack ist kein Hauptrack.

Die LEDs zeigen, dass der Befehl ausgeführt wird. Eine Aufzeichnung des Ereignisses wird im Spannungsversorgungsspeicher erfasst, und zwar im ersten Abschnitt des Faktbausteins.

Darstellung in FBD



Parameter

Eingangsparameter:

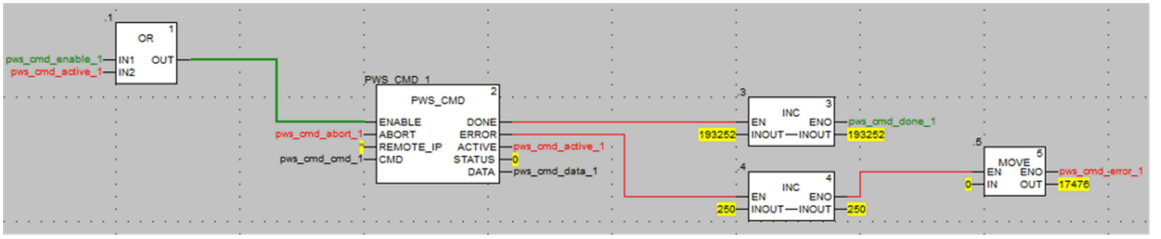
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine Variable an den Stift an, um die Spannungsversorgung im lokalen Rack anzusprechen.
CMD	ANY	Verwenden Sie für die richtige Interpretation die Variable des Typs PWS_CMD_DDT. Verfügbarer Befehlscode: • 1 = Austauschen • 3 = Zurücksetzen
PWS_TARGET	BYTE	Anzusprechende Spannungsversorgung: • 1 = Links • 2 = Rechts • 3 = Beide

Ausgangsparameter:

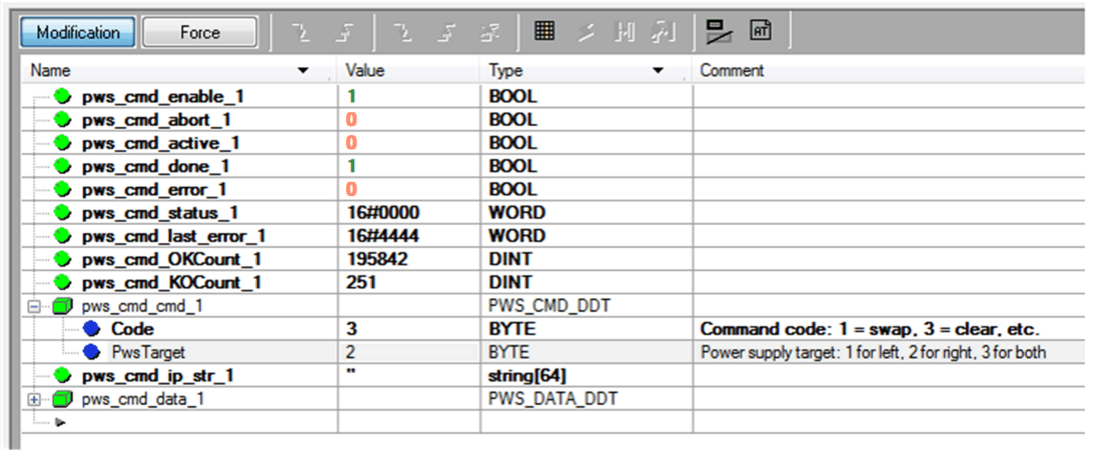
Parametername	Datentyp	Beschreibung
DONE	BOOL	EIN: Die Operation wurde erfolgreich abgeschlossen.
ERROR	BOOL	EIN: Die Operation wurde erfolglos abgebrochen.
ACTIVE	BOOL	EIN: Die Operation ist aktiv.
STATUS	WORT	Bezeichner des erkannten Fehlers
DATA	ANY	Antwortdaten (abhängig vom Befehlscode). Für Austausch- und Löschbefehle werden keine Daten aufgezeichnet.

Beispiel

Die folgende Abbildung zeigt, wie der Funktionsbaustein PWS_CMD für eine Austauschanforderung genutzt wird:



Der folgende Screenshot eines Dateneditors zeigt die Variablenwerte einer Austauschanforderung:



Name	Value	Type	Comment
pws_cmd_enable_1	1	BOOL	
pws_cmd_abort_1	0	BOOL	
pws_cmd_active_1	0	BOOL	
pws_cmd_done_1	1	BOOL	
pws_cmd_error_1	0	BOOL	
pws_cmd_status_1	16#0000	WORD	
pws_cmd_last_error_1	16#4444	WORD	
pws_cmd_OKCount_1	195842	DINT	
pws_cmd_KOCount_1	251	DINT	
pws_cmd_cmd_1		PWS_CMD_DDT	
Code	3	BYTE	**Command code: 1 = swap, 3 = clear, etc.**
PwsTarget	2	BYTE	Power supply target: 1 for left, 2 for right, 3 for both
pws_cmd_ip_str_1	''	string[64]	
pws_cmd_data_1		PWS_DATA_DDT	

Verwaltung der Anwendungssicherheit

Einführung

Control Expert ermöglicht Ihnen die Begrenzung des Zugriffs auf den M580-Sicherheits-PAC für Benutzer mit zugewiesenen Passwörtern. In diesem Abschnitt werden die in Control Expert verfügbaren Prozesse zur Passwortzuweisung ausgewiesen.

Anwendungsschutz

Übersicht

Control Expert stellt einen Passwortmechanismus bereit, der den unberechtigten Zugriff auf die Anwendung verhindert.

Control Expert greift in folgenden Situationen auf das Passwort zurück:

- Sie öffnen die Anwendung in Control Expert.
- Sie stellen in Control Expert eine Verbindung zum PAC her.

Die Festlegung eines Anwendungspassworts verhindert unerwünschte Anwendungsänderungen, -downloads oder das Öffnen von Anwendungsdateien. Das Passwort wird verschlüsselt in der Anwendung gespeichert.

Zusätzlich zum Festlegen des Passworts können Sie die Dateien `.STU`, `.STA` und `.ZEF` verschlüsseln. Die Dateiverschlüsselungsfunktion in Control Expert trägt dazu bei, Änderungen durch böswillige Personen zu verhindern und verstärkt den Schutz vor Diebstahl geistigen Eigentums. Die Dateiverschlüsselungsoption ist durch einen Passwortmechanismus geschützt.

HINWEIS: Wenn eine Steuerung im Rahmen eines Systemprojekts verwaltet wird, sind Anwendungspasswort und Dateiverschlüsselung im Control Expert-Editor deaktiviert und müssen über den Topology Manager verwaltet werden.

Passworterstellung

Die Passworterstellung basiert auf den Empfehlungen der IEEE-Norm 1686-2013.

Ein Passwort sollte mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben (A, B, C, ...), einen Kleinbuchstaben (a, b, c, ...), eine Zahl und ein nicht alphanumerisches Zeichen (!, $, %, &, ...) kombinieren.

HINWEIS: Beim Exportieren eines Projekts, das nicht in einer `.XEF`- oder `.ZEF`-Datei verschlüsselt ist, wird das Anwendungspasswort gelöscht.

Erstellen eines neuen Projekts

Standardmäßig ist ein Projekt nicht passwortgeschützt und Anwendungsdateien werden nicht verschlüsselt.

Bei der Projekterstellung können Sie im Fenster **Sicherheitsdurchsetzung**:

- Legen Sie ein Anwendungspasswort fest. Oder:
- Legen Sie ein Anwendungspasswort fest und wenden Sie die Verschlüsselung auf Ihre Anwendungsdateien an. Für die Anwendung der Dateiverschlüsselung muss zudem ein Passwort festgelegt werden. Wir empfehlen, zwei verschiedene Passwörter einzustellen.

Wenn kein Passwort eingegeben wird, ist es nicht möglich, Anwendungsdateien zu verschlüsseln. Dann wird beim nächsten Öffnen des Control Expert-Projekts das Dialogfeld **Passwort** geöffnet. Um auf Ihr Projekt zuzugreifen, geben Sie keinen Passworttext ein, um die leere Zeichenfolge zu übernehmen, und klicken Sie auf **OK**. Anschließend können Sie wie nachfolgend beschrieben ein Anwendungspasswort festlegen und die Dateiverschlüsselung aktivieren.

HINWEIS: Sie können jederzeit ein Anwendungspasswort erstellen oder ändern.

Für die Aktivierung der Dateiverschlüsselung muss ein Anwendungspasswort festgelegt werden.

Wenn die Dateiverschlüsselung aktiviert ist:

- Das Anwendungspasswort kann geändert werden.
- Das Löschen des Anwendungspassworts ist nicht zulässig.

Festlegen eines Anwendungspassworts

Gehen Sie zur Einstellung des Anwendungspassworts vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Anwendung** auf **Passwort ändern**. **Ergebnis**: Das Fenster **Passwort ändern** wird angezeigt.
5	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
6	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.

Schritt	Aktion
7	Bestätigen Sie diesen Vorgang mit **OK**.
8	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Ändern des Anwendungspassworts

Gehen Sie zur Änderung des Passworts zum Schutz der Datensicherung vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Anwendung** auf **Passwort ändern**. **Ergebnis**: Das Fenster **Passwort ändern** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.
8	Bestätigen Sie diesen Vorgang mit **OK**.
9	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Löschen des Anwendungspassworts

Das Löschen des Anwendungspassworts ist bei aktivierter Dateiverschlüsselung nicht zulässig.

Gehen Sie zum Löschen des Passworts zum Schutz der Anwendung vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Anwendung** auf **Passwort löschen...**. **Ergebnis**: Das Fenster **Passwort** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Passwort** ein.
6	Bestätigen Sie diesen Vorgang mit **OK**.
7	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Automatische Verriegelungsfunktion

Es steht eine optionale Funktion zur automatischen Verriegelung zur Verfügung, um den Zugriff auf das Softwareprogrammiertool Control Expert nach einer konfigurierten Inaktivitätsdauer zu begrenzen. Sie können die automatische Verriegelungsfunktion durch Aktivieren des Kontrollkästchens **Selbst-Verriegelung** aktivieren und den Timeout für die Inaktivitätsdauer über die Option **Minuten bis zur Selbst-Verriegelung** konfigurieren.

Es gelten folgende Standardwerte:

- Die Funktion **Selbst-Verriegelung** ist nicht aktiviert.
- **Min. bis zur Selbst-Verriegelung** auf 10 Min. (Mögliche Werte: 1...999 Minuten)

Wenn bei aktivierter Selbst-Verriegelungsfunktion das Ende der konfigurierten Inaktivitätsdauer erreicht wird, wird ein modales Dialogfeld mit der Aufforderung zur Eingabe des Anwendungspassworts angezeigt. Hinter dem modalen Dialogfeld bleiben alle aktiven Editoren in derselben Position geöffnet. Das bedeutet, dass jeder Benutzer den aktuellen Inhalt des Control Expert-Fensters lesen, die Arbeit in Control Expert jedoch nicht fortsetzen kann.

HINWEIS: Wenn Sie dem Projekt kein Passwort zugewiesen haben, wird das modale Dialogfeld nicht angezeigt.

Situationen mit Aufforderung zur Passworteingabe

Öffnen einer vorhandenen Anwendung (Projekt) in Control Expert:

Passwortverwaltung	
Beim Öffnen einer Anwendungsdatei wird das Dialogfeld **Anwendungspasswort** angezeigt.	
Geben Sie das Passwort ein.	
Klicken Sie auf **OK**.	Wenn das eingegebene Passwort gültig ist, wird die Anwendung geöffnet.
	Bei Eingabe eines falschen Passworts wird ein Meldungsfenster mit dem Hinweis angezeigt, dass das eingegebene Passwort ungültig ist, und das Dialogfeld **Anwendungspasswort** wird erneut geöffnet.
Wenn Sie auf **Abbrechen** klicken, wird die Anwendung nicht geöffnet.	

Zugreifen auf die Anwendung in Control Expert nach einer automatischen Verriegelung, wenn Control Expert nicht mit dem PAC verbunden ist oder das Projekt in Control Expert dem Projekt im PAC ENTSPRICHT:

Passwortverwaltung	
Nach Ablauf der Inaktivitätsdauer für die Selbst-Verriegelung wird das Dialogfeld **Anwendungspasswort** angezeigt:	
Geben Sie das Passwort ein.	
Klicken Sie auf **OK**.	Wenn das eingegebene Passwort gültig ist, wird Control Expert wieder aktiv.
	Bei Eingabe eines falschen Passworts wird ein Meldungsfenster mit dem Hinweis angezeigt, dass das eingegebene Passwort ungültig ist, und das Dialogfeld **Anwendungspasswort** wird erneut geöffnet.
Wenn Sie auf **Schließen** klicken, wird die Anwendung ohne Speichern geschlossen.	

Zugreifen auf die Anwendung im PAC nach einer automatischen Verriegelung, wenn Control Expert mit dem PAC verbunden ist und die Anwendung in Control Expert sich von der Anwendung im PAC UNTERSCHEIDET:

Passwortverwaltung	
Wenn beim Aufbau einer Verbindung die Softwareanwendung Control Expert und die CPU-Anwendung voneinander abweichen, wird das Dialogfeld **Anwendungspasswort** geöffnet.	
Geben Sie das Passwort ein.	
Klicken Sie auf **OK**.	Wenn das eingegebene Passwort gültig ist, wird die Verbindung hergestellt.
	Bei Eingabe eines falschen Passworts wird ein Meldungsfenster mit dem Hinweis angezeigt, dass das eingegebene Passwort ungültig ist, und das Dialogfeld **Anwendungspasswort** wird erneut geöffnet.

Passwortverwaltung
Wenn Sie auf **Abbrechen** klicken, wird keine Verbindung hergestellt.
HINWEIS: Wenn beim Aufbau einer Verbindung die Softwareanwendung Control Expert und die CPU-Anwendung übereinstimmen, braucht kein Passwort eingegeben zu werden. Wurde ursprünglich kein Passwort eingegeben (leeres Feld bei der Projekterstellung), dann klicken Sie auf **OK**, um die Verbindung bei der Aufforderung zur Passworteingabe herzustellen.

HINWEIS: Nach drei fehlgeschlagenen Passwort-Eingabeversuchen müssen Sie zwischen jeder weiteren Passworteingabe einen immer längeren Zeitraum abwarten. Die Wartezeit verlängert sich von 15 Sekunden bis 1 Stunde, wobei nach jedem weiteren fehlgeschlagenen Versuch mit einem falschen Passwort der Inkrementfaktor 2 auf die Wartezeit angewendet wird.

HINWEIS: Halten Sie sich bei einem Passwortverlust an die im Kapitel Passwortverlust, Seite 330 beschriebene Vorgehensweise.

Option zur Aktivierung der Dateiverschlüsselung

HINWEIS: Sie müssen ein Anwendungspasswort festlegen, bevor Sie die Dateiverschlüsselung aktivieren können.

Gehen Sie zur Aktivierung der Dateiverschlüsselungsoption vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Aktivieren Sie das Kontrollkästchen **Dateiverschlüsselung aktiv**. **Ergebnis**: Das Fenster **Passwort erstellen** wird angezeigt.
5	Geben Sie das Passwort in das Feld **Eingabe** ein.
6	Geben Sie die Bestätigung des Passworts in das Feld **Bestätigung** ein.
7	Bestätigen Sie diesen Vorgang mit **OK**.
8	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Deaktivieren der Dateiverschlüsselungsoption

Gehen Sie zur Deaktivierung der Dateiverschlüsselungsoption vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Deaktivieren Sie das Kontrollkästchen **Dateiverschlüsselung aktiv**. **Ergebnis**: Das Fenster **Dateiverschlüsselungspasswort** wird angezeigt.
5	Geben Sie das Passwort ein und klicken Sie zur Bestätigung auf **OK**. **HINWEIS:** Die Anwendung ist nicht mehr verschlüsselt.
6	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Ändern des Dateiverschlüsselungspassworts

Gehen Sie zur Änderung des Dateiverschlüsselungspassworts vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Dateiverschlüsselung** auf **Passwort ändern...**. **Ergebnis**: Das Fenster **Passwort ändern** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.

Schritt	Aktion
8	Bestätigen Sie diesen Vorgang mit **OK**.
9	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Löschen des Dateiverschlüsselungspassworts

Gehen Sie zum Löschen des Dateiverschlüsselungspassworts vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Dateiverschlüsselung** auf **Passwort löschen...**. **Ergebnis**: Das Fenster **Passwort** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Passwort** ein.
6	Bestätigen Sie diesen Vorgang mit **OK**.
7	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

HINWEIS: Sollten Sie einen Passwortverlust bei der Dateiverschlüsselung feststellen, halten Sie sich an die im Kapitel Passwortverlust, Seite 330 beschriebene Vorgehensweise.

Kompatibilitätsregeln

Verschlüsselte Anwendungsdateien (`.STA` und `.ZEF`) können nicht in Control Expert 15.0 Classic oder früheren Versionen geöffnet werden, und verschlüsselte Dateien (`.ZEF`) können nicht in Control Expert mit Topology Manager importiert werden.

Die Kompatibilitätsregeln zwischen Anwendungsversion und Control Expert/Unity Pro-Version gelten für `.ZEF`-Dateien, die ohne Verschlüsselungsoption exportiert wurden.

HINWEIS: Wenn die Dateiverschlüsselungsoption in Ihrem Projekt aktiviert ist, können archivierte Anwendungsdateien (`.STA`) nicht verschlüsselt gespeichert werden.

Passwortschutz für die sicheren Bereiche

Einführung

Sicherheits-CPUs umfassen eine Funktion zum passwortgestützten Schutz der sicheren Bereiche, die über das Fenster **Eigenschaften** des Projekts aufgerufen werden kann. Diese Funktion ermöglicht den Schutz der in den sicheren Bereichen des Sicherheitsprojekts befindlichen Projektelemente.

HINWEIS: Wenn die Funktion zum Passwortschutz für die sicheren Bereiche aktiviert ist, können keine Änderungen an den sicheren Teilen der Anwendung vorgenommen werden.

Bei aktiviertem Passwortschutz für die sicheren Bereiche sind keine Änderungen an den folgenden sicheren Teilen zulässig:

Sicherer Teil	**Unzulässige Aktion (offline UND online)**
Konfiguration	Ändern der CPU-Eigenschaften
	Hinzufügen, Löschen, Ändern eines Sicherheitsmoduls im Rack
	Ändern der Sicherheitsspannungsversorgung
Typen	Erstellen, Löschen, Ändern eines Sicherheits-DDT
	Ändern eines DDT-Attributs: von nicht sicher -> sicher
	Ändern eines DDT-Attributs: von sicher -> nicht sicher
	Erstellen, Löschen, Ändern eines Sicherheits-DFB
	Ändern eines DFB-Attributs: von nicht sicher -> sicher
	Ändern eines DFB-Attributs: von sicher -> nicht sicher
Programm-SAFE	Alle Änderungen unter dem Knoten **Variablen und FB-Instanzen**
	Erstellen einer Task
	Importieren einer Task
	Ändern einer Task
	Erstellen einer Section
	Löschen einer Section
	Importieren einer Section

Sicherer Teil	Unzulässige Aktion (offline UND online)
	Ändern einer Section
Projekteinstellungen	Ändern der SAFE-Projekteinstellungen
	Ändern der COMMON-Projekteinstellungen

Verschlüsselung

Für das Passwort für die sicheren Bereiche wird die Standardverschlüsselung SHA-256 + Salt verwendet.

Passwortschutz für sichere Bereiche und Benutzerrechte für Sicherheitsprojekte

Die Aktivierung des Passworts für die sicheren Bereiche und die Implementierung der im **Sicherheitseditor** erstellten Benutezrrechte sind zwei Sicherheitsfunktionen, die sich gegenseitig ausschließen:

- Wenn dem Benutzer, der Control Expert startet, ein Benutzerprofil zugewiesen wurde, dann kann er auf die sicheren Bereiche der Sicherheitsanwendung zugreifen, sofern ihm das Passwort für die sicheren Bereiche bekannt ist und ihm im **Sicherheitseditor** Zugriffsrechte eingeräumt wurden.
- Wenn keine Benutzerprofile zugewiesen wurden, kann ein Benutzer auf die sicheren Bereiche der Sicherheitsanwendung zugreifen, wenn er das Passwort für die sicheren Bereiche kennt.

Anzeigen in Control Expert

Der Status der Funktion zum Passwortschutz der sicheren Bereiche kann durch Anzeige des Knotens **Programm-SAFE** im **Projekt-Browser** festgestellt werden:

- Ein geschlossenes Sicherheitsschloss gibt an, dass ein Passwort für die sicheren Bereiche erstellt und aktiviert wurde.
- Ein geöffnetes Sicherheitsschloss verweist darauf, dass ein Passwort für die sicheren Bereich erstellt, jedoch nicht aktiviert wurde.
- Kein Sicherheitsschloss bedeutet, dass kein Passwort für die sicheren Bereiche erstellt wurde.

HINWEIS: Wenn ein Passwort für die sicheren Bereiche erstellt, jedoch nicht aktiviert wurde und die Sicherheitsanwendung geschlossen und anschließend wieder geöffnet wird, wird das Passwort automatisch beim erneuten Öffnen aktiviert. Dieses Verhalten dient als Vorsichtsmaßnahme, wenn das Passwort für die sicheren Bereiche versehentlich nicht aktiviert wird.

Kompatibilität

Die Passwortfunktion für die sicheren Bereiche ist für Control Expert ab V14.0 sowie für M580-Sicherheits-CPUs mit einer Firmware ab 2.80 verfügbar.

HINWEIS:

- Anwendungsprogrammdateien `.STU`, `.STA` und `.ZEF`, die in Control Expert ab Version V14.0 erstellt wurden, können in Unity Pro bis V13.1 nicht geöffnet werden.
- Der Austausch einer M580-Sicherheits-CPU in Control Expert v14.0 hat folgende Auswirkungen:
  - Bei der Aktualisierung der Firmware von 2.70 auf 2.80 (oder höher) wird die Passwortfunktion für sichere Bereiche auf der Registerkarte **Programm- und Safety-Schutz** im Fenster **Projekt > Eigenschaften** hinzugefügt.
  - Beim Downgrading der Firmware von 2.80 (oder höher) auf 2.70 wird die Passwortfunktion für sichere Bereiche entfernt.

Aktivierung des Schutzes und Erstellung eines Passworts

Gehen Sie zur Aktivierung des Section-Schutzes und zur Erstellung eines Passworts vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Aktivieren Sie im Bereich **Sicherheit** den Schutz durch Aktivierung des Kontrollkästchens **Schutz aktiv**. **Ergebnis**: Das Dialogfeld **Passwort ändern** wird angezeigt.
5	Geben Sie ein Passwort in das Feld **Eingabe** ein.
6	Geben Sie die Bestätigung des Passworts in das Feld **Bestätigung** ein.

Schritt	Aktion
7	Bestätigen Sie den Vorgang mit **OK**.
8	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Ändern des Passworts

Gehen Sie zur Änderung des Passworts zum Schutz der Projekt-Sections vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Klicken Sie im Bereich **Sicherheit** auf **Passwort ändern...**. **Ergebnis**: Das Dialogfeld **Passwort ändern** wird angezeigt:
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.
8	Bestätigen Sie den Vorgang mit **OK**.
9	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Löschen des Passworts

Gehen Sie zum Löschen des Passworts zum Schutz der Projekt-Sections vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus.

Schritt	Aktion
	Ergebnis: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Klicken Sie im Bereich **Sicherheit** auf **Passwort löschen...**. **Ergebnis**: Das Dialogfeld **Zugriffskontrolle** wird angezeigt:
5	Geben Sie das alte Passwort in das Feld **Passwort** ein.
6	Bestätigen Sie den Vorgang mit **OK**.
7	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Schutz der Programmeinheiten, Sections und Unterprogramme

Einführung

Auf die Schutzfunktion kann über das Fenster **Eigenschaften** des Projekts im Offline-Betrieb zugegriffen werden.

Diese Funktion ermöglicht den Schutz der Programmelemente (Sections, Programmeinheite).

HINWEIS: Der Schutz ist nicht aktiv, solange der Schutz nicht im Projekt aktiviert wurde.

HINWEIS: Der Projektschutz ist nur für die markierten Programmelemente gültig. Dieser Schutz behindert nicht folgende Aktionen:

- Herstellen einer Verbindung zur CPU
- Hochladen der Anwendung aus der CPU
- Ändern der Konfiguration
- Hinzufügen neuer Programmeinheiten und/oder Sections
- Ändern der Logik in einer neuen (nicht geschützten) Section

Aktivieren des Schutzes und Erstellen eines Passworts

Gehen Sie vor wie folgt, um den Schutz zu aktivieren und ein Passwort für Sections und Programmeinheiten zu erstellen:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Aktivieren Sie im Bereich **Sections und Programmeinheiten** den Schutz durch Auswahl der Option **Schutz aktiv**. **Ergebnis**: Das Dialogfeld **Passwort ändern** wird angezeigt:
5	Geben Sie ein Passwort in das Feld **Eingabe** ein.
6	Geben Sie die Bestätigung des Passworts in das Feld **Bestätigung** ein.
7	Aktivieren Sie das Kontrollkästchen **Verschlüsselt**, wenn ein erweiterter Passwortschutz erforderlich ist. **HINWEIS:** Eini Projekt mit verschlüsseltem Passwort kann nicht mit Unity Pro bis V4.0 bearbeitet werden.
8	Bestätigen Sie den Vorgang mit **OK**.
9	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Hinweise

Wenn ein Programmelement mit Zugriffsschutz (Lesen oder Lesen/Schreiben) konfiguriert ist, wird durch die Aktivierung des Schutzes ein geschlossenes Vorhängeschloss für das betreffende Programmelement angezeigt.

Wenn ein Programmelement mit Zugriffsschutz konfiguriert ist, dieser jedoch deaktiviert ist, wird ein offenes Vorhängeschloss angezeigt.

Ändern des Passworts

Gehen Sie vor wie folgt, um den passwortbasierten Projektschutz für Sections und Programmeinheiten zu ändern:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Klicken Sie im Bereich **Sections und Programmeinheiten** auf **Passwort ändern**. **Ergebnis**: Das Dialogfeld **Passwort ändern** wird angezeigt:
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.
8	Aktivieren Sie das Kontrollkästchen **Verschlüsselt**, wenn ein erweiterter Passwortschutz erforderlich ist. **HINWEIS:** Eini Projekt mit verschlüsseltem Passwort kann nicht mit Unity Pro bis V4.0 bearbeitet werden. Unity Pro ist die vorherige Bezeichnung von Control Expert bis Version 13.1.
9	Bestätigen Sie den Vorgang mit **OK**.
10	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Löschen des Passworts

Gehen Sie vor wie folgt, um den passwortbasierten Projektschutz für Sections und Programmeinheiten zu löschen:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Programm- und Safety-Schutz** aus.
4	Klicken Sie im Bereich **Sections und Programmeinheiten** auf **Passwort löschen**. **Ergebnis**: Das Dialogfeld **Zugriffskontrolle** wird angezeigt:
5	Geben Sie das alte Passwort in das Feld **Passwort** ein.

Schritt	Aktion
6	Bestätigen Sie den Vorgang mit **OK**.
7	Klicken Sie auf im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Firmwareschutz

Übersicht

Durch den passwortbasierten Firmwareschutz wird unerwünschter Zugriff auf die Modul-Firmware verhindert.

Passwort

Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, sie umfassen 8 bis 16 alphanumerische Zeichen. Die Passwortstärke wird verbessert, wenn das Passwort sowohl Klein- als auch Großbuchstaben, alphabetische, numerische und Sonderzeichen enthält.

HINWEIS: Beim Importieren einer ZEF-Datei wird das Firmwarepasswort nur dann im Modul gespeichert, wenn die Option **Dateiverschlüsselung** aktiviert ist.

Ändern des Passworts

Es ist jederzeit möglich, das Passwort zu ändern.

HINWEIS: Der Standardwert des Firmwarepassworts in der Control Expert-Anwendung lautet: **`fwdownload`**.

- Bei einer Firmware ab V4.01 müssen Sie den Standardwert für das Firmwarepasswort ändern, da andernfalls keine Generierung der Control Expert-Anwendung möglich ist.
- Für Firmwareversionen vor V4.01 ist es nicht zwingend erforderlich, es wird jedoch dringend empfohlen, den Standardwert für das Firmwarepasswort zu ändern.

Gehen Sie zur Änderung des Passworts zum Schutz der Firmware vor wie folgt:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Bereich **Firmware** auf **Passwort ändern...**. **Ergebnis**: Das Fenster **Passwort ändern** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.
8	Bestätigen Sie diesen Vorgang mit **OK**.
9	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Zurücksetzen des Passworts

Beim Zurücksetzen des Passworts wird bei Bestätigung des aktuellen Passworts der Standardwert für das Firmwarepasswort in der Control Expert-Anwendung zugewiesen.

Gehen Sie vor wie folgt, um das Passwort zurückzusetzen:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Bereich **Firmware** auf **Passwort zurücksetzen...**. **Ergebnis**: Das Fenster **Passwort** wird angezeigt.
5	Geben Sie das aktuelle Passwort in das Feld **Passwort** ein.

Schritt	Aktion
6	Bestätigen Sie diesen Vorgang mit **OK**.
7	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Als neues Passwort wird das Standardpasswort verwendet: **`fwdownload`**. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Datenspeicher-/Webschutz

Übersicht

Der Passwortschutz verhindert unerwünschten Zugriff auf den Datenspeicherbereich der SD-Speicherkarte (wenn eine gültige Karte in die CPU eingeführt wird).

Für Modicon M580-CPUs in einem von Control Expert mit Version erstellten Projekt:

- Vor Version 15.1 können Sie Passwortschutz für den Datenspeicherzugriff bereitstellen.
- Version 15.1 oder höher: Sie können Passwortschutz sowohl für die Webdiagnose als auch für den Datenspeicherzugriff bereitstellen.

Passwort

Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, sie umfassen 8 bis 16 alphanumerische Zeichen. Die Passwortstärke wird verbessert, wenn das Passwort sowohl Klein- als auch Großbuchstaben, alphabetische, numerische und Sonderzeichen enthält.

HINWEIS: Beim Importieren einer ZEF-Datei wird das Datenspeicher-/Webpasswort nur dann im Modul gespeichert, wenn die Option **Dateiverschlüsselung** ausgewählt ist.

Ändern des Passworts

Es ist jederzeit möglich, das Passwort zu ändern.

HINWEIS: Das Datenspeicher-/Webpasswort hat einen Standardwert in der Control Expert-Anwendung. Dieser Standardwert ist abhängig von der Version von Control Expert und lautet:

- **`datadownload`** für Control Expert-Versionen vor V15.1
- **`webuser`** für Control Expert-Versionen ab einschließlich V15.1

Je nach Firmwareversion des Moduls ist eine Änderung des Standard-Passworts obligatorisch oder nicht erforderlich:

- Für Firmware ab V4.01 müssen Sie den Standardwert für das Datenspeicher-/Webpasswort ändern, da andernfalls die Control Expert-Anwendung nicht erstellt werden kann.
- Bei Firmwareversionen vor V4.01 ist es nicht zwingend erforderlich, aber es wird dringend empfohlen, den Standardwert für das Datenspeicher-/Webpasswort zu ändern.

Vorgehensweise zur Änderung des Passworts für den Datenspeicher bzw. das Web:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Datenspeicher** (oder im Feld **Webdiagnose/Datenspeicher** auf **Passwort ändern...**. **Ergebnis**: Das Fenster **Passwort ändern** wird angezeigt.
5	Geben Sie das alte Passwort in das Feld **Altes Passwort** ein.
6	Geben Sie das neue Passwort in das Feld **Eingabe** ein.
7	Geben Sie das neue Passwort zur Bestätigung noch einmal in das Feld **Bestätigung** ein.
8	Bestätigen Sie diesen Vorgang mit **OK**.
9	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Zurücksetzen des Passworts

Durch das Zurücksetzen des Passworts wird dem Datenspeicher-/Webpasswort in der Control Expert-Anwendung der Standardwert zugewiesen, wenn das aktuelle Passwort bestätigt wird.

Gehen Sie vor wie folgt, um das Passwort zurückzusetzen:

Schritt	Aktion
1	Klicken Sie im Projekt-Browser mit der rechten Maustaste auf **Projekt**.
2	Wählen Sie im Kontextmenü den Befehl **Eigenschaften** aus. **Ergebnis**: Das Fenster **Eigenschaften von Projekt** wird angezeigt.
3	Wählen Sie die Registerkarte **Projekt- und Steuerungsschutz** aus.
4	Klicken Sie im Feld **Datenspeicher** (oder im Feld **Webdiagnose/Datenspeicher** auf **Passwort zurücksetzen...**. **Ergebnis**: Das Fenster **Passwort** wird angezeigt.
5	Geben Sie das aktuelle Passwort in das Feld **Passwort** ein.
6	Bestätigen Sie diesen Vorgang mit **OK**.
7	Klicken Sie im Fenster **Eigenschaften von Projekt** auf **OK** oder **Übernehmen**, um alle Änderungen zu bestätigen. Das neue Passwort ist das Standardpasswort: **`datadownload`**. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Passwortverlust

Übersicht

Wenn Sie Ihr Passwort vergessen haben, halten Sie sich an die nachstehend beschriebenen Vorgehensweisen und setzen Sie sich mit dem Kundendienst von Schneider Electric in Verbindung.

HINWEIS: Der Vorgang zur Wiederherstellung des Anwendungspassworts hängt davon ab, ob die Option zur Dateiverschlüsselung aktiviert oder deaktiviert ist.

Control Expert-Anwendungspasswort ohne Dateiverschlüsselungsoption

Die folgende Vorgehensweise zum Zurücksetzen des Anwendungspassworts ist anzuwenden, wenn die Dateiverschlüsselungsoption deaktiviert ist oder wenn die Anwendungsdatei mit Control Expert 15.0 Classic oder früheren Versionen verwaltet wird.

Schneider Electric benötigt eine Folge alphanumerischer Zeichen, die im Popup-Fenster **Passwort vergessen** angezeigt werden, sobald Sie im Dialogfeld `SHIFT+F2` die Tastenkombination **SHIFT+F2** drücken.

Um das Dialogfeld **Passwort** aufzurufen, müssen folgende Voraussetzungen erfüllt sein:

- Beim Öffnen wählen Sie die Anwendung aus, daraufhin wird das Dialogfeld **Passwort** angezeigt.
- Zum Zeitpunkt der Selbst-Verriegelung wird das Dialogfeld **Passwort** angezeigt. Wenn Sie sich nicht mehr an Ihr Passwort erinnern, wählen Sie **Schließen** aus. Öffnen Sie dann die Anwendung erneut, sodass das Dialogfeld **Passwort** wieder angezeigt wird.

  HINWEIS: Wenn die Anwendung im Anschluss an eine Selbst-Verriegelung ohne Eingabe eines Passworts geschlossen wird, gehen alle Änderungen verloren.

Vorgehensweise zum Zurücksetzen des Anwendungspassworts:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Passwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **HINWEIS:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein.
6	Ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Klicken Sie auf **Generieren > Änderungen generieren**.
8	**Speichern** Sie die Anwendung.

Control Expert-Anwendungspasswort mit Dateiverschlüsselungsoption

Wenn Sie bei aktivierter Dateiverschlüsselung Ihr Anwendungspasswort vergessen, müssen Sie die Anwendungsdatei an den Support von Schneider Electric senden. Anschließend erhalten Sie die verschlüsselte Anwendungsdatei mit einem neuen Anwendungspasswort vom Schneider Electric-Kundendienst.

HINWEIS: Es wird dringend empfohlen, das Anwendungspasswort zu ändern.

Passwort für die CPU-Anwendung

Gehen Sie zum Zurücksetzen des Passworts für die CPU-Anwendung vor wie folgt, wenn die zugehörige Datei **.STU* verfügbar ist:

Schritt	Aktion
1	Öffnen Sie die betroffene Datei **.STU*.
2	Wenn das Dialogfeld **Passwort** angezeigt wird, drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein.
6	Ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Stellen Sie über **Verbinden** eine Verbindung zur SPS her.
8	Klicken Sie auf **Generieren > Änderungen generieren**.
9	**Speichern** Sie die Anwendung.

Gehen Sie zum Zurücksetzen des Passworts für die CPU-Anwendung vor wie folgt, wenn die zugehörige Datei **.STU* nicht verfügbar ist:

Schritt	Aktion
1	**Voraussetzung:** Beim Aufbau einer Verbindung wird das Dialogfeld **Passwort** angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Das vom Schneider Electric-Kundendienst bereitgestellte Passwort ist ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein.
6	Laden Sie die Anwendung von der SPS.

Schritt	Aktion
7	**Speichern** Sie die Anwendung.
8	Ändern Sie das Passwort (altes Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
9	Klicken Sie auf **Generieren > Änderungen generieren**.
10	**Speichern** Sie die Anwendung.

Dateiverschlüsselungspasswort

Schneider Electric benötigt eine Folge alphanumerischer Zeichen, die im Popup-Fenster **Passwort vergessen** angezeigt werden, sobald Sie im Dialogfeld `SHIFT+F2` die Tastenkombination **SHIFT+F2** drücken.

So greifen Sie auf das Dialogfeld **Passwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Feld **Dateiverschlüsselung** auf **Passwort löschen...**. Daraufhin erscheint das Dialogfeld **Passwort**.

Gehen Sie zum Zurücksetzen des Dateiverschlüsselungspassworts vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Passwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein und klicken Sie dann auf **OK**, um das Dialogfeld **Passwort** wieder zu schließen.

Schritt	Aktion
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (das alte Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** wieder zu schließen, und klicken Sie anschließend auf **OK** bzw. **Übernehmen** im Fenster **Eigenschaften von Projekt**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Passwort für sichere Bereiche

Schneider Electric benötigt eine Folge alphanumerischer Zeichen, die im Popup-Fenster **Passwort vergessen** angezeigt werden, sobald Sie im Dialogfeld `SHIFT+F2` die Tastenkombination **SHIFT+F2** drücken.

So greifen Sie auf das Dialogfeld **Passwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Feld **Sicherheit** auf **Passwort ändern...**. Daraufhin erscheint das Dialogfeld **Passwort**.

Gehen Sie zum Zurücksetzen des Passworts für sichere Bereiche vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Passwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein und klicken Sie dann auf **OK**, um das Dialogfeld **Passwort** wieder zu schließen.

Schritt	Aktion
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (das alte Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** wieder zu schließen, und klicken Sie anschließend auf **OK** bzw. **Übernehmen** im Fenster **Eigenschaften von Projekt**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Passwort für die Firmware

Schneider Electric benötigt eine Folge alphanumerischer Zeichen, die im Popup-Fenster **Passwort vergessen** angezeigt werden, sobald Sie im Dialogfeld `SHIFT+F2` die Tastenkombination **SHIFT+F2** drücken.

So greifen Sie auf das Dialogfeld **Passwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Bereich **Firmware** auf **Passwort zurücksetzen...**. Daraufhin erscheint das Dialogfeld **Passwort**.

Gehen Sie zum Zurücksetzen des Firmwarepassworts vor wie folgt:

Schritt	Aktion
1	**Voraussetzung:** Das Dialogfeld **Passwort** wird angezeigt.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein und klicken Sie dann auf **OK**, um das Dialogfeld **Passwort** wieder zu schließen.

Schritt	Aktion
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (das alte Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** wieder zu schließen, und klicken Sie anschließend auf **OK** bzw. **Übernehmen** im Fenster **Eigenschaften von Projekt**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Datensicherung/Web-Passwort

Schneider Electric benötigt eine Folge alphanumerischer Zeichen, die im Popup-Fenster **Passwort vergessen** angezeigt werden, sobald Sie im Dialogfeld `SHIFT+F2` die Tastenkombination **SHIFT+F2** drücken.

So greifen Sie auf das Dialogfeld **Passwort** zu:

- Gehen Sie zu **Projekt > Eigenschaften von Projekt > Projekt- und Steuerungsschutz**.
- Klicken Sie im Bereich **Datenspeicher** auf **Passwort zurücksetzen...**. Daraufhin erscheint das Dialogfeld **Passwort**.

Gehen Sie zum Zurücksetzen des Passworts für den Datenspeicher vor wie folgt:

Schritt	Aktion
1	**Bedingung:** Daraufhin erscheint das Dialogfeld **Passwort**.
2	Drücken Sie `SHIFT+F2`. **Ergebnis:** Das Popup-Fenster **Passwort vergessen** wird geöffnet und eine Folge alphanumerischer Zeichen wird angezeigt.
3	Kopieren Sie diese Zeichenfolge und geben Sie sie an den Kundendienst von Schneider Electric weiter.
4	Sie erhalten das generierte Passwort vom Schneider Electric-Kundendienst. **Hinweis:** Bei dem Passwort handelt es sich um ein temporäres Passwort, das gültig ist, solange keine Änderungen an der Anwendung vorgenommen werden.
5	Geben Sie dieses Passwort ein und klicken Sie dann auf **OK**, um das Dialogfeld **Passwort** wieder zu schließen.

Schritt	Aktion
6	Klicken Sie auf **Passwort ändern** und ändern Sie das Passwort (das alte Passwort = das vom Schneider Electric-Kundendienst bereitgestellte Passwort).
7	Klicken Sie auf **OK**, um das Dialogfeld **Passwort ändern** wieder zu schließen, und klicken Sie anschließend auf **OK** bzw. **Übernehmen** im Fenster **Eigenschaften von Projekt**, um alle Änderungen zu bestätigen. Wenn Sie im Fenster **Eigenschaften von Projekt** auf **Abbrechen** klicken, werden die vorgenommenen Änderungen verworfen.

Verwaltung der Workstation-Sicherheit

Einführung

Schneider Electric stellt das Tool **Sicherheitseditor** für die Zugriffsverwaltung bereit, mit dem Sie den Zugriff auf die Workstation mit installierter Software Control Expert begrenzen und kontrollieren können. In diesem Abschnitt werden die Eigenschaften dieses Tools beschrieben, das speziell für M580-Sicherheitsprojekte entwickelt wurde.

Verwaltung des Zugriffs auf Control Expert

Einführung

Schneider Electric stellt das Konfigurationstool **Sicherheitseditor** zur Verwaltung des Zugriffs auf die auf einer Workstation installierte Software Control Expert bereit. Die Verwendung des Konfigurationstools *Sicherheitseditor* zur Verwaltung des Zugriffs auf die Software Control Expert ist optional.

HINWEIS: Die Zugriffsverwaltung bezieht sich auf die Hardware - in der Regel die Workstation -, auf der die Software Control Expert installiert ist, und nicht auf das Projekt, das über ein eigenes Schutzsystem verfügt.

Weitere Informationen finden Sie in folgendem Handbuch: *EcoStruxure™ Control Expert, Security Editor, Operation Guide*.

HINWEIS: Die Sicherheitsprofile der Benutzer umfassen Rechte für den Zugriff auf den Prozessteil der Sicherheitsanwendung. Bei der Erstellung oder Änderung eines Benutzerprofils müssen Sie sicherstellen, dass alle erforderlichen Änderungen ordnungsgemäß vorgenommen werden.

Benutzerkategorien

Der **Sicherheitseditor** unterstützt zwei Benutzerkategorien:

- **Super User (Supervisor):**

  Der Super User ist die einzige Person, die zur Verwaltung der Zugriffssicherheit der Software berechtigt ist. Der Super User bestimmt die Benutzer, die Zugriff auf die Software erhalten, und legt deren Zugriffsrechte fest. Bei der Installation von Control Expert auf der Workstation kann nur der Super User die Sicherheitskonfiguration ohne Einschränkung der Rechte (ohne Passwort) aufrufen.

  HINWEIS: Der für den Super User reservierte Benutzername lautet Supervisor.

- **Benutzer:**

  Software-Benutzer werden in der Liste der Benutzer vom Super User definiert, wenn die Zugriffssicherheit in Control Expert aktiv ist. Wenn Ihr Name in der Benutzerliste enthalten ist, können Sie auf eine Software-Instanz zugreifen, indem Sie Ihren Namen (so wie er in der Liste enthalten ist) und Ihr Passwort eingeben.

Benutzerprofil

Das Benutzerprofil enthält alle Zugriffsrechte eines Benutzers. Das Benutzerprofil kann vom Super User benutzerspezifisch eingestellt oder durch Anwendung eines im Tool **Sicherheitseditor** verfügbaren vorkonfigurierten Profils erstellt werden.

Vorkonfigurierte Benutzerprofile

Der **Sicherheitseditor** stellt folgende vorkonfigurierte Benutzerprofile für das Sicherheits- oder das Prozessprogramm zur Auswahl:

Profil	Anwendbarer Programmtyp		Beschreibung
	Process (Prozess)	Safety (Sicherheit)	
ReadOnly (Schreibgeschützt)	✓	✓	Der Benutzer kann nur im schreibgeschützten Modus auf das Projekt zugreifen. Eine Ausnahme ist die PAC-Adresse, die geändert werden kann. Der Benutzer kann das Projekt ebenfalls kopieren oder herunterladen.
Operate (Betrieb)	✓	–	Der Benutzer verfügt über dieselben Rechte wie beim Profil **ReadOnly (Schreibgeschützt)**, allerdings zusätzlich die Ausführungsparameter des Prozessprogramms (Konstanten, Initialwerte, Task-Zykluszeiten usw.) ändern.
Safety_Operate (Sicherheitsbetrieb)	–	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Operate (Betrieb)**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen: • Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Anforderung des Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Adjust (Anpassung)	✓	–	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Operate (Betrieb)** und kann außerdem ein Projekt hochladen (in den PAC übertragen) und die Betriebsart des PAC (**Run**, **Stop** usw.) ändern.

Profil	Anwendbarer Programmtyp		Beschreibung
	Process (Prozess)	Safety (Sicherheit)	
Safety_Adjust (Sicherheitsanpassung)	–	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Adjust (Anpassung)**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen: • Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Anforderung des Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Debug (Debugging)	✓	–	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Adjust (Anpassung)** und kann außerdem die Debugging-Tools verwenden.
Safety_Debug (Sicherheitsdebugging)	–	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Debug (Debugging)**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen: • Der Stopp bzw. Start des Programms ist nicht zulässig. • Die Aktualisierung der Initialisierungswerte ist nicht zulässig. • Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Forcierung der Eingänge, Ausgänge oder internen Bits ist nicht zulässig. • Die Anforderung des Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Program (Programm)	✓	–	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Debug (Debugging)** und kann außerdem Änderungen am Programm vornehmen.

Profil	Anwendbarer Programmtyp		Beschreibung
	Process (Prozess)	Safety (Sicherheit)	
Safety_Program (Sicherheitsprogramm)	–	✓	Der Benutzer verfügt über dieselben Rechte wie beim Profil **Program (Programm)**, jedoch in Bezug auf das Sicherheitsprogramm. Hierbei gelten folgende Ausnahmen: • Der Stopp bzw. Start des Programms ist nicht zulässig. • Die Aktualisierung der Initialisierungswerte ist nicht zulässig. • Die Übertragung von Datenwerten an den PAC ist nicht zulässig. • Die Wiederherstellung des Projekts im PAC aus einer Sicherungskopie ist nicht zulässig. • Die Forcierung der Eingänge, Ausgänge oder internen Bits ist nicht zulässig. • Die Anforderung des Übergangs des Sicherheitsprogramms in den Wartungsmodus ist zulässig.
Disabled (Deaktiviert)	✓	✓	Der Benutzer kann nicht auf das Projekt zugreifen.

Zuweisung eines vorkonfigurierten Benutzers

Der Super User kann einem bestimmten Benutzer auf der Registerkarte **Benutzer** im **Sicherheitseditor** ein vorkonfiguriertes Benutzerprofil auf der Basis eines vorkonfigurierten Profils zuweisen. Folgende vorkonfigurierte Benutzerprofile stehen zur Auswahl:

- safety_user_Adjust (Sicherheitsbenutzer - Anpassung)
- safety_user_Debug (Sicherheitsbenutzer - Debugging)
- safety_user_Operate (Sicherheitsbenutzer - Betrieb)
- safety_user_Program (Sicherheitsbenutzer - Programm)
- user_Adjust (Benutzer - Anpassung)
- user_Debug (Benutzer - Debugging)
- user_Operate (Benutzer - Betrieb)
- user_Program (Benutzer - Programm)

Weitere Informationen über die Zuweisung eines vorkonfigurierten Benutzerprofils für einen Benutzer durch einen Super User finden Sie unter *Benutzerfunktionen* (siehe EcoStruxure™ Control Expert, Sicherheitseditor, Betriebshandbuch).

Zugriffsrechte

Einführung

Die Zugriffsrechte von Control Expert sind in folgende Kategorien untergliedert:

- Projektdienste
- Einstellung/Debugging
- Bibliotheken
- Globale Änderung
- Elementare Änderung einer Variablen
- Elementare Änderung von DDT-Daten
- Elementare Änderung eines DFB-Typs
- Elementare Änderung einer DFB-Instanz
- Bus-Konfigurationseditor
- Konfigurationseditor der Ein- und Ausgänge
- Laufzeitfenster
- Cybersicherheit
- Sicherheit

In diesem Abschnitt werden die für jedes vorkonfigurierte Benutzerprofil verfügbaren Zugriffsrechte vorgestellt.

Projektdienste

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	**Vorkonfiguriertes Benutzerprofil**							
	Adjust	**Safety_ Adjust**	**Debug**	**Safety_ Debug**	**Operate**	**Safety_ Operate**	**Program**	**Safety_ Program**
Neues Projekt erstellen	–	–	–	–	–	–	✓	✓
Vorhandenes Projekt öffnen	✓	✓	✓	✓	✓	✓	✓	✓
Projekt speichern	–	–	–	–	–	–	✓	✓
Projekt speichern unter	✓	✓	✓	✓	✓	✓	✓	✓
Projekt importieren	–	–	–	–	–	–	✓	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Offline erstellen	–	–	–	–	–	–	✓	✓
Online in Stop erstellen	–	–	–	–	–	–	✓	✓
Online in Run erstellen	–	–	–	–	–	–	✓	✓
SPS starten, stoppen oder initialisieren*	✓	–	✓	–	–	–	✓	✓
Anfangswerte mit aktuellen Werten aktualisieren (nur nicht-sichere Daten)	–	–	✓	–	–	–	✓	✓
Projekt von SPS übertragen	✓	✓	✓	✓	✓	✓	✓	✓
Projekt an SPS übertragen	✓	✓	✓	✓	–	–	✓	✓
Datenwerte von Datei an SPS übertragen (nur nicht-sichere Daten)	✓	–	✓	–	✓	–	✓	✓
Projekt-Backup in SPS wiederherstellen	–	–	–	–	–	–	✓	✓
In Projekt-Backup in SPS speichern	–	–	–	–	–	–	✓	✓
Adresse festlegen	✓	✓	✓	✓	✓	✓	✓	✓
Optionen ändern	✓	✓	✓	✓	✓	✓	✓	✓

* Nur Prozesstasks werden gestartet oder gestoppt. Bei einem Nicht-Sicherheits-PAC bedeutet das, dass der PAC gestartet bzw. gestoppt wird. Bei einem M580-Sicherheits-PAC bedeutet das, dass alle Tasks außer der SAFE-Task gestartet bzw. gestoppt werden.

✓ : Inbegriffen

– : Nicht inbegriffen

Einstellung/Debugging

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Variablenwerte ändern	✓	–	✓		✓		✓	✓
Werte der Sicherheitsvariablen ändern	–	✓	–	✓	–	✓	–	✓
Interne Bits forcieren	–	–	✓	–	–	–	✓	✓
Ausgänge forcieren	–	–	✓	–	–	–	✓	✓
Eingänge forcieren	–	–	✓	–	–	–	✓	✓
Task-Management	–	–	✓	–	–	–	✓	✓
SAFE-Task - Verwaltung	–	–	–	✓	–	–	–	✓
Änderung der Task-Zykluszeit	✓	–	✓		✓	–	✓	✓
SAFE-Task - Änderung der Zykluszeit	–	✓	–	✓	–	✓	–	✓
Meldung im Viewer löschen	✓	✓	✓	✓	✓	✓	✓	✓
Ausführbare Datei debuggen	–	–	✓	✓	–	–	✓	✓
Projektvariable ersetzen	–	–	–	–	–	–	✓	✓
Projektvariable ersetzen	–	–	–	–	–	–	–	✓

✓ : Inbegriffen

– : Nicht inbegriffen

Bibliotheken

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Bibliotheken oder Familien erstellen	–	–	–	–	–	–	✓	✓
Sicherheitsbibliotheken oder -familien erstellen	–	–	–	–	–	–	–	✓
Bibliotheken oder Familien löschen	–	–	–	–	–	–	✓	✓
Sicherheitsbibliotheken oder -familien löschen	–	–	–	–	–	–	–	✓
Objekt in Bibliothek speichern	–	–	–	–	–	–	✓	✓
Objekt in Sicherheitsbibliothek speichern	–	–	–	–	–	–	–	✓
Objekt aus Bibliothek löschen	–	–	–	–	–	–	✓	✓
Objekt aus Sicherheitsbibliothek löschen	–	–	–	–	–	–	–	✓
Objekt aus Bibliothek laden	–	–	–	–	–	–	✓	✓
Objekt aus Sicherheitsbibliothek abrufen	–	–	–	–	–	–	–	✓

✓ : Inbegriffen

– : Nicht inbegriffen

Globale Änderung

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Dokumentation ändern	✓	✓	✓	✓	✓	✓	✓	✓
Funktionsansicht ändern	–	–	–	–	–	–	✓	✓
Animationstabellen ändern	✓	✓	✓	✓	✓	✓	✓	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Konstantwerte ändern	✓	–	✓	–	✓	–	✓	✓
Sicherheitskonstantwerte ändern	–	✓	–	✓	–	✓	–	✓
Programmstruktur ändern	–	–	–	–	–	–	✓	✓
Sicherheitsprogrammstruktur ändern	–	–	–	–	–	–	–	✓
Programm-Sections ändern	–	–	–	–	–	–	✓	✓
Sicherheitsprogrammsections ändern	–	–	–	–	–	–	–	✓
Projekteinstellungen ändern	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Elementare Änderung einer Variablen

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Variable hinzufügen/ entfernen	–	–	–	–	–	–	✓	✓
Sicherheitsvariablen - Hinzufügen/Entfernen	–	–	–	–	–	–	–	✓
Hauptattribute von Variablen ändern	–	–	–	–	–	–	✓	✓
Sicherheitsvariablen - Änderung der Hauptattribute	–	–	–	–	–	–	–	✓
Nebenattribute von Variablen ändern	✓	–	✓	–	✓	–	✓	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Sicherheitsvariablen - Änderung der Nebenattribute	–	✓	–	✓	–	✓	–	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Elementare Änderung von DDT-Daten

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DDT hinzufügen/ entfernen	–	–	–	–	–	–	✓	✓
DDT ändern	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Elementare Änderung eines DFB-Typs

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DFB-Typ hinzufügen/ entfernen	–	–	–	–	–	–	✓	✓
Sicherheits-DFB-Typ - Hinzufügen/ Entfernen	–	–	–	–	–	–	–	✓
Struktur eines DFB-Typs ändern	–	–	–	–	–	–	✓	✓
Sicherheits-DFB-Typ - Strukturänderung	–	–	–	–	–	–	–	✓

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Sections eines DFB-Typs ändern	–	–	–	–	–	–	✓	✓
Sicherheits-DFB-Typ - Sectionänderung	–	–	–	–	–	–	–	✓

✓ : Inbegriffen

– : Nicht inbegriffen

Elementare Änderung einer DFB-Instanz

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
DFB-Instanz ändern	–	–	–	–	–	–	✓	✓
Sicherheits-DFB - Instanzänderung	–	–	–	–	–	–	–	✓
Nebenattribute einer DFB-Instanz ändern	✓	–	✓	–	✓	–	✓	✓
Sicherheits-DFB-Instanz - Änderung der Nebenattribute	–	✓	–	✓	–	✓	–	✓

✓ : Inbegriffen

– : Nicht inbegriffen

Bus-Konfigurationseditor

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Konfiguration ändern	–	–	–	–	–	–	✓	✓
Sicherheitskonfiguration ändern	–	–	–	–	–	–	–	✓
E/A-Sniffing	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Konfigurationseditor der Ein- und Ausgänge

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
E/A-Konfiguration ändern	–	–	–	–	–	–	✓	✓
Sicherheits-E/A-Konfiguration ändern	–	–	–	–	–	–	–	✓
E/A anpassen	✓	–	✓	–	✓	–	✓	✓
Sicherheits-E/A anpassen	–	✓	–	✓	–	✓	–	✓
Parameter speichern	–	–	✓	–	–	–	✓	✓
Parameter wiederherstellen	–	–	✓	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Laufzeitfenster

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Fenster ändern	–	–	–	–	–	–	✓	✓
Meldungen ändern	–	–	–	–	–	–	✓	✓
Fenster oder Familien hinzufügen/entfernen	–	–	–	–	–	–	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Cybersicherheit

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	Safety_ Adjust	Debug	Safety_ Debug	Operate	Safety_ Operate	Program	Safety_ Program
Anwendungspasswort erstellen oder ändern	–	–	–	–	–	–	✓	✓
Wartungsmodus aktivieren	–	✓	–	✓	–	✓	–	✓
Timeout für Selbst-Verriegelung anpassen	✓	✓	✓	✓	✓	✓	✓	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Sicherheit

Nachfolgend sind die Zugriffsrechte für diese Kategorie aufgeführt:

Zugriffsrecht	Vorkonfiguriertes Benutzerprofil							
	Adjust	**Safety_ Adjust**	**Debug**	**Safety_ Debug**	**Operate**	**Safety_ Operate**	**Program**	**Safety_ Program**
Wartungsmodus aktivieren	–	✓	–	✓	–	✓	–	✓
✓ : Inbegriffen – : Nicht inbegriffen								

Änderungen an Control Expert für das M580-Sicherheitssystem

Einführung

In diesem Abschnitt werden Control Expert-Funktionen beschrieben, die für das M580-Sicherheitssystem geändert oder beschränkt wurden.

Übertragung und Import von M580-Sicherheitsprojekten und -Code in Control Expert

Übertragung eines Sicherheitsprojekts von Control Expert in den Sicherheits-PAC

Mit dem Befehl **SPS > Projekt zu SPS übertragen** können Sie Ihr Projekt von Control Expert in den PAC übertragen, wenn folgende Bedingungen gegeben sind:

- Control Expert ist im Programmierungsmodus (siehe EcoStruxure™ Control Expert, Betriebsarten) mit dem M580-Sicherheits-PAC verbunden.
- In Control Expert ist ein Projekt geöffnet.
- Alle PAC-Tasks befinden sich im Zustand STOP.

HINWEIS: Eine Sicherheitsanwendung lässt sich nur auf einen Sicherheits-PAC übertragen. Eine Sicherheitsanwendung kann nicht auf einen nicht-sicheren PAC übertragen werden.

Übertragung eines Sicherheitsprojekts vom Sicherheits-PAC in Control Expert

Ebenso können Sie mit dem Befehl **SPS > Projekt von SPS übertragen** Ihr Projekt vom PAC in Control Expert übertragen, wenn folgende Bedingungen gegeben sind:

- Control Expert ist im Programmierungsmodus (siehe EcoStruxure™ Control Expert, Betriebsarten) mit dem M580-Sicherheits-PAC verbunden.
- In Control Expert ist kein Projekt geöffnet.

Sie können Inhalt in alle Tasks (SAFE, MAST, FAST, AUX0 oder AUX1) im Sicherheits- oder Wartungsmodus übertragen.

Import von Projekten und Code-Sections in Control Expert

Control Expert Safety unterstützt den Import kompletter Projekte (über **Datei > Öffnen**) und Code-Sections (über **Tasks > Importieren...** oder **Sections > Importieren...**). Dafür gilt Folgendes:

- Nur Funktionen oder Funktionsbausteintypen, die in der Sicherheitsbibliothek (**Datenumfangseditor > <Libset> > Sicherheit**) oder der benutzerdefinierten Bibliothek (**Datenumfangseditor > <Libset> > Benutzerdefinierte Datei**) vorhanden sind, können in eine Code-Section aufgenommen werden, die von der SAFE-Task bearbeitet wird.
- Nur Funktionen oder Funktionsbausteintypen, die in anderen Bibliotheken als der Sicherheitsbibliothek vorhanden sind, können in eine nicht-sichere Code-Section aufgenommen werden, die von einer Prozesstask bearbeitet wird (MAST, FAST, AUX0 oder AUX1).

Speicherung und Wiederherstellung von Daten zwischen Datei und PAC

Funktion zur Speicherung und Wiederherstellung nicht-sicherer Daten

Control Expert unterstützt für Prozessdaten und Daten aus dem globalen Bereich die Befehle **SPS > Daten von SPS in Datei speichern** und **SPS > Daten aus Datei auf SPS wiederherstellen**. In den gespeicherten und wiederhergestellten Daten fehlen jedoch die Variablen und Funktionsbausteininstanzen, die im sicheren Namespace erstellt wurden.

Informationen zur Verwendung dieser Befehle für nicht-sichere Daten finden Sie unter *Speichern/Wiederherstellen von Daten zwischen einer Datei und der SPS* im Dokument *EcoStruxure™ Control Expert Betriebsarten*.

CCOTF für einen M580-Sicherheits-PAC

Ändern einer Konfiguration „on the Fly“

Mit der Funktion „Change Configuration On The Fly“ (CCOTF) können Sie eine Control Expert-Konfiguration ändern, während der PAC in Betrieb ist. Folgende Funktionen werden ggf. unterstützt:

- Hinzufügen einer Station
- Hinzufügen eines E/A-Moduls

- Löschen eines E/A-Moduls
- Bearbeiten der Konfiguration eines E/A-Moduls, inklusive:
  - Ändern einer Parametereinstellung
  - Hinzufügen einer Kanalfunktion
  - Löschen einer Kanalfunktion
  - Ändern einer Kanalfunktion

HINWEIS: Die CCOTF-Funktion ist nicht für CIP Safety-Geräte verfügbar.

Die CCOTF-Funktion wird aktiviert, indem Sie **Online-Änderung im RUN- oder STOP-Modus** auf der Registerkarte **Konfiguration** des CPU-Moduls auswählen.

Die grundlegende CCOTF-Funktionalität wurde in den M580-Sicherheits-PAC integriert, aber es gelten die folgenden Beschränkungen.

Eine vollständige Beschreibung von CCOTF finden Sie in *Modicon M580 CCOTF (Change Configuration On The Fly) Benutzerhandbuch*.

Beschränkungen der CCOTF-Funktion für einen M580-Sicherheits-PAC

Die CCOTF-Funktion wurde im M580-Sicherheits-PAC implementiert. Es gelten jedoch Beschränkungen, die von der jeweiligen Funktion und dem Typ der E/A-Module abhängig ist:

CCOTF-Funktion	**E/A-Modultyp und Betriebsmodus**			
	Nicht-störende E/A		**SIL3-E/A-Sicherheitsmodul**	
	Wartungsmodus	**Sicherheitsmodus**	**Wartungsmodus**	**Sicherheitsmodus**
Station hinzufügen	✓	✓	✓[1]	✓
Modul hinzufügen	✓	✓	✓[1]	**X**
Modul löschen	✓	✓	✓	**X**
E/A-Modulkonfiguration bearbeiten	✓	✓	**X**	**X**

✓: Zulässig

X: Nicht zulässig

1. Zum Hinzufügen einer Station und eines Sicherheitsmoduls sind zwei CCOTF-Sitzungen erforderlich: eine zum Hinzufügen der Station, die zweite zum Hinzufügen des Sicherheitsmoduls. Diese beiden Aktionen können nicht in nur einer CCOTF-Sitzung durchgeführt werden.

HINWEIS: Bearbeitungen in einer einzigen CCOTF-Sitzung können sich nur auf eine einzige Task beziehen (SAFE, MAST, FAST, AUX0 oder AUX1).

Änderungen an Tools für den M580-Sicherheits-PAC

Einführung

Der M580-Sicherheits-PAC unterstützt verschiedene verbundene Tools. Einige davon wurden für die Verwendung mit dem M580-Sicherheits-PAC verändert. In diesem Abschnitt werden diese Tools erläutert.

Speicherverwendung

Im Fenster **Speicherverwendung** werden die folgenden Informationen angezeigt:

- Physische Aufteilung des PAC-Speichers (interner Speicher und Speicherkarte)
- Speicherbelegung eines Projekts (Daten, Programm, Konfiguration, System)

Für den M580-Sicherheits-PAC zeigt dieser Bildschirm zwei neue Parameter an – **Angegebene Sicherheitsdaten** und **Ausführbarer Sicherheitscode**. Diese werden im Folgenden beschrieben.

HINWEIS: Sie können außerdem den Befehl **Packen** in diesem Fenster verwenden, um den Speicher neu zu organisieren, wo möglich.

Weitere Informationen finden Sie im Kapitel *Speicherverwendung* im Handbuch *EcoStruxure™ Control Expert Betriebsarten* .

Für den M580-Sicherheits-PAC werden die folgenden Parameter angezeigt:

Parameter	Beschreibung
Benutzerdaten	Dieses Feld zeigt den Speicherplatz (in Wörtern) an, der durch Benutzerdaten (Objekte in Bezug auf die Konfiguration) eingenommen wird: • **Daten**: Mit dem Prozessor (%M, %MW, %S, %SW usw.) oder den Ein-/Ausgangsmodulen verknüpfte lokalisierte Daten. • **Deklarierte Daten**: Nicht lokalisierte (im Prozessdaten-Editor deklarierte) Daten. Diese Daten werden bei einem Spannungsausfall gespeichert. • **Ungesicherte deklarierte Daten**: Nicht lokalisierte (im Prozessdaten-Editor deklarierte) Daten. Diese Daten werden bei einem Spannungsausfall nicht gespeichert. • **Angegebene Sicherheitsdaten**: Nicht lokalisierte (im Sicherheitsdaten-Editor deklarierte) Daten. Diese Daten werden bei einem Spannungsausfall nicht gespeichert.
Benutzerprogramm	Dieses Feld gibt den Speicherplatz (in Worten) an, der vom Projektprogramm belegt ist:

Parameter	Beschreibung
	• **Konstanten**: Mit dem Prozessor (%KW) und den Ein-/Ausgangsmodulen verknüpfte statische Konstanten, Initialwerte der Daten. • **Ausführbarer Code**: Ausführbarer Code des Prozessbereichsteils des Projektprogramms, EFs, EFBs und DFB-Typen. • **Auslese-Information**: Informationen für das Auslesen (den Upload) des Projekts (grafischer Sprachcode, Symbole usw.). • **Ausführbarer Sicherheitscode**: Ausführbarer Code des Sicherheitsbereichsteils des Projektprogramms, EFs, EFBs und DFB-Typen.
Andere	Dieses Feld gibt den Speicherplatz (in Wörtern) an, der von den sonstigen, mit der Konfiguration und der Projektstruktur zusammenhängenden Daten belegt ist: • **Konfiguration**: Andere Daten, die sich auf die Konfiguration beziehen (Hardwarekonfiguration, Softwarekonfiguration). • **System**: Vom Betriebssystem genutzte Daten (Task-Stapel, Kataloge usw.). • **Diagnose**: Informationen im Zusammenhang mit der Prozess- oder Systemdiagnose oder dem Diagnosepuffer. • **Datenwörterbuch**: Wörterbuch symbolisierter Variablen und deren Eigenschaften (Adresse, Typ usw.).
Interner Speicher	Dieses Feld stellt die Organisation des internen Speichers des PAC dar. Weiterhin werden der verfügbare Speicherplatz (**Gesamt**), der größtmögliche zusammenhängende Speicherplatz (**Größter**) und die Fragmentierungsebene (durch Änderungen im Online-Betrieb) dargestellt.

Ereignisanzeige

Die *Ereignisanzeige* ist ein Dienstprogramm von MS Windows, das die von Control Expert protokollierten Ereignisse erfasst In der *Ereignisanzeige* können Sie den Verlauf der protokollierten Ereignisse anzeigen.

Der Zugriff auf die *Ereignisanzeige* erfolgt in MS Windows im Ordner *Verwaltung* der *Systemsteuerung*. Wenn Sie das Dienstprogramm öffnen, wählen Sie **Aktionsbereich anzeigen** und klicken Sie auf **Benutzerdefinierte Ansicht erstellen**, um das Dialogfeld zu öffnen. Dort können Sie eine benutzerdefinierte Ansicht für Control Expert-Ereignisse erstellen.

HINWEIS: Im Dialogfeld **Benutzerdefinierte Ansicht erstellen** wählen Sie zuerst **Nach Quelle** und dann als Quelle **TraceServer** aus, um Control Expert-Ereignisse anzuzeigen.

CIP Safety

Inhalt dieses Kapitels

Übersicht

In diesem Kapitel wird die von den M580-Sicherheits-CPUs BMEP58•040S im Standalone-Betrieb unterstützte CIP Safety-Kommunikation nach IEC 61784-3 beschrieben.

Beschreibung von CIP Safety für M580-Sicherheits-PACs

CIP-Safety-Kommunikation

Einführung

Die Sicherheits-CPUs BMEP58•040S im Standalone-Betrieb unterstützen die CIP-Safety-Kommunikation (IEC 61784-3) und können dieses Protokoll zur Herstellung einer Verbindung mit einem CIP-Safety-Gerät über EtherNet/IP heranziehen.

CIP Safety greift für den Austausch von Daten zwischen sicheren Knoten über EtherNet/IP auf den Consumer-Producer-Mechanismus zurück. (Die DeviceNet- oder Sercos III-Kommunikation wird nicht unterstützt.) Die CPU fungiert als Ursprungsgerät, das eine Unicast-EtherNet/IP-Verbindung (eins-zu-eins) zu jedem Zielsicherheitsgerät herstellt. Die CPU kann eine CIP-Safety-Verbindung zu Zielgeräten aufbauen, die das CIP-Safety-Protokoll unterstützen, sowie eine (nicht-sichere) CIP-Verbindung zu Zielgeräten, die das CIP-Protokoll unterstützen.

Wie bei allen Sicherheits-PACs führen die CIP-Safety-CPU und der CIP-Safety-Kopro den CIP-Safety-Stapel parallel aus und vergleichen dann die Verarbeitungsergebnisse.

Unterstützte Architekturen

M580-Sicherheits-CPUs im Standalone-Betrieb unterstützen CIP-Safety-Geräte in DIO-Clouds.

HINWEIS: Zurzeit existieren keine CIP-Safety-Geräte, die RSTP unterstützen und in einem eX80-Rack installiert werden können. Deshalb können CIP-Safety-Geräte zurzeit nicht mit den zwei Gerätenetzwerk-Ports der CPU, aber mit dem CPU-Service-Port verbunden werden.

DIO-Clouds benötigen nur eine einzelne Kupferverbindung (kein Ring) und können mit folgenden Komponenten verbunden werden:

- Schaltmodul für Netzwerkoptionen BMENOS0300
- Service-Port der CPU
- Service-Port eines eX80-Ethernet-E/A-Adaptermoduls BM•CRA312•0 in einer RIO-Station
- Kupferport eines Ethernet-Dual-Ring-Switch

HINWEIS: Wenn ein CIP-Safety-Gerät mit dem Service-Port eines eX80-Ethernet-E/A-Adaptermoduls BM•CRA312•0 in einer RIO-Station verbunden wird, wird das CIP-Safety-Zielgerät ggf. nicht automatisch gestartet, während das CRA seine Konfiguration lädt. Damit die CIP-Safety-Verbindungen wie beabsichtigt geöffnet werden, müssen Sie unter Umständen das Steuerungsbit der CIP-Safety-Verbindung im Ziel-DDDT (CTRL_IN oder CTRL_OUT) durch Umschaltung von False zu True verwalten, sobald das Modul BM•CRA312•0 seine Konfiguration vollständig geladen hat.

Wie bei allen anderen Geräten in DIO-Clouds werden die CIP-Safety-Geräte nicht als Teil des RIO-Hauptrings abgefragt und ihr Verbindungsstatus wird nicht anhand der LEDs der CPU signalisiert.

Zusätzliche Informationen zu DIO-Clouds finden Sie in folgenden Handbüchern: *Modicon M580 Standalone, Systemplanungshandbuch für häufig verwendete Architekturen* und *Modicon M580 Systemplanungshandbuch für komplexe Topologien*.

Konfigurationsübersicht

Die Konfiguration der CIP-Safety-Kommunikation umfasst drei separate Konfigurationsaufgaben:

- Konfiguration der M580-Standalone-Sicherheits-CPU mit CIP-Safety-Einstellungen in Control Expert, Seite 362. Dazu gehört die Erstellung einer OUNID (Originator Unique Network Identifier), die die CPU eindeutig identifziert. Die OUNID wird in Control Expert als Verkettung zweiter Komponenten erstellt:
  - Netzwerk-Sicherheitsnummer (SNN): Eine Kennung für die in Control Expert erstellte CPU.
  - IP-Hauptadresse der CPU, in Control Exprt als Teil der IP-Adresseinstellungen der CPU eingegeben.

  Schneider Electric empfiehlt eine einmalige Einstellung der CPU-OUNID in der Erstkonfiguration. Wenn Sie die OUNID-Einstellung anschließend ändern, müssen Sie alle mit der CPU verbundenen CIP-Safety-Geräte neu konfigurieren.
- Konfiguration des CIP-Safety-Geräts, Seite 366 mithilfe eines vom Gerätehersteller bereitgestellten Tools zur Sicherheitsnetzwerkkonfiguration (SNCT: Safety Network Configuration Tool). Dies umfasst zwei Aufgaben:
  - Erstellung einer SCID (Safety Configuration Identifier): Die SCID, auch als Konfigurationssignatur bezeichnet, wird im SNCT erstellt und von Control Expert bei der Konfiguration der CIP-Safety-Verbindung zwischen dem Ursprung (CPU) und dem Ziel (CIP Safety-Gerät) verwendet.
  - Zuweisung einer SNN (Safety Network Number): Die SNN wird in der Regel von Control Expert für das CIP-Safety-Gerät erstellt und dem Gerät vom SNCT zugeordnet.

- Konfiguration der CIP-Safety-Verbindung zwischen der CPU und dem CIP-Safety-Gerät, Seite 368. Die Verbindung wird durch eine TUNID identifiziert, die mithilfe des Geräteverbindungs-DTM in Control Expert unter Verwendung eines CIP-Safety-DTM erstellt wird, der auf einer vom Hersteller bereitgestellten EDS-Datei basiert oder allein eingesetzt wird, wenn keine EDS-Datei vorhanden ist.

Verwaltung der CIP-Safety-Geräteverbindungen

Die CIP-Safety-CPU stellt eine Verbindung zu einem konfigurierten CIP-Gerät her und verwaltet dann das verbundene Gerät. Da Control Expert sowohl das CIP- als auch das CIP-Safety-Protokoll unterstützt, kann es CIP-Verbindungen zu folgenden Komponenten verwalten:

- CIP-Geräte, die CIP over EtherNet/IP, jedoch nicht CIP Safety implementieren.
- CIP-Geräte, die CIP Safety over EtherNet/IP, jedoch nicht CIP implementieren.
- CIP-Geräte, die sowohl CIP als auch CIP Safety over EtherNet/IP implementieren.

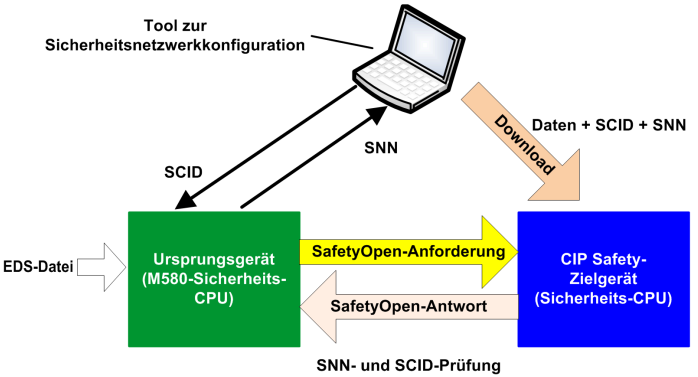
HINWEIS: Für jedes CIP- und CIP-Safety-Gerät ist ein einzelner DTM zur Konfiguration erforderlich. Ein CIP-Hybridgerät - das beide Protokolle, CIP und CIP Safety, implementiert - benötigt zwei DTMs: ein als CIP-Gerät und ein als CIP-Safety-Gerät konfigurierter DTM.

Herstellen einer Verbindung Ursprung -> Ziel

Die M580-Standalone-CPU verwendet ausschließlich SafetyOpen-Requests vom Typ 2, um eine Verbindung zu einem CIP-Safety-Gerät herzustellen. Eine SafetyOpen-Verbindung vom Typ 2 zu einem Sicherheitsgerät kann erst nach dessen Konfiguration mithilfe eines SNCT hergestellt werden. Sollte es sich bei dem CIP-Safety-Gerät um ein Drittherstellergerät handeln, verfügt Control Expert über keine Konfigurationsdatei, die in das CIP-Safety-Gerät heruntergeladen werden könnte, und kann somit nicht als SNCT fungieren.

HINWEIS: Im Gegensatz dazu stattet eine SafetyOpen-Verbindung vom Typ 1 das Sicherheitsgerät mit Konfigurationseinstellungen aus und stellt darüber hinaus eine Verbindung her. M580-CIP-Safety-CPUs bieten keine Unterstützung für SafetyOpen-Verbindungsrequests vom Typ 1.

Das nachstehende Diagramm bietet eine Übersicht über die Einrichtung einer CIP-Safety-Verbindung zwischen der CPU als Verbindungsursprung und dem CIP-Safety-Gerät als Verbindungsziel:



In diesem Diagramm treten folgende Ereignisse auf:

1. Control Expert verwendet eine vom Hersteller bereitgestellte EDS-Datei als Grundlage für die Erstellung eines DTM für die Verbindung zwischen dem CPU und dem CIP-Safety-Gerät.
2. Die Geräte-SNN wird in Control Expert erstellt und dann im SNCT eingegeben.
3. Das SNCT erstellt die SCID für das Gerät, die in Control Expert als Teil der Verbindungskonfiguration eingegeben wird.
4. Das SNCT lädt die Konfigurationseinstellungen, die vom SNCT erstellte SCID und die von Control Expert für die Verbindung erstellte SNN in das Gerät herunter.
5. Die CPU als Ursprungsgerät sendet einen SafetyOpen-Request vom Typ 2 an das Gerät.
6. Das CIP-Safety-Gerät sendet eine SafetyOpen-Antwort an die CPU.
7. Wenn die Prüfsummen von Anforderung und Antwort übereinstimmen, wird die Verbindung hergestellt.

Konfiguration der M580-CIP Safety-CPU

Übersicht

In diesem Abschnitt wird die Konfiguration der CIP Safety-Standalone-CPU als Ursprungs der CIP Safety-Kommunikation beschrieben.

Konfiguration der CPU-OUNID

CPU als Ursprungsgerät

Verwenden Sie die Registerkarte (siehe Modicon M580, Hardware, Referenzhandbuch) **Sicherheit** der M580-Standalone-Sicherheits-CPU zur Konfiguration der CPU als CIP Safety-Ursprungsgerät, indem Sie ihr eine OUNID (Originator Unique Network Identifier) zuweisen.

Eine OUNID ist ein verketteter 10-Byte-Hexadezimalwert, bestehend aus:

- Netzwerk-Sicherheitsnummer (6 Byte)
- IP-Adresse (4 Byte)

HINWEIS: Änderungen an der OUNID können nur offline vorgenommen werden. Nach der Generierung der geänderten Konfiguration kann die Anwendung in den PAC heruntergeladen werden.

SNN (Safety Network Number)

Die SNN-Komponente (Netzwerk-Sicherheitsnummer) der OUNID kann von Control Expert automatisch oder durch manuelle Eingabe vom Benutzer generiert werden. Erstellen Sie die SNN:

- Automatisch durch Auswahl von **Zeitbasiert** und anschließendes Klicken auf die Schaltfläche **Generieren**. Der automatisch generierte Wert wird dann im Feld **Nummer** angezeigt.
- Manuell durch Auswahl von **Manuell** und anschließende Eingabe einer hexadezimalen 6-Byte-Zeichenfolge in das Feld **Nummer**.

HINWEIS: Der Benutzer sollte jedem mit demselben Sicherheitsnetzwerk verbundenen M580-CPU-Ursprungsgerät eine eindeutige SNN zuweisen.

IP-Adresse

Diese schreibgeschützte Einstellung wird automatisch auf der Grundlage der konfigurierten CPU-Einstellung der **IP-Hauptadresse** auf der Registerkarte (siehe Modicon M580, Hardware, Referenzhandbuch) **IP-Konfig.** eingegeben.

OUNID

Nach der Erstellung der OUNID wird die Kennung als Parameter in der SafetyOpen-Anforderung vom Typ 2, Seite 381 zur Herstelllung einer Verbindung zwischen der CPU als Ursprungsgerät und dem CIP Safety-Gerät als Zielgerät verwendet.

Konfiguration des CIP Safety-Zielgeräts

Übersicht

Dieser Abschnitt enthält einen Überblick über den Konfigurationsprozess für das CIP Safety-Zielgerät, einschließlich der Konfiguration des CIP Safety-Geräts mithilfe eines vom Hersteller bereitgestellten Konfigurationstools.

Überblick über die CIP Safety-Gerätekonfiguration

Einführung

Die Konfiguration des CIP Safety-Zielgeräts umfasst zwei Aufgaben:

- Konfiguration der CIP Safety-Geräteeinstellungen, Seite 366 mithilfe eines vom Hersteller bereitgestellten Tools zur Sicherheitsetzwerkkonfiguration (SNCT: Safety Network Configuration Tool).
- Konfiguration der Verbindung zwischen dem CIP Safety-Ursprungsgerät (CPU) und dem CIP Safety-Zielgerät mithilfe eines DTM in Control Expert. Der DTM kann:
  - auf einer herstellerspezifischen EDS-Datei basieren.
  - ein generischer DTM von Control Expert sein, wenn keine EDS-Datei verfügbar ist.

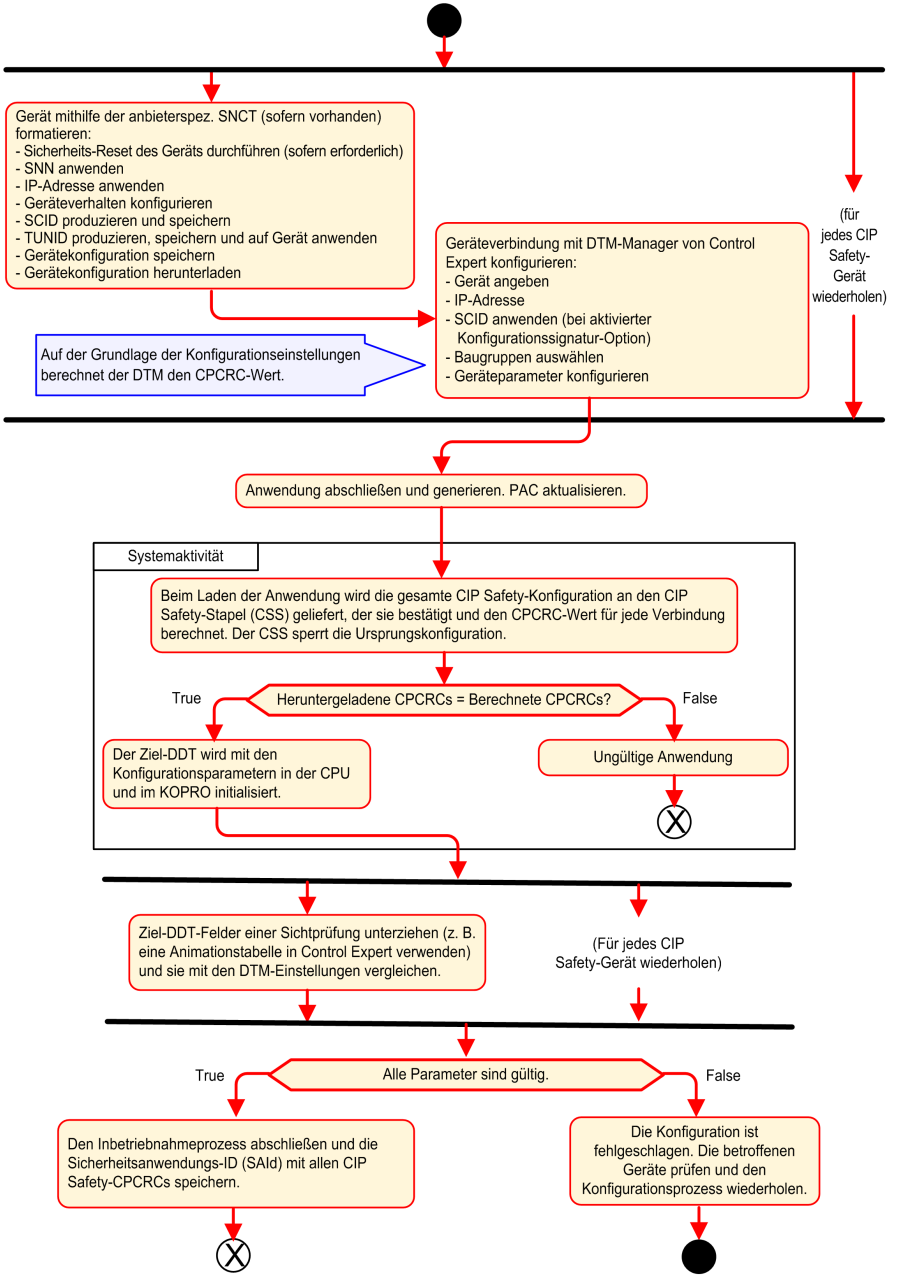
Doppelte Konfigurationsprüfung

Die folgenden zwei Prozesse gewährleisten gemeinsam eine hohe Integritätsbestätigung, um zu gewährleisten, dass die mithilfe der Software Control Expert erstellte Konfiguration ordnungsgemäß in die als Ursprungsgerät fungierende M580-CIP Safety-CPU heruntergeladen und dort gespeichert wurde.

- Ein vom Benutzer durchgeführter visueller Vergleich (nach Abschluss des Anwendungsdownloads) der im Ziel-DDDT angezeigten Konfigurationsparameter der CIP Safety-Verbindung mit denselben im Ziel-DTM angezeigten Parametern.
- Ein von der CPU und vom Kopro durchgeführter automatischer Vergleich des vom DTM berechneten Verbindungsparameter-CRC (CPCRC: Connection Parameter CRC) mit dem vom CIP Safety-Stapel (CSS), der in der CPU und im Kopro ausgeführt wird, berechneten CPCRC.

Überblick über den Konfigurationsprozess

Prozess der CIP Safety-Gerätekonfiguration und -validierung:



Konfiguration des CIP Safety-Geräts mithilfe eines herstellerspezifischen Tools

Einführung

Das CIP Safety-Zielgerät wird mithilfe eines Tools zur Sicherheitsnetzwerkkonfiguration (SNCT: Safety Network Configuration Tool) konfiguriert. Zu dessen Konfiguration wird nicht die Software Control Expert verwendet. Das SNCT wird vom Hersteller des CIP Safety-Geräts bereitgestellt und ist somit geräteabängig.

Verwenden Sie das SNCT zur Durchführung folgender Aufgaben:

- Konfiguration und Download der für den Gerätebetrieb erforderlichen Einstellungen in das Gerät.
- Konfiguration einer gerätespezifischen Sicherheitskonfigurationskennung (SCID: Safety Configuration Identifier) für das Gerät, deren Kopie und Übertragung in die Software Control Expert. Die SCID wird auch als gerätespezifische Konfigurationssignatur bezeichnet. Sie wird in Control Expert bei der Konfiguration der Verbindung Ursprung -> Ziel, Seite 373 verwendet.
- Zuweisung einer eindeutigen TUNID zum Gerät, bestehend aus:
  - einer Netzwerk-Sicherheitsnummer (SNN: Safety Network Number), Seite 372 und
  - einer eindeutigen IP-Adresse.

    HINWEIS: Die SNN wird in der Regel von der Konfigurationssoftware Control Expert (als Teil der Konfiguration der Verbindung Ursprung -> Ziel) generiert und auf das Gerät angewendet. Die IP-Adresse wird sowohl im SNCT als auch im DTM der Geräteverbindung in Control Expert eingegeben.

Konfiguration der SCID

Die SCID wird im SNCT festgelegt und dient als eindeutige hexadezimale Konfigurationskennung für das CIP Safety-Zielgerät. Die Kennung ist eine Verkettung folgender Elemente:

- Sicherheitskonfigurations-CRC (SCCRC: Safety Configuration CRC): Ein zyklischer Redundanz-Prüfwert (CRC: Cyclic Redundancy Check) der Konfigurationseinstellungen des CIP Safety-Geräts mit 4 Byte.
- Sicherheitskonfigurations-Zeitstempel (SCTS: Safety Configuration Time Stamp): Ein hexadezimaler Zeitstempelwert mit 6 Byte, der auf Datum und Uhrzeit verweist.

HINWEIS
GEFAHR DES UNBEABSICHTIGTEN BETRIEBS VON GERÄTEN Wenn Sie eine M580-CPU als CIP Safety-Ursprungsgerät konfigurieren, testen und überprüfen Sie das Verhalten der CIP Safety-Funktion des Systems, bevor Sie CIP Safety-Kommunikation zur Steuerung der entsprechenden Sicherheitsfunktion einsetzen. Nach erfolgreichem Abschluss des Test und der Überprüfung können Sie die Konfigurationssignatur des CIP Safety-Zielgeräts (sofern vorhanden) in den CIP Safety-DTMs von Control Expert aktivieren. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Nach der Erstellung der SCID mithilfe des SNCT können Sie die Elemente der SCID auf der Registerkarte **Sicherheit** des Geräte-DTM in Control Expert eingeben:

- **ID**: Geben Sie den SCCRC-Wert ein.
- **Datum**: Geben Sie das Datum der SCID-Erstellung ein (mm/tt/jjjj).
- **Uhrzeit**: Geben Sie die Uhrzeit der SCID-Erstellung ein (hh/mm/ss/ms).

Sequenz der CIP Safety-Gerätekonfiguration

Die nachfolgende Sequenz beschreibt einen typischen Prozess zur CIP Safety-Gerätekonfiguration:

1. Rufen Sie die Geräte-SNN ab (von Control Expert ausgegeben).
2. Übernehmen Sie die SNN in das herstellerspezifische SNCT.
3. Führen Sie einen Sicherheits-Reset des Geräts durch (optional: wenn sich die Ursprungs-OUNID seit dem letzten Aufbau einer Verbindung zum Gerät geändert hat).
4. Übernehmen Sie die TUNID in das Gerät.
5. Ermitteln Sie die Konfigurationseinstellungen, die das Geräteverhalten steuern.
6. Konfigurieren Sie das Gerät mithilfe des herstellerspezifischen SNCT (Tool zur Sicherheitsnetzwerkkonfiguration).
7. Sperren Sie die Konfiguration und überprüfen Sie deren Genauigkeit.
8. Zeichen Sie die Parameter auf und speichern Sie sie zur späteren Verwendung in der Ursprungskonfiguration (SCID, Baugruppennummern, IP-Adresse usw.).
9. Speichern Sie eine Kopie der Gerätekonfiguration für späteren Gebrauch (z. B. wenn das Gerät ausgetauscht werden muss).

Konfiguration der DTMs von Sicherheitsgeräten

Übersicht

In diesem Abschnitt wird die Konfiguration der Sicherheitszielgeräte und deren Verbindungen zum CPU-Ursprungsgerät mithilfe der DTMs in Control Expert beschrieben.

Verwendung der DTMs

Verwendung der DTMs

Die Konfiguration der Verbindung zwischen dem CPU-Ursprungsgerät und dem CIP Safety-Zielgerät wird in einem DTM vorgenommen. Control Expert unterstützt je nach Geräteprofil die Verwendung folgender DTMs:

- CIP Safety-DTM: Zur Konfiguration einer Verbindung zu einem CIP Safety-Gerät. Das kann mit oder ohne herstellerspezifische EDS-Datei erfolgen.
- Generischer DTM: Zur Konfiguration einer Standardverbindung (d. h. einer nicht-sicheren Verbindung) zu einem Gerät auf der Grundlage einer herstellerspezifischen EDS-Datei.

Die von Ihnen über einen DTM eingegebenen Einstellungen werden in Control Expert im T_CIP_SAFETY_CONF-DDDT, Seite 391 gespeichert und von der SafetyOpen-Anforderung vom Typ 2, Seite 381 zur Herstellung einer Verbindung zwischen der Ursprungs-CPU und dem Zielgerät verwendet.

Bei Verfügbarkeit einer EDS-Datei

Wenn für ein Gerät eine EDS-Datei verfügbar ist, verwenden Sie diese, um einen neuen DTM zu erstellen und wie folgt im **DTM-Katalog** in Control Expert hinzuzufügen:

Element	Beschreibung
1	Wählen Sie in Control Expert **Extras** > **DTM-Browser** aus.
2	Klicken Sie im **DTM-Browser** mit der rechten Maustaste auf den CPU-DTM (BMEP58_ECPU_EXT), um das Kontextmenü zu öffnen.
3	Navigieren Sie zum **Gerätemenü** > **Zusätzliche Funktionen** > **EDS in Bibliothek hinzufügen** und wählen Sie diesen Befehl aus. Der Assistent **EDS hinzufügen** wird geöffnet.
4	Detaillierte Anweisungen zur Vervollständigung des Prozesses durch Hinzufügen einer EDS-Datei zum DTM-Katalog finden Sie unter Hinzufügen einer EDS-Datei im Hardwarekatalog (siehe EcoStruxure™ Control Expert, Betriebsarten).

Sobald Sie den DTM im **DTM-Katalog** hinzugefügt haben, können Sie ihn in Ihrem Control Expert-Projekt hinzufügen.

Bei Nichtverfügbarkeit einer EDS-Datei

Control Expert stellt einen generischen Sicherheits-DTM im **DTM-Katalog** bereit. Sie können diesen DTM zur Konfiguration eines CIP Safety-Geräts verwenden, wenn für das Gerät keine EDS-Datei verfügbar ist.

Hybridgeräte

Ein Hybridgerät ist ein einzelnes Gerät, das sowohl sicherheitsbezogene als auch standardmäßige Verbindungen unterstützt. Wenn Sie im **DTM-Katalog** ein Hybridgerät über den Befehl **EDS in Bibliothek hinzufügen** hinzufügen, werden im **DTM-Katalog** für das Gerät zwei DTMs erstellt: ein Standard-DTM und ein Sicherheits-DTM.

Beim Hinzufügen eines Hybridgeräts zu Ihrem Projekt müssen Sie sowohl den Standard- als auch den Sicherheits-DTM für das Gerät konfigurieren.

Hinzufügen eines DTM zu einem Control Expert-Projekt

Gehen Sie vor wie folgt, um einen DTM zu einem Control Expert-Projekt hinzuzufügen:

Element	Beschreibung
1	Klicken Sie im **DTM-Browser** mit der rechten Maustaste auf den CPU-DTM (BMEP58_ECPU_EXT) und wählen Sie **Hinzufügen...** aus. Daraufhin wird das Dialogfeld **Hinzufügen** geöffnet.
2	Wählen Sie den DTM aus, den Sie hinzufügen möchten. Dabei kann es sich um Folgendes handeln: • einen CIP Safety-DTM, der ausgehend von einer vom Hersteller für das CIP Safety-Gerät bereitgestellten EDS-Datei erstellt wurde oder: • einen CIP Safety-DTM ohne herstellerspezifische EDS-Datei
3	Klicken Sie auf **DTM hinzufügen**. Der ausgewählte DTM wird im **DTM-Browser** unter dem CPU-DTM angezeigt.
4	Klicken Sie mit der rechten Maustaste auf den neuen DTM und wählen Sie **Öffnen** aus. Das Fenster zur Konfiguration des DTM wird geöffnet.

Konfiguration des DTM

Für den CIP Safety-DTM stehen in Control Expert - ob er mit oder ohne herstellerspezifischer EDS-Datei erstellt wurde - eine Reihe vergleichbarer Konfigurationsfenster zur Verfügung.

Navigationsstruktur / Registerkarten zur Konfiguration		**DTM-Typ**	
		Mit Hersteller-EDS	**Ohne Hersteller-EDS**
<Oberster Knoten>		✓	✓
Allgemeiner Knoten			
	Registerkarte „Gerät“	✓	**X**
	Registerkarte „Sicherheit“	✓	✓
<Verbindungen>			
	Registerkarte „Verbindung“	✓	✓
	Registerkarte „Konfigurationseinstellungen“	✓	**X**
	Registerkarte „Konfigurationsüberprüfung“	✓	✓
< > Verweist auf den benutzerdefinierten Namen. ✓ = Enthalten **X** = Nicht enthalten			

In den nachfolgenden Abschnitten werden die verschiedenen Konfigurationsregisterkarten in Control Expert für jeden DTM-Typ beschrieben.

Sicherheitsgerät-DTM - Datei- und Herstellerinformationen

Einführung

Der ausgehend von einer herstellerspezifischen EDS-Datei (oder nicht) erstellte CIP Safety-DTM enthält eine Beschreibung der EDS-Quelldatei und verweist auf den Gerätehersteller. Für:

- einen ausgehend von einer EDS-Datei des Herstellers erstellten CIP Safety-DTM: Diese Informationen sind schreibgeschützt und können durch Auswahl des <Obersten Knotens> in der DTM-Navigationsstruktur (linkes Teilfenster) angezeigt werden.

- einen ohne herstellerspezifische EDS-Datei erstellten CIP Safety-DTM: Diese Informationen werden an zwei separaten Stellen angezeigt:
  - Bei Auswahl des <Obersten Knotens> werden die schreibgeschützten EDS-Dateiinformationen angezeigt.

    HINWEIS: Bei der EDS-Dateireferenz handelt es sich um eine interne, generische EDS-Sicherheitsdatei mit Schneider Electric als Hersteller, die von Control Expert zur Erstellung des CIP Safety-DTM verwendet wird.
  - Bei Auswahl der Registerkarte **Allgemein > Gerät** werden die Herstellerinformationen angezeigt, die bearbeitet werden können.

EDS-Dateiinformationen

Die EDS-Dateiinformationen umfassen folgende schreibgeschützte Daten:

- Beschreibung
- Datum der Dateierstellung
- Uhrzeit der Dateierstellung
- Datum der letzten Änderung
- Uhrzeit der letzten Änderung
- EDS-Revision

Herstellerinformationen

Die folgenden Herstellerinformationen sind für einen ausgehend von einer herstellerspezifischen EDS-Datei erstellten CIP Safety-DTM schreibgeschützt:

- Herstellername
- Gerätetyp
- Hauptreversion
- Nebenrevision
- Produktname

Die folgenden Herstellerinformationen können für einen ohne herstellerspezifische EDS-Datei erstellten CIP Safety-DTM angezeigt und bearbeitet werden:

- Hersteller-ID
- Produkttyp
- Produktcode
- Hauptreversion
- Nebenrevision

HINWEIS: Für DTM-Konfigurationen, die ohne EDS-Datei vorgenommen wurden, können Sie die Herstellerinformationseinstellungen mit den vom Hersteller bereitgestellten Informationen eingeben. Standardmäßig werden die DTM-Herstellerwerte auf 0 gesetzt, und 0-Werte werden nicht unterstützt.

Sicherheitsgeräte-DTM - Netzwerk-Sicherheitsnummer

Sicherheitnetzwerknummer

Verwenden Sie die Registerkarte **Allgemein > Sicherheit** des DTM des CIP Safety-Geräts, um für das Gerät eine Netzwerk-Sicherheitsnummer (SNN: Safety Network Number) zu konfigurieren. Die SNN ermöglicht die Festlegung der TUNID-Kennung (Target Unique Network Identifier). Die TUNID identifiziert das CIP Safety-Gerät und ist ein wesentlicher Bestandteil der von der Ursprungs-CPU zur Initialisierung einer CIP Safety-Verbindung ausgegebenen SafetyOpen-Anforderung vom Typ 2, Seite 381.

Konfiguration der SNN

Die SNN ist ein Hexadezimalwert, der sowohl zur CIP Safety-Verbindungskonfiguration (in Control Expert konfiguriert) gehört als auch zur CIP Safety-Gerätekonfiguration (mithilfe eines SNCT konfiguriert). In der Regel wird die SNN in Control Expert generiert und in das SNCT kopiert (bzw. eingegeben). Das SNCT erzeugt dann die TUNID auf der Grundlage der SNN und IP-Adresse und überträgt diesen Wert in das CIP Safety-Gerät.

Es besteht ebenfalls die Möglichkeit, die SNN direkt vom DTM der CIP Safety-Verbindung in Control Expert an das Zielgerät, Seite 389 zu senden.

Gehen Sie vor wie folgt, um die SNN zu konfigurieren:

Schritt	Aktion
1	Klicken Sie auf der Registerkarte **Allgemein > Sicherheit** auf die Schaltfläche mit den Auslassungszeichen (...). Daraufhin wird das Dialogfeld **Netzwerk-Sicherheitsnummer** geöffnet.
2	Wählen Sie im Dialogfeld **Netzwerk-Sicherheitsnummer** eine der folgenden Optionen aus: • **Zeitbasiert**: Zur Generierung eines Hexadezimalwerts auf der Grundlage von Monat, Tag, Jahr, Minuten, Sekunden und Millisekunden zum Zeitpunkt der Generierung. • **Manuell**: Zur Generierung eines Werts auf der Grundlage eines Dezimaleingangswerts zwischen 1 und 9999, der wie folgt mit zwei Hexadezimalwerten verkettet wird; ◦ Wort 1: 0004 (fest) ◦ Wort 2: 0000 (fest) ◦ Wort 3: 0001 bis 270F (Hexadezimalwert des Eingangswerts 1 bis 9999)

Schritt	Aktion
	• **Herstellerspezifisch**: Eine herstellerspezifische Kennung auf der Grundlage von 3 Hexadezimaleingangswerten: ◦ Wort 1: 05B5 bis 2DA7 (vom Hersteller) ◦ Wort 2: 0000 (fest) ◦ Wort 3: 0001 bis 270F (vom Hersteller) • Ein direkt eingegebener Hexadezimalwert (eingegeben oder eingefügt), bestehend aus: ◦ Wort 1: 2DA8 bis FFFE ◦ Wörter 2 und 3: 00000000 bis 05265BFF
3	Klicken Sie für ein zeitbasiertes, manuelles oder herstellerspezifisches Format auf **Generieren**. Wenn Sie direkt einen Hexadezimalwert eingegeben haben, klicken Sie auf **Einstellen**.
4	Klicken Sie auf **OK**, um die SNN zu speichern und das Dialogfeld zu schließen. Die SNN wird im Feld **Netzwerk-Sicherheitsnummer** angezeigt.

Konfiguration der SCID

Die SCID, auch als Konfigurationssignatur bezeichnet, wird in dem vom Hersteller bereitgestellten Tool zur Sicherheitsnetzwerkkonfiguration (SNCT: Safety Network Configuration Tool) festgelegt und entspricht einer eindeutigen Konfigurationskennung im Hexadezimalformat des CIP Safety-Geräts. Die Kennung ist eine Verkettung folgender Elemente:

- einem Sicherheitskonfigurations-CRC (SCCRC: Security Configuration CRC), d. h. einem CRC-Wert (Cyclic Redundancy Check) aus den Konfigurationseinstellungen des Sicherheitsgeräts, in Form eines Hexadezimalwerts mit 4 Byte.
- einem Sicherheitskonfigurations-Zeitstempel (SCTS: Safety Configuration Time Stamp), d. h. einem hexadezimalen Datums- und Uhrzeitwert mit 6 Byte.

Gehen Sie vor wie folgt, um die SCID einzugeben:

Schritt	Aktion
1	Entnehmen Sie der mithilfe des SNCT vorgenommenen Gerätekonfiguration Folgendes: • den SCCRC • das Datum (mm/tt/jjjj) und die Uhrzeit (hh/mm/ss/ms) der SNCT-Konfiguration
2	Wählen Sie **Konfigurationssignatur** aus.
3	Geben Sie den SCCRC im Feld **ID** ein.
4	Geben Sie Datum und Uhrzeit in den Feldern **Datum** und **Uhrzeit** ein.

HINWEIS: Wenn Sie Sicherheitsverbindungen mit einer SCID = 0 ('SCID-Konfiguration deaktiviert') konfigurieren, beachten Sie, dass Sie in diesem Fall sicherstellen müssen, dass das M580-Sicherheitsursprungsgerät und die CIP Safety-Zielgeräte die richtigen Konfigurationen aufweisen.

Sicherheitsgeräte-DTM - Prüfung und Validierung der Konfiguration

Sichtprüfung der DTM-Konfiguration

Verwenden Sie die Registerkarte **Allgemein > Konfigurationsüberprüfung** für den mit oder ohne herstellerspezifische EDS-Datei erstellten CIP Safety-DTM, um die in diesem DTM definierten (und auf dieser Registerkarte angezeigten) Parameter mit den im Zielgeräte-DDDT festgelegten Parameter zu vergleichen. Sie können diese mithilfe einer Animationstabelle in Control Expert durchführen, wenn Control Expert im verbundenen Modus betrieben wird und mit der CPU verbunden ist.

HINWEIS: Nach einem Anwendungsdownload müssen Sie für jedes CIP Safety-Zielgerät per Sichtprüfung sicherstellen, dass alle in das M580-Ursprungsgerät für das betreffende Zielgerät heruntergeladenen CIP Safety-Konfigurationsparameter mit den im Ziel-DTM konfigurierten Parametern übereinstimmen. Vergleichen Sie dazu die im DDDT des CIP Safety-Zielgeräts angezeigten Konfigurationsparameter (mithilfe einer Animationstabelle mit Control Expert im verbundenen Modus) mit den im DTM konfigurierten und auf der Registerkarte „Konfigurationsüberprüfung“ angezeigten Parametern.

Validierung der heruntergeladenen Konfiguration

Nach dem Download aller CIP Safety-Konfigurationen können alle Downloads anhand von Benutzertests validiert werden. Bei einem der Validierungstests werden die Konfigurationen der Sicherheitsverbindungen nach deren Anwendung in einem Ursprungsgerät überprüft, um sicherzustellen, dass die Zielverbindung erwartungsgemäß funktioniert.

Sicherheitsgeräte-DTM - E/A-Verbindungen

Einführung

Der mit oder ohne herstellerspezifischer EDS-Datei erstellte CIP Safety-DTM verweist auf Sicherheitsverbindungsknoten. Sowohl Sicherheitseingänge als auch Sicherheitsausgänge werden unterstützt - je nach Funktionsumfang eines spezifischen Geräts. Die Registerkarte

Verbindung enthält die Verbindungsparameter für die jeweils ausgewählte Eingangs- oder Ausgangsverbindung.

Für mit einer herstellerspezifischen EDS-Datei erstellte DTMs sind Standardverbindung vorausgewählt. Mit den Befehlen **Verbindung entfernen** und **Verbindung hinzufügen** können Sie die Verbindungseinstellungen an die Anforderungen Ihrer Anwendung anpassen.

Einstellungen für die Sicherheitseingangsverbindungen

Für jede sicherheitsbezogene Eingangsverbindung sind folgende Parameter gegeben:

- **Eingangsgröße** (Lesen/Schreiben-Zugriff): Die im CIP Safety-Gerät konfigurierte Größe der Eingangsdaten in Byte. Standardmäßig auf 0 gesetzt.

  HINWEIS: Sie müssen den Standardwert durch die vom Hersteller bereitgestellten Einstellungen ersetzen. Der Wert 0 wird nicht unterstützt.

- **Angefordertes Paketintervall** (Lesen/Schreiben-Zugriff): RPI verweist auf die Periode zur Aktualisierung der Verbindung. Standardmäßig auf die Periode der SAFE-Task / 2 gesetzt.

  HINWEIS: Die Periode der SAFE-Task (Tsafe) wird im Dialogfeld **Eigenschaften von SAFE** (**Projekt-Browser > Tasks > SAFE > Eigenschaften**) in Control Expert festgelegt.

- **Netzwerkzeitvorgabe** (Lesen/Schreiben-Zugriff): Die von der CIP Safety-Kommunikation, Seite 165 beanspruchte Zeit in Millisekunden. Wenn der Wert niedriger ist als die *minimale Netzwerkzeitvorgabe* wird eine entsprechende Fehlerbenachrichtigung angezeigt. Standardmäßig sollte der Wert der *minimalen Netzwerkzeitvorgabe* * 1,5 entsprechen.

- **Timeout-Multiplikator** (Lesen/Schreiben-Zugriff): Der Timeout-Multiplikator ist eine Komponente bei der Erzeugung der *minimalen Netzwerkzeitvorgabe*, die der Netzwerkzeitvorgabe / 128 µs entspricht. Die *minimale Netzwerkzeitvorgabe* = RPI * Timeout-Multiplikator + Tsafe + 40.

- **Max. Netzwerkübertragung** (Lesen/Schreiben-Zugriff): Das ungünstigste (älteste) Alter (in ms) der Daten zum Zeitpunkt des Empfangs des Pakets durch den Consumer. Dieser Parameter wird nur zur Berechnung des für die Netzwerkzeitvorgabe einzugebenden Mindestwerts (siehe nachstehende Beschreibung) verwendet. Er kann durch Prüfung des *max. Datenalters* im Consumer-Gerät nach der Kommunikation zwischen CIP Safety-Modul und eingerichtetem Netzwerk während längerer Zeit angepasst werden.

  Dieser Parameter ermöglicht die Berechnung des Mindestwerts für den Parameter „Netzwerkzeitvorgabe“ wie folgt:

  Min. (Netzwerkzeitvorgabe) = RPI * Timeout-Multiplikator + Max. Netzwerkübertragung

  Bei einer Änderung von Tsafe sollte der Wert dieses Parameters und infolgedessen auch der Mindestwert der *Netzwerkzeitvorgabe* geändert werden.

  Für diesen Parameter gelten folgende Attribute:

  - Mindestwert = 1 ms
  - Höchstwert = 5800 ms
  - Standardwert = 40 + Tsafe

Der Geräte-DTM verwendet diese Eingangseinstellungen für folgende Berechnungen:

Variable	**Wert**		
	Standard	**Minimum**	**Maximum**
SAFE-Periode (ms)	20	10	255
Eingang Request Packet Interval (ms)	RPI = Tsafe / 2	5	500
Timeout-Multiplikator	2	1	255
Max. Netzwerkübertragung (ms)	40 + 2 * Tsafe	10	5800
Netzwerkzeitvorgabe	Min. Netzwerkzeitvorgabe * 1,5	RPI * Timeout-Multiplikator + Max. Netzwerkübertragung	5800

Einstellungen für die Sicherheitsausgangsverbindungen

Für jede sicherheitsbezogene Ausgangsverbindung sind folgende Parameter gegeben:

- **Ausgangsgröße** (Lesen/Schreiben-Zugriff): Die im CIP Safety-Gerät konfigurierte Größe der Ausgangsdaten in Byte. Standardmäßig auf 0 gesetzt.

  HINWEIS: Sie müssen den Standardwert durch die vom Hersteller bereitgestellten Einstellungen ersetzen. Der Wert 0 wird nicht unterstützt.

- **Angefordertes Paketintervall** (Nur-Lesen-Zugriff): RPI verweist auf die Periode zur Aktualisierung der Verbindung. Auf den Wert der SAFE-Taskperiode (Tsafe) gesetzt.

- **Netzwerkzeitvorgabe** (Lesen/Schreiben-Zugriff): Die von der CIP Safety-Kommunikation, Seite 165 beanspruchte Zeit in Millisekunden. Wenn der Wert niedriger ist als die *minimale Netzwerkzeitvorgabe* wird eine entsprechende Fehlerbenachrichtigung angezeigt. Standardmäßig sollte der Wert der *minimalen Netzwerkzeitvorgabe* * 1,5 entsprechen.
- **Timeout-Multiplikator** (Lesen/Schreiben-Zugriff): Der Timeout-Multiplikator ist eine Komponente bei der Erzeugung der *minimalen Netzwerkzeitvorgabe*, die der Netzwerkzeitvorgabe / 128 µs entspricht. Die *minimale Netzwerkzeitvorgabe* = RPI * Timeout-Multiplikator + Tsafe + 40.
- **Max. Netzwerkübertragung** (Lesen/Schreiben-Zugriff): Das ungünstigste (älteste) Alter (in ms) der Daten zum Zeitpunkt des Empfangs des Pakets durch den Consumer. Dieser Parameter wird nur zur Berechnung des für die Netzwerkzeitvorgabe einzugebenden Mindestwerts (siehe nachstehende Beschreibung) verwendet. Er kann durch Prüfung des *max. Datenalters* im Consumer-Gerät nach Ausführung der CIP Safety-Netzwerkkommunikation während eines bestimmten Zeitraums angepasst werden.

  Dieser Parameter ermöglicht die Berechnung des Mindestwerts für den Parameter „Netzwerkzeitvorgabe“ wie folgt:

  Min. (Netzwerkzeitvorgabe) = RPI * Timeout-Multiplikator + Max. Netzwerkübertragung

  Bei einer Änderung von Tsafe sollte der Wert dieses Parameters und infolgedessen auch der Mindestwert der *Netzwerkzeitvorgabe* geändert werden.

  Für diesen Parameter gelten folgende Attribute:

  - Mindestwert = 1 ms
  - Höchstwert = 5800 ms
  - Standardwert = 40 + 2*Tsafe

Der Geräte-DTM verwendet diese Ausgangseinstellungen für folgende Berechnungen:

Variable	**Wert**		
	Standard	**Minimum**	**Maximum**
SAFE-Periode (ms)	20	10	255
Eingang Request Packet Interval (ms)	RPI = Tsafe	10	255
Timeout-Multiplikator	2	1	255
Max. Netzwerkübertragung (ms)	40 + 2 * Tsafe	10	5800
Netzwerkzeitvorgabe	Min. Netzwerkzeitvorgabe * 1,5	RPI * Timeout-Multiplikator + Max. Netzwerkübertragung	5800

Sicherheitsgeräte-DTM - E/A-Verbindungseinstellungen

Einführung

Der ohne herstellerspezifische EDS-Datei erstellte CIP Safety-DTM enthält die Registerkarte **Konfigurationseinstellungen** des Verbindungsknotens.

Auf der Registerkarte **Konfigurationseinstellungen** können Sie die Konfiguration der Verbindung zwischen CPU und dezentralem Gerät abschließen.

Parameter

Die Registerkarte **Konfigurationseinstellungen** enthält folgende Parameter:

- **Eingangsinstanz**: Die den Eingangsübertragungen (T -> O) zugeordnete gerätespezifische Baugruppennummer.
- **Ausgangsinstanz**: Die den Ausgangsübertragungen (O -> T) zugeordnete gerätespezifische Baugruppennummer.
- **Konfigurationsinstanz**: Die den Gerätekonfigurationseinstellungen zugeordnete gerätespezifische Baugruppennummer.

IP-Adresseinstellungen der Sicherheitsgeräte

Bearbeiten des M580-CPU-Master-DTM

Die IP-Adresse und die DHCP-Einstellungen für ein CIP Safety-Gerät können im Master-DTM der M580-CPU konfiguriert werden.

HINWEIS: Im Gegensatz zu anderen Verbindungskonfigurationseinstellungen für das Zielgerät wird die IP-Adresse des Geräts nicht im Geräteverbindungs-DTM festgelegt.

Zugriff auf die IP-Adresseinstellungen eines Sicherheitsgeräts

Halten Sie sich an die nachstehend beschriebene Vorgehensweise, um die IP-Adresse und DHCP-Parameter eines CIP Safety-Geräts zu bearbeiten:

Schr-itt	Aktion
1	Trennen Sie Control Expert vom Zielgerät und nehmen Sie die folgenden Änderungen offline vor.
2	Doppelklicken Sie im **DTM-Browser** von Control Expert auf den Master-DTM der M580-CPU (BMEP58_ECPU_EXT), um die zugehörige Konfiguration zu öffnen.
3	Erweitern Sie in der Navigationsstruktur die Geräteliste, um die zugeordneten lokalen Slave-Instanzen anzuzeigen.
4	Wählen Sie das Gerät aus, das dem CIP Safety-Gerät entspricht.
5	Wählen Sie die Registerkarte **Adresseinstellungen** aus.

Konfiguration der IP-Adresseinstellungen eines Sicherheitsgeräts

Bearbeiten Sie auf der Registerkarte **Adresseinstellungen** die folgenden Parameter für das ausgewählte Sicherheitsgerät:

Feld	Parameter	Beschreibung
IP-Konfiguration	**IP-Adresse**	Geben Sie die IP-Adresse für das ausgewählte Gerät ein.
	Subnetzmaske	Die Subnetzmaske des Geräts. **HINWEIS:** Legen Sie die Subnetzmaske so fest, dass sich die IP-Adresse des Geräts im selben Subnetz befindet wie die IP-Hauptadresse des CPU-Ursprungsgeräts.
	Gateway	Die Gateway-Adresse, die zum Erreichen dieses Geräts verwendet wird. Der Standardwert 0.0.0.0 weist darauf hin, dass sich das Gerät in selben Subnetz befindet Ursprungs-CPU.
Adressserver	**DHCP für dieses Gerät**	• **Deaktiviert** (Standard) deaktiviert den DHCP-Client im Gerät. • **Aktiviert** aktiviert den DHCP-Client in diesem Gerät.
	Identifiziert nach	Wählen Sie bei aktiviertem DHCP-Dienst den Typ der Gerätekennung aus: • **MAC-Adresse** • **Gerätename**
	Kennung	Wenn DHCP aktiviert und **Gerätename** ausgewählt ist, geben Sie den Gerätenamen ein.

Weitere Informationen zur Konfiguration der Geräteparameter im Master-DTM der M580-CPU finden Sie in den Parametern der Geräteliste (siehe Modicon M580, Hardware, Referenzhandbuch).

CIP Safety-Betriebsvorgänge

Übersicht

In diesem Abschnitt werden die verschiedenen CIP Safety-Betriebsvorgänge beschrieben.

Übertragung einer CIP Safety-Anwendung von Control Expert in den PAC

Start des Anwendungsdownloads

Verwenden Sie den Befehl **SPS > Projekt zur SPS übertragen**, um den Downloadvorgang zu starten.

Wenn die SPS mit einer bereits vorhandenen Anwendung („alte“ Anwendung) konfiguriert wurde, wird diese beim Downloadstart der neuen Anwendung ungültig. Wenn die alte Anwendung konfigurierte Geräte enthält, trennt der PAC die Verbindung zu diesen Geräten.

Ende des Anwendungsdownloads

Die CIP Safety-Konfiguration wird in den CIP Safety-Stapel der CPU (CSS) geschrieben, der einen Verbindungsparameter-CRC (CPCRC: Connection Parameter CRC) für jede Verbindung berechnet. Im Anschluss daran wird jeder vom CSS berechnete CPCRC mit dem entsprechenden, in der Konfiguration gespeicherten und vom Ziel-DTM berechneten CPCRC verglichen. Wenn:

- die CPCRC-Werte nicht übereinstimmen, weist der CSS die Anwendung zurück und der PAC verbleibt im Zustand NOCONF (keine Konfiguration).
- die CPCRC-Werte übereinstimmen:
  - Die CPCRC- und Verbindungsparameterwerte werden in den entsprechenden Ziel-DDDT, Seite 390 kopiert.
  - Der Parameter CSIO_HEALTH, Seite 397 im CPU-DDDT (T_BMEP58_ECPU_EXT) wird auf 0 gesetzt.
  - Die Funktionsfähigkeitsbits des Geräte-DDDT, Seite 390 des CIP Safety-Zielgeräts werden auf 0 gesetzt.
  - Der PAC stellt über SafetyOpen-Verbindungen vom Typ 2, Seite 381 eine Verbindung zu den konfigurierten Geräten her.

Bei Nichtübereinstimmung der CPCRC-Werte weist der CSS die Anwendung zurück und der PAC verbleibt im Zustand NOCONF (keine Konfiguration).

Neuberechnung der Kennung der Sicherheitsanwendung

Die Kennung der Sicherheitsanwendung (SAId: Safety Application ID) ist eine Signatur des sicheren Teils der Control Expert-Anwendung. Sie wird im Systemwort %SW169, Seite 414 gespeichert. Der CSS berechnet einen CRC für alle CPCRC-Instanzen. Dieser CRC wird zur Berechnung der SAId hinzugefügt. Das bedeutet, dass bei einer Änderung der Konfiguration des CIP Safety-Zielgeräts auch der SAId-Wert geändert wird.

SafetyOpen-Anforderung vom Typ 2

Frame-Struktur der CIP-SafetyOpen-Verbindungen vom Typ 2

Die M580-Standalone-Sicherheits-CPUs unterstützen über SafetyOpen-Verbindungsanforderungen vom Typ 2 eingerichtete CIP Safety-Verbindungen. Die Struktur der Frames zur Verbindungsanforderung wird nachstehend beschrieben:

Parametername		**Beschreibung**
Connection Timeout Multiplier		Vom Consumer einer Verbindung verwendet, um zu ermitteln, ob eine der drei Standardverbindungen das Timeout erreicht hat. Der Timeout-Wert für die Verbindung wird folgendermaßen definiert: Verbindungs-RPI * (CTM+1) * 4
O_to_T RPI		Angefordertes Paketintervall (RPI: Requested Packet Interval) Ursprung zu Ziel
T_to_O RPI		Angefordertes Paketintervall (RPI: Requested Packet Interval) Ziel zu Ursprung
Electronic Key.Vendor ID		Gerätehersteller-ID
Electronic Key.Prod Type		Gerätetyp
Electronic Key.Prod Code		Produktcode des Geräts
Electronic Key.Compatible/Major Rev		Hauptversion
Electronic Key.Minor Rev		Nebenrevision
SCID	Safety Configuration CRC	ID der Sicherheitskonfiguration: Vom SNCT (Safety Network Configuration Tool) bereitgestellt, verwendet bei Inbetriebnahme, Verbindungsaufbau und Geräteaustausch
	Configuration Date	
	Configuration Time	
TUNID	TUNID Date	Target Unique Network Identifier: Identifiziert das Zielgerät in der SafetyOpen-Anforderung.
	TUNID Time	
	Target Node ID	

Parametername		Beschreibung
OUNID	OUNID Date	Originator Unique Network Identifier: Identifiziert das Ursprungsgerät in der SafetyOpen-Anforderung.
	OUNID Time	
	Originator Node ID	
Ping_Interval_EPI_Multiplier		Definiert das Ping-Zählintervall für die Verbindung.
Time_Coord_Msg_Min_Multiplier		Die Mindestanzahl an 128-µs-Inkrementen, die die Übermittlung einer Zeitkoordinationsnachricht vom Consumer zum Producer in Anspruch nehmen kann.
Network_Time_Expectation_Multiplier		Das von einem Consumer zugelasse Höchstalter der Sicherheitsdaten, gemessen in Inkrementen zu je 128 µs.
Timeout_Multiplier		Die Anzahl der Datenproduktionswiederholungen, die in die Gleichung zur Erkennung einer nicht erfolgreichen Verbindung aufzunehmen sind.
Max_Fault_Number		Die Anzahl fehlerhafter Paket, die verworfen werden können, bevor eine Verbindung getrennt wird.
Connection Parameters CRC (CPCRC)		Verbindungsparameter-CRC. Ein CRC-S32 der Zielverbindungsparameter, enthalten in der SafetyOpen-Anforderung vom Typ 2.

Betriebsvorgänge eines CIP Safety-Geräts

Einführung

In diesem Abschnitt werden die verschiedenen Betriebsvorgänge eines CIP Safety-Geräts, einschließlich Erkennung von Systemfehlern und Antwortmechanismen, sowie die Betriebszustände des Geräts beschrieben:

- Selbsttest beim Einschalten
- Antwort bei Erkennung eines nicht behebbaren Fehlers
- Erkennung eines behebbaren Fehlers
- Verwaltung der Funktionsfähigkeit der Zielverbindung
- Run/Idle-Zustand des CIP Safety-Geräts

Selbsttest beim Einschalten des CIP Safety-Ursprungsgeräts und -Zielgeräts

Beim Einschalten sowie bei jedem Laden einer neuen Anwendung führt das CIP Safety-System folgende Vorgänge aus:

- Die CPU überträgt die Konfigurationsparameter an den CIP Safety-Stapel (CSS) in CPU und Kopro.
- Der CSS, sowohl in der CPU als auch im Kopro, überprüft den CPCRC für jede Verbindung.
- Für jede Verbindung vergleicht das CIP Safety-System den heruntergeladenen CPCRC (com Ursprungs-DTM berechnet) mit den von CPU und Kopro berechneten Werten.
- Der CSS sperrt die Ursprungskonfiguration.
- Die Anwendung gibt SafetyOpen-Anforderungen vom Typ 2 für den Aufbau einer Verbindung zu jedem CIP Safety-Gerät aus.
- Jedes CIP Safety-Gerät:
  - berechnet seinen CPCRC und vergleicht ihn mit dem vom Ursprungsgerät empfangenen CPCRC.
  - vergleicht die empfangene SCID mit der intern gespeicherten SCID (Hinweis: Diese Prüfung erfolgt nur bei konfigurierbaren Geräten.).

Der E/A-Austausch zwischen dem Ursprungs- und den Zielgeräten startet erst nach erfolgreichem Abschluss dieser Tests.

HINWEIS: Zusätzlich zu den oben beschriebenen Selbsttests beim Einschalten führt das System alle von der CIP Safety-Norm IEC 61784-3 vorgeschriebenen betriebsbegleitenden Selbsttests durch.

Antwort bei Erkennung eines nicht behebbaren Fehlers

Wenn die CPU oder E/A-Diagnose einen nicht behebbaren Fehler erkennt, wird der betroffene Teil des Systems vom Sicherheitssystem in einen sicheren Zustand gesetzt. Der betroffene Systemteil wird heruntergefahren und in einen spannungsfreien Zustand gesetzt, die Sicherheitseingänge werden auf 0 gesetzt. Alle betroffenen Sicherheitsausgänge werden in den für sie konfigurierten Fehlerausweichzustand gesetzt.

Antwort bei Erkennung eines behebbaren Fehlers

Behebbare Fehlern sind in der Regel Ereignisse wie der Verlust einer Modulverbindung usw. Diese Fehler werden im Funktionsfähigkeitsbit des Geräte-DDDT (T_CIP_SAFETY_IO, Seite 390) signalisiert, der den logischen AND-Wert der Funktionsfähigkeitsbits Status_IN und Status_OUT enthält. Wenn ein behebbarer Fehler für einen Eingang erkannt wird, wird der betreffende Eingang in den sicheren Zustand forciert und auf 0 gesetzt.

Verwaltung der Funktionsfähigkeit der Zielverbindung

Die Funktionsfähigkeit einer Verbindung zum CIP Safety-Zielgerät wird im Funktionsfähigkeitsbit der Parameter Status_IN und Status_OUT signalisiert, wie im Datentyp T_CIP_SAFETY_STATUS, Seite 391 beschrieben. Die Funktionsfähigkeit des Ziels kann 'Öffen' und 'Betriebsbereit' sein, oder es wird ein Fehler erkannt.

Für Eingänge wird der Verbindungszustand vom Sicherheitsvalidierer des Servers bereitgestellt, für Ausgänge vom Sicherheitsvalidierer des Clients.

Run/Idle-Zustand

Der Betriebszustand eines CIP Safety-Geräts - im Run- oder Idle-Zustand - wird im Bit Run_Idle des Parameters Status_IN oder Status_OUT signalisiert, wie im Datentyp T_CIP_SAFETY_STATUS, Seite 391 beschrieben.

Für ein Eingangsgerät:

Wenn eine Verbindung zu einem Eingangsmodul hergestellt wird, wird das Bit Run_Idle vom Producer (Eingang) bis zum erfolgreichen Abschluss der Sequenz zur erstmaligen Zeitkoordination auf 'Idle' (0) gesetzt. Anschließend kann das Bit den Wert 1 (Run-Zustand) oder 0 (Idle-Zustand) annehmen. Wenn das Bit Run_Idle bit auf 0 gesetzt wird (Idle-Zustand), werden die Eingangsdatenwerte auf 0 forciert (sicherer Zustand).

Für ein Ausgangsgerät:

Das Bit Run_Idle der Ausgänge wird vom Ursprung (CPU) auf 1 gesetzt, wenn sich der PAC im Run-Zustand befindet und die Sequenz zur erstmaligen Zeitkoordination erfolgreich abgeschlossen wurde. Das Run/Idle-Bit der Ausgänge wird vom Ursprung (CPU) auf 0 gesetzt, wenn sich der PAC im Stop- oder Halt-Zustand befindet, die Sequenz zur erstmaligen Zeitkoordination nicht erfolgreich abgeschlossen oder die Verbindung getrennt wurde. Wenn das Bit Run_Idle auf 0 gesetzt wird (Idle-Zustand), wird erwartet, das das Ausgangsgerät seine Ausgänge in ihren Fehlerausweichzustand setzt.

Interaktionen zwischen Betriebsvorgängen des Sicherheits-PAC und der Zielverbindung

Einführung

In diesem Abschnitt werden die Interaktionen zwischen den folgenden Zuständen/Betriebsvorgängen des CPU-Sicherheitsursprungsgeräts und der Verbindung zum Zielgerät beschrieben:

- Systemreaktionszeit

- Run-Zustand
- Stop/Halt-Zustand
- Aus- und Wiedereinschalten / Neustart
- Safety-Init-Befehl
- Wartungsmodus
- CCOTF
- Anschließen / Trennen / Auswechseln eines Geräts

Systemreaktionszeit

Die von der CIP-Safety-Kommunikation beanspruchte Zeit - als *Netzwerkzeitvorgabe* bezeichnet - wird der *Systemreaktionszeit* des M580-Sicherheitssystems als fester Bestandteil hinzugefügt. Weitere Informationen finden Sie im Abschnitt zu den *Auswirkungen der CIP-Safety-Kommunikation auf die Reaktionszeit des Sicherheitssystems*.

Run-Zustand

Wenn sich das CIP-Safety-System im Run-Zustand befindet:

- Die Funktionsfähigkeitsbits des Kommunikations-DDDT, Seite 390 des CIP-Safety-Geräts werden zu Beginn des SAFE-Taskzyklus aktualisiert.
- Die Eingangswerte werden zu Beginn des SAFE-Taskzyklus auf der Grundlage des zuletzt empfangenen Werts aktualisiert.
- Die Ausgangswerte werden nach der Ausführung des SAFE-Taskprogramms aktualisiert und übertragen.
- Das Bit Run_Idle für die Ausgänge im Kommunikations-DDDT des CIP-Safety-Geräts wird auf 1 gesetzt.
- Die Funktionsfähigkeitsbits des Kommunikations-DDDT des CIP-Safety-Geräts werden aktualisiert.

Stop-Zustand

Wenn die SAFE-Task in den Stop-Zustand wechselt, beispielsweise wenn die SAFE-Task gestoppt wird oder einen Haltepunkt erreicht:

- Die Verbindung Ursprung - Ziel bleibt aktiv.
- Zwischen der CPU und dem CIP-Safety-Gerät werden Daten ausgetauscht.

- Die Funktionsfähigkeitsbits des Kommunikations-DDDT, Seite 390 des CIP-Safety-Geräts werden weiterhin aktualisiert.
- Das Bit Run_Idle der Ausgänge im Kommunikations-DDDT des CIP-Safety-Geräts wird auf 0 gesetzt und die Ausgangsgeräte wenden ihre konfigurierte Fehlerausweicheinstellung an.

Halt-Zustand

Im Halt-Zustand werden die Ausgangswerte nicht von der CPU an das CIP-Safety-Gerät gesendet und die Funktionsfähigkeitsbits des CIP-Safety-Geräts werden auf 0 gesetzt.

Aus- und Wiedereinschalten oder Zurücksetzen

Beim Aus- und Wiedereinschalten oder bei einem Reset:

- Der Sicherheitsteil der Anwendung führt einen Kaltstart, Seite 278 durch.
- Der PAC führt dieselbe Betriebssequenz aus wie bei einem Anwendungsdownload, Seite 380.

Safety-Init-Befehl

Bei Ausführung des Befehls **SPS > Safety init.** in Control Expert werden die Werte des Kommunikations-DDDT, Seite 390 des CIP-Safety-Geräts durch Setzen auf die zugehörigen, werkseitig vordefinierten Standardwerte initialisiert.

Wartungsmodus

Der Betrieb der M580-Sicherheits-CPU im Wartungsmodus, Seite 265 hat keine Auswirkungen auf den Betrieb des CIP-Safety-Geräts. Die CPU vergleicht weiterhin die separat von der CPU und vom Kopro durchgeführten Berechnungen. Allerdings wird kein zusätzlicher Vergleich mit den Werten im Ziel-DDDT vorgenommen. Aus diesem Grund wird der PAC-Betrieb im Wartungsmodus als nicht sicher eingestuft.

CCOTF

Die CCOTF-Funktion (Change Configuration On The Fly) wird von CIP-Safety-Geräten nicht unterstützt. Da ein CIP-Safety-Gerät seine Konfigurationseinstellungen von einem herstellerspezifischen Tool zur Sicherheitsnetzwerkkonfiguration (SNCT: Safety Network

Configuration Tool) - und nicht von der Ursprungs-CPU - erhält, können an den Geräteeinstellungen keine Änderungen über die CPU vorgenommen werden.

Anschließen / Trennen / Auswechseln eines CIP-Safety-Geräts

Standardmäßig werden beim Anwendungsstart oder bei der Ausführung des Befehls **SPS > Safety init.** die Bits CTRL_IN und CTRL_OUT im DDDT, Seite 390 auf 'Aktiviert' (1) gesetzt. Wenn ein Gerät mit einem PAC im Stop- oder Run-Zustand verbunden wird und das Bit CTRL_IN oder CTRL_OUT des Geräts auf 'Aktiviert' (1) gesetzt ist, initialisiert das Gerät automatisch den Datenaustausch.

HINWEIS: Da die Bits CTRL_IN und CTRL_OUT beim Aus- und Wiedereinschalten auf 'Aktiviert' gesetzt werden, müssen Sie angemessene Maßnahmen in der SAFE-Taskanwendung ergreifen, um bei diesem Vorgang einen unerwarteten Betrieb zu vermeiden.

⚠WARNUNG

GEFAHR DES UNBEABSICHTIGTEN GERÄTEBETRIEBS

Setzen Sie die Bits CTRL_IN und CTRL_OUT nicht als Sicherheitsfunktion ein, um die Zieldaten in einen sicheren Zustand zu setzen.

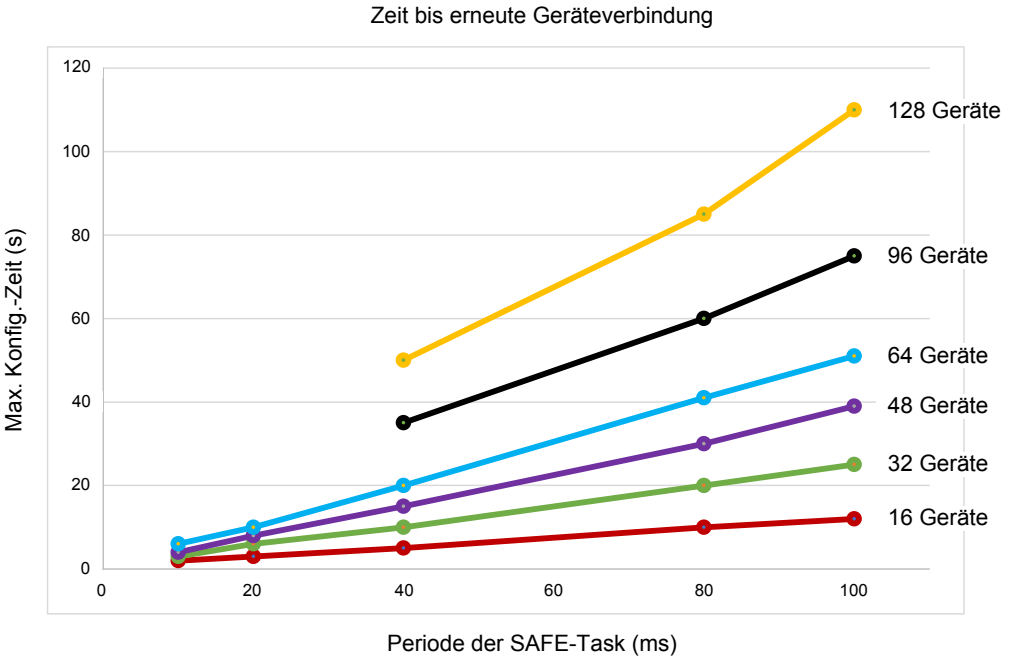
Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Wenn der PAC einen Fehler erkennt, der das Trennen einer Geräteverbindung erforderlich macht, setzt er das entsprechende Bit CTRL_IN oder CTRL_OUT auf 'Deaktiviert' (0). Das Geräte verbleibt im deaktivierten Zustand und wechselt nur in den Zustand 'Aktiviert' (1), wenn der Übergang beabsichtigt ist. Wenn beispielsweise der Fehler behoben und eine Anforderung zum erneuten Aufbau einer Verbindung ausgegeben wird.

Sie können eine Anforderung zum erneuten Verbindungsaufbau ausgeben, indem Sie das entsprechende Steuerungsbit (CTRL_IN oder CTRL_OUT) (1) im DDDT von 'Deaktiviert' (0) auf 'Aktiviert' setzen.

Beim Wiederaufbau der Verbindung zu einem Gerät ist die dafür benötigte Zeit von der Periode der SAFE-Task und der Anzahl der zu verbindenden Geräte abhängig:

- Für ein einzelnes Gerät mit einer SAFE-Taskperiode unter 100 ms dauert der Verbindungswiederaufbau voraussichtlich weniger als 2 Sekunden.
- Für mehrere Geräte finden Sie die voraussichtliche Dauer des Verbindungswiederaufbaus in der nachstehenden Tabelle.



Der CIP-Safety-PAC verwaltet den Geräteaustausch genau wie das Trennen und Wiederverbinden eines Geräts. Die Vorgänge zur Neukonfiguration des neuen Geräts mit denselben Einstellungen wie das ausgewechselte Gerät erfolgen lokal im Gerät und betreffen den PAC nicht.

Befehle des CIP Safety-DTM

Einführung

Der CIP Safety-DTM umfasst die Registerkarte **Sicherheit**, auf der folgende Befehle zur Verfügung stehen:

- **Eigentümer ZURÜCKSETZEN**
- **Platzieren TUNID**

Der Zugriff auf diese Befehle erfolgt durch die Auswahl einer Verbindung in der DTM-Navigationsstruktur. Sie sind nur aktiviert, wenn der DTM mit dem online betriebenen CIP Safety-Gerät verbunden ist.

Eigentümer ZURÜCKSETZEN

Über den Befehl **Eigentümer ZURÜCKSETZEN** können Sie die Konfigurationseinstellungen des CIP Safety-Geräts auf die werkseitig voreingestellten Standardwerte zurücksetzen. Das Zurücksetzen ist nur in folgenden Fällen möglich:

- Der Befehl wird von der Ursprungs-CPU ausgeführt, die anhand der im Gerät gespeicherten OUNID identifiziert wird.
- Die Modulkonfigurationseinstellungen sind nicht gesperrt.

Nach dem Zurücksetzen verfügt das Modul über keinen Eigentümer und kann von einem anderen Ursprungsgerät konfiguriert werden.

HINWEIS: Wenn der Befehl zum Zurücksetzen auf ein Modul mit aktiven Verbindungen angewendet wird, bleibt er ohne Wirkung.

Platzieren TUNID

Über den Befehl **Platzieren TUNID** können Sie die Netzwerk-Sicherheitsnummer (SNN: Safety Network Number) im CIP Safety-Zielgerät festlegen. Bei Ausführung des Befehls wird die in der DTM-Konfiguration des CIP Safety-Geräts gespeicherte Netzwerk-Sicherheitsnummer, Seite 372 (SNN) in das Zielgerät übertragen, wodurch eine ggf. bereits vorhandene SNN im Gerät ersetzt wird.

HINWEIS: Vor der Befehlsausführung müssen Sie sicherstellen, dass Sie das richtige Gerät für den Empfang der zu übertragenden SNN identifiziert haben.

CIP Safety-Diagnose

Übersicht

In diesem Abschnitt werden die Diagnosetools für das CIP Safety-Gerät und die CIP Safety-Verbindung zwischen dem Gerät und der M580-Standalone-Sicherheits-CPU beschrieben.

CIP Safety-Geräte-DDDT

T_CIP_SAFETY_IO DDDT

Jede CIP Safety-Geräteinstanz wird vom T_CIP_SAFETY_IO-DDDT beschrieben, der folgende Parameter umfasst:

Parameter	Datentyp	Beschreibung
Health	BOOL	Globale Funktionsfähigkeit = Logisches AND von: • Status_IN.Health • Status_OUT.Health Für eine Beschreibung dieser Funktionsfähigkeitsbits siehe den Datentyp T_CIP_SAFETY_STATUS, Seite 391.
Status_IN	T_CIP_SAFETY_STATUS	Eingangsstatus
Status_OUT	T_CIP_SAFETY_STATUS	Ausgangsstatus
CTRL_IN	BOOL	Eingangsverbindung aktivieren/deaktivieren
CTRL_OUT	BOOL	Ausgangsverbindung aktivieren/deaktivieren
Conf_In	T_CIP_SAFETY_CONF	CIP-Signaturen und -Parameter für Eingangsverbindung
Conf_Out	T_CIP_SAFETY_CONF	CIP-Signaturen und -Parameter für Ausgangsverbindung
Eingang	Array[0...n] of BYTE	Eingangswerte, Größe vom Gerätetyp abhängig. Modul um 4 Byte ausgerichtet an der im DTM konfigurierten Größe.
Ausgang	Array[0...m] of BYTE	Ausgangswerte, Größe vom Gerätetyp abhängig. Modul um 4 Byte ausgerichtet an der im DTM konfigurierten Größe.

Die oben referenzierten CIP Safety-Datentypen werden nachstehend beschrieben.

T_CIP_SAFETY_STATUS

Der Datentyp T_CIP_SAFETY_SATATUS umfasst folgende Parameter:

Parameter	Datentyp	Beschreibung
Health	BOOL	Eingangs- oder Ausgangsfunktionsfähigkeit: • Für Eingang: ◦ 1: Eingangskommunikation aktiv und betriebsbereit ◦ 0: Fehler bzg. Eingangskommunikation vom Sicherheitsvalidierer des Servers erkannt • Für Ausgang: ◦ 1: Ausgangskommunikation aktiv und betriebsbereit ◦ 0: Fehler bzg. Ausgangskommunikation vom Sicherheitsvalidierer des Clients erkannt
Run_Idle	BOOL	Zustand der Ein- oder Ausgänge des CIP Safety-Geräts: • Für Eingänge vom Producer (Eingang) gesetzt auf: ◦ 1: wenn Eingang in Run-Zustand ◦ 0: wenn Eingang im Idle-Zustand oder bis erfolgreicher Abschluss der Sequenz zur erstmaligen Zeitkoordination • Für Ausgänge vom Usprung (CPU) gesetzt: ◦ 1: wenn PAC in Run-Zustand, nach erfolgreichem Abschluss der Sequenz zur erstmaligen Zeitkoordination ◦ 0: wenn PAC in Stop- oder Halt-Zustand, bei getrennter Verbindung oder bei nicht erfolgreichem Abschluss der Sequenz zur erstmaligen Zeitkoordination
Error_Code	WORD	Siehe die Liste der Fehlercodes, Seite 393
Error_Sub_Code	WORD	Siehe die Liste der Fehleruntercodes, Seite 394

T_CIP_SAFETY_CONF

Der Datentyp T_CIP_SAFETY_CONF umfasst folgende, in der SafetyOpen-Anforderung vom Typ 2, Seite 381 übergebene Parameter:

Parameter	Datentyp	Beschreibung
TO_MULTIPLIER	BYTE	Timeout-Multiplikator. Vom Consumer einer Verbindung verwendet, um zu ermitteln, ob eine der drei Standardverbindungen das Timeout erreicht hat. Der Timeout-Wert für die Verbindung wird folgendermaßen definiert: Verbindungs-RPI * (CTM+1) * 4
Output_RPI	UDINT	Angefordertes Paketintervall der O->T-Verbindung (Ursprung -> Ziel)
Input_RPI	UDINT	Angefordertes Paketintervall der T->U-Verbindung (Ziel -> Ursprung)
Device_Vendor_ID	UINT	Herstellerspezifische ODVA-Kennung
Device_Type	UINT	ODVA-Gruppierung, der das Gerät angehört.
Device_Product_Code	UINT	Zugewiesener ODVA-Produktcode
Major_Revision	BYTE	Hauptrevisionsnummer der Gerätefirmware
Minor_Revision	BYTE	Nebenrevisionsnummer der Gerätefirmware
Configuration_Assembly_Nb	UINT	Mit den Konfigurationseinstellungen des Geräts verknüpfte gerätespezifische Baugruppennummer
Output_Assembly_Nb	UINT	Mit den Ausgangsübertragungen (O -> T) verknüpfte gerätespezifische Baugruppennummer
Input_Assembly_Nb	UINT	Mit den Eingangsübertragungen (T -> O) verknüpfte gerätespezifische Baugruppennummer
SC_CRC	UDINT	Sicherheitskonfigurations-CRC. Ein CRC-Wert (Cyclic Redundancy Check) der CIP Safety-Gerätekonfiguration.
Configuration_Date	UINT	Monat, Tag und Jahr der Konfigurationsgenerierung
Configuration_Time	UDINT	Stunde, Minute, Sekunde und Millisekunde der Konfigurationsgenerierung
TUNID_Time	UDINT	Monat, Tag und Jahr der TUNID-Generierung (Target Unique Network Identifier)
TUNID_Date	UINT	Stunde, Minute, Sekunde und Millisekunde der TUNID-Generierung (Target Unique Network Identifier)
TUNID_NodeID	UDINT	Eindeutige Netzwerkkennung für das Zielgerät
OUNID_Time	UDINT	Monat, Tag und Jahr der OUNID-Generierung (Originator Unique Network Identifier)
OUNID_Date	UINT	Stunde, Minute, Sekunde und Millisekunde der OUNID-Generierung (Originator Unique Network Identifier)
OUNID_NodeID	UDINT	Eindeutige Netzwerkkennung für das Ursprungsgerät
Ping_Interval_EPI_Multiplier	UINT	Definiert das Ping-Zählintervall für die Verbindung.

Parameter	Datentyp	Beschreibung
Time_Coordination_Msg_Min_Mult	UINT	Die Mindestanzahl an 128-µs-Inkrementen, die die Übermittlung einer Zeitkoordinationsnachricht vom Consumer zum Producer in Anspruch nehmen kann.
Network_Time_Expectation_Mult	UINT	Das von einem Consumer zugelasse Höchstalter der Sicherheitsdaten, gemessen in Inkrementen zu je 128 µs.
Timeout_Multiplier	BYTE	Die Anzahl der Datenproduktionswiederholungen, die in die Gleichung zur Erkennung einer nicht erfolgreichen Verbindung aufzunehmen sind.
Max_Fault_Number	UDINT	Die Anzahl fehlerhafter Paket, die verworfen werden können, bevor eine Verbindung getrennt wird.
CPCRC	UDINT	Verbindungsparameter-CRC (Connection Parameters CRC). Ein CRC-S32 der Zielverbindungsparameter, enthalten in der SafetyOpen-Anforderung vom Typ 2.

Fehlercodes des CIP Safety-Geräts

Fehlercodes

Die folgenden Fehlercodes und Fehleruntercodes beziehen sich auf den Datentyp T_CIP_SAFETY_STATUS und sind in den Parametern Status_IN und Status_OUT des CIP Safety-Geräte-DDDT enthalten.

Fehlercodes

Fehlercode	Bedeutung
0001	Aktive Verbindung: Keine Antwort
0002	Aktive Verbindung: Fehlerantwort von Gerät
0003	Aktive Verbindung: Ungültige Antwort von Gerät
0004	Server (Consumer) nicht betriebsbereit
0005	Client (Producer) nicht betriebsbereit

Fehleruntercodes

HINWEIS: Alle Fehleruntercodes, die nachstehend nicht aufgeführt sind, sind einem internen Gebrauch durch Schneider Electric vorbehalten. Geben Sie in diesem Fall den Fehleruntercode an den Kundensupport von Schneider Electric weiter.

Fehleruntercodes für aktive Verbindungen:

Fehleruntercode (hex.)	Bedeutung
0100	Verbindung wird verwendet oder doppelter Forward_Open
0103	Transportklasse und Trigger-Kombination nicht unterstützt
0105	Konfiguration bereits von einem anderen Ursprungsgerät verwendet
0106	Ausgang bereits von einem anderen Ursprungsgerät verwendet
0107	Zielverbindung nicht gefunden (Forward_Close)
0108	Ungültiger Netzwerkverbindungsparameter
0109	Ungültige Verbindungsgröße
0110	Gerät nicht konfiguriert
0111	O->T RPI, T->O RPI oder Zeitkorrektur-RPI nicht unterstützt
0113	Alle Sicherheitsvalidator-Instanzen bereits verwendet
0114	Im elektronischen Schlüssel angegebene Gerätehersteller-ID bzw. der Geräteproduktcode nicht identisch
0115	Im elektronischen Schlüssel angegebener Gerätetyp nicht identisch
0116	Im elektronischen Schlüssel angegebene Haupt- oder Nebenrevision nicht identisch
0117	Ungültiger Producer- oder Consumer-Anwendungspfad
0118	Ungültiger oder inkohärenter Anwendungspfad der Konfiguration
011 A	Zielobjekt hat keine Verbindungen mehr
011B	RPI ist kleiner als die Produktionssperrzeit
011C	Transportklasse nicht unterstützt
011D	Produktionstrigger nicht unterstützt
011E	Richtung nicht unterstützt
0123	Ungültiger Typ der Netzwerkverbindung Ursprung zu Ziel
0124	Ungültiger Typ der Netzwerkverbindung Ziel zu Ursprung
0126	Ungültige Konfigurationsgröße
0127	Ungültige Größe Ursprung zu Ziel

Fehleruntercode (hex.)	Bedeutung
0128	Ungültige Größe Ziel zu Ursprung
0129	Ungültiger Anwendungspfad der Konfiguration
012 A	Ungültiger Consumer-Anwendungspfad
012B	Ungültiger Producer-Anwendungspfad
012C	Konfigurationssymbol existiert nicht
012D	Consumer-Symbol existiert nicht
012E	Producer-Symbol existiert nicht
012F	Inkohärente Anwendungspfadkombination
0130	Inkohärentes Consumer-Datenformat
0131	Inkohärentes Producer-Datenformat
0203	Timeout der Verbindung
0204	Ziel antwortet nicht auf nicht-verbundene Anforderung
0205	Parameterfehler in SafetyOpen-Anforderung
0207	Nicht-verbundene Quittierung ohne Antwort
0315	Ungültiger Segmenttyp in Verbindungspfad
031B	Modulverbindung bereits hergestellt
031C	Kein anderer erweiterter Statuscode zutreffend
031F	Keine vom Benutzer konfigurierbaren Consumer-Ressourcen mehr im Producer-Modul verfügbar
0801	EIP-Multiplikator für Ping-Intervall bzw. max. Consumer-Anzahl ungültig oder Multicast-Verbindung
0802	Ungültige Größe der Sicherheitsverbindung
0803	Ungültiges Format der Sicherheitsverbindung
0804	Ungültige Parameter der Zeitkorrektur-Verbindung
0805	EIP-Multiplikator für Ping-Intervall ungültig
0806	Multiplikator für min. Zeitkoordinationsnachrichten ungültig
0807	Multiplikator für Netzwerkzeitvorgabe ungültig
0808	Ungültiger Timeout-Multiplikator
0809	Max. Consumer-Anzahl ungültig
080 A	CPCRC ungültig

Fehleruntercode (hex.)	Bedeutung
080B	ID der Zeitkorrektur-Verbindung ungültig
080C	SCID nicht identisch
080D	TUNID nicht festgelegt
080E	TUNID nicht identisch
080F	Konfigurationsvorgang nicht zulässig

Fehleruntercodes für Server oder Client:

Fehleruntercode (hex.)	Bedeutung
271D	Zeitkorrekturnachricht mit nicht gesetztem Bit Ping_Response empfangen
2730	Zeitkoordinationsnachricht: Nicht in zugewiesenem Zeitraum empfangen
2732	Prüfung der Zeitkoordinationsnachricht: Bereits Nachricht mit gleichem Zeitstempel von diesem Consumer empfangen
2733	Prüfung der Zeitkoordinationsnachricht: Fehler bei Paritätsprüfung
2734	Prüfung der Zeitkoordinationsnachricht: Fehler bei Prüfung von Quittierungsbyte 2
2735	Prüfung der Zeitkoordinationsnachricht: Nicht innerhalb des vorgegebenen 5-Sekunden-Zeitraums (ungefähr) empfangen
2736	Prüfung der Zeitkoordinationsnachricht: Nicht innerhalb desselben oder des nächsten Ping-Intervalls empfangen
2738	Prüfung der Zeitkoordinationsnachricht: CRC nicht identisch
2820	Zeitstempel-CRC nicht identisch
2821	Zeitstempel-Delta null
2822	Zeitstempel-Delta größer als Netzwerkzeitvorgabe
2823	Datenalter einer fehlerhaften Nachricht größer als Netzwerkzeitvorgabe
2824	Datenalter einer in anderer Hinsicht gültigen Nachricht größer als Netzwerkzeitvorgabe
2825	Tatsächlicher Daten-CRC nicht identisch
2826	Komplementärer Daten-CRC nicht identisch
282E	Tatsächlicher Daten-CRC nicht identisch (kein Trennen der Verbindung)
282F	Komplementärer Daten-CRC nicht identisch (kein Trennen der Verbindung)
2832	Timeout der Consumer-Aktivitätsüberwachung

DDDT der CIP-Safety-Standalone-CPU

CIP-Safety-Zusätze zum T_BMEP58_ECPU_EXT

Der DDDT M580 der Standalone-Sicherheits-CPU (T_BMEP58_ECPU_EXT) enthält zwei CIP-Safety-Variablen:

- CSIO_SCANNER: Status des Steuerungsbits des CIP-Safety-E/A-Abfragegeräts. Dieses boolesche Feld kann folgende Werte annehmen:
  - 1: Dienst läuft im Normalbetrieb.
  - 0: Dienst läuft nicht im Normalbetrieb.

Weitere Informationen finden Sie in der Liste der Eingangsparameter (siehe Modicon M580, Hardware, Referenzhandbuch) des SERVER_STATUS2-DDDT.

- CSIO_HEALTH: Funktionsfähigkeit der verbundenen CIP-Safety-Geräte. Diese Variable ist ein Array aus 128 booleschen Werten, wobei jedes Bit auf die Funktionsfähigkeit eines einzelnen verbundenen Geräts verweist:
  - 1: Dienst läuft im Normalbetrieb.
  - 0: Dienst läuft nicht im Normalbetrieb.

Weitere Informationen finden Sie unter Geräteintegritätsstatus (siehe Modicon M580, Hardware, Referenzhandbuch).

Diagnose des CPU-DTM

Diagnose über den DTM der M580-CPU

Der M580-CPU-DTM stellt folgende Diagnosedienste bereit:

- Geräteerkennung
- Funktionsfähigkeit der CIP-Safety-E/A-Geräte

CIP-Safety-Geräteerkennung

Wenn Control Expert online ausgeführt wird, können Sie den zugehörigen Dienst zur Feldbuserkennung heranziehen, um die CIP-Safety-Geräte auf erster Ebene in Ihrem Netzwerk zu erkennen, d. h. diejenigen Geräte, die direkt mit der CPU verbunden sind. Nur Geräte mit einem DTM, der einem im **DTM-Katalog** des Host-PC registrierten DTM entspricht, können erkannt werden.

Die Geräteerkennung erfolgt durch einen Rechtskick auf den DTM der CPU (BMEP58_ECPU_EXT) im **DTM-Browser** und durch anschließende Auswahl von **Feldbus-**

Erkennung, um ein Dialogfeld desselben Namens zu öffnen, in dem die erkannten Geräte angezeigt werden. Mithilfe der Tools in diesem Dialogfeld können Sie Geräte-DTMs zu Ihrem Projekt hinzufügen. Die von Ihnen hinzugefügten Geräte werden unter der CPU im **DTM-Browser** und in der Navigationsstruktur des CPU-DTM angezeigt.

Weitere Informationen zur Verwendung dieses Dienstes finden Sie unter Dienst zur Feldbuserkennung (siehe ™EcoStruxure Control Expert, Betriebsarten).

Funktionsfähigkeit der CIP-Safety-Geräteverbindung

Wenn Control Expert online ausgeführt wird, wird in der Navigationsstruktur des CPU-DTM ein Symbol angezeigt, das auf die Funktionsfähigkeit jeder Verbindung für die im Projekt hinzugefügten CIP-Safety-E/A-Geräte verweist:

-  gibt an, dass sich die Verbindung im RUN-Zustand befindet.
-  gibt an, dass sich die Verbindung im STOP-Zustand befindet, getrennt wurde oder unbekannt ist.

Weitere Informationen zur Verwendung dieser Funktion finden Sie unter Einführung der Diagnosefunktion im Control Expert-DTM (siehe Modicon M580, Hardware, Referenzhandbuch).

Verbindungsdiagnose für CIP Safety-Geräte

Einführung

Die Verbindungsknoten eines CIP Safety-DTM umfassen zwei Registerkarten, auf denen Sie die Geräteverbindung identifizieren und diagnostizieren können:

- Modulinformationen
- Statusinformationen

Registerkarte „Modulinformationen“

Der CIP Safety-DTM stellt die Registerkarte **Modulinformationen** mit statischen Werten für die folgenden Parameter zur Modulidentifikation bereit:

- Hersteller-ID
- Produkttyp
- Produktcode
- Softwarerevision

- Seriennummer
- Produktname
- MAC-Adresse

Registerkarte „Statusinformationen“

Der CIP Safety-DTM stellt die Registerkarte **Statusinformationen** mit dynamischen Werten für die Verbindung CPU zu CIP Safety-Gerät bereit:

Status	Beschreibung
CIP Safety-Status	Der aktuelle Status des Geräts, gemäß der Definition im Abschnitt 5-4.2.1.5 zum Gerätestatus in der CIP Safety-Norm: • 0: Nicht definiert • 1: Selbsttest • 2: Leerlauf • 3: Selbsttest-Ausnahme • 4: Betrieb • 5: Abbruch • 6: Kritischer Fehler • 7: Konfiguration • 8: Warten auf TUNID • 9 bis 50: Reserviert • 51: Warten auf TUNID mit zulässigem Drehmoment Siehe HINWEIS • 52: Betrieb mit zulässigem Drehmoment Siehe HINWEIS • 53 bis 99: Gerätespezifisch • 100 bis 255: Herstellerspezifisch **HINWEIS:** Nur in den Profilen von Sicherheitsbewegungsgeräten zulässig und definiert: 0x2E 0x2F.
Ausnahmestatus	Ein einzelnes Byteattribut, desesn Wert auf den Status der Alarme und Warnungen für das Gerät verweist. Es kann mit einer Basis- oder erweiterten Methode bereitgestellt werden. Detaillierte Informationen finden Sie im Abschnitt 5-4.2.1.6 zum Ausnahmestatus in der CIP Safety-Norm.
Schwerwiegender Fehler	Gerätespezifischer Zustand. Detaillierte Informationen finden Sie im Gerätehandbuch.
Geringfügiger Fehler	Gerätespezifischer Zustand. Detaillierte Informationen finden Sie im Gerätehandbuch.
IP-Adresse	IP-Adresse des CIP Safety-Geräts, festgelegt im M580 CPU-DTM, Seite 378.
TUNID	(Target Unique Network Identifier) Eindeutige Netzwerkkennung des Zielgeräts
OUNID	(Originator Unique Network Identifier, Seite 362) Eindeutige Netzwerkkennung des Ursprungsgeräts

Status	Beschreibung
Sperrstatus	Status der Gerätekonfiguration gemäß der Definition durch ein Tool zur Sicherheitsnetzwerkkonfiguration (SNCT: Safety Network Configuration Tool). • Gesperrt: Konfiguration schreibgeschützt • Freigegeben: Lese-/Schreibzugriff auf die Konfiguration möglich
Konfigurationssignatur	Sicherheitskonfigurationskennung der Verbindung zum Zielgerät (SCID, Seite 373: Safety Configuration Identifier).

Anhang

Inhalt dieses Abschnitts

Einführung

Der Anhang enthält Informationen zur Norm IEC 61508 und zur zugehörigen SIL-Richtlinie. Des Weiteren werden technische Daten für sicherheitsbezogene und nicht störende Module bereitgestellt und Beispielberechnungen durchgeführt.

IEC 61508

Inhalt dieses Kapitels

Einführung

Dieses Kapitel enthält Informationen zu den Sicherheitskonzepten nach IEC 61508 im Allgemeinen sowie zu den entsprechenden SIL-Richtlinien im Besonderen.

Allgemeine Informationen zur Norm IEC 61508

Einführung

Sicherheitsbezogene Systeme, die für eine Verwendung in Prozessen entwickelt wurden und keinerlei Gefahr für Menschen, Umwelt, Geräte und Produktion mit sich bringen, müssen auf einem akzeptablen Niveau gehalten werden. Die Gefahr ist von Schweregrad und Wahrscheinlichkeit abhängig und gibt dementsprechend die erforderlichen Schutzmaßnahmen vor.

In Bezug auf die Sicherheit der Prozesse sind 2 Seiten zu berücksichtigen:

- Die von den amtlichen Behörden vorgegebenen Vorschriften und Anforderungen zum Schutz von Menschen, Umwelt, Geräten und Produkten
- Die Maßnahmen zur Erfüllung der Vorschriften und Anforderungen

Beschreibung der Norm IEC 61508

Der technische Standard, der die Anforderungen an sicherheitsbezogene Systeme definiert:

- IEC 61508

Der Standard behandelt die funktionale Sicherheits elektrischer, elektronischer oder programmierbarer elektronischer sicherheitsbezogener Systeme. Ein sicherheitsbezogenes System ist ein System, das ein oder mehrere spezifische Funktionen ausführen muss, um die Risiken auf einem akzeptablen Niveau zu halten. Diese Funktionen werden als Sicherheitsfunktionen definiert. Ein System wird als funktional sicher definiert, wenn zufällige und systematische Ausfälle sowie Ausfälle mit einer gemeinsamen Ursache nicht zu einer Fehlfunktion des Systems führen und keine Verletzungen oder gar den Tod von Menschen, Emissionen in die Umwelt oder den Verlust von Ausrüstungsgegenständen oder der Produktion zur Folge haben.

Der Standard definiert ein allgemeines Konzept für alle Aktivitäten während des Lebenszyklus von Systemen, die Sicherheitsfunktionen gewährleisten. Er stellt Verfahren für die Gestaltung, Entwicklung und Validierung der Hardware und der Software in sicherheitsbezogenen Systemen bereit. Darüber hinaus werden Regeln sowohl für die Vewaltung der funktionalen Sicherheit als auch für die Dokumentation festgelegt.

Beschreibung der Norm IEC 61511

Die Anforderungen an die funktionale Sicherheit nach IEC 61508 werden im Detail speziell für den Sektor der Prozessindustrie im folgenden technischen Standard vorgegeben:

- IEC 61511: Funktionale Sicherheit: Sicherheitstechnische Systeme für die Prozessindustrie

Dieser Standard unterstützt den Benutzer bei der Anwendung eines sicherheitsbezogenen Systems von der Anfangsphase des Projekts über den Systemanlauf bis hin zu Änderungen und zur letztendlichen Außerbetriebnahme. Im Großen und Ganzen definiert der Standard den Sicherheitslebenszyklus aller Komponenten eines sicherheitsbezogenen Systems in der Prozessindustrie.

Beschreibung der Risiken

IEC 61508 basiert auf den Konzepten der Risikoanalyse und Sicherheitsfunktion. Das Risiko ist von Schweregrad und Wahrscheinlichkeit abhängig. Es kann durch Anwendung einer Sicherheitsfunktion, bestehend aus einem elektrischen, elektronischen oder programmierbaren elektronischen System, auf ein tolerierbares Niveau reduziert werden. Des Weiteren sollte das Risiko auf ein angemessen niedriges, praktisch durchführbares Niveau reduziert werden.

Zusammenfassend gibt IEC 61508 folgende risikobezogene Angaben vor:

- Ein Nullrisiko kann nicht erreicht werden.
- Sicherheit ist von Anfang von grundlegender Bedeutung.
- Nicht tolerierbare Risiken müssen reduziert werden.

SIL-Richtlinie

Einführung

Mit dem SIL-Wert wird die Robustheit einer Anwendung gegenüber Störungen und Ausfällen bewertet und damit die Fähigkeit eines System zur Ausführung einer Sicherheitsfunktion in Bezug auf eine vorgegebene Wahrscheinlichkeit eingestuft. Die Norm IEC 61508 stellt 4 Sicherheitsleistungsstufen bereit, in Abhängigkeit vom Risiko bzw. von den Auswirkungen des Prozesses, für den das sicherheitsbezogene System eingesetzt wird. Je gefährlicher die potenziellen Auswirkungen auf Menschen und Umwelt, umso höher die Sicherheitsanforderungen zur Risikominderung.

Definition der SIL-Werte

(Safety Integrity Level) Sicherheitsanforderungsstufe (1 von möglichen 4) für die Festlegung der Anforderungen an die Sicherheitsintegrität für die Sicherheitsfunktionen, die den sicherheitsbezogenen Systemen zugeordnet werden sollen, wobei der Sicherheits-Integritätslevel 4 der höchsten Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 der niedrigsten Stufe entspricht. Siehe SIL-Werte bei niedriger Anforderungsrate, Seite 407.

Definition der SIL-Anforderungen

Zur Erreichung der funktionalen Sicherheit sind 2 Typen von Anfoderungen erforderlich:

- Anforderungen an die Sicherheitsfunktion, d. h. Definition der auszuführenden Sicherheitsfunktionen.
- Anforderungen an die Sicherheitsintegrität, d. h. erforderlicher Grad der Gewissheit, dass die Sicherheitsfunktionen ausgeführt werden.

Die Anforderungen an die Sicherheitsfunktion werden von der Risikoanalyse abgeleitet und diejenigen an die Sicherheitsintegrität von der Risikobewertung.

Sie umfassen folgende Einheiten:

- MTBF (Mean Time Between Failures): Mittlere Betriebsdauer zwischen Ausfällen
- PF (Probability of Failure): Ausfallwahrscheinlichkeit
- FR (Failure Rate): Ausfallrate
- DC (Diagnostic Coverage): Diagnosedeckung
- SFF (Safe Failure Fraction): Sicherer Ausfallanteil

- HFT (Hardware Fault Tolerance): Hardwarefehlertoleranz

Je nach Sicherheits-Integritätslevel müssen sich diese Einheiten innerhalb der vorgegebenen Grenzwerte befinden.

HINWEIS: Die Kombination von Geräten mit unterschiedlichem Sicherheits-Integritätslevel in einem Netzwerk bzw. einer Sicherheitsfunktion erfordert besondere Berücksichtigung der Anforderungen gemäß IEC 61508 und bringt spezifische konzeptionsbezogene und betriebliche Einschränkungen mit sich.

Definition der SIL-Einstufung

Gemäß der Definition in IEC 61508 wird der SIL-Wert sowohl durch den sicheren Ausfallanteil (SFF) als auch durch die Hardwarefehlertoleranz (HFT) des Teilsystems begrenzt, das die Sicherheitsfunktion ausführt. Der HFT-Wert n bedeutet, dass n+1 Fehler einen Verlust der Sicherheitsfunktion verursachen können. Der sichere Zustand kann nicht erreicht werden. Der SFF-Wert ist von der Fehlerraten und der Diagnosedeckung abhängig.

Die nachstehende Tabelle zeigt die Beziehung zwischen SFF, HFT und SIL für komplexe sicherheitsbezogene Teilsysteme nach IEC 61508-2, in denen die Fehlermodi aller Komponenten nicht vollständig definiert werden können:

SFF	HFT = 0	HFT = 1	HFT = 2
SFF ≤ 60 %	-	SIL1	SIL2
60 % < SFF ≤ 90 %	SIL1	SIL2	SIL3
90 % < SFF ≤ 99 %	SIL2	SIL3	SIL4
SFF > 99 %	SIL3	SIL4	SIL4

Zur Erreichung eines bestimmten Sicherheits-Integritätslevel sind zwei Möglichkeiten gegeben:

- Erhöhung des HFT-Werts durch Bereitstellung zusätzlicher unabhängiger Abschaltpfade
- Erhöhung des SFF-Werts durch zusätzliche Diagnose

Definition der SIL-Anforderungsraten

Die Norm IEC 61508 unterscheidet zwischen einem Betrieb mit niedriger und mit hoher Anforderungsrate (Dauerbetrieb).

Bei niedriger Anforderungsrate beträgt die Frequenz des Einsatzbedarfs für ein sicherheitsbezogenes Systems nicht mehr als 1 pro Jahr und nicht mehr als das 2-Fache der Prüftestfrequenz. Der SIL-Wert eines sicherheitsbezogenen Systems mit niedriger

Anforderungsrate steht in direktem Bezug zur durchschnittlichen Ausfallwahrscheinlichkeit der Sicherheitsfunktion im Anforderungsfall bzw. PFD (Probability of Failure on Demand).

Bei hoher Anforderungsrate bzw. im Dauerbetrieb beträgt die Frequenz des Einsatzbedarfs für ein sicherheitsbezogenes Systems mehr als 1 pro Jahr und mehr als das 2-Fache der Prüftestfrequenz. Der SIL-Wert eines sicherheitsbezogenen Systems mit hoher Anforderungsrate steht in direktem Bezug zur Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde bzw. PFH (Probability of Failure per Hour).

SIL-Werte bei niedriger Anforderungsrate

In der folgenden Tabelle werden die Anforderungen für ein System mit niedriger Einsatzbedarfsrate aufgeführt:

Sicherheits-Integritätslevel	PDF (Ausfallwahrscheinlichkeit im Anforderungsfall)
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

SIL-Werte bei hoher Anforderungsrate

In der folgenden Tabelle werden die Anforderungen für ein System mit hoher Einsatzbedarfsrate aufgeführt:

Sicherheits-Integritätslevel	PFH (Ausfallwahrscheinlichkeit einer Sicherheitsfunktion pro Stunde)
4	$\geq 10^{-9}$ bis $< 10^{-8}$
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

Für SIL3 gilt folgende Ausfallwahrscheinlichkeit für das komplette sicherheitsintegrierte System:

- PFD $\geq 10^{-4}$ bis $< 10^{-3}$ bei niedriger Anforderungsrate
- PFH $\geq 10^{-8}$ bis $< 10^{-7}$ bei hoher Anforderungsrate

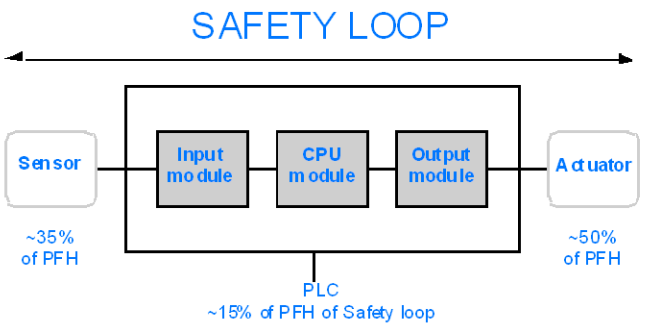
Beschreibung der Sicherheitsregelung

Die Sicherheitsregelung in Verbindung mit dem M580-Sicherheits-PAC umfasst folgende 3 Teile:

- Sensoren
- M580-Sicherheits-PAC mit Sicherheitsspannungsversorgung, Sicherheits-CPU, Sicherheits-Koprozessor und E/A-Sicherheitsmodulen
- Stellglieder

Ein Baugruppenträger oder eine dezentrale Verbindung mit einem Switch oder einem CRA-Modul, das die Sicherheitsregelung nicht beeinträchtigt. Baugruppenträger, Switches und CRA-Module sind Teil des Black Channel („Schwarzer Tunnel“). Das bedeutet, dass die von den E/A und dem PAC ausgetauschten Daten nicht ohne Erkennung durch den Empfänger beschädigt werden können.

Die nachstehende Abbildung zeigt eine typische Sicherheitsregelung:



Wie in obiger Abbildung gezeigt macht der Anteil des PAC nur 10 bis 20 % aus, da die Ausfallwahrscheinlichkeit der Sensoren und Stellglieder in der Regel ziemlich hoch ist.

Eine konservative Einstufung des Anteils des Sicherheits-PAC an der globalen Ausfallwahrscheinlichkeit in Höhe von 10 % lässt einen größeren Spielraum für den Benutzer und ergibt folgende erforderliche Ausfallwahrscheinlichkeit für den Sicherheits-PAC:

- PFD ≥ 10^{-5} bis < 10^{-4} bei niedriger Anforderungsrate
- PFH ≥ 10^{-9} bis < 10^{-8} bei hoher Anforderungsrate

Definition der PFD-Gleichung

Die Norm IEC 61508 geht davon aus, dass die Hälfte der Ausfälle in einem sicheren Zustand endet. Aus diesem Grund wird die Ausfallrate λ untergliedert in:

- λ_S - sicherer Ausfall
- λ_D - gefährlicher Ausfall, bestehend aus
  - λ_{DD} - gefährlicher Ausfall, identifiziert durch interne Diagnose
  - λ_{DU} - gefährlicher Ausfall, nicht identifiziert

Die Ausfallrate kann mithilfe des MTBF-Werts (Mittlere Betriebsdauer zwischen Ausfällen), einem modulspezifischen Wert, berechnet werden:

$\lambda = 1/MTBF$

Folgende Gleichung ermöglicht die Berechung der Ausfallwahrscheinlichkeit im Anforderungsfall:

$PFD(t) = \lambda_{DU} \times t$

t entspricht der Zeit zwischen 2 Prüftests.

Für die Ausfallwahrscheinlichkeit pro Stunde wird ein Zeitintervall von 1 Stunde vorausgesetzt. Damit wird die PDF-Gleichung auf Folgendes begrenzt:

$PFH = \lambda_{DU}$

Systemobjekte

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die Systembits und -wörter des M580-Sicherheits-PAC beschrieben.

HINWEIS: Die jedem Bitobjekt oder Systemwort zugeordneten Symbole in den beschreibenden Tabellen dieser Objekte sind nicht grundsätzlich in der Software implementiert. Sie können mit dem Dateneditor eingegeben werden

Bits des M580-Sicherheitssystems

Systembits für die Ausführung der SAFE-Task

Die nachstehend aufgeführten Systembits sind für den M580-Sicherheits-PAC verfügbar. Eine Beschreibung der Systembits, die sowohl für den M580-Sicherheits-PAC als auch für nicht-sichere M580-PACs zur Verfügung stehen, finden Sie im Abschnitt zu den *Systembits* im *EcoStruxure™ Control Expert Systembits und -wörter - Referenzhandbuch*.

Diese Systembits stehen in Verbindung mit der Ausführung der SAFE-Task, sind jedoch nicht im sicherheitsspezifischen Programmcode zugänglich. Der Zugriff ist ausschließlich über die Bausteine `S_SYST_READ_TASK_BIT_MX` und `S_SYST_RESET_TASK_BIT_MX` möglich.

Bit Symbol	Funktion	Beschreibung	Initial-status	Typ
%S17 CARRY	Ausgang Zirkularver-schiebung	Bei einer Zirkularverschiebung in der SAFE-Task nimmt dieses Bit den Status des Ausgangsbits an.	0	R/W
%S18 OVERFLOW	Überlauf oder arithmetischer Fehler	Dieses Bit befindet sich normalerweise im Status 0 und wird bei einem Kapazitätsüberlauf auf 1 gesetzt: • Ergebnis größer als +32 767 oder kleiner als -32 768, in einfacher Länge • Ergebnis größer ls +65 535, als nicht vorzeichenbehaftete Ganzzahl • Ergebnis größer als +2 147 483 647 oder kleiner als -2 147 483 648, in doppelter Länge • Ergebnis größer als +4 294 967 296, in doppelter Länge oder als nicht vorzeichenbehaftete Ganzzahl • Division durch 0 • Wurzel einer negativen Zahl • Forcierung auf einen in einem Drum nicht vorhandenen Schritt • Stapelung eines bereits vollen Registers, Leeren eines bereits leeren Register	0	R/W
%S21 1RSTTASKRUN	Erste Abfrage der SAFE-Task im RUN-Betrieb	Dieses Bit wurde in der SAFE-Task getestet und verweist auf den ersten Zyklus der Task. Eswird zu Beginn des Zyklus auf 1 gesetzt und am Ende des Zyklus wieder auf 0 zurückgesetzt. **HINWEIS:** • Der Status des ersten Taskzyklus kann am Ausgang SCOLD des Systemfunktionsbausteins S_SYST_STAT_MX gelesen werden. • Dieses Bit ist für M580-Hot Standby-Sicherheitssysteme ohne Wirkung.	0	R/W

Hinweise zu nicht-sicherheitsspezifischen Systembits

Systembit	Beschreibung	Hinweise
%S0	Kaltstart	Kann nur in Prozesstasks (nicht SAFE) verwendet werden und hat keinerlei Wirkung auf die SAFE-Task.
%S9	Ausgänge in den Fehlerzustand gesetzt	Keine Wirkung auf Sicherheitsausgangsmodule.

Systembit	Beschreibung	Hinweise
%S10	Globaler E/A- Fehler	Meldet einige, aber nicht alle der möglicherweise erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.
%S11	Watchdog-Überlauf	Berücksichtigt einen Überlauf der SAFE-Task.
%S16	E/A-Taskfehler	Meldet einige, aber nicht alle der möglicherweise erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.
%S19	Überschreitung der Task-Dauer	Keine Informationen zu einer Überschreitung der SAFE-Task verfügbar.
%S40...47	E/A-Fehler Rack *n*	Meldet einige, aber nicht alle der möglicherweise erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.
%S78	STOP bei Fehler	Gilt sowohl für die Prozesstasks als auch für die SAFE-Task. Bei gesetztem Bit wechselt die SAFE-Task beispielsweise bei einem Überlauf von %S18 in den HALT-Zustand.
%S94	Speichern angepasster Werte	Gilt nicht für SAFE-Variablen. Die SAFE-Initialwerte können durch eine Aktivierung dieses Bits geändert werden.
%S117	RIO-Fehler im Ethernet-E/A-Netzwerk	Meldet einige, aber nicht alle der möglicherweise erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.
%S119	Allgemeiner rackinterner Fehler	Meldet einige, aber nicht alle der möglicherweise erkannten Fehler in Verbindung mit den E/A-Sicherheitsmodulen.

M580-Sicherheitssystem – Systemwörter

Systemwörter für M580-Sicherheits-PACs

Die nachstehend aufgeführten Systemwörter sind für den M580-Sicherheits-PAC verfügbar. Eine Beschreibung der Systemwörter, die sowohl für den M580-Sicherheits-PAC als auch für nicht-sichere M580-PACs zur Verfügung stehen, finden Sie im Abschnitt zu den *Systemwörtern* im *EcoStruxure™ Control Expert Systembits und -wörter - Referenzhandbuch*.

Die folgenden Systemwörter und -werte sind in Verbindung mit der SAFE-Task verfügbar. Sie sind über den anwendungsspezifischen Programmcode in nicht-sicheren Sections zugänglich (MAST, FAST, AUX0 oder AUX1), jedoch nicht über Code in der Section der SAFE-Task.

Wort	Funktion	Typ
%SW4	In der Konfiguration definierte Dauer der SAFE-Task. Die Dauer kann vom Bediener nicht geändert werden.	R
%SW12	Gibt die Betriebsart des Koprozessormoduls an: • 16#A501 = Wartungsmodus • 16#5AFE = Sicherheitsmodus Alle anderen Werte werden als Fehler interpretiert.	R
%SW13	Gibt die Betriebsart der CPU an: • 16#501A = Wartungsmodus • 16#5AFE = Sicherheitsmodus Alle anderen Werte werden als Fehler interpretiert.	R
%SW42	Aktuelle Zeit der SAFE-Task. Gibt die Ausführungszeit des letzten Zyklus der SAFE-Task an (in ms).	R
%SW43	Maximale Zeit der SAFE-Task. Gibt die längste Ausführungszeit der SAFE-Task seit dem letzten Kaltstart an (in ms).	R
%SW44	Minimale Zeit der SAFE-Task. Gibt die kürzeste Ausführungszeit der SAFE-Task seit dem letzten Kaltstart an (in ms).	R
%SW110	Vom System für interne Dienste verwendeter Prozentsatz der CPU-Systemlast.	R
%SW111	Von der MAST-Task verwendeter Prozentsatz der CPU-Systemlast.	R
%SW112	Von der FAST-Task verwendeter Prozentsatz der CPU-Systemlast.	R
%SW113	Von der SAFE-Task verwendeter Prozentsatz der CPU-Systemlast.	R
%SW114	Von der AUX0-Task verwendeter Prozentsatz der CPU-Systemlast.	R
%SW115	Von der AUX1-Task verwendeter Prozentsatz der CPU-Systemlast.	R

Wort	Funktion	Typ
%SW116	Gesamte CPU-Systemlast.	R
%SW124	Enthält die Ursache des nicht-behebbaren Fehlers, wenn sich der M580-Sicherheits-PAC im HALT-Zustand befindet: • 0x5AF2: RAM-Fehler bei Speicherprüfung • 0x5AFB: Fehler im Code der Sicherheitsfirmware • 0x5AF6: Überlauf des Sicherheitswatchdogs in der CPU • 0x5AFF: Überlauf des Sicherheitswatchdogs im Coprozessor • 0x5B01: Coprozessor bei Anlauf nicht erkannt • 0x5AC03: Nicht-behebbarer Fehler in Verbindung mit der CIP-Sicherheit von der CPU erkannt • 0x5AC04: Nicht-behebbarer Fehler in Verbindung mit der CIP-Sicherheit vom Coprozessor erkannt **HINWEIS:** Die oben aufgeführten Fehler stellen keine vollständige Liste dar. Weitere Informationen finden Sie im *EcoStruxure™ Control Expert Systembits und -wörter - Referenzhandbuch*.	R
%SW125	Enthält die Ursache des im M580-Sicherheits-PAC erkannten nicht-behebbaren Fehlers: • 0x5AC0: CIP-Sicherheitskonfiguration ungültig (von der CPU erkannt) • 0x5AC1: CIP-Sicherheitskonfiguration ungültig (vom Coprozessor erkannt) • 0x5AF3: Vergleichsfehler von der Haupt-CPU erkannt • 0x5AFC: Vergleichsfehler vom Coprozessor erkannt • 0x5AFD: Interner Fehler vom Coprozessor erkannt • 0x5AFE: Synchronisierungsfehler zwischen CPU und Coprozessor • 0x9690: Prüfsummenfehler im Anwendungsprogramm **HINWEIS:** Die oben aufgeführten Fehler stellen keine vollständige Liste dar. Weitere Informationen finden Sie im *EcoStruxure™ Control Expert Systembits und -wörter - Referenzhandbuch*.	R
%SW126 %SW127	Diese zwei Systemwörter enthalten Informationen zur internen Verwendung durch Schneider Electric bei der detaillierten Analyse erkannter Fehler.	R
%SW128	Mit einer CPU-Firmwareversion bis 3.10 wird die Zeitsynchronisierung zwischen der NTP-Zeit und der SAFE-Zeit für die sicheren E/A-Module und die SAFE-CPU-Task forciert: • Eine Wertänderung von 16#1AE5 zu 16#E51A forciert eine Synchronisierung. Siehe die *Vorgehensweise zur Synchronisierung der NTP-Zeiteinstellungen*, Seite 182. • Andere Sequenzen und Werte forcieren keine Synchronisierung.	R/W
%SW142	Enthält die Firmwareversion des Sicherheitscoprozessors in 4-stelligem BCD-Format. Beispiel: Firmwareversion 21.42 entspricht %SW142 = 16#2142.	R
%SW148	ECC-Fehlerzähler (Error Correcting Code) für von der CPU erkannte Fehler	R
%SW152	Status der NTP-CPU-Zeit, vom Ethernet-Kommunikationsmodul (z. B. BMENOC0301/11) über den X Bus-Baugruppenträger mithilfe der optionalen Funktion zur forcierten Zeitsynchronisation aktualisiert:	R

Wort	Funktion	Typ
	• 0: CPU-Zeit nicht vom Ethernet-Kommunikationsmodul aktualisiert • 1: CPU-Zeit vom Ethernet-Kommunikationsmodul aktualisiert	
%SW169	ID der Sicherheitsanwendung: Enthält die ID des Sicherheitscodeteils der Anwendung. Die ID wird bei Änderung des Codes der Sicherheitsanwendung automatisch geändert. **HINWEIS:** • Wenn seit dem vorhergehenden Befehl **Alle wiederherstellen** der Sicherheitscode geändert und der Befehl **Änderungen generieren** ausgeführt (und dadurch die ID der Sicherheitsanwendung geändert) wurde, wird die ID der Sicherheitsanwendung durch die Ausführung des Befehls **Alle wiederherstellen** ggf. erneut geändert. • Die eindeutige Kennung des SAFE-Programms kann am Ausgang `SAID` des Systemfunktionsbausteins `S_SYST_STAT_MX` gelesen werden.	R
%SW171	Status der FAST-Tasks: • 0: Keine FAST-Tasks vorhanden • 1: Stop • 2: Run • 3: Breakpoint (Haltepunkt) • 4: Halt	R
%SW172	Status der SAFE-Task: • 0: Keine SAFE-Task vorhanden • 1: Stop • 2: Run • 3: Breakpoint (Haltepunkt) • 4: Halt	R
%SW173	Status der MAST-Task: • 0: Keine MAST-Task vorhanden • 1: Stop • 2: Run • 3: Breakpoint (Haltepunkt) • 4: Halt	R

Wort	Funktion	Typ
%SW174	Status der AUX0-Task: • 0: Keine AUX0-Task vorhanden • 1: Stop • 2: Run • 3: Breakpoint (Haltepunkt) • 4: Halt	R
%SW175	Status der AUX1-Task: • 0: Keine AUX1-Task vorhanden • 1: Stop • 2: Run • 3: Breakpoint (Haltepunkt) • 4: Halt	R

SRAC-Referenzen

Der Prüfplan der Sicherheitsbedingungen (SRAC) bietet einen allgemeinen Rahmen, um nachzuweisen, dass die Anweisungen der zugehörigen Installation und des Sicherheitshandbuchs erfüllt sind. Diese Anweisungen im *Modicon M580-Sicherheitshandbuch* sind als Anforderungen aufgeführt.

Die folgende Tabelle enthält den Titel des Absatzes, in dem Sie die Anforderungen im Zusammenhang mit dem Anwendungslebenszyklus finden:

Anforderungen an den Anwendungslebenszyklus (LC)	
ID	**An diesem Ort**
LC Nr. 1	Schritt 9: Sicherheitsanforderungen für E/E/PE-Systeme – Technische Daten, Seite 37
LC Nr. 2	Schritt 9: Sicherheitsanforderungen für E/E/PE-Systeme – Technische Daten, Seite 37
LC Nr. 3	Schritt 10: Umsetzung von sicherheitsbezogenen E/E/PE-Systemen, Seite 37
LC Nr. 4	Schritt 12: Allgemeine Installation und Inbetriebnahme, Seite 41
LC Nr. 5	Schritt 12: Allgemeine Installation und Inbetriebnahme, Seite 41
LC Nr. 6	Schritt 13: Allgemeine Sicherheitsprüfung, Seite 42
LC Nr. 7	Schritt 14: Allgemeiner Betrieb, Wartung und Reparatur, Seite 43
LC Nr. 8	Schritt 15: Allgemeine Änderungen und Nachrüstung, Seite 43

Die folgende Tabelle enthält den Titel des Absatzes, in dem Sie die Anforderungen im Zusammenhang mit der Sicherheitsinformationsmeldung finden:

Anforderungen an Sicherheitsinformationsmeldungen (SM)	
ID	**An diesem Ort**
SM Nr. 1	Bevor Sie beginnen, Seite 10
SM Nr. 2	Start und Test, Seite 11
SM Nr. Nr. 3	Sicherheitsschleife, Seite 17
SM Nr. 4	Nicht störende Module, Seite 29

Anforderungen an Sicherheitsinformationsmeldungen (SM)	
ID	**An diesem Ort**
SM Nr. 5	Externe Spannungsversorgung mit digitalem E/A-Sicherheitsmodul, Seite 47
SM Nr. 6	Verdrahtungsbeispiele für Eingangsanwendung BMXSAI0410, Einführung, Seite 54
SM Nr. 7	Verdrahtungsbeispiele für Eingangsanwendung BMXSAI0410, SIL3 Cat2/PLd, Seite 56
SM Nr. 8	Verdrahtungsbeispiele für Eingangsanwendung BMXSAI0410, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 57
SM Nr. 9	Verdrahtungsbeispiele für Eingangsanwendung BMXSAI0410, SIL3 Cat4/PLe, Seite 58
SM Nr. 10	Verdrahtungsbeispiele für Eingangsanwendung BMXSAI0410, SIL3 Cat4/PLe mit hoher Verfügbarkeit, Seite 59
SM Nr. 11	Anschlussstecker BMXSDI1602, Prozessspannungsversorgung, Seite 66
SM Nr. 12	Anschlussstecker BMXSDI1602, Sicherung, Seite 67
SM Nr. 13	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602 , Einführung, Seite 72
SM Nr. 14	Konfigurierbare Verdrahtungsdiagnose in Control Expert, Seite 73
SM Nr. 15	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd, Seite 74
SM Nr. 16	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd, Seite 74
SM Nr. 17	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd, Seite 74
SM Nr. 18	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 77
SM Nr. 19	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 77
SM Nr. 20	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 77
SM Nr. 21	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 77
SM Nr. 22	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, SIL3 Cat2/PLd mit hoher Verfügbarkeit, Seite 77
SM Nr. 23	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81

Anforderungen an Sicherheitsinformationsmeldungen (SM)	
ID	**An diesem Ort**
SM Nr. 24	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 25	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 26	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 27	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 28	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 29	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 30	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe, Seite 81
SM Nr. 31	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 32	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 33	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 34	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 35	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 36	Verdrahtungsbeispiele für Eingangsanwendung BMXSDI1602, Cat4/PLe mit hoher Verfügbarkeit, Seite 89
SM Nr. 37	Anschlussstecker BMXSDO0802, Sicherung, Seite 100
SM Nr. 38	Verdrahtungsbeispiele für Ausgangsanwendung BMXSDO0802, Einführung, Seite 102
SM Nr. 39	Verdrahtungsbeispiele für Ausgangsanwendung BMXSDO0802, Einführung, Seite 102
SM Nr. 40	Konfigurierbare Verdrahtungsdiagnose in Control Expert, Seite 103
SM Nr. 41	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106
SM Nr. 42	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106
SM Nr. 43	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106

Anforderungen an Sicherheitsinformationsmeldungen (SM)	
ID	**An diesem Ort**
SM Nr. 44	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106
SM Nr. 45	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106
SM Nr. 46	Übersicht über die Ausgangsverdrahtungsdiagnose, Seite 106
SM Nr. 47	Anschlussstecker BMXSRA0405, Sicherung, Seite 115
SM Nr. 48	Anwendung_1: 4 Ausgänge, SIL2 / Cat2 / PLc, spannungsfreier Zustand, kein automatischer Signaltest, Seite 118
SM Nr. 49	Anwendung_3: 4 Ausgänge, SIL2 / Cat2 / PLc, spannungsfreier Zustand, kein automatischer Signaltest, Seite 119
SM Nr. 50	Anwendung_5: 2 Ausgänge, SIL3 / Cat4 / PLe, spannungsfreier Zustand, kein automatischer Signaltest, Seite 120
SM Nr. 51	Anwendung_7: 2 Ausgänge, SIL3 / Cat4 / PLe, spannungsführender Zustand, kein automatischer Signaltest, Seite 121
SM Nr. 52	M580-Sicherheitsspannungsversorgungen, Einführung, Seite 132
SM Nr. 53	Beschreibung der Zeit für Ausgangsmodule, Seite 159
SM Nr. 54	Konfiguration der maximalen Perioden für SAFE- und FAST-Task auf der CPU, Seite 163
SM Nr. 55	Zertifizierte Sicherheitsfunktionen und Funktionsbausteine, Seite 169
SM Nr. 56	Konfiguration der Zeitsynchronisation mit der CPU-Firmware 3.10 oder früher, Einleitung, Seite 180
SM Nr. 57	Änderung der NTP-Zeiteinstellungen während des Betriebs, Seite 181
SM Nr. 58	Vorgehensweise zur Synchronisation der NTP-Zeiteinstellungen, Seite 182
SM Nr. 59	Vorgehensweise zur Synchronisation der NTP-Zeiteinstellungen, Seite 182
SM Nr. 60	Konfiguration des DFB S_WR_ETH_MX, Seite 195
SM Nr. 61	Konfiguration des DFB S_RD_ETH_MX, Seite 198
SM Nr. 62	Konfiguration des DFB S_WR_ETH_MX2, Seite 210
SM Nr. 63	Konfiguration des DFB S_RD_ETH_MX2, Seite 212

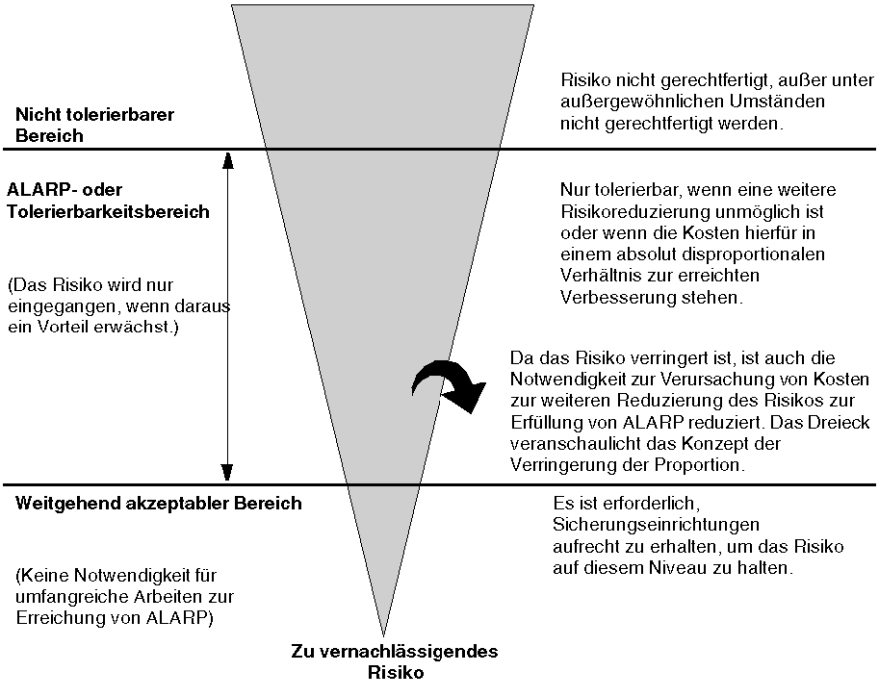
Anforderungen an Sicherheitsinformationsmeldungen (SM)	
ID	**An diesem Ort**
SM Nr. 64	M580 Black-Channel-Kommunikation, Seite 216
SM Nr. 65	M580 Black-Channel-Kommunikation, Seite 216
SM Nr. 66	LED-Diagnose der M580-Sicherheits-CPU, Seite 227
SM Nr. 67	Funktion des Wartungsmodus, Seite 265
SM Nr. 68	Anlaufsequenzen, Warmstart, Seite 278
SM Nr. 69	Sperre der Konfiguration der E/A-Sicherheitsmodule, Seite 291
SM Nr. 70	Anzeige der Daten in den Bedienerfenstern, Seite 298
SM Nr. 71	Konfiguration des CIP Safety-Geräts mithilfe eines herstellerspezifischen Tools, Seite 366
SM Nr. 72	Interaktionen zwischen Betriebsvorgängen des Sicherheits-PAC und der Zielverbindung, Seite 387

Glossar

A

ALARP:

(*As Low As Reasonably Practicable*) Dt.: So gering wie vernünftigerweise durchführbar (Definition nach IEC 61508)



C

CCF:

(*Common Cause Failure*) Dt.: Ausfall aufgrund/infolge gemeinsamer Ursache. Diese Art eines Ausfalls ist die Folge von einem oder mehreren Ereignissen, die zum gleichzeitigen Ausfall von mindestens zwei voneinander getrennten Kanälen in einem aus mehreren Kanälen bestehenden System führen, was den Ausfall des Gesamtsystems zur Folge hat. (Definition nach IEC 61508) Der „CC-Faktor“ in einem aus zwei Kanälen bestehenden System ist entscheidend für die Ausfallwahrscheinlichkeit des Gesamtsystems im Anforderungsfall (PFD).

CPCRC:

(*Connection Parameter Cyclic Redundancy Check*) Ein vom CSS für jede CIP Safety-Verbindung erzeugter und in SafetyOpen-Requests vom Typ 2 enthaltener CRC-S32-Wert der Zielverbindungsparameter.

D

DDDT:

(*Device Derived Data Type* = Abgeleiteter Gerätedatentyp) DDTs sind vom Hersteller vordefiniert und können vom Benutzer nicht geändert werden. Sie enthalten die E/A-Sprachelemente eines E/A-Moduls.

DIO-Netzwerk:

Netzwerk mit verteilten Geräten, in dem die E/A von einer CPUmit DIO-Scannerdienst im lokalen Rack abgefragt werden. Der Datenverkehr in einem DIO-Netzwerk erfolgt im Anschluss an den RIO-Verkehr, der in einem Gerätenetzwerk prioritär behandelt wird.

DRS:

(*Dual-Ring-Switch*) Erweiterter, verwalteter ConneXium-Switch, der für den Betrieb in einem Ethernet-Netzwerk konfiguriert wurde. Schneider Electric stellt vordefinierte Konfigurationsdateien bereit, die in einen DRS heruntergeladen werden können und Unterstützung für die spezifischen Funktionen einer Hauptring-/Teilring-Architektur bieten.

DTM:

(*Device Type Manager*) Ein DTM ist ein Gerätetreiber, der auf einem Host-PC ausgeführt wird . Er stellt eine vereinheitlichte Struktur für den Zugriff auf Geräteparameter, für die Konfiguration und den Betrieb der Geräte sowie für die Fehlerbehebung bereit. Bei DTMs kann es sich um einfache grafische Benutzeroberflächen zur Einstellung von Geräteparametern bis hin zu hoch entwickelten Anwendungen handeln, die komplexe Echtzeitberechnungen zu Diagnose- und Wartungszwecken durchführen können. Im Zusammenhang mit einem DTM kann ein Gerät ein Kommunikationsmodul oder ein dezentrales Gerät im Netzwerk sein.

Siehe FDT.

E

EDS:

(*Electronic Data Sheet; elektronisches Datenblatt*) Bei einem EDS handelt es sich um eine einfache Textdatei, in der die Konfigurationsmöglichkeiten eines Geräts beschrieben sind. EDS-Dateien werden vom Hersteller des Geräts erstellt und gepflegt.

EUC:

(*Equipment Under Control*) (Definition nach IEC 61508) Dieser Begriff bezeichnet Ausrüstungen, Maschinen, Geräte oder Anlagen, die für Fertigungs-, Prozess-, Transport-, medizinische oder andere Tätigkeiten genutzt werden.

H

HFT:

(*Hardware Fault Tolerance*) Dt.: Hardwarefehlertoleranz (Definition nach IEC 61508)

Eine Hardwarefehlertoleranz von N bedeutet, dass N + 1 Fehler zu einem Ausfall der Sicherheitsfunktion führen können. Beispiel:

- HFT = 0: Der 1. Fehler kann zu einem Ausfall der Sicherheitsfunktion führen.
- HFT = 1: Zwei Fehler in Verbindung können zu einem Ausfall der Sicherheitsfunktion führen. (Es gibt zwei verschiedene Methoden, zu einem sicheren Zustand zu gelangen. Ausfall der Sicherheitsfunktion bedeutet, dass kein sicherer Zustand erreicht werden kann.)

O

OUNID:

(*Originator Unique Network Identifier*) Ein Wert, der das Ursprungsgerät einer Verbindung in einem CIP Safety-Sicherheitsnetzwerk eindeutig identifiziert (in der Regel eine CPU). Die OUNID besteht aus:

- einer Netzwerk-Sicherheitsnummer (SNN: Safety Network Number), die ein Zeitstempel oder ein anderer benutzerdefinierter Wert sein kann.
- einer Knotenadresse (für EtherNet/IP-Netzwerke die IP-Adresse).

P

PST:

(*Process Safety Time*) Die Prozesssicherheitszeit ist definiert als die Zeit zwischen dem Auftreten eines Fehlers im EUC oder im EUC-Steuerungssystem (mit dem Potenzial, zu einem gefährlichen Ereignis zu führen) und dem Auftreten des gefährlichen Ereignisses, wenn die Sicherheitsfunktion nicht ausgeführt wird. (Definition nach IEC 61508)

R

RIO-Station:

Rack mit Ethernet-E/A-Modulen, die über einen RIO-Adapter verwaltet werden und Ein- und Ausgänge umfassen, die bei der RIO-Abfrage der CPU berücksichtigt werden. Eine Station kann einem einzelnen Rack oder einem Hauptrack mit Erweiterungsracks entsprechen.

S

SAId:

(*Safety Application Identifier*) Eine per Algorithmus berechnete Signatur des Sicherheitsteils einer Control Expert-Anwendung, gespeichert in %SW169.

SCID:

(*Safety Configuration Identifier*) Siehe TUNID.

SFF:

(*Safe Failure Fraction*) Dt.: Sicherer Ausfallanteil

SNCT:

(*Safety Network Configuration Tool*) Vom Hersteller bereitgestelltes Tool zur Konfiguration von CIP Safety-Geräten. Siehe TUNID.

SRAC:

(*Safety Related Application Condition*: Sicherheitsbezogener Anwendungszustand)

SRT:

(*System Reaction Time*) Die Systemreaktionszeit ist der Zeitraum zwischen der Erfassung eines Signals an der Eingangsmodulklemme und der Reaktion in Form des Setzens eines Ausgangs an der Ausgangsmodulklemme.

T

TFFR:

(*Tolerable Functional Failure Rate*: Tolerierbare funktionale Ausfallrate) Rate pro Stunde gemäß EN 5012x-Normen für den Schienenverkehr.

TUNID:

(*Target Unique Network Identifier*) Ein Wert, der das Zielgerät einer Verbindung in einem CIP Safety-Sicherheitsnetzwerk eindeutig identifiziert. Die TUNID besteht aus:

- einer Netzwerk-Sicherheitsnummer (SNN: Safety Network Number), die ein Zeitstempel oder ein anderer benutzerdefinierter Wert sein kann.
- einer Sicherheitskonfigurationskennung (SCID), ebenfalls als Konfigurationssignatur bezeichnet, die in einem vom Hersteller bereitgestellten Tool zur Sicherheitsnetzwerkkonfiguration (SNCT) erstellt wird und aus folgenden Elementen besteht:
  - einem Sicherheitskonfigurations-CRC (SCCRC), d. h. einem CRC-Wert aus den Konfigurationseinstellungen des Sicherheitsgeräts, in Form eines Hexadezimalwerts mit 4 Byte.
  - einem Sicherheitskonfigurations-Zeitstempel (SCTS), d. h. einem hexadezimalen Datums- und Uhrzeitwert mit 6 Byte.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

V

W

Z

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Da Normen, Spezifikationen und Bauweisen sich von Zeit zu Zeit ändern, ist es unerlässlich, dass Sie die in dieser Veröffentlichung gegebenen Informationen von uns bestätigen.

QGH46984.05