Modicon M580

Sicherheitssystem - Planungshandbuch

Übersetzung der Originalbetriebsanleitung

QGH60285.07
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 Planungshandbuch für Sicherheitssysteme beschreibt die Module des M580-Sicherheitssystems mit besonderem Schwerpunkt auf deren 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 XL 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.

Gültigkeitsanmerkung

Dieses Dokument ist gültig ab EcoStruxure™ Control Expert 15.0.

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	EIO0000004742.00 (Englisch)
Modicon M580, Sicherheitshandbuch	QGH46982 (Englisch), QGH46983 (Französisch), QGH46984 (Deutsch), QGH46985 (Italienisch), QGH46986 (Spanisch), QGH46987 (Chinesisch)

Titel der Dokumentation	Referenznummer
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 – 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)
Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen	NHA58880 (Englisch), NHA58881 (Französisch), NHA58882 (Deutsch), NHA58883 (Italienisch), NHA58884 (Spanisch), NHA58885 (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.

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 AG nach folgenden Normen zertifiziertes sicherheitsbezogenes System:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50128 (IEC 62279), EN 50129 (IEC 62245), EN 50126 (IEC 62278)
- 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
- BMEP586040S Standalone-CPU
- Hot Standby-CPU BMEH582040S
- Hot Standby-CPU BMEH584040S
- Hot Standby-CPU BMEH586040S
- Koprozessor BMEP58CPROS3
- Analoges Eingangsmodul BMXSAI0410
- Digitales Eingangsmodul BMXSDI1602
- Digitales Ausgangsmodul BMXSDO0802
- Digitales Relais-Ausgangsmodul 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 16 aufgenommen werden.

HINWEIS: Das Modicon-Sicherheitsangebot umfasst bis zu SIL3 (gem. IEC 61508) und PLe (gem. ISO 13849), d. h. sie ist auch SIL1/SIL2- und PLa-, b-, c-, d-fähig.

HINWEIS:

- Jedes Mal, wenn im Dokument SIL2 oder SIL3 ohne eine Standardreferenz erwähnt wird, bezieht sich dies auf IEC 61508 / IEC 61511.
- Jedes Mal, wenn SIL2 erwähnt wird, ist es auch SIL3 gemäß EN 50126 / EN 50128 / EN 50129.
- Jedes Mal, wenn SIL3 erwähnt wird, ist es auch SIL4 gemäß 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 Beschränkungen 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.
- Unter *M580-CPU- und Koprozessor-Leistungsmerkmale*, Seite 53 im *Modicon M580 Sicherheitssystem – Planungshandbuch* finden Sie eine Beschreibung der CPU-Beschränkungen.

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 selben Rack installiert werden wie die Sicherheitsmodule (ungeachtet der Position des Sicherheitsmoduls, ob im Haupt- oder Erweiterungsrack).
- **Typ 2**: Ein nicht-störendes Modul des Typs 2 kann nicht im selben Rack installiert werden wie die Sicherheitsmodule (ungeachtet der Position des Sicherheitsmoduls, ob im Haupt- oder Erweiterungsrack).

  HINWEIS: Eine Liste der Module des Typs 1 und 2 finden Sie auf der Website von TÜV Rheinland: www.certipedia.com.

  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 jeweils neueste Liste finden Sie auf der Website von TÜV Rheinland: 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 für Dual-Steckplätze für redundante Spannungsversorgungen	BMEXBP0602
Baugruppenträger mit 10 Steckplätzen für Dual-Steckplätze 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 K, 100 Mb	BMXNRP0200
Kommunikation: Glasfaserkonverter SM/LC, 2 K, 100 Mb	BMXNRP0201
Kommunikation: M580 IEC 61850 Kommunikationsmodul	BMENOP0300
Kommunikation: Integrierter OPC-UA-Server	BMENUA0100
Zählen: SSI-Modul, 3 K	BMXEAE0300

Modultyp	Modulreferenz
Zählen: Hochgeschwindigkeitszähler 2 K	BMXEHC0200
Zählen: Hochgeschwindigkeitszähler 8 K	BMXEHC0800
Bewegung: Impulswellenausgang, 2 unabhängige K	BMXMSP0200
Analog: Ana 8 Ein, Strom, potentialgetrennt, HART	BMEAHI0812
Analog: Ana 4 Ein, Strom, potentialgetrennt, HART	BMEAHO0412
Analog: Ana 4 U/I Ein, potentialgetrennt, Hochgeschwindigkeit	BMXAMI0410
Analog: Ana 4 U/I Ein, nicht-potentialgetrennt, Hochgeschwindigkeit	BMXAMI0800
Analog: Ana 8 U/I Ein, potentialgetrennt, Hochgeschwindigkeit	BMXAMI0810
Analog: Ana 4 U/I Ein, 4 U/I Aus	BMXAMM0600
Analog: Ana 2 U/I Aus, potentialgetrennt	BMXAMO0210
Analog: Ana 4 U/I Aus, potentialgetrennt	BMXAMO0410
Analog: Ana 8 Aus, Strom, nicht potentialgetrennt	BMXAMO0802
Analog: Ana 4 TC/RTD Ein, potentialgetrennt	BMXART0414.2
Analog: Ana 8 TC/RTD Ein, potentialgetrennt	BMXART0814.2
Digital: Dig 8 Ein, 220 VAC	BMXDAI0805
Digital: Dig 8 Ein, 100 bis 120 VAC, potentialgetrennt	BMXDAI0814
Digital: Dig 16 Ein, 24 VAC/24 VDC, Source	BMXDAI1602
Digital: Dig 16 Ein, 48 VAC	BMXDAI1603
Digital: Dig 16 Ein, 100 bis 120 VAC, 20-polig	BMXDAI1604
Digital: Dig 16 überwachte Eingangskanäle, 100 bis 120 VAC, 40-polig	BMXDAI1614
Digital: Dig 16 überwachte Eingangskanäle, 200 bis 240 VAC, 40-polig	BMXDAI1615
Digital: Dig 16 Triac-Ausgänge, 100 bis 240 VAC, 20-polig	BMXDAO1605
Digital: Dig 16 Triac-Ausgänge, 24 bis 240 VAC, 40-polig	BMXDAO1615
Digital: Dig 16 Ein, 24 VDC, Sink	BMXDDI1602
Digital: Dig 16 Ein, 48 VDC, Sink	BMXDDI1603
Digital: Dig 16 Ein, 125 VDC, Sink	BMXDDI1604T
Digital: Dig 32 Ein, 24 VDC, Sink	BMXDDI3202K
Digital: Dig 64 Ein, 24 VDC, Sink	BMXDDI6402K
Digital: Dig 8 Ein, 24 VDC, 8Q, Source, Tr	BMXDDM16022

Modultyp	Modulreferenz
Digital: Dig 8 Ein, 24 VDC, 8Q, Relais	BMXDDM16025
Digital: Dig 16 Ein, 24 VDC, 16Q, Source, Tr	BMXDDM3202K
Digital: Dig 16Q, Trans, Source, 0,5 A	BMXDDO1602
Digital: Dig 16 Aus, Trans, Sink	BMXDDO1612
Digital: Dig 32Q, Trans, Source, 0,1 A	BMXDDO3202K
Digital: Dig 64Q, Trans, Source, 0,1 A	BMXDDO6402K
Digital: Dig 8Q, 125 VDC	BMXDRA0804T
Digital: Dig 8Q, 24 VDC oder 24 bis 240 VAC, potentialgetrennte Relais	BMXDRA0805
Digital: Dig 16 nicht-potentialgetrennte Relaisausgangskanäle, 5 bis 125 VDC oder 25 bis 240 VAC	BMXDRA0815
Digital: Dig 16Q, Relais	BMXDRA1605
Digital: Dig NC-Ausgang, 5 bis 125 VDC oder 24 bis 240 VAC, Relais	BMXDRC0805
Digital: Dig 16 Ein, 24/125 VDC, TSTAMP	BMXERT1604
Mx80-Schalter für Netzwerkoptionen	BMENOS0300
Turbomaschinen Frequenzeingang, 2 K	BMXETM0200
Unterstützung für Profibus DP/DPV1-Mastermodul	PMEPXM0100
Mx80 Erweitertes 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 eingesetzt werden.

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

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

Modultyp	Modulreferenz
Hochleistungsspannungsversorgung 24–48 VDC, potentialgetrennt	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 Port RS485/232	BMXNOM0200
Digital: Dig 32 Ein, 12/24 VDC, Sink oder Source	BMXDDI3232
Digital: Dig 32 Ein, 48 VDC, Sink	BMXDDI3203
CANopen-X80-Master	BMECXM0100
Wägemodul	PMESWT0100
Diagnose-Partnermodul	PMXCDA0400
Universelles Kommunikationsmodul Ethernet TCP Open	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.

Auswahl der Topologie für ein M580-Sicherheitssystem

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die von einem M580-Sicherheitssystem unterstützten Topologien beschrieben.

Planung der Topologie eines M580-Sicherheitssystems

Unterstützung für Standalone- und Hot Standby-PACs

Ein M580-Sicherheitssystem bietet Unterstützung für SIL3-Anwendungen für Standalone- und für Hot Standby-PACs. Jedes CPU-Rack umfasst ein CPU- und ein Koprozessor-Modul.

HINWEIS: Eine Beschreibung der verfügbaren Racks und deren zulässiger Nutzung finden Sie unter *Racknutzung*, Seite 85.

Integration der Sicherheitsmodule in den RIO-Hauptring

Installieren Sie die M580-Sicherheitsmodule nur im RIO-Hauptring, der folgende Elemente umfasst:

- Lokales Hauptrack. Standalone-Sicherheits-PACs können ebenfalls bis zu 7 optionale lokale Erweiterungsracks umfassen.
  - Das lokale Hauptrack muss eine Sicherheitsspannungsversorgung, eine Sicherheits-CPU und einen Sicherheits-Koprozessor enthalten.
  - Bei einem Standalone-Sicherheits-PAC können das lokale Hauptrack und die lokalen Erweiterungsracks zudem Sicherheits-E/A umfassen. Ein M580-Hot Standby-PAC bietet keine Unterstützung für E/A im lokalen Hauptrack oder in den lokalen Erweiterungsracks.

    HINWEIS: Die maximale Entfernung zwischen dem Hauptrack und dem letzten Erweiterungsrack beträgt 30 m.
- Bis zu 31 RIO-Stationen für die BME•586040S-CPU, 16 RIO-Stationen für die BME•584040S-CPU, 8 RIO-Stationen für die BME•582040S-CPU, wobei jede Station ein dezentrales Hauptrack und ein optionales dezentrales Erweiterungsrack umfasst.

Jedes Rack mit Sicherheitsmodulen muss darüber hinaus über eine Sicherheitsspannungsversorgung verfügen.

HINWEIS: Ein Rack mit Sicherheitsmodulen kann ebenfalls nicht-störende Module des Typs 1, Seite 17 enthalten. Allerdings dürfen keine nicht-störenden Module des Typs 2, Seite 19 im gleichen Rack wie die Sicherheitsmodule untergebracht werden. Nicht-störende Module des Typs 2 können in Racks ohne Sicherheitsmodule integriert werden – beispielsweise in den Racks der dezentralen Geräte. Andere nicht-sichere Module dürfen nicht in ein M580-Sicherheitssystem aufgenommen werden.

Erweiterung eines Hauptracks

Verwenden Sie Rack-Erweiterungsmodule BMXXBE1000 zur Prioritätsverkettung (Daisy-Chain) von Haupt- und Erweiterungsracks. Jedes Paar Erweiterungsmodule muss mithilfe von Verbindungskabeln BMXXBC•••K angeschlossen und jedes Kettenende mithilfe von Leitungsabschlüssen TSXELYEX abgeschlossen werden.

Kommunikation des lokalen Racks mit einer RIO-Station

Um Unterstützung für RIO-Stationen in einem M580-Sicherheitssystem mit einer CPU-Firmware bis Version 3.10 zu gewährleisten, muss die M580-Sicherheits-CPU als NTP-Server oder NTP-Client (wobei ein anderes Gerät als NTP-Server konfiguriert wird) konfiguriert werden. Ohne ordnungsgemäß eingerichtete Uhr (NTP) funktioniert die Kommunikation mit den Sicherheits-E/A unter Umständen nicht fehlerfrei.

Verwenden Sie ein dezentrales Adaptermodul BM•CRA312•0 (einen Adapter BM•CRA31200 für ein dezentrales Rack mit ausschließlich nicht-störenden Modulen und einen Adapter BM•CRA31210 für ein dezentrales Rack, das nicht-störende und/oder Sicherheits-E/A-Module enthält), um die RIO-Station mit dem RIO-Hauptring zu verbinden. Verbinden Sie jedes Ende des RIO-Hauptrings mit den zwei Dual-Ports der BME•58•040S-Sicherheits-CPU.

Wenn die Verbindung über Cat5e-Kupferkabel hergestellt wird, ist ein Mindestabstand von 100 m zwischen den Stationen einzuhalten.

HINWEIS: Eine andere Möglichkeit ist die Verbindung des lokalen Hauptracks mit dem dezentralen Adapter BM•CRA312•0 in der RIO-Station durch Aufnahme eines Glasfaser-Repeater-Moduls BMXNRP020• in jedes Rack. Zusätzliche Informationen finden Sie unter *Verwenden von Glasfaserkonvertermodulen* im *Modicon M580 Standalone, Systemplanungshandbuch für häufig verwendete Architekturen*.

Verbindung von 2 M580-Sicherheits-PACs

Ein M580-Sicherheitssystem unterstützt ebenfalls eine Peer-to-Peer-Black-Channel-Kommunikation zwischen zwei Sicherheits-PACs. Diese Verbindung wird in der Regel über ein BMENOC0321-Modul in jedem Sicherheitssystem hergestellt. Unter Peer-to-Peer-Kommunikation im *Modicon M580 Sicherheitshandbuch* finden Sie hierzu weitere Informationen.

HINWEIS: Zur Unterstützung der „Black-Channel“-Kommunikation zwischen zwei PACs mit einer CPU-Firmware bis Version 3.10 müssen Sie den NTP-Dienst in beiden PACs aktivieren. Sie können einen PAC als NTP-Server und den anderen als NTP-Client konfigurieren. Oder Sie konfigurieren beide PACs als NTP-Client und ein anderes Gerät als NTP-Server.

Hinzufügen dezentraler Geräte zu einem M580-Sicherheitssystem

Sie können in Ihrem M580-Sicherheitssystem dezentrale Geräte hinzufügen. Dezentrale Geräte werden in der Regel über eine Prioritätsverkettung (Daisy-Chain) mit offenem oder geschlossenem Regelkreis verbunden.

Eine Prioritätsverkettungsschleife (geschlossener Regelkreis) aus dezentralen Geräten wird an die zwei Netzwerk-Ports eines der folgenden Module im RIO-Hauptring angeschlossen:

- Ethernet-Kommunikationsmodul BMENOC0301/11
- Ethernet-Schaltmodul für Netzwerkoptionen BMENOS0300
- ConneXium-Dual-Ring-Switch

Sie können auch den Service-Port eines Ethernet-Kommunikationsmoduls BMENOC0301/11, ein Ethernet-Schaltmodul für Netzwerkoptionen BMENOS0300 oder die BME•58•040S-Sicherheits-CPU für die Verbindung dezentraler Geräte in Form einer Prioritätsverkettung mit offenem Regelkreis verwenden.

HINWEIS: Nehmen Sie ausschließlich nicht-störende Module des Typs 1 und 2 in ein dezentrales Gerätenetzwerk auf. Sicherheitsmodule dürfen nur im lokalen Rack (Haupt- oder Erweiterungsrack) und im RIO-Netzwerk untergebracht werden. Nicht-sichere Module, die keine nicht-störenden Module des Typs 1 oder 2 sind, sind vom Sicherheitsprojekt auszuschließen.

Weitere Informationen zur Verbindung dezentraler Geräte mit einer M580-CPU finden Sie unter *Auswahl der geeigneten Topologie* im *Modicon M580 Standalone, Systemplanungshandbuch für häufig verwendete Architekturen*.

Hinzufügen von CIP Safety-Geräten zum M580 Safety-System

Sie können CIP Safety-E/A-Geräte (CSIO) als verteilte CSIO-Geräte in Ihr M580-Sicherheitssystem einfügen.

Sie können verteilte CSIO-Geräte an den RIO-Hauptring anschließen über:

- den Service-Port einer CPU oder eines BM•CRA31210 X80 EIO-Adaptermoduls.
- ein BMENOS0300 Ethernet-Schaltmodul für Netzwerkoptionen.
- einen ConneXium-Dual-Ring-Switch (DRS).

Jeder Typ von E/A (CSIO, RIO, DIO) weist seine eigene Beschränkung auf. Um ein akzeptables Leistungsniveau aufrechtzuerhalten, empfiehlt es sich, nicht die maximale Anzahl aller E/A-Typen in derselben Architektur zu verwenden.

Eine typische M580 CIP Safety-Architektur sollte möglichst auf einer dezentralen oder verteilten Topologie basieren.

Dezentrale Topologie empfohlene Einschränkungen:

	CSIO-Geräte	**DIO-Geräte**	**RIO-Stationen**
BMEP582040S	10	10	8
BMEP584040S	32	10	16
BMEP586040S	(nb CSIO) + 0,5*(nb DIO) + (nb RIO) ≤ 128		

Verteilte Topologie empfohlene Einschränkungen:

	CSIO-Geräte	**DIO-Geräte**	**RIO-Stationen**
BMEP582040S	16	61	2
BMEP584040S	64	61	2
BMEP586040S	(nb CSIO) + 0,5*(nb DIO) + (nb RIO) ≤ 128		

Der CSIO-Zeitbeitrag zur SAFE-Task umfasst ca. 100 µs/Gerät bei einer BMEP584040S- oder BMEP586040S-CPU und 400 µs/Gerät bei einer BMEP582040S-CPU.

M580-Sicherheitstopologien

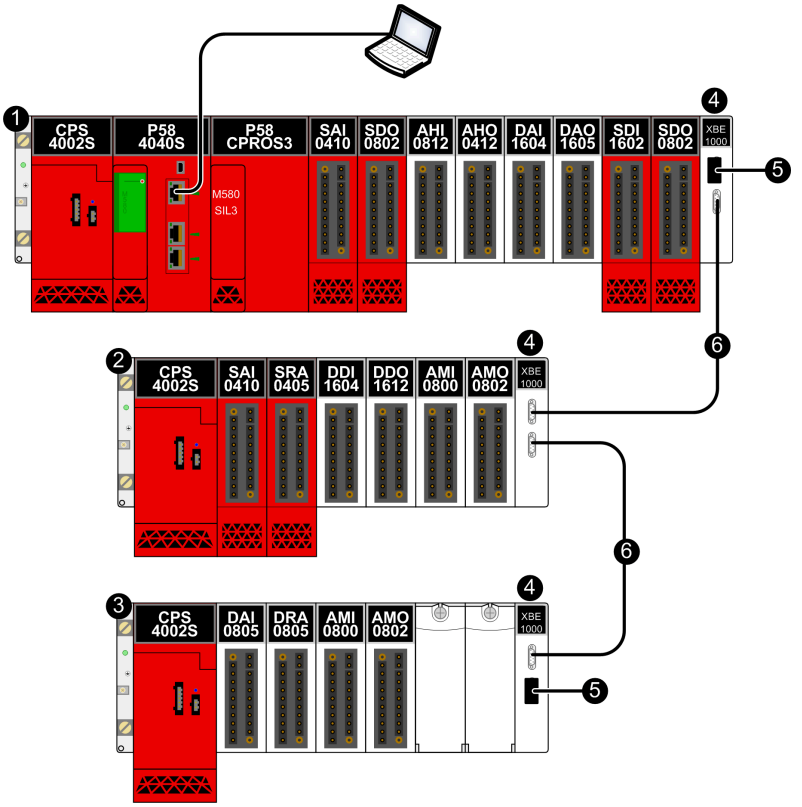
Einführung

Die nachstehenden Abbildungen zeigen Beispiele für M580-Sicherheitstopologien. Diese Beispieltopologien bilden nur einen Teil der von einem M580-Sicherheitssystem unterstützten möglichen Topologien.

Zusätzliche Informationen zur Einrichtung einer M580-Topologie finden Sie in folgenden Handbüchern: *Modicon M580 Standalone, Systemplanungshandbuch für häufig verwendete Architekturen*, *Modicon M580 Systemplanungshandbuch für komplexe Topologien* und *Modicon M580 Hot Standby, Systemplanungshandbuch für häufig verwendete Architekturen*.

Erweiterung des lokalen Hauptracks

Die nachstehende Abbildung zeigt ein lokales Hauptrack mit zwei Erweiterungsracks. Beachten Sie, dass das M580-Sicherheitssystem ein einzelnes lokales Rack sowie bis zu 7 Erweiterungsracks über eine maximale Länge von 30 m unterstützt:



1 Lokales Hauptrack mit Sicherheits- und nicht-störenden Modulen des Typs 1

2 Lokales Erweiterungsrack mit Sicherheits- und nicht-störenden Modulen des Typs 1

3 Lokales Erweiterungsrack mit nicht-störenden Modulen des Typs 1

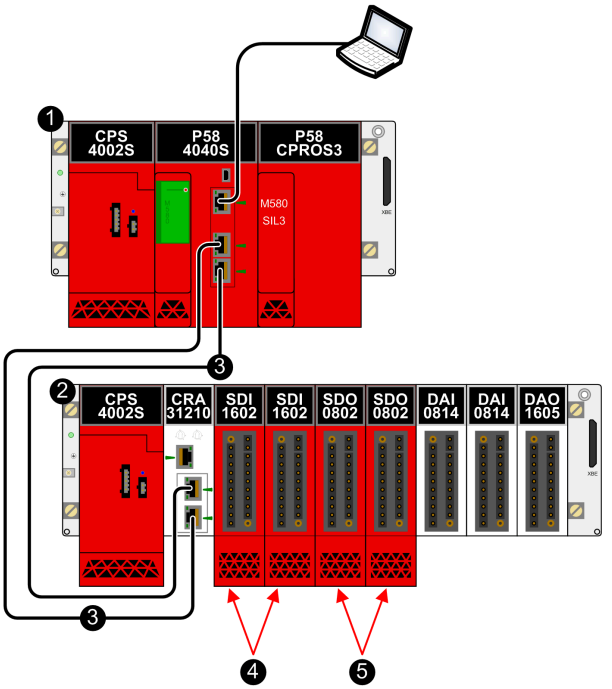
4 BMXXBE1000-Rack-Erweiterungsmodule

5 TSXELYEX-Leitungsabschlüsse

6 BMXXBC•••K-Verbindungskabel

E/A-Topologien mit hoher Verfügbarkeit

Die nachstehende Abbildung zeigt ein Beispiel für redundante E/A in derselben RIO-Station:



1 Lokales Hauptrack

2 RIO-Station

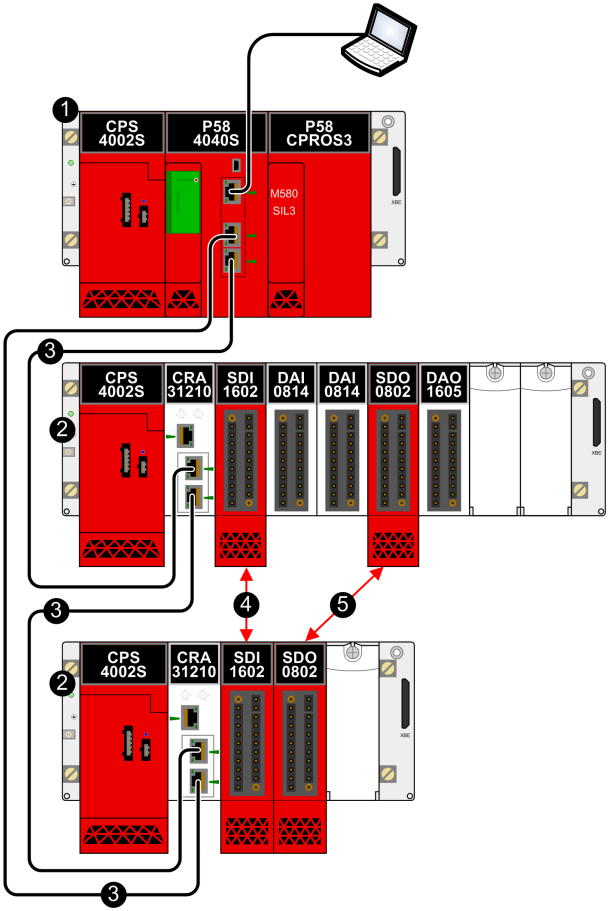
3 RIO-Hauptring

4 Zwei redundante Eingangsmodule in derselben RIO-Station

5 Zwei redundante Ausgangsmodule in derselben RIO-Station

HINWEIS: Bei einer CPU-Firmware bis Version 3.10 müssen Sie den NTP-Dienst für den M580-Sicherheits-PAC aktivieren, um die „Black-Channel“-Kommunikation zwischen dem lokalen Hauptrack und den RIO-Stationen im RIO-Hauptring zu unterstützen, und die Zeit im PAC konfigurieren, wenn der PAC als NTP-Server fungieren soll. Der Sicherheits-PAC kann entweder als NTP-Server oder als NTP-Client konfiguriert werden (in letzterem Fall wird ein anderes Gerät als NTP-Server konfiguriert).

Die nachstehende Abbildung zeigt ein Beispiel für die Integration redundanter E/A in 2 separate RIO-Stationen:



1 Lokales Hauptrack

2 RIO-Station

3 RIO-Hauptring

4 Zwei redundante Eingangsmodule in separaten RIO-Stationen

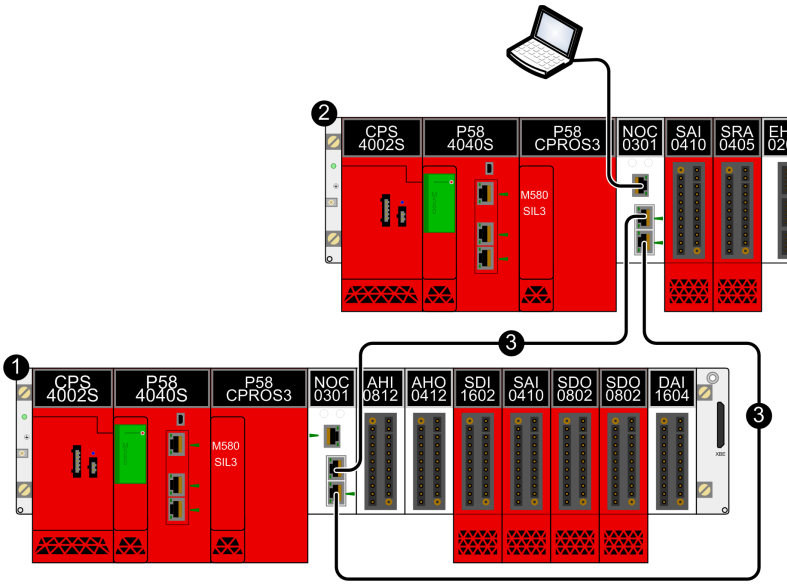
5 Zwei redundante Ausgangsmodule in separaten RIO-Stationen

HINWEIS:

- Schneider Electric empfiehlt die Installation redundanter E/A-Sicherheitsmodule in separaten RIO-Stationen.
- Bei einer CPU-Firmware bis Version 3.10 müssen Sie den NTP-Dienst für den M580-Sicherheits-PAC aktivieren, um die „Black-Channel“-Kommunikation zwischen dem lokalen Hauptrack und den RIO-Stationen im RIO-Hauptring zu unterstützen. Der Sicherheits-PAC kann entweder als NTP-Server oder als NTP-Client konfiguriert werden (in letzterem Fall wird ein anderes Gerät als NTP-Server konfiguriert).

Peer-to-Peer-Topologie für 2 Standalone-Sicherheits-PACs

Die nachstehende Abbildung zeigt ein Beispiel für die Verbindung 2 separater M580-Sicherheits-PACs. In diesem Beispiel kann ein mit einem Sicherheitseingangsmodul im PAC 1 verbundener Sensor konfiguriert werden, um eine Reaktion eines mit einem Sicherheitsausgangsmodul im PAC 2 verbundenen Stellglieds auszulösen:



1 Standalone M580-Sicherheits-PAC 1

2 M580-Sicherheits-PAC 2

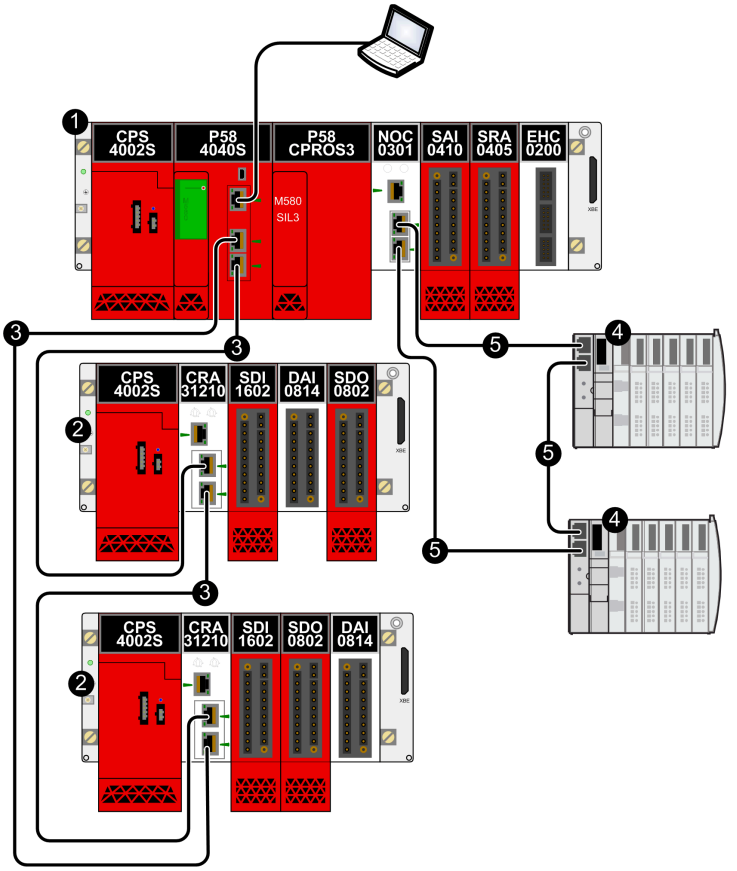
3 „Black-Channel“-Kommunikation zwischen PACs

HINWEIS: Zur Unterstützung der „Black-Channel“-Kommunikation zwischen zwei PACs mit einer CPU-Firmware bis Version 3.10 müssen Sie den NTP-Dienst in beiden PACs aktivieren. Sie können einen PAC als NTP-Server und den anderen als NTP-Client konfigurieren. Oder Sie konfigurieren beide PACs als NTP-Client und ein anderes Gerät als NTP-Server.

Hinzufügen verteilter Geräte zum M580-Sicherheits-PAC

Sie können Ihrem M580-Sicherheitsprojekt nicht-störende Module des Typs 1 und 2 als verteilte Geräte in einer Prioritätsverkettung (Daisy-Chain) mit offenem oder geschlossenem Regelkreis hinzufügen.

Die nachstehende Abbildung zeigt ein Beispiel für verteilte Geräte, die in einer Prioritätsverkettung im offenen Regelkreis hinzugefügt wurden. In diesem Beispiel werden die verteilten Geräte in einer Prioritätsverkettung über die ETH2- und ETH3-EIO-Ports eines Ethernet-Kommunikationsmoduls BMENOC0301/11 mit dem PAC verbunden:



1 Lokales Hauptrack mit Ethernet-Baugruppenträger

2 RIO-Station mit Sicherheitsmodulen und nicht-störenden Modulen des Typs 1

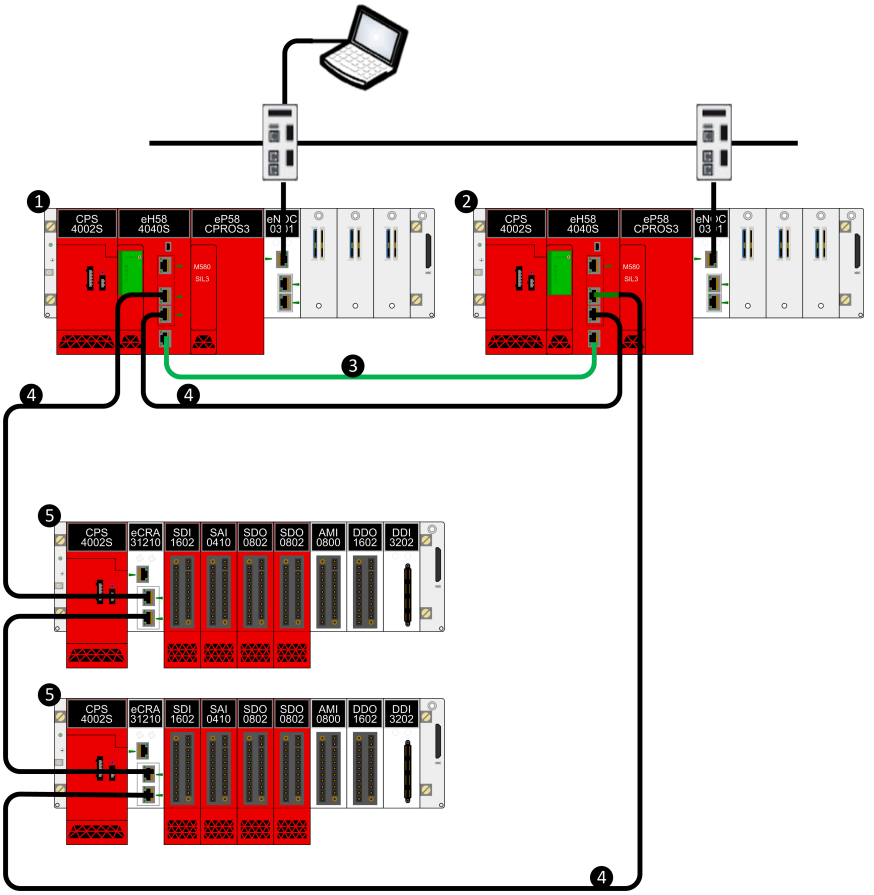
3 RIO-Hauptring

4 Verteilte Geräte

5 Ring mit verteilten Geräten

Hot Standby-Topologie

Die nachstehende Abbildung zeigt eine Hot Standby-Topologie:



1 Primäres lokales Rack mit primärer CPU

2 Lokales Standby-Rack mit Standby-CPU

3 Hot Standby-Kommunikationsverbindung

4 Ethernet-RIO-Hauptring

5 (e)X80 RIO-Station

CPU und Koprozessor des M580-Sicherheitssystems

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die CPUs BME•58•040S und der Koprozessor BMEP58CPROS3 (Kopro) beschrieben.

Physische Merkmale von CPU und Koprozessor eines M580-Sicherheitssystems

Einführung

In diesem Abschnitt werden die gemeinsamen physischen Merkmale der CPUs BME•58•040S und des Koprozessors (Kopro) BMEP58CPROS3 beschrieben.

Physische Beschreibung der M580 Sicherheits-CPU und des Koprozessors

Position im lokalen Rack

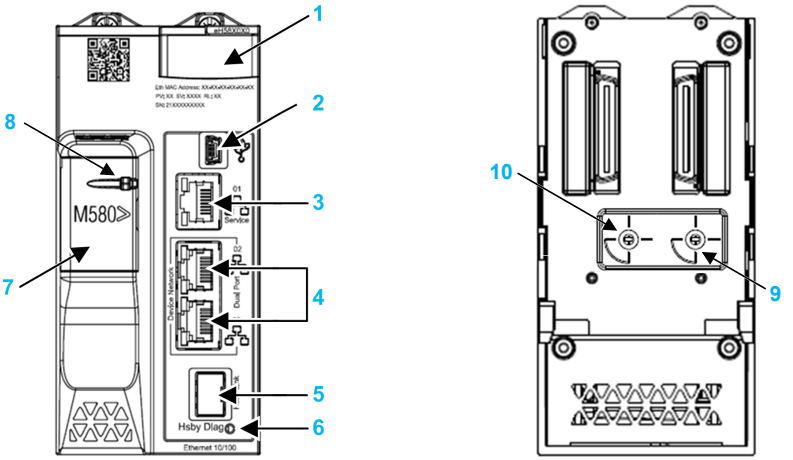
Jedes M580-Standalone-SIL3-Sicherheitssystem benötigt eine BME•58•040S-CPU und einen BMEP58CPROS3-Koprozessor (Kopro). Für die CPU sind zwei Modulsteckplätze erforderlich. Sie wird in den Steckplätzen 0 und 1 direkt rechts neben der Spannungsversorgung im lokalen Hauptrack installiert. Der Koprozessor benötigt ebenfalls zwei Modulsteckplätze und wird in den Steckplätzen 2 und 3 direkt rechts neben der CPU untergebracht. Weder die Sicherheits-CPU (CPU) noch der Kopro darf in anderen Steckplätzen oder in anderen Racks installiert werden. Wenn in der Konfiguration des lokalen Racks Erweiterungsracks vorhanden sind, weisen Sie die dem Rack mit CPU und Kopro (00) die Adresse CPU and Copro zu.

HINWEIS: Sicherheits-CPU und Kopro dürfen nur in einem Ethernet-Rack BMEXBP•••• installiert werden. Eine Beschreibung der verfügbaren M580-Racks finden Sie unter *Lokale und dezentrale Racks* im *Modicon M580 Hardware-Referenzhandbuch*.

Vorder- und Rückansicht der CPU

Die BME•58•040S-Sicherheits-CPU unterstützt sowohl eine RIO- als auch eine DIO-Abfrage.

Physische Merkmale der CPU:



Legende:

1 LED-Diagnoseanzeigetafel

2 Mini-B USB-Anschluss für die Modulkonfiguration mit einem PC, auf dem Control Expert läuft

3 RJ45-Ethernet-Service-Anschlussstecker

4 RJ45-Stecker, die zusammen als dualer Anschluss zum Ethernet-Netzwerk fungieren

5 SFPSFP-Steckbuchse für Hot Standby-Verbindungen aus Kupfer oder Glasfaser

6 Hot Standby-Statusverbindung-LED

7 SD-Speicherkartensteckplatz (hinter der Tür)

8 SD-Speicherkarte, verriegelbare Tür

9 Drehschalter der Betriebsart, mit den Einstellungen **Communication Security Reset**, **Secured**, **Standard**

> **HINWEIS:** Der Drehwahlschalter der Betriebsart wird für zukünftige Produktversionen betriebsbereit gemacht. Für diese Produktversion wird die Betriebsart unabhängig von der Schalterposition automatisch auf **Standard** eingestellt.

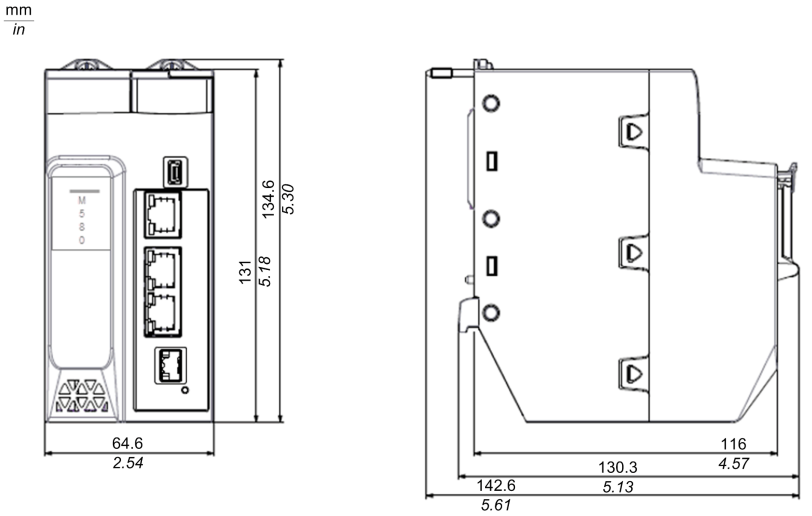
10 A/B/Löschen-Drehwahlschalter, der verwendet wird, um den PAC entweder als PAC A oder PAC B zu bestimmen oder um die bestehende Control Expert-Anwendung zu löschen.

Koprozessor-Frontplatte

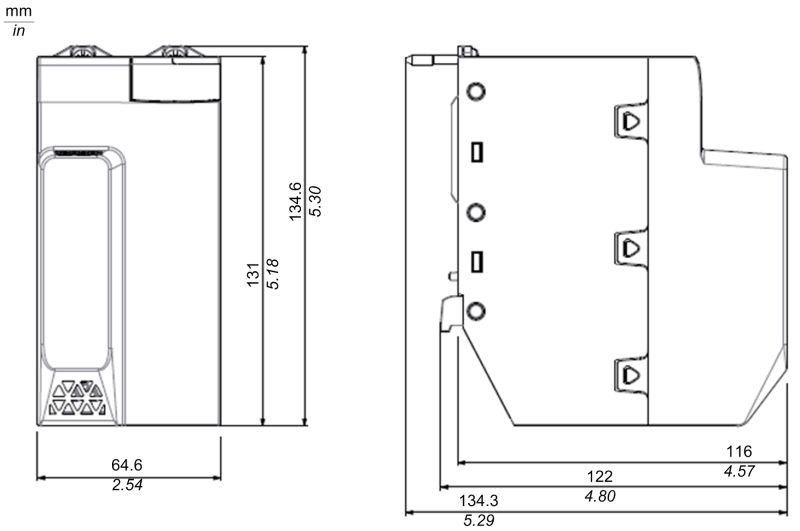
Der BMEP58CPROS3-Koprozessor verfügt nur über eine LED-Anzeige an seiner Frontplatte.

Abmessungen von CPU und Koprozessor

Für die Sicherheits-CPU BME•58•040S gelten folgende physischen Abmessungen:



Für den BMEP58CPROS3-Koprozessor gelten folgende physischen Abmessungen: Im Gegensatz zur CPU ist der Koprozessor nicht mit physischen Steckanschlüssen oder entsprechenden Beschriftungen ausgestattet.

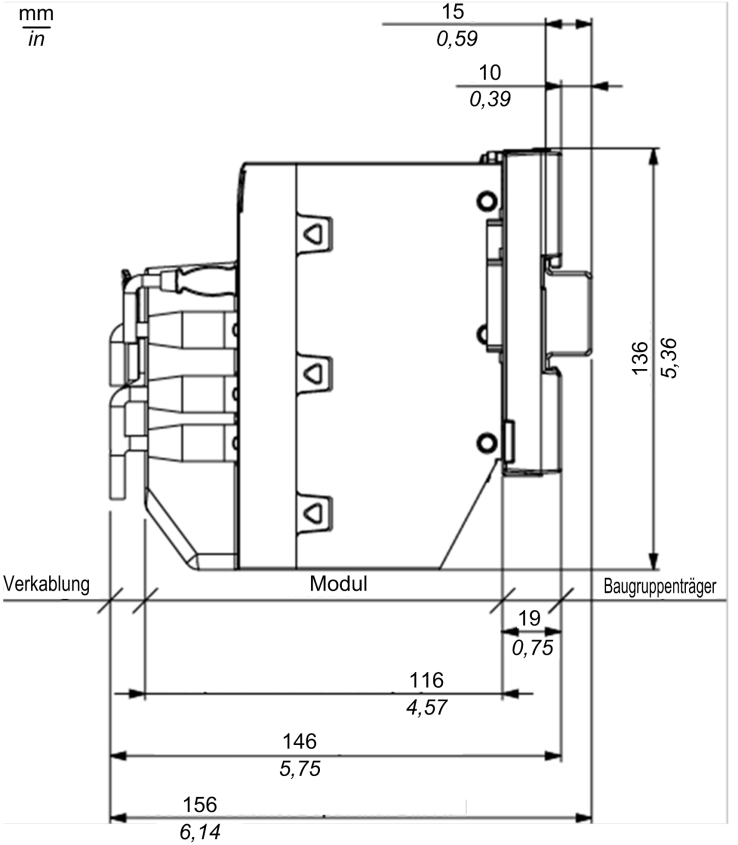


HINWEIS: Bei der Planung der Installation des lokalen Racks ist die Höhe der CPU und des Koprozessors zu berücksichtigen. Sowohl die CPU als auch der Koprozessor stehen um folgende Länge über den unteren Rand des Racks hervor:

- 29,49 mm für ein Ethernet-Rack
- 30,9 mm für ein X Bus-Rack

Abmessungen der CPU-Verkabelung

Für die Sicherheits-CPUs BME•58•040S gelten bei einer DIN-Schienenmontage mit Verkabelung folgende Abmessungen:

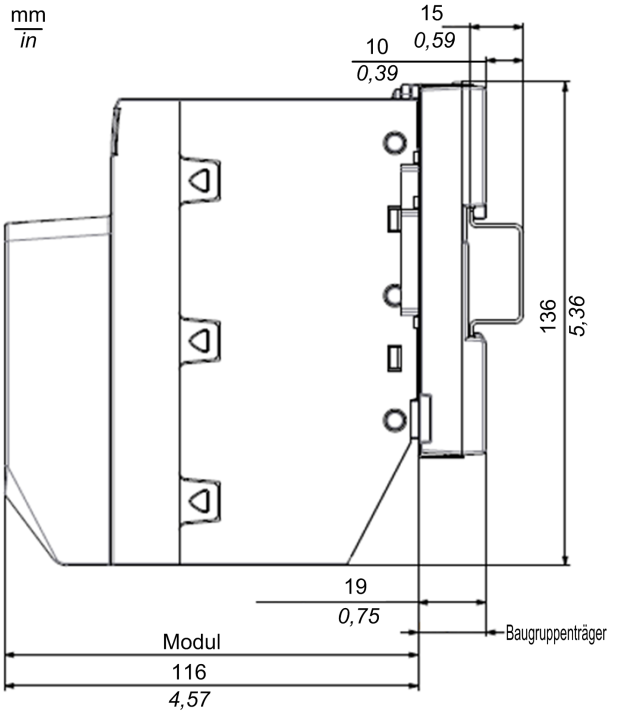


Globale Tiefe für die CPU:

- 146 mm mit Verkabelung
- 156 mm mit Verkabelung und DIN-Schiene

Abmessungen der Koprozessor-Verkabelung

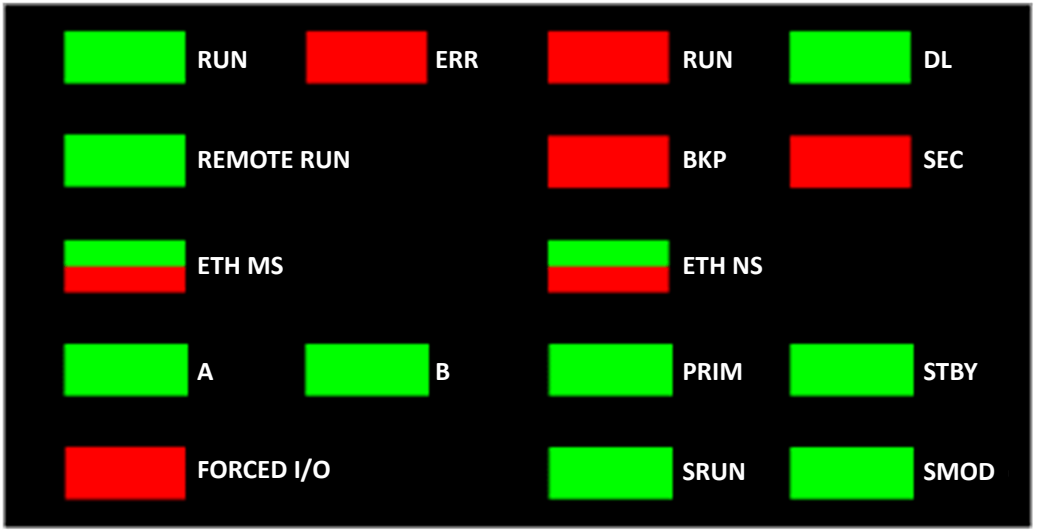
Für den BMEP58CPROS3-Koprozessor gelten folgende Abmessungen bei einer DIN-Schienenmontage:



LED-Anzeigen für die M580 Sicherheits-CPU und den Koprozessor

LED-Anzeige der CPU (LED Display)

Eine LED-Anzeige befindet sich an der Frontplatte der CPU:



HINWEIS: Die **SEC**-LED, die den sicheren Kommunikationsstatus anzeigt, ist für diese Version nicht implementiert.

HINWEIS: Das LED-Display des Koprozessors entspricht einer Teilgruppe des CPU-Displays und umfasst folgende LED-Anzeigen:

- **ERR**
- **DL**
- **SRUN**
- **SMOD**

LED Beschreibung

HINWEIS: Siehe folgende Themen:

- Informationen zur Verwendung der LED-Anzeigen von CPU und Koprozessor für die Diagnose des Zustands des Sicherheits-PAC finden Sie unter *Diagnose-LEDs der M580-Sicherheits-CPU* und *Diagnose-LEDs des M580-Koprozessors* im *Modicon M580 Sicherheitshandbuch*.
- Informationen zur Verwendung der LED-Anzeigen der Hot Standby-CPU **A**, **B**, **PRIM**, **STBY** und **REMOTE RUN** finden Sie unter *LED-Diagnose für M580 Hot Standby-CPUs* im *Modicon M580 Hot Standby Systemplanungshandbuch für häufig verwendete Architekturen*.

LED Anzeige	Gilt für ...		Beschreibung
	CPU	Kopro	
RUN	✓	–	**EIN**: Die CPU verwaltet ihre Ausgänge und mindestens eine Task befindet sich im RUN-Zustand.
ERR	✓	✓	**EIN**: Die CPU hat einen internen CPU-Fehler erkannt (z. B. keine Konfiguration, Watchdog-Fehler, Selbsttest-Fehler).
I/O	✓	–	**EIN**: Die CPU hat einen CPU-externen Fehler in einem oder mehreren E/A-Modulen erkannt.
DL (*Herunterladen*)	✓	+	• **EIN**: Eine Firmwareaktualisierung für CPU, Koprozessor, Baugruppenträger oder andere rackinterne Module wird durchgeführt. • **AUS**: Es wird keine Firmware-Aktualisierung durchgeführt.
BACKUP	✓	–	**EIN**: • Speicherkarte oder CPU-Flash-Speicher fehlt oder ist nicht funktionsfähig. • Die Speicherkarte ist unbrauchbar (ungültiges Format, unbekannter Typ). • Inhalt der Speicherkarte oder des CPU-Flash-Speichers ist nicht kohärent mit der aktuellen Anwendung. • Speicherkarte wurden entnommen und wieder eingesetzt • Ein Befehl **SPS > Projekt-Backup... > Löschen** wurde ausgeführt, obwohl keine Speicherkarte vorhanden ist. Die LED **BACKUP** bleibt **EIN**, bis das Projekt erfolgreich gesichert wurde. **AUS**: Inhalt der Speicherkarte oder des Flash-Speichers der CPU ist gültig und die Anwendung im Ausführungsspeicher ist identisch.
ETH MS	✓	–	MOD STATUS (grün/rot): Das Muster gibt den Konfigurationsstatus des Ethernet-Ports an. **HINWEIS:** Bei Erkennung eines behebbaren Fehlers kann die LED **ETH MS** grün oder rot aufleuchten und ein- oder ausgeschaltet sein.
ETH NS	✓	–	NET STATUS (grün/rot): Das Muster gibt den Ethernet-Verbindungsstatus an.

LED Anzeige	Gilt für ...		Beschreibung
	CPU	Kopro	
FORCED I/O	✓	–	**EIN**: Mindestens ein Ein- oder Ausgang eines digitalen E/A-Moduls ist forciert.
SRUN	✓	✓	**EIN**: Der PAC verwaltet seine Sicherheitsausgänge und die SAFE-Task befindet sich im RUN-Zustand.
SMOD	✓	✓	• **EIN**: Der PAC läuft im Sicherheitsmodus, Seite 117. • **BLINKEN**: Der PAC läuft im Wartungsmodus, Seite 118.
✓: Gilt – : Nicht anwendbar.			

Ethernet-Ports

Einführung

An der Frontseite des CPUsind drei RJ45-Ethernet-Ports verfügbar: Ein Service-Port und zwei Gerätenetzwerk-Ports (Device Network). Die Ports weisen gemeinsame Merkmale auf, die im Folgenden beschrieben werden.

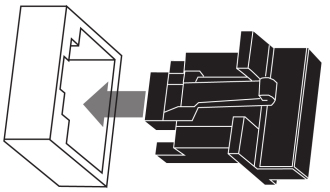
Gemeinsame Merkmale

Alle drei Ports verfügen über denselben RJ45-Anschluss und verwenden denselben Typ von Ethernet-Kabeln.

HINWEIS: Die drei Ethernet-Ports sind mit der Gehäuseerdung verbunden, und für das System ist eine äquipotenziale Erdung erforderlich.

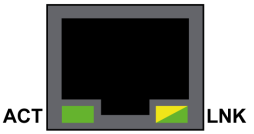
Staubschutz

Um ein Eindringen von Staub in die nicht verwendeten Ethernet-Ports zu verhindern, decken Sie die Ports mit Verschlüssen ab:

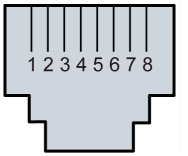


Ethernet-Ports

Jeder RJ45-Anschluss ist mit einem Paar LED-Anzeigen ausgestattet:



Pin-Positionen, Pinbelegung und Kabelanschlüsse sind für alle drei RJ45-Ethernet-Ports identisch:

Stift	Beschreibung	
1	TD+	Anschlussbelegung: 
2	TD-	
3	RD+	
4	nicht verbunden	
5	nicht verbunden	
6	RD-	
7	nicht verbunden	
8	nicht verbunden	
—	Shell-/Gehäuseerdung	

HINWEIS: Die TD-Stifte (1 und 2) und die RD-Stifte (3 und 6) sind Auto-MDIX-fähig und kehren ihre Rolle je nach verbundenem Medium (d. h. gerade oder gekreuzte Kabel) automatisch um.

Die Ports verfügen über eine Auto-MDIX-Funktion, die automatisch die Übertragungsrichtung erkennt.

Treffen Sie unter den folgenden Ethernet-Kabeln eine Auswahl für den Anschluss an die Ethernet-Ports:

- TCSECN3M3M••••: Ethernet-Straight-Through-Kabel Cat 5E, für den Einsatz in industriellen Anwendungen, CE- oder UL-konform
- TCSECE3M3M••••: Ethernet-Straight-Through-Kabel Cat 5E, für den Einsatz in industriellen Anwendungen, CE-konform
- TCSECU3M3M••••: Ethernet-Straight-Through-Kabel Cat 5E, für den Einsatz in industriellen Anwendungen, UL- oder -konform

Die maximale Länge für ein Kupferkabel beträgt 100 m. Bei Entfernungen über 100 m ist ein Glasfaserkabel zu verwenden. Die CPU ist mit keinen Glasfaserports ausgestattet. Nach Bedarf können Sie Dual-Ring-Switches oder BMX NRP ••••-Glasfaserkonvertermodule

(siehe Modicon M580 Standalone, Systemplanungshandbuch für, häufig verwendete Architekturen) einsetzen, um den Übergang von Kupfer- zu Glasfaserkabeln zu verwalten.

Ethernet-Ports in eigenständigen CPUs (Standalone-Betrieb)

Bei Standalone-CPUs ist die **ACTIVE**-LED grün. Die LED-**LNK** ist entweder grün oder gelb, je nach Status:

LED	LED-Status	Beschreibung
ACTIVE	AUS	Am Ethernet-Anschluss wird keine Aktivität angezeigt.
	EIN/Blinken	Über die Ethernet-Verbindung werden Daten übertragen und empfangen.
LNK	AUS	Über diese Leitung wurde keine Verbindung hergestellt.
	EIN Grün	Über diese Leitung wurde eine 100-Mbit/s-Verbindung* hergestellt.
	EIN Gelb	Über diese Leitung wurde eine 10-Mbit/s-Verbindung* hergestellt.
* Die 10/100-Mbit/s-Verbindungen unterstützen eine Datenübertragung und Autonegotiation sowohl im Halb- als auch im Vollduplexmodus.		

Service-Port

Der Service-Port ist derjenige der drei Ethernet-Ports, die sich ganz oben an der Frontseite der CPU befinden. Dieser Port dient folgenden Zwecken:

- Bereitstellung eines Zugriffspunkts, den andere Geräte oder Systeme zur Überwachung oder Kommunikation mit der M580-CPU verwenden können.
- Verwendung als eigenständiger DIO-Port, der eine Stern- oder Prioritätsverkettungstopologie mit verteilten Geräten unterstützt.
- Spiegelung der CPU-Ports für die Ethernet-Diagnose. Als Service-Tool zur Anzeige der Aktivität am gespiegelten Port kann ein PC oder ein HMI-Gerät verwendet werden.

  HINWEIS: Verwenden Sie den Service-Port nicht zur Anbindung an das Gerätenetzwerk, es sei denn unter ganz spezifischen Bedingungen gemäß der Beschreibung in folgendem Handbuch: *Modicon M580, Open Ethernet Network, System Planning Guide*.

  Der Service-Port bietet möglicherweise nicht die volle Leistung und nicht alle Funktionen, die von den **Gerätenetzwerk**-Ports der CPU bereitgestellt werden.

  Die Verbindung des Service-Ports, ob direkt oder über einen Switch/Hub, mit dem Gerätenetzwerk kann sich negativ auf die Systemleistung auswirken.

Gerätenetzwerk-Dual-Ports

Sie können einen **Device Network**-Port zur Unterstützung einer Stern- oder Prioritätsverkettungstopologie mit verteilten Geräten verwenden. Verwenden Sie beide **Device Network**-Ports zur Unterstützung einer Ringtopologie.

Bei einer Verwendung als RIO-Ports verbinden beide Ports die CPU mit dem Hauptring in einer Ethernet-Prioritätsverkettungsschleife.

Weitere Informationen zu RIO/DIO-Architekturen finden Sie im Kapitel *Modicon M580-System* (siehe Modicon M580 Standalone, Systemplanungshandbuch für, häufig verwendete Architekturen).

Hinweise zur Erdung

Befolgen Sie alle landesspezifischen und örtlichen Sicherheitsnormen und -vorschriften.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS

Wenn Sie nicht mit Sicherheit feststellen können, dass das Ende eines geschirmten Kabels örtlich geerdet ist, muss das Kabel als gefährlich eingestuft und es muss angemessene persönliche Schutzausrüstung (PSA) getragen werden.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

USB-Port

Einführung

Der USB-Port ist ein hochgeschwindigkeitsfähiger, Mini-B-USB-Anschluss, Version 2.0 (480 Mbps) , der für ein Control Expert-Programm oder eine Mensch-Maschine-Schnittstelle (HMI) verwendet werden kann. Der USB-Port kann an einen anderen USB-Port, Version 1.1 oder höher angeschlossen werden.

HINWEIS: Installieren Sie die M580-USB-Treiber, bevor Sie die USB und den CPU über ein PC-Kabel miteinander verbinden.

Transparenz

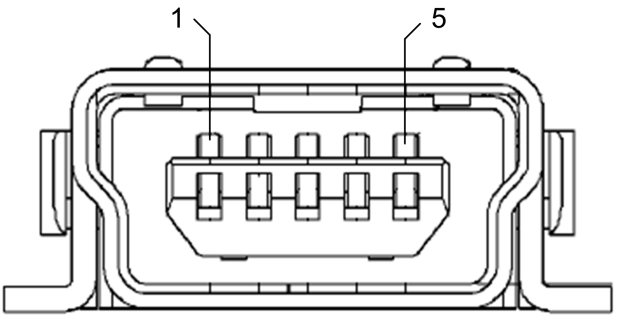
Wenn für Ihr System Transparenz zwischen dem an den USB-Port angeschlossenen Gerät und dem M580-Gerätenetzwerk erforderlich ist, müssen Sie in der Routing-Tabelle des Geräts eine persistente statische Route hinzufügen.

Beispiel für einen Befehl zur Adressierung eines Gerätenetzwerks mit der IP-Adresse `X.X.0.0` (für einen Windows-PC): `route add X.X.0.0 mask 255.255.0.0 90.0.0.1 -p`

(In diesem Fall entspricht `X.X.0.0` der vom M580-Gerätenetzwerk verwendeten Netzwerkadresse, `255.255.0.0` ist die zugehörige Teilnetzmaske).

Pinbelegung

Der USB-Anschluss verfügt über die folgenden Pinpositionen und entsprechender Pinbelegung:



Legende:

Pin	Beschreibung
1	VBus
2	D-
3	D+
4	Nicht angeschlossen
5	Erde
Shell	Gehäuseerdung

Kabel

Verwenden Sie ein BMX XCA USB H018- (1,8 m/5,91 ft) oder BMX XCA USB H045-Kabel (4,5 m/14,764 ft), um das Panel an die CPU anzuschließen. (Diese Kabel sind mit einem Anschlussstecker vom Typ A an einer Seite und einem mini-B-USB-Anschluss an der anderen Seite ausgestattet).

Wenn eine feste Baugruppe mit einer Konsole des Typs XBT mit der CPU verbunden wird, schließen Sie das USB-Kabel an die Schutzschiene (siehe Modicon X80, Racks und Spannungsversorgungen, Hardware-Referenzhandbuch) an. Verwenden Sie den freigelegten Schirmungsteil oder die Metalllasche am BMX XCA-Kabel zur Herstellung der Verbindung.

SFP-Steckbuchse

Redundanter Verbindungsport

Jedes Hot Standby-CPU-Modul verfügt über eine SFP-Steckbuchse, an die entweder ein Kupfer- oder ein Glasfaser-Transceiver angeschlossen werden kann:

Informationen zur Installation und Deinstallation einer SFP-Steckbuchse sowie eine Liste der verfügbaren SFP-Transceiver finden Sie im *Modicon M580 Hot Standby Systemplanungshandbuch für häufig verwendete Architekturen*.

SD-Speicherkarte

SD-SpeicherkarteBMXRMS004GPF

Bei der BMXRMS004GPF-Speicherkarte handelt es sich um eine Karte mit 4 GB der Klasse 6 für industrielle Anwendungen. Der Steckplatz für die SD-Speicherkarte befindet sich hinter der Tür an der Frontseite der CPU.

Sie können die BMXRMS004GPF-Speicherkarte zur Speicherung von Anwendungen und Daten heranziehen.

Auf der BMXRMS004GPF-Speicherkarte können folgende Elemente gespeichert werden:

- M580-Sicherheitsprojekt-Anwendung
- Daten für nicht-sichere Tasks (MAST, FAST, AUX0, AUX1)

HINWEIS:

- Für die SAFE-Task können keine Daten auf der SD-Speicherkarte abgelegt werden.
- Die SD-Speicherkarte ist nicht in die Sicherheitsschleife integriert.

Sie können die Karte bei eingeschalteter Spannungsversorgung und mit dem PAC im RUN-Betrieb einführen und entnehmen. Um Datenverlust zu vermeiden, sollte jedoch das Systembit %S65 verwendet werden, um einen Systemrequest zum Stopp des Datenzugriffs auf die Karte auszugeben, bevor die Karte aus der CPU entnommen wird.

HINWEIS: Andere Speicherkarten, wie diejenigen, die in M340-CPUs zum Einsatz kommen, sind mit den M580-CPUs nicht kompatibel. Beim Einstecken einer inkompatiblen SD-Speicherkarte in die CPU geschieht Folgendes:

- Die CPU verbleibt im Zustand NOCONF (siehe Modicon M580, Hardware, Referenzhandbuch).
- Die CPU-LED-**BACKUP** leuchtet auf.
- Die LED für den Speicherkartenzugriff blinkt.

Die BMXRMS004GPF-Speicherkarte wurde speziell für dieM580-CPUs formatiert. Wenn Sie diese Karte mit einer anderen CPU oder einem anderen Tool verwenden, wird die Karte unter Umständen nicht erkannt.

Eigenschaften der Speicherkarte

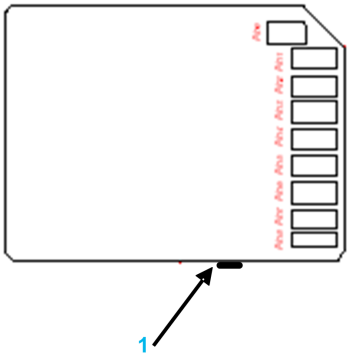
Die BMXRMS004GPF-Speicherkarte weist folgende Eigenschaften auf:

Merkmal	Wert
Globale Speichergröße	4 GB
Größe der Anwendungssicherung	200 MB
Größe der Datenspeicherung	3,8 GB
Schreib-/Löschzyklen (typisch)	100.000
Betriebstemperatur	-40...+85 °C (-40...+185 °F)
Dauer der Dateispeicherung	10 Jahre
Speicherbereich für FTP-Zugriff	Nur Datenspeicherverzeichnis

HINWEIS: Aufgrund von Formatierung, Abnutzung und anderen internen Mechanismen ist die tatsächlich verfügbare Kapazität der Speicherkarte etwas geringer als ihre globale Größe.

Lesen/Schreiben-Kartenschalter

Die BMXRMS004GPF-Speicherkarte ist an der nicht abgeschrägten Kante mit einem Schalter für den Lese-/Schreibzugriff ausgestattet, die Sie zum Schutz der Karte vor unberechtigtem Schreibzugriff heranziehen können:



1 Schalter für Lese-/Schreibzugriff

Formatieren der Speicherkarte

Der Formatierungsvorgang wird im Abschnitt *Formatieren der Speicherkarte* im Handbuch der *EcoStruxure™ Control Expert Systembausteinbibliothek* beschrieben.

Sicherheitsetiketten und verriegelbare SD-Kartentür

Sicherheitsetiketten

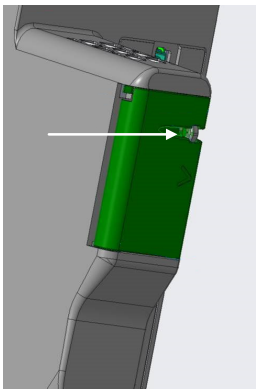
Auf der rechten Seite der Standalone- und Hot Standby M580-CPUs befinden sich zwei Sicherheitsetiketten zum Schutz vor Manipulation, wobei die Einfassung (d. h. der vordere Bereich des Modulcontainers) mit dem Gehäuse verbunden wird (d. h. der hintere Abschnitt des Modulcontainers). Diese Etiketten zeigen an, ob das Modul geöffnet und möglicherweise manipuliert wurde.

Der Modulcontainer wurde nicht geöffnet, wenn die Sicherheitsetiketten wie folgt aussehen:

Der Modulcontainer wurde geöffnet, wenn die Sicherheitsetiketten wie folgt aussehen:

Verriegelbare SD-Kartentür

Die Tür, die den SD-Kartensteckplatz abdeckt, kann verriegelt oder verplombt werden.



Gehen Sie dazu wie folgt vor:

1. Schließen Sie die SD-Kartentür.

2. Führen Sie das Drahtende einer Plombe (oder das Kabel eines Vorhängeschlosses) durch das Loch im Teil, das durch die SD-Kartentür herausragt.

   HINWEIS: Sie können einen Draht oder ein Kabel mit einem maximalen Durchmesser von 1,50 mm verwenden.

3. Schließen Sie die Plombe (oder verriegeln Sie das Vorhängeschloss).

HINWEIS: Die Plombe oder das Vorhängeschloss sind nicht im Lieferumfang des Moduls enthalten.

Leistungsmerkmale von CPU und Koprozessor eines M580-Sicherheitssystems

Einführung

In diesem Abschnitt werden die Leistungsmerkmale der CPU BMEP584040S und des Koprozessors (Kopro) BMEP58CPROS3 beschrieben.

Leistungsmerkmale von M580 CPU und Koprozessor

CPU und Koprozessor des Sicherheitssystems

Die CPU BME•58•040S und der Koprozessor BMEP58CPROS3 (Kopro) stellen folgende Leistungsmerkmale in einer SIL3-M580-Sicherheitslösung bereit:

Leistungsmerkmal		**BME**					
		P582040S	**P584040S**	**P586040S**	**H582040S**	**H584040S**	**H586040S**
Lokale Racks		4 (1 Hauptrack + bis zu 3 Erweiterungsracks)	8 (1 Hauptrack + bis zu 7 Erweiterungsracks)	8 (1 Hauptrack + bis zu 7 Erweiterungsracks)	1	1	1
RIO-Stationen (max. 2 Racks/ Station: Hauptrack + Erweiterungsrack)		8 Stationen (bis zu 2 Racks pro Station)	16 Stationen (bis zu 2 Racks pro Station)	31 Stationen (bis zu 2 Racks pro Station)	8 Stationen (bis zu 2 Racks pro Station)	16 Stationen (bis zu 2 Racks pro Station)	31 Stationen (bis zu 2 Racks pro Station)
E/A-Kanäle	Digitale E/A	2048	4096	6144	0[1]	0[1]	0[1]
	Analoge E/A	512	1024	1536	0[1]	0[1]	0[1]
	Experte	72	144	216	0[1]	0[1]	0[1]
Ethernet-Ports	Baugruppenträger	1	1	1	1	1	1
	Dienst	1	1	1	1	1	1
	RIO	2	2	2	2	2	2
Steuerungsnetzwerk	Max. Anzahl Module/ Geräte	64	128	128	64	128	128
	Max. Eingangskapazität	16 KB	24 KB	24 KB	16 KB	24 KB	24 KB

Leistungsmerkmal		BME					
		P582040S	P584040S	P586040S	H582040S	H584040S	H586040S
	Max. Ausgangskapazität	16 KB	24 KB	24 KB	16 KB	24 KB	24 KB
	Max. FAST-Eingangskapazität	3 KB	5 KB	5 KB	3 KB	5 KB	5 KB
	Max. FAST-Ausgangskapazität	3 KB	5 KB	5 KB	3 KB	5 KB	5 KB
Verteiltes Geräte-netzwerk	Max. Anzahl Module/ Geräte	61	61	61	61	61	61
	Max. Eingangskapazität	2 KB	8 KB	8 KB	2 KB	2 KB	2 KB
	Max. Ausgangskapazität	2 KB	8 KB	8 KB	2 KB	2 KB	2 KB
	Max. CIP Safety-Geräte	16	64	128	–	–	–
	Max. CIP Safety-Verbindungen	32	128	256	–	–	–
Ethernet-Kommuni-kations-module im lokalen Rack	Max. Ethernet-Kommunikationsmo-dule	2	4	4	2	4	4
	Max. BMENOC0301/ 0311	2	3	3	2	3	3
	Max. BMENOC0321	2	2	2	2	2	2
Speicher-zuweisung (max.)	Nicht-sicheres Anwendungspro-gramm	8 MB	16 MB	64 MB[4]	8 MB	16 MB	64 MB[4]
	Sicheres Anwendungspro-gramm	2 MB	4 MB	16 MB[4]	2 MB	4 MB	16 MB[4]
	Nicht-sichere Daten	768 KB	2048 KB	Bis zu 65536 KB[4]	768 KB	2048 KB	Bis zu 65536 KB[4]
	Max. konfigurierbare Retain-Daten	768 KB	2048 KB	4096 KB	768 KB	2048 KB	4096 KB
	Max. konfigurierbare redundante Übertragungsdaten	–	–	–	768 KB	2048 KB	4096 KB[5]
	Sichere Daten (keine Retain-Daten)	512 KB	1024 KB	1024 KB[4]	512 KB	1024 KB	1024 KB[4]

Leistungsmerkmal		BME					
		P582040S	P584040S	P586040S	H582040S	H584040S	H586040S
	Maximal konfigurierbare sichere redundante Übertragungsdaten	–	–	–	512 KB	1024 KB	1024 KB[5]
	Gemeinsam genutzt: Global -> Sicher	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Gemeinsam genutzt: Sicher -> Global	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Gemeinsam genutzt: Global -> Prozess	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Gemeinsam genutzt: Prozess -> Global	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Datenspeicher insg.	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]
Ausführungsrate für Anweisungen	MAST- und FAST-Task:						
	Boolesch	10 K Anweisungen / ms	40K Anweisungen / ms	60K Anweisungen / ms	10 K Anweisungen / ms	40K Anweisungen / ms	60K Anweisungen / ms
	Typisiert	7,5K Anweisungen / ms	30K Anweisungen / ms	40K Anweisungen / ms	7,5K Anweisungen / ms	30K Anweisungen / ms	40K Anweisungen / ms
	SAFE-Task:						
	Boolesch	10 K Anweisungen / ms	40K Anweisungen / ms	40K Anweisungen / ms	10 K Anweisungen / ms[3]	40K Anweisungen / ms[3]	40K Anweisungen / ms[3]
	Typisiert	7,5K Anweisungen / ms	30K Anweisungen / ms	30K Anweisungen / ms	7,5K Anweisungen / ms[3]	30K Anweisungen / ms[3]	30K Anweisungen / ms[3]

1. Für M580-Hot Standby-Sicherheits-PACs werden keine E/A-Module im lokalen Rack unterstützt.

2. Diese Daten werden sowohl in die sicheren als auch die nicht-sicheren Bereiche aufgenommen.

3. Da die SAFE-Task Daten über den Baugruppenträger austauscht, sind Leistungseinbußen zu verzeichnen. Für BMEH584040S und BMEH586040S sind für die Übertragung von 10 KB 1 ms und für BMEH582040S 2 ms erforderlich.

4. Anwendungsprogramm (nicht-sicher) + Anwendungsdaten (nur nicht-sichere, nicht-beibehaltene Daten) + Anwendungsprogramm (sicher) + Anwendungsdaten (sicher) machen weniger als 64 MByte aus. In der CPU BME•586040S ist für das Anwendungsprogramm und die Anwendungsdaten ein globaler Speicherpool von 64 MByte vorhanden.

5. Die maximale Größe der Übertragungsdaten (nicht-sicher + sicher) für redundante Daten beträgt 4 MB.

6. 2 GB ohne externe Speicherkarte

M580-Sicherheitsspannungsversorgungen

Inhalt dieses Kapitels

Einführung

In diesem Kapitel werden die Sicherheitsspannungsversorgungen M580 beschrieben.

Physische Beschreibung der M580-Sicherheitsspannungsversorgungen

Verwendung in einer M580-Sicherheitsschleife

Verwenden Sie die Sicherheitsspannungsversorgung BMXCPS4002S, BMXCPS4022S oder BMXCPS3522S nur in einem Rack, das Sicherheitsmodule enthält. Sie können die Sicherheitsspannungsversorgung in einem der folgenden X Bus- und Ethernet-Racks einsetzen:

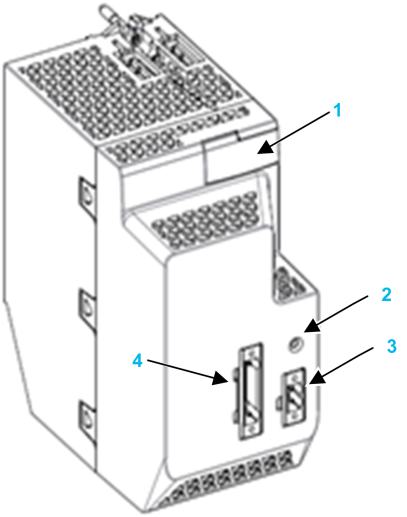
- Lokales Hauptrack
- Lokales Erweiterungsrack
- Dezentrales Hauptrack
- Dezentrales Erweiterungsrack

In Ethernet-Racks, die Redundanz unterstützen, können zwei Sicherheitsspannungsversorgungsmodule installiert werden. Eine Sicherheitsspannungsversorgung benötigt zwei Modulsteckplätze und wird in der Position ganz links in einem Rack untergebracht.

HINWEIS: Eine Beschreibung der verfügbaren M580-Racks finden Sie unter *Lokale und dezentrale Racks* im *Modicon M580 Hardware-Referenzhandbuch*.

Frontplatte der Spannungsversorgung

Die M580-Sicherheitsspannungsversorgungen sind mit folgender Frontplatte ausgestattet:



1 LED-Display- Panel

2 RESET-Taste

3 Alarmrelais-Kontakt

4 5-poliger Anschluss der Haupteingangsspannungsversorgung 100...240 VAC

LED-Panel

Die M580-Sicherheitsspannungsversorgungen sind mit folgendem LED-Panel ausgestattet:

Das LED-Panel umfasst folgende LED-Anzeigen:

- **OK**: Betriebszustand
- **ACT**: Aktivität
- **RD**: Redundanz

Jede LED verfügt über zwei Zustände: EIN (grün) und AUS.

Informationen zur Verwendung dieser LED-Anzeigen für die Diagnose des Zustands der Spannungsversorgung finden Sie unter *Diagnose-LEDs der Spannungsversorgung* (siehe Modicon M580, Sicherheitshandbuch) im *M580 Sicherheitshandbuch*.

RESET

Durch Drücken der **RESET**-Taste an der Spannungsversorgung wird die Reinitialisierung aller Module im gleichen Rack wie die Spannungsversorgung ausgelöst. Wenn sich das M580-Sicherheitsspannungsversorgungsmodul im lokalen Hauptrack befindet, drücken Sie die **RESET**-Taste, um die CPU neu zu initialisieren.

HINWEIS: In einer redundanten Architektur mit 2 M580-Sicherheitsspannungsversorgungen können Sie die RESET-Taste an beiden Sicherheitsspannungsversorgungsmodulen drücken, um die Reset-Funktion auszuführen.

Hinweise zur Eingangsspannungsversorgung

Die M580-Sicherheitsspannungsversorgungen sind mit Anschlusspins mit folgenden Merkmalen ausgestattet:

- 5 Punkte
- Typ des abnehmbaren Anschlusses:
  - am Modul: Kopf mit Gewindeflansch
  - Steckklemmenleiste mit Schraubflansch
- Abstand: 5,08 mm
- Min. Leiterquerschnitt: 0,5 mm^2 bis 2,0 mm^2

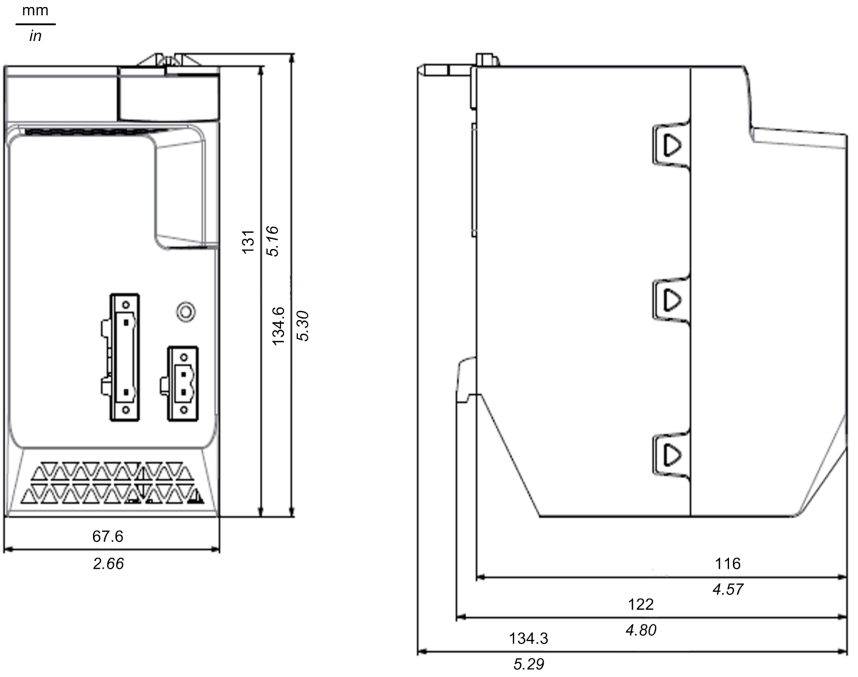
Die M580-Sicherheitsspannungsversorgungen weisen folgende Eingangsleistung und Pinzuweisung auf:

Beschreibung	**BMXCPS4002S**	**BMXCPS4022S**	**BMXCPS3522S**
Haupteingangsleistung	100...240 VAC	24...48 VDC	125 VDC
Pin 1	NC	DC-Leitung	NC
Pin 2	NC	DC-Leitung	NC
Pin 3	PE	DC-Neutralleiter	PE
Pin 4	AC-Neutralleiter	DC-Neutralleiter	DC-Neutralleiter
Pin 5	AC-Leitung	Erde	DC-Leitung

HINWEIS: Im Lieferumfang des Moduls ist eine Steckklemmenleiste verfügbar.

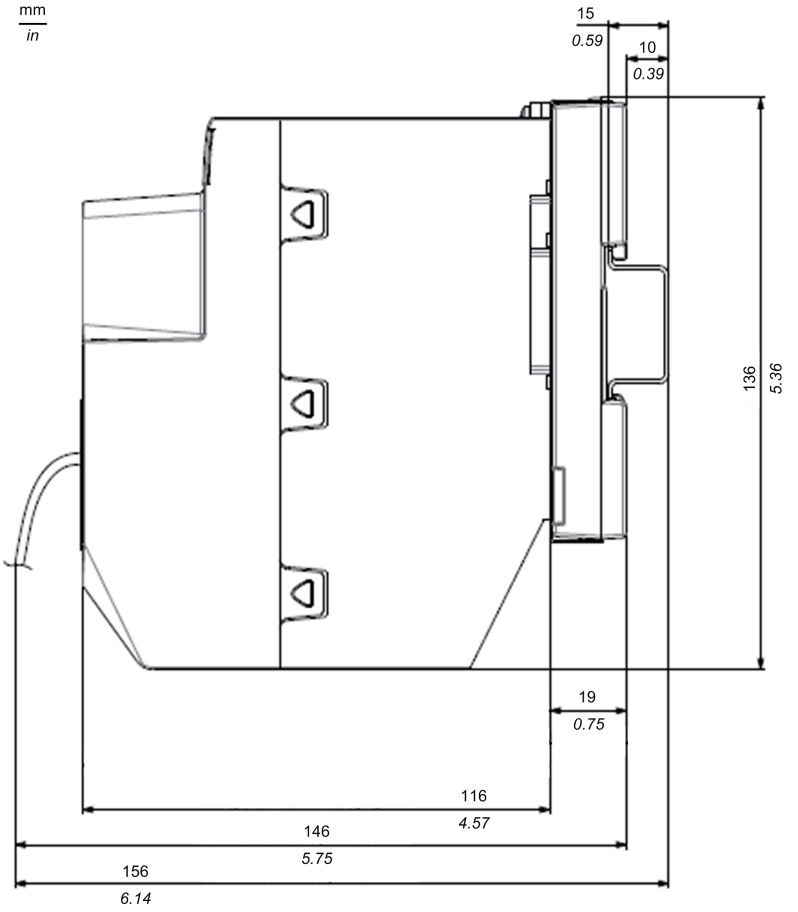
Abmessungen der Spannungsversorgung

Die M580-Sicherheitsspannungsversorgungen weisen folgende Abmessungen auf:



Abmessungen der Verkabelung der Spannungsversorgung

Unter Berücksichtigung der Verkabelung weisen die M580-Sicherheitsspannungsversorgungen folgende Abmessungen auf:



Leistungsmerkmale der Sicherheitsspannungsversorgung M580

Sicherheitsspannungsversorgung BMXCPS4002S

Die Sicherheitsspannungsversorgung BMXCPS4002S weist folgende Leistungsmerkmale auf:

Merkmale der Eingänge		
Nennspannung		100...240 V effektiv
Spannungsbereich		85...132 V effektiv 170...264 V effektiv
Frequenzbereich		47 bis 63 Hz
Maskierte Eingangsversorgungsausfälle		Max. 10 ms bei100 Veff -15 % und bei 200 Veff -15 %
Typische Eingangsscheinleistung		130 VA
Typischer Eingangsstrom		1,1 Aeff bei 115 Veff 0,55 Aeff bei 230 Veff
Einschaltstrom bei 25° bei Erstanlauf	Spitzenwert	30 Aeff bei 115 Veff 60 Aeff bei 230 Veff
	I^2t (Bemessung externe Sicherung)	1 A 2s bei 115 Veff 4 A 2s bei 230 Veff
	It (Bemessung externer Leistungsschalter)	0,1 As bei 115 Veff 0,15 As bei 230 Veff
Integrierter Schutz		Interne, nicht zugängliche Sicherung an L-Eingang

Merkmale der Ausgänge		
Ausgangsstrom MAX 3V3_BAC		5,5 A (18,2 W)
Ausgangsstrom MAX 24V_BAC		1,67 A (40 W)
Ausgangsgesamtleistung MAX		40 W
Erkennung	Überlast	Ja - Trennung
	Kurzschluss	Ja - Trennung

Merkmale der Ausgänge		
	Überspannung	Ja - Trennung

Sonstige Merkmale		
Dielektrikum	Primär/Alle sekundär	SELV / PELV
Festigkeit	Primär/Masse	SELV / PELV
Isoliationswiderstand	Primär/Alle sekundär	100 MΩ
	Primär/Masse	100 MΩ

Sicherheitsspannungsversorgung BMXCPS4022S

Merkmale der Eingänge		
Nennspannung Typ		24...48 VDC
Spannungsbereich		18...62,4 VDC
Effizienz		Max. Verlust ≤ 7 W (Effizienz ≥ 84,8 %) bei maximaler Dauerlast, für den gesamten Eingangsspannungs- und Temperaturbereich
Nennstrom		1,9 A bei 24 VDC
		1,0 A bei 48 VDC
Einschaltstrom beim ersten Einschalten bei 25 °C	Spitzenstrom	≤ 60 A bei 24 VDC
		≤ 60 A bei 48 VDC
	I^2t (Bemessung externe Sicherung)	≤ X A^2s bei 24 VDC
		≤ X A^2s bei 48 VDC
	It (Bemessung externer Leistungsschalter)	≤ X As bei 24 VDC
		≤ X As bei 48 VDC
Maskierte Eingangsversorgungsausfälle		Eingangsversorgungsausfälle einer Dauer von max.:
		• 1 ms bei Volllast und min. Leitungsspannung (d. h. 19,2 VDC)
		• 10 ms bei Volllast und Leitungsnennspannung (d. h. 24 oder 48 VDC)
		Es darf zu keiner Änderung der Ausgangsmerkmale kommen. Zeitraum zwischen Unterbrechungen: 1 Sek.

Merkmale der Eingänge	
Eingangsschutz	• Brandschutz: Über eine platinenmontierte Sicherung, für den Benutzer nicht zugänglich und nicht austauschbar, angebracht am Eingang DC+ Die Nennleistung der Sicherung hat den Sicherheitsstandards zu entsprechen. Sie darf bei Prüfungen der Störfestigkeit gegenüber Leitungsrauschen unter keinen Umständen beschädigt werden.
	• Eingangsverpolungsschutz: Das Modul ist über einen integrierten Schaltkreis zu schützen. Die interne (und ggf. externe) Sicherung darf nicht durchbrennen. Die Spannungsversorgung muss ordnungsgemäß eingeschaltet werden, sobald die richtige Polarität wiederhergestellt wird.

Merkmale der Ausgänge:	
Nennspannung	24,35 V
Ruhespannungsbereich	23,3 bis 24,7 V für den gesamten Eingangsspannungsbereich, den gesamten Ausgangslastbereich und den kompletten Temperaturbereich
Rauschen und Welligkeit	240 mV Spitze zu Spitze (gemessen mit einer Bandbreite ≥ 100 MHz, an den Anschlusspins des Moduls)
Dauerstrombereich	• Max. 1,63 A
	• Min. 0 A
Ausgleichsstromkapazität	Max. 1,9 A während 500 ms, Mindestzeitraum 20 Sek.
Widerstand in Bezug auf Frequenz	180 mΩ
Ausgangsspannung bei transienter Last an 24V_BAC	Für folgende transiente Ausgangslast an 24V_BAC:
	• Lastschwankung I von min. Dauerstromgrenze bis max. transienter Stromgrenze (und umgekehrt)
	• Übergangszeit 4 µs – Pulsbreite 500 ms – Zeitraum 20 Sek.
	• Die transiente Ausgangsspannung an 24V_BAC muss innerhalb des Bereichs 23,0 bis 25,0 V bleiben, die Antwortzeit muss ≤ 50 ms sein.
	• Ungeachtet des Werts der kapazitiven Last an 24V_BAC innerhalb der vorgegebenen Grenzen.
Überlast-/Kurzschlussschutz	• Bei einer Überlast- oder Kurzschlusssituation an 24V_BAC (d. h. ungeachtet von Pegel, Dauer, Temperatur, Eingangsspannung) muss die Platine vor jeglichen Schäden geschützt werden.
	• Der globale Höchstwert der Überlastschutzgrenze (d. h. einschließlich aller Toleranzen, Abweichungen usw.) muss geringer sein als Imax.
	• Imax = 2 A.

Merkmale der Ausgänge:	
Überspannungsschutz	Trennung der Spannungsversorgung bei Anstieg der Ausgangsspannung auf 30,0 VDC ± 0,8 V
Externe kapazitive Lastkapazität	Alle obigen Eigenschaften müssen mit der folgenden externen kapazitiven Last erfüllt sein. Diese Funktion muss insbesondere für Stromanstiege, Regelkreisstabilität und Überlasterkennung/-schutz in Betracht gezogen werden.
	11500 µF kapazitive Last

Sicherheitsspannungsversorgung BMXCPS3522S

Merkmale der Eingänge:		
Nennspannung		125 VDC
Spannungsbereich		100...150 VDC
Effizienz		Max. Verlust ≤ 7 W (Effizienz ≥ 84,8 %) bei maximaler Dauerlast, für den gesamten Eingangsspannungs- und Temperaturbereich
Nennstrom		0,6 A bei 125 VDC
Einschaltstrom beim ersten Einschalten bei 25 °C	Spitzenstrom	≤ 60 A bei 125 VDC
	I^2t (Bemessung externe Sicherung)	≤ X A^2s bei 125 VDC
	It (Bemessung externer Leistungsschalter)	≤ X As bei 4 VDC
Maskierte Eingangsversorgungsausfälle		Eingangsversorgungsausfälle einer Dauer von max.:
		• 1 ms bei Volllast und min. Leitungsspannung (d. h. 100 VDC)
		• 10 ms bei Volllast und Leitungsnennspannung (d. h. 125 VDC)
		Es darf zu keiner Änderung der Ausgangsmerkmale kommen. Zeitraum zwischen Unterbrechungen: 1 Sek.
Eingangsschutz		• Brandschutz: Über eine platinenmontierte Sicherung, für den Benutzer nicht zugänglich und nicht austauschbar, angebracht am Eingang DC+ Die Nennleistung der Sicherung hat den Sicherheitsstandards zu entsprechen. Sie darf bei Prüfungen der Störfestigkeit gegenüber Leitungsrauschen unter keinen Umständen beschädigt werden.

Merkmale der Eingänge:	
	• Eingangsverpolungsschutz: Das Modul ist über einen integrierten Schaltkreis zu schützen. Die interne (und ggf. externe) Sicherung darf nicht durchbrennen. Die Spannungsversorgung muss ordnungsgemäß eingeschaltet werden, sobald die richtige Polarität wiederhergestellt wird.

	BMXCPS3522 /S Hochleistungsmodul
Nennspannung	24,35 V
Ruhespannungsbereich	23,3 bis 24,7 V für den gesamten Eingangsspannungsbereich, den gesamten Ausgangslastbereich und den kompletten Temperaturbereich
Rauschen und Welligkeit	240 mV Spitze zu Spitze (gemessen mit einer Bandbreite ≥ 100 MHz, an den Anschlusspins des Moduls)
Dauerstrombereich	• Max. 1,63 A
	• Min. 0 A
Ausgleichsstromkapazität	Max. 1,9 A während 500 ms, Mindestzeitraum 20 Sek.
Widerstand in Bezug auf Frequenz	180 mΩ
Ausgangsspannung bei transienter Last an 24V_BAC	Für folgende transiente Ausgangslast an 24V_BAC:
	• Lastschwankung I von min. Dauerstromgrenze bis max. transienter Stromgrenze (und umgekehrt)
	• Übergangszeit 4 µs – Pulsbreite 500 ms – Zeitraum 20 Sek.
	• Die transiente Ausgangsspannung an 24V_BAC muss innerhalb des Bereichs 23,0 bis 25,0 V bleiben, die Antwortzeit muss ≤ 50 ms sein.
	• Ungeachtet des Werts der kapazitiven Last an 24V_BAC innerhalb der vorgegebenen Grenzen.
Überlast-/Kurzschlussschutz	• Bei einer Überlast- oder Kurzschlusssituation an 24V_BAC (d. h. ungeachtet von Pegel, Dauer, Temperatur, Eingangsspannung) muss die Platine vor jeglichen Schäden geschützt werden.
	• Der globale Höchstwert der Überlastschutzgrenze (d. h. einschließlich aller Toleranzen, Abweichungen usw.) muss geringer sein als Imax.
	• Imax = 2 A.
Überspannungsschutz	Trennung der Spannungsversorgung bei Anstieg der Ausgangsspannung auf 30,0 VDC ± 0,8 V

	BMXCPS3522 /S Hochleistungsmodul
Externe kapazitive Lastkapazität	Alle obigen Eigenschaften müssen mit der folgenden externen kapazitiven Last erfüllt sein. Diese Funktion muss insbesondere für Stromanstiege, Regelkreisstabilität und Überlasterkennung/-schutz in Betracht gezogen werden.
	11500 µF kapazitive Last

Alarmrelais der M580-Sicherheitsspannungsversorgungen

Leistungsmerkmale

Die Alarmrelais-Klemmenleiste der M580-Sicherheitsspannungsversorgungen weist folgende Leistungsmerkmale auf:

Eigenschaften	
Bemessungsschaltspannung/-strom	24 VDC / 2 A (ohmsche Last)
	240 VAC / 2 A (Cos Φ = 1)
Minimale Schaltlast	5 VDC / 1 mA
Maximale Schaltspannung	62,4 VDC
	264 VAC
Kontakttyp	Schließkontakt
Kontaktzeit	
• AUS → EIN	10 ms oder weniger
• EIN → AUS	12 ms oder weniger
Integrierte Schutzfunktion	Gegen Überlast/Kurzschluss: Keine. Es muss eine flinke Sicherung angebracht werden.
	Gegen induktive Überspannung bei Wechselstrom (AC): Keine. Bauen Sie parallel zu den Klemmen jedes Vorstellglieds eine (für die Spannung geeignete) RC-Schaltung oder einen MOV-Entstörfilter (ZNO) ein.
	Gegen induktive Überspannung bei Gleichstrom (DC): Keine. Schließen Sie eine Entladungsdiode an die Klemmen jedes Vorstellglieds an.
Dielektrische Spannungsfestigkeit	Kontakt zu Masse: 2000 Vrms, 50 Hz, 1 Min.(Höhenlage 0...2000 m)
Isolationswiderstand	10 MΩ oder höher bei 500 VDC

M580-E/A-Sicherheitsmodule

Inhalt dieses Kapitels

Einführung

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

Physische Beschreibung der M580-E/A-Sicherheitsmodule

Einführung

In diesem Abschnitt werden die allgemeinen physischen Merkmale der M580-E/A-Sicherheitsmodule beschrieben.

Physische Abmessungen der M580-E/A-Module

Positionierung der E/A-Sicherheitsmodule

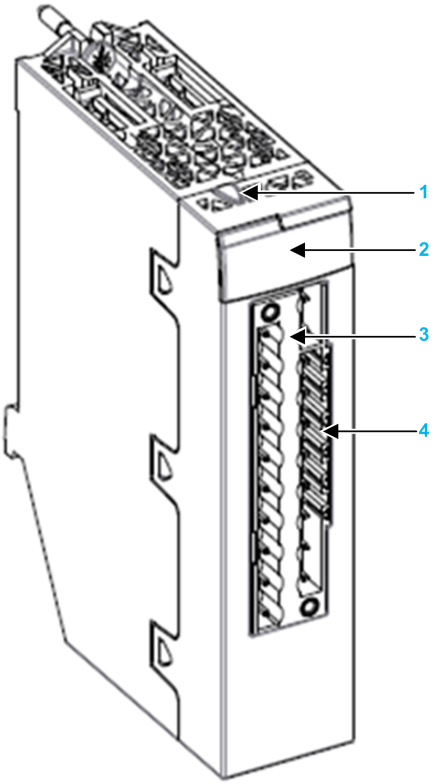
Sie können ein M580-E/A-Sicherheitsmodul in folgenden Positionen installieren:

- Beliebiger Steckplatz im lokalen Rack, der nicht für die Spannungsversorgung oder die CPU reserviert ist.
- Beliebiger Steckplatz in einem dezentralen Rack, der nicht für die Spannungsversorgung oder den dezentralen Adapter reserviert ist.

  HINWEIS: Ein E/A-Sicherheitsmodul kann entweder in einem X Bus-Rack BMXXBP•••• oder in einem Ethernet-Rack BMEXBP•••• untergebracht werden. Eine Beschreibung der verfügbaren M580-Racks finden Sie unter *Lokale und dezentrale Racks* im *Modicon M580 Hardware-Referenzhandbuch*.

Frontplatte der E/A-Sicherheitsmodule

Die Frontplatte jede E/A-Sicherheitsmoduls weist folgende Merkmale auf:



1 Taste zum Sperren/Entsperren der Konfiguration

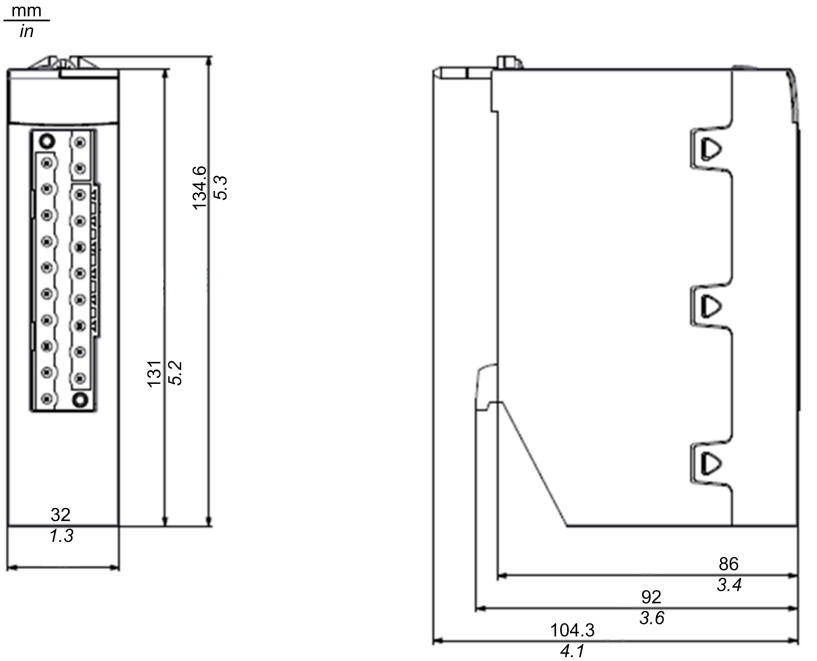
2 LED-Panel

3 20-poliger Steckverbinder

4 Steckplätze für Kodierstifte

Abmessungen der E/A-Sicherheitsmodule

Jedes E/A-Sicherheitsmodul weist folgende physische Abmessungen auf:

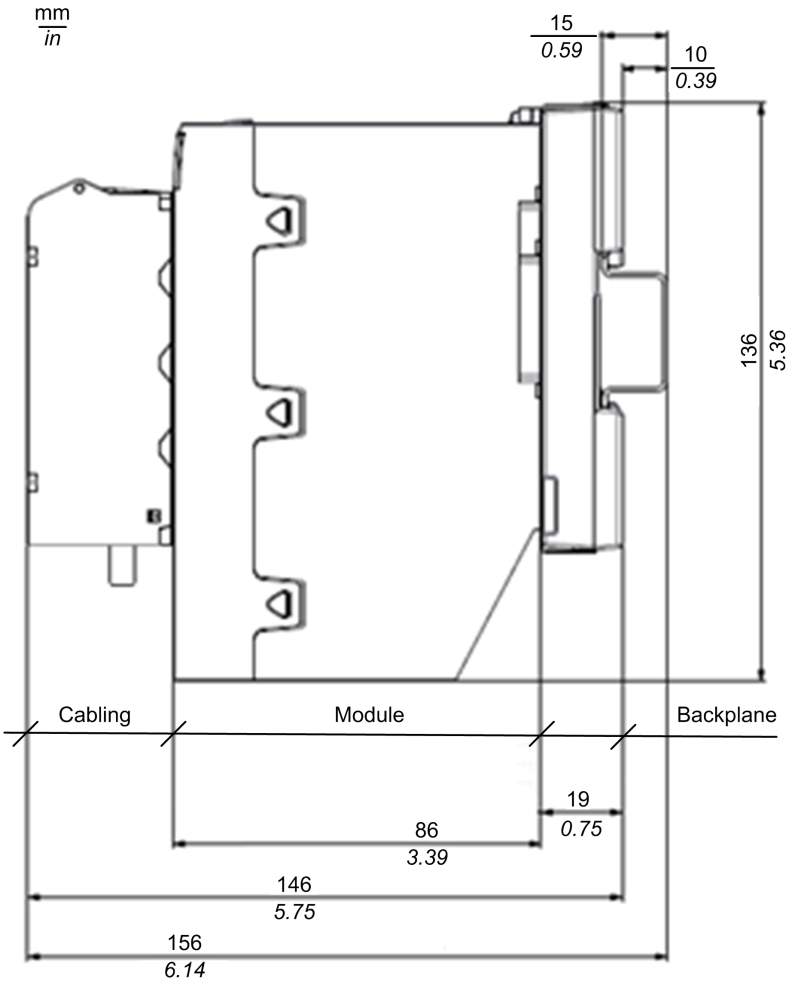


HINWEIS: Berücksichtigen Sie bei der Planung einer Rackinstallation die Höhe der E/A-Sicherheitsmodule. Jedes E/A-Sicherheitsmodul steht über die untere Kante des Racks hervor:

- 29,49 mm (1.161 in.) bei einem Ethernet-Rack
- 30,9 mm (1.217 in.) bei einem X Bus-Rack

Abmessungen der Verkabelung von E/A-Sicherheitsmodulen

Die Verkabelung jedes E/A-Sicherheitsmoduls weist folgende Abmessungen auf:



LEDs

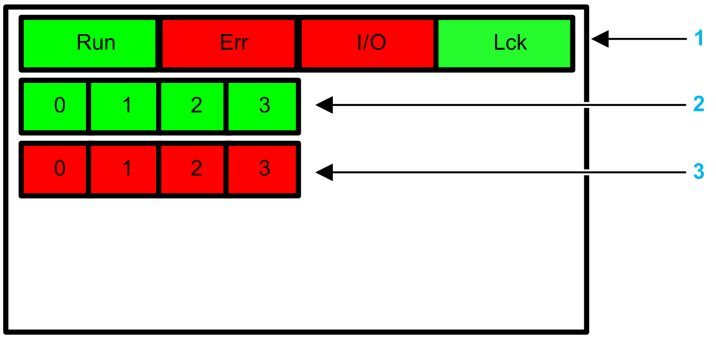
An der Frontplatte jedes E/A-Sicherheitsmoduls stehen LEDs zur Modul- und Kanaldiagnose bereit:

- Die oberen 4 LED-Anzeigen (**Run**, **Err**, **I/O** und **Lck**) signalisieren zusammen den Zustand des Moduls.

- Die unteren LED-Reihen gemeinsam mit den oberen 4 LEDs beschreiben den Zustand und die Funktionsfähigkeit jedes Eingangs- und Ausgangskanals.

  HINWEIS: Informationen zur Verwendung der Modul-LEDs für die Diagnose des Zustands der M580-Sicherheitsmodule finden Sie im Kapitel zur *Diagnose* im *M580 Sicherheitshandbuch*.

LED-Anzeigen der analogen Sicherheitseingangsmodule BMXSAI0410 und digitalen Relay-Ausgangsmodule BMXSRA0405:

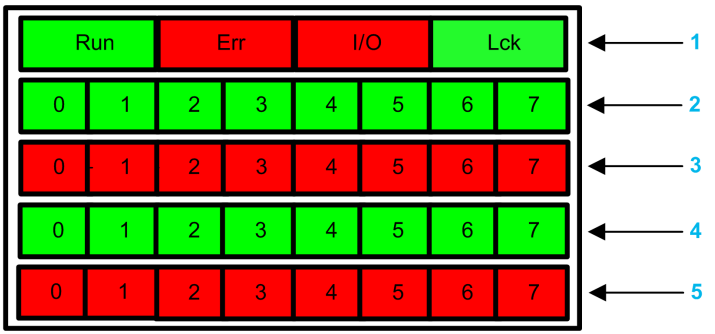


1 Modulstatus-LEDs

2 Kanalstatus-LEDs

3 Kanalfehler-LEDs

LEDs der digitalen BMXSDI1602-Sicherheitseingangsmodule:



1 Modulstatus-LEDs

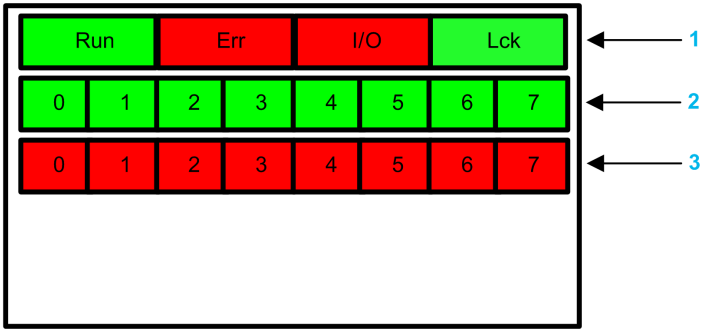
2 Kanalstatus-LEDs für Rang A

3 Kanalfehler-LEDs für Rang A

2 Kanalstatus-LEDs für Rang B

3 Kanalfehler-LEDs für Rang B

LEDs der digitalen BMXSDO0802-Sicherheitsaugangsmodule:



1 Modulstatus-LEDs

2 Kanalstatus-LEDs

3 Kanalfehler-LEDs

Leistungsmerkmale der M580-E/A-Sicherheitsmodule

Einführung

In diesem Abschnitt werden die Leistungsmerkmale der M580-E/A-Sicherheitsmodule beschrieben.

Leistungsmerkmale des analogen Sicherheitseingangsmoduls BMXSAI0410

Leistungsmerkmale des analogen Eingangsmoduls

Das analoge Sicherheitseingangsmodul BMXSAI0410 weist folgende Leistungsmerkmale auf:

Statische Eigenschaften		**Wert**
Eingangsimpedanz im Signalbereich		286 Ω
Analoger Eingangsfehler	Max. Skalenendwert bei 25 °C	0,30 %
Analoger Eingangsfehler (= Sicherheitstoleranz)	Fehler max. Skalendendwert, kompletter Temperaturbereich -25 °C bis 70 °C	0,35 %
Zuverlässigkeit	MTTF bei 25 °C	54,2 Jahre
Linearer Messbereich		0 bis 25 mA und 12.500 Schaltvorgänge (500 ct/mA)
Außerhalb des Erfassungsbereichs		< 3,75 mA and > 20,75 mA
Digitale Auflösung	Auflösung	16 Bit
	Anzahl gleichzeitig konvertierter Kanäle	4
Vom Anwendungsprogramm zurückgegebenes Datenformat		binary
LSB-Wert		0,191 µA
Max. zulässige Dauerüberlast		25 mA
Lesen der digitalen Ausgänge bei Überlast	Überlast an Client-Anwendung gemeldet	I = 25 mA
Eingangstyp	Typ	4 bis 20 mA

Statische Eigenschaften		**Wert**
	Typ	Potentialfrei getrennte Eingänge
	Max. Eingangsbereich	0 bis 25 mA
Gleichtakt	Gleichtaktunterdrückung	Zu messen

Dynamische Merkmale		**Wert**
Eingangsfilter	Reihenfolge	Sekunde
	Frequenzgrenze bei -3 dB	10,47 Hz

Allgemeine Merkmale		**Wert**
Konvertierungsmethode		Sukzessive Approximation
Schutzart		Schutzdiode
Isolationspotential bei Normalbetrieb	Isolation zwischen Kanälen	500 VAC effektiv für 1 Minute.
	Isolation Kanal - Baugruppenträger	1500 VAC effektiv für 1 Minute.
Externe Spannungsversorgungsdaten - sofern erforderlich		Nicht erforderlich
Kabeltyp und -länge - Empfohlene Installationsregeln zur Gewährleistung der Störfestigkeit		Geschirmtes Kabel
Kalibrierung oder Prüfung zur Gewährleistung der Nenngenauigkeit		Keine Kalibrierung
Typische Beispiele für externe Verbindungen		Temperaturfühler und Drucksensor

Sonstige Merkmale		**Wert**
Monotonie ohne fehlenden Code		Ja
Nebensprechen ziwschen DC und AC bei 50 Hz und AC bei 60 Hz		–
Nicht-Linearität	+/-	0,006 % (LSB)
Wiederholgenauigkeit bei stabiler Temperatur nach vorgegebener Stabilisierungszeit		–
Aufnahme 3,3 V	Typisch	223 mA
	Maximum	256 mA
Aufnahme 24 V	Typisch	92 mA
	Maximum	115 mA
Verlustleistung	Maximum	3,98 W

Leistungsmerkmale des digitalen Sicherheitseingangsmoduls BMXSDI1602

Leistungsmerkmale des digitalen Eingangsmoduls

Das Sicherheitseingangsmodul BMXSDI1602 weist folgende Leistungsmerkmale auf:

Merkmal		**Wert**
Eingangsbemessung	Spannung	24 VDC
Typ Spannungsversorgung externer Sensor	SELV/PELV, Überspannung II	(Max. 60 V)
Typischer Eingangsstrom	Strom	3,2 mA
Eingangsgrenzwerte	Spannung im Zustand 1	≥ 11 V
	Spannung im Zustand 0	≤ 5 V
	Strom im Zustand 1	> 2 mA für U ≥ 11 V
	Strom im Zustand 0	< 1,5 mA
	Sensorversorgung (inkl. Welligkeit)	19 bis 30 V (bis 33 möglich - begrenzt auf 1 Std. pro Tag)
Eingangsimpedanz	Bei Unenn	7,5 kΩ
Ansprechzeit	Typisch/Max.	100 µs / 250 µs
Zuverlässigkeit	MTTF bei Tumg. = 25 °C	31,5 Jahre
Verpolung		Geschützt
IEC61131-2 - Ausgabe 3.0 (2007)		Typ 3
Kompatibilität	(Näherungssensoren 2-/3-Draht)	IEC 947-5-2
Dielektrische Spannungsfestigkeit	Primär/Sekundär	1500 Veff (bei 4000 m) 50/60 Hz für 1 Min.
Isolationswiderstand		> 10 MΩ (bei 500 VDC)
Eingangstyp		Strom ziehend (Sink)
Eingangsparallelschaltung(1)		Ja
Sensorspannung Überwachungsschwellen-wert	OK	> 18,6 VDC < 32 VDC
	Fehler	< 18,6 VDC > 33 VDC

Merkmal		Wert
Sensorspannung Antwortzeitüberwachung	Bei Verschwinden	4,4 ms < T < 30 ms
	Bei Auftreten	0,18 ms < T < 0,3 ms
Max. externe Kapazität bei VS-Verwendung 24-V-Kurzschlusserkennung	Maximum	80 nF
Aufnahme 3,3 V	Typisch	200 mA
	Maximum	256 mA
Aufnahme 24 V	Typisch	63 mA
	Maximum	100 mA
Max. Verlustleistung		3,57 W
(1) Dieses Merkmal ermöglicht die Verdrahtung mehrerer Eingänge am gleichen Modul bzw. an unterschiedlichen Modulen, wenn redundante Eingänge benötigt werden.		

Leistungsmerkmale des digitalen Sicherheitsausgangsmoduls BMXSDO0802

Leistungsmerkmale des digitalen Ausgangsmoduls

Das digitale Sicherheitsausgangsmodul BMXSDO0802 weist folgende Leistungsmerkmale auf:

Merkmal		Wert
Nennwerte	Spannung	24 VDC
	Strom	0,5 A
Grenzwerte	Spannung	19 bis 30 V(1)
	Strom/Kanal	0,625 A
	Strom/Modul	5 A
Typ Spannungsversorgung externes Stellglied		SELV/PELV (max. 60 V), Überspannungskategorie II
Leistung der Wolframlampe	max.	6 W
Kriechstrom	Im Zustand 0	< 0,5 mA
Restspannung	Im Zustand 1	< 1,2 V
Schutzfunktionen	Transiente Spannung	Ja

Merkmal		**Wert**
	Überlast-Trennstrom	> 0,625 A
	Kurzschluss	Ja
	Verpolung	Ja
	Übertemperatur	Ja
Mindestlast Widerstandswert (für Vorstellglied)		48 Ω
Vollständige Erkennung eines Drahtbruchs: Max. Kabellastkapazität (einschließlich Vorstellglied-Kapazität) zwischen Ausgang und Vorstellglied		10 nF
Antwortzeit(2)		1,2 ms
Zuverlässigkeit: MTTF		45,8 Jahre bei 25 °C
Schaltfrequenz bei induktiver Last		0,5/LI²Hz mit Fmax = 2 Hz
Parallelschaltung der Ausgänge		Ja (max. 2)
Kompatibilität mit DC-Eingängen		Ja (nur Sink-Typ 3 oder Nicht-IEC-Sink)
Integrierte Schutzfunktion	Gegen Überspannung	Ja - über interne TVS
	Gegen Verpolung	Ja - über umgekehrt montierte Diode. 24-V-Vorstellglied mit Sicherung ausstatten.
	Gegen Kurzschluss und Überlast	Ja - über Strombegrenzer und elektronischen Leistungsschalter 1,5 In < Id < 2 In
Spannung 24-V-Vorstellglied Überwachungs-schwellenwert	OK	> 19,0 V und < 31,8 V
	Fehler	< 18,0 V und < 31,8 V
Vorstellglied-Spannung Antwortzeitüberwa-chung	Bei Verschwinden	2 ms < T < 5,6 ms
	Bei Auftreten	10 ms < T < 15,6 ms
Aufnahme 3,3 V	Typisch	240 mA
	Maximum	264 mA
Aufnahme 24-V-Baugruppenträger	Typisch	80 mA
	Maximum	90 mA
Aufnahme 24-V-Vorstellglied (ohne Laststrom)	Typisch	5 mA
	Maximum	15 mA
Verlustleistung		4,4 W max.
Dielektrische Spannungsfestigkeit (Ausgang/Masse oder interne Logik)		1500 Veff, 50/60 Hz für 1 Minute

Merkmal	Wert
Isolationswiderstand	> 10 MΩ bei 500 VDC
(1) 33 V zulässig für 1 Stunde pro 24 Std. **(2)** Alle Ausgänge verfügen über Entmagnetisierungskreise für Elektromagneten. Elektromagnetische Entladungszeit < L/R.	

Leistungsmerkmale des digitalen Sicherheits-Relais-Ausgangsmoduls BMXSRA0405

Merkmale des digitalen RelaisAusgangsmoduls

Das digitale Sicherheits-Relais-Ausgangsmodul BMXSRA0405 weist folgende Leistungsmerkmale auf:

Merkmal		Wert
Nennschalt- spannung/strom		24 VDC / 5 A (Ohmsche Last)
		240 VAC / 5 A (Cos Φ = 1)
Max. Strom für Kontakte mit ohmscher Last		5 A (DC12 und AC12)
Max. Strom für Kontakte mit induktiver Last		4 A (DC13) und 3A (AC15)
Betriebstemperatur		0 bis 60 °C
Typ Spannungsversorgung externes Stellglied		Überspannungskategorie II
Min. Schaltlast		5 VDC / 10 mA
Max. Schaltlast		26 VAC / 30 VDC
Schaltdauer	AUS → EIN (Betätigung)	12 ms typisch
	EIN → AUS (Freigabe)	6 ms typisch
Lebensdauer (basiert auf Elesta-Relais SIF3)	Mechanisch	10 Million Zyklen oder mehr
	Elektrisch	DC12 24 VDC / 5 A → 300.000 Zyklen
		DC12 24 VDC / 2 A → 500.000 Zyklen
		DC12 24 VDC / 1 A → 1.000.000 Zyklen
	L/R = 40 ms	DC13 24 VDC (0,1 Hz) / 4 A → 30.000 Zyklen
		DC13 24 VDC (0,1 Hz) / 2 A → 50.000 Zyklen

Merkmal		Wert
		DC13 24 VDC (0,1 Hz) / 1 A → 80.000 Zyklen
	–	AC12 250 VAC / 5 A → 70.000 Zyklen
		AC12 250 VAC / 2 A → 30.000 Zyklen
		AC12 250 VAC / 1 A → 250.000 Zyklen
	–	AC15 250 VAC / 3 A → 40.000 Zyklen
		AC15 250 VAC / 2 A → 80.000 Zyklen
		AC15 250 VAC / 1 A → 80.000 Zyklen
Integrierte Schutzfunktion	Gegen Überlast und Kurzschluss	Kein - Jeder Kanal bzw. jede Kanalgruppe kann mit einer flinken Sicherung ausgestattet werden.
	Gegen induktive Überlast in ~	Kein - Über die Klemmen jedes Vorschaltglieds muss ein für die jeweilige Spannung geeigneter RC-Schaltkreis oder MOV-Spitzenwertbegrenzer (ZNO) parallel zugeschaltet werden.
	Gegen induktive Überlast in =	Kein - Über die Klemmen jedes Vorschaltglieds muss eine Entladungsdiode zugeschaltet werden.
Max. Schaltfrequenz		5 Zyklen pro Sekunde
Max. dielektrische Spannung zwischen Kanälen		3000 V effektiv, 50/60 Hz für 1 Minute
Max. dielektrische Spannung zwischen Kanälen und Baugruppenträger		3000 V effektiv, 50/60 Hz für 1 Minute
Verstärkter Isolationsstandard		3000-VAC-Isolation zwischen Prozessseite (Relais-Kontakt) und Baugruppenträger
Isoliationswiderstand		> 10 MW oder mehr per Messgerät zur Messung des Isolationswiderstands
Zuverlässigkeit: MTTF bei Tumg. = 2 5°C		36,9 Jahre
Verschmutzungsgrad		IP20
Aufnahme 3,3 V	Typisch	215 mA
	Max.	240 mA
24 V Relais-interne Stromaufnahme	Typisch	95 mA
	Max.	130 mA
Verlustleistung	4 erregte Relais	3 W typisch, 3,9 W max.

Installation des M580-Sicherheits-PAC

Inhalt dieses Kapitels

Übersicht

In diesem Kapitel wird die Installation des M580-Sicherheits-PAC beschrieben.

HINWEIS: Weitere Informationen zur Installation von M580-PACs finden Sie unter *Installation eines lokalen Racks* im *Modicon M580 Hardware-Referenzhandbuch*.

Installation von M580-Racks und -Erweiterungsmodulen

Einführung

In diesem Abschnitt wird die Installation von M580-Racks und -Erweiterungsmodulen für einen M580-Sicherheits-PAC beschrieben.

Plannung der Installation des lokalen Racks

Einleitung

Größe und Anzahl der Racks und der in den Racks installierten Module sind wichtige Faktoren bei der Planung einer Anlage. Die Installation kann entweder innerhalb oder außerhalb eines Gehäuses erfolgen. Höhe, Breite und Tiefe des installierten Systemkopfs sowie die erforderlichen Abstände zwischen den lokalen und den Erweiterungsracks müssen im Detail bekannt sein.

⚠WARNUNG

UNERWARTETER BETRIEB VON GERÄTEN

Installieren Sie die Racks längs und horizontal, um die Belüftung zu erleichtern.

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

Module wie die Spannungsversorgung, die CPU und die E/A werden durch natürliche Konvektion belüftet. Bringen Sie sie in einem horizontal installierten Rack unter, wie in diesem Handbuch gezeigt, um die erforderliche thermische Kühlung zu gewährleisten. Andere Rackmontage-Positionen können zu einer Überhitzung und einem unerwarteten Verhalten der Geräte führen.

Nutzung der Racks

Nachstehend werden die in Control Expert verfügbaren Racks und deren zulässige Nutzung beschrieben:

Referenz	Steck-platz	Bus	Verwendung			
			Lokales Haupt-rack	Lokales Erweite-rungsrack	Dezentra-les Hauptrack	Dezentrales Erweite-rungsrack
BME-Racks:						
BME XBP 0400	4	X Bus und Ethernet	x	x	x	x
BME XBP 0800	8	X Bus und Ethernet	x	x	x	x
BME XBP 1200	12	X Bus und Ethernet	x	x	x	x
BME XBP 0602	6	X Bus und Ethernet	x	x	x	x
BME XBP 1002	10	X Bus und Ethernet	x	x	x	x
BMX-Racks:						
BMX XBP 0400	4	X Bus	–	x	x	x
BMX XBP 0600	6	X Bus	–	x	x	x
BMX XBP 0800	8	X Bus	–	x	x	x
BMX XBP 1200	12	X Bus	–	x	x	x
Premium-Racks:						
HINWEIS: Premium-Racks werden von M580-Sicherheits-PACs nicht unterstützt.						
Quantum-Racks:						
140 XBP 002 00	2	Quantum	–	–	x	x
140 XBP 003 00	3	Quantum	–	–	x	x
140 XBP 004 00	4	Quantum	–	–	x	x
140 XBP 006 00	6	Quantum	–	–	x	x
140 XBP 010 00	10	Quantum	–	–	x	x
140 XBP 016 00	16	Quantum	–	–	x	x
X: Zulässig –: Nicht zulässig						

Mindestabstsand um die Racks

Halten Sie zur Gewährleistung der Kühlung einen Mindestabstand von 12 mm an der rechten Seite jedes Racks ein.

Wenn Ihre Planung Erweiterungsracks umfasst, ist ein Mindestabstand von 35 mm vor den Modulen einzuhalten. Für die Rack-Erweiterungsmodule BMX XBE 1000 ist dieser Mindestabstand für den lokalen Busanschluss und den Abschlusswiderstand erforderlich.

Platzbedarf der M580 CPU in einem lokalen Hauptrack

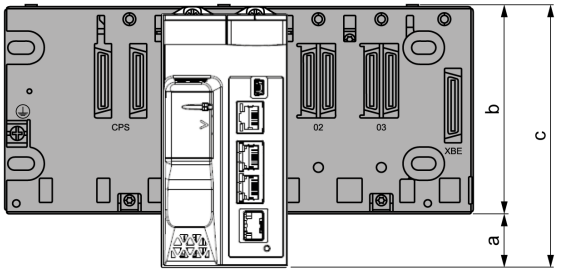
⚠WARNUNG

ÜBERHITZUNG UND UNERWARTETER BETRIEB VON GERÄTEN

Achten Sie bei der Installation der Racks auf geeignete thermische Abstände.

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

Im lokalen Hauptrack ist ein zusätzlicher Abstand am unteren Rand des Racks für die CPU- vorzusehen. Diese Abbildung zeigt die Montageabmessungen bei Verwendung eines X Bus- oder eines Ethernet-Racks. Die Gesamthöhe des lokalen Hauptracks beträgt in beiden Fällen 134, 6 mm.



a Zusätzlicher Abstand unter dem Rack zur Berücksichtigung der Höhe der CPU. X Bus-Rack: Der Abstand beträgt 32,0 mm (1.260 in.).Ethernet-Rack: Der Abstand beträgt 30,59 mm (1.204 in.).

b Höhe des Racks. X Bus-Rack: Die Höhe beträgt 103,7 mm.Ethernet-Rack: Die Höhe beträgt 105,11 mm.

c Höhe des lokalen Hauptracks: 135,7 mm.

Thermische Faktoren innerhalb eines Gehäuses

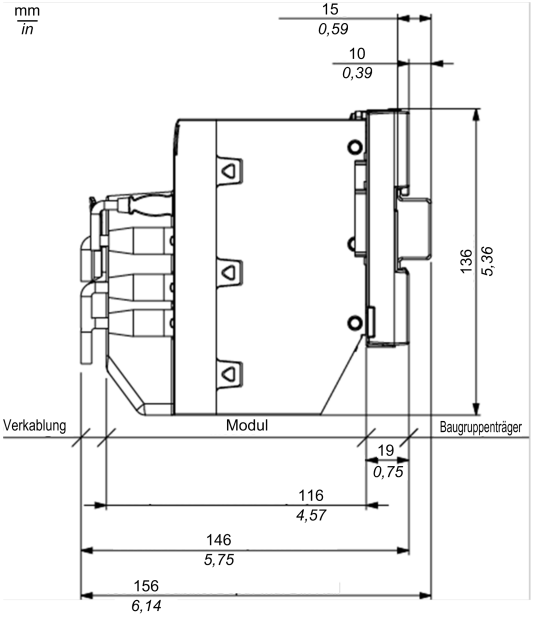
Wenn die Racks in einem Gehäuse installiert werden, muss für eine ausreichende Luftzirkulation gesorgt werden. Verwenden Sie ein Gehäuse mit folgenden Mindestabständen:

- 80 mm (3.15 in.) über dem oberen Rand der Module im Rack
- 60 mm (2.36 in.) unter dem unteren Rand der Module im Rack
- 60 mm (2.36 in.) zwischen den Modulen und Leitungsführungen

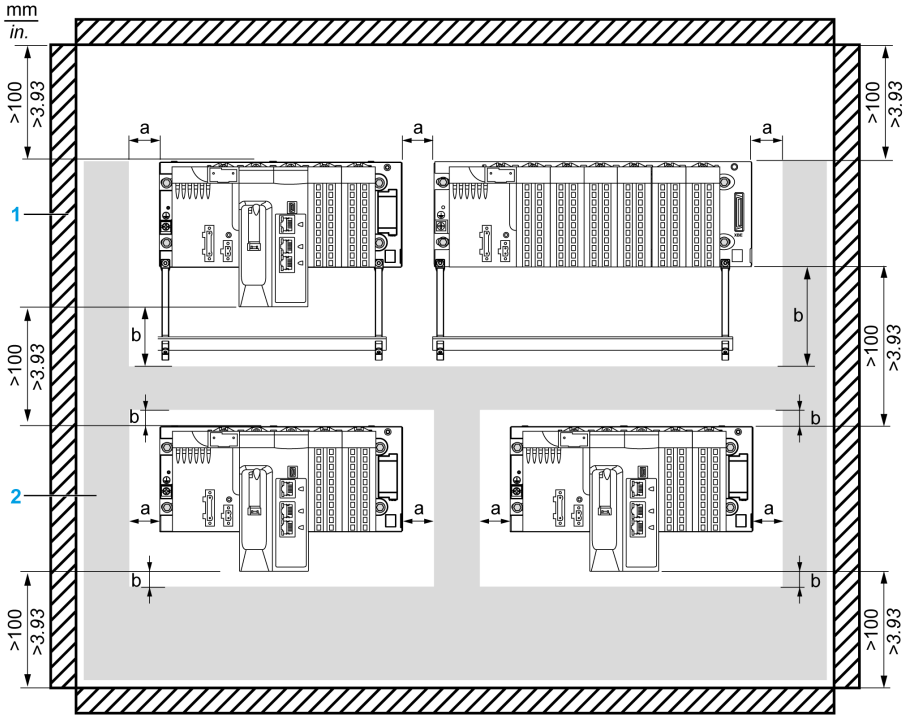
Mindesttiefe des Gehäuses:

- 150 mm (5.91 in.) bei einer Befestigung des Racks auf einer Platte
- 160 mm (6.30 in.) bei einer Montage des Racks auf einer 15 mm (0.59 in.) DIN-Schiene
- Wenn BMX XBE 1000Rack-Erweiterungsmodule angeschlossen werden, wird die Verwendung von Kabeln des Typs BMX XBC •••K mit rechtwinkligen 45°-Anschlüssen empfohlen.

Nachstehend die Seitenansicht eines Racks auf einer DIN-Schiene mit in einem Gehäuse untergebrachten Modulen und Kabeln:



Die folgende Abbildung zeigt die Regeln zu einer typischen Installation in einem Schaltschrank mit Kabelkanälen:



1 Apparatur bzw. Gehäuse

2 Kabelkanal oder -wanne

a Seitlicher Abstand: > 40 mm (1.57 in.)

b Oberer und unterer Abstand mit umliegenden Gegenständen > 20 mm (0.79 in.)

HINWEIS: Um die Dichte zu erhöhen, ist ein geringerer Abstand unter folgenden Bedingungen zulässig:

- Zwischen den Racks befinden sich weder eine Erdungsleiste noch Kabelkanäle.
- Der Abstand zwischen den Racks beträgt nicht weniger als 40 mm (1.57 in).
- Es erfolgt eine Herabsetzung von 5 °C (9 °F) der maximal zulässigen Umgebungstemperatur. Das bedeutet 55 °C (131 °F) bei Standardmodulen und beschichteten Modulen und 65 °C (149 °F) bei Hardened-Modulen.

Montage der Racks

Einführung

Für Ethernet- und X Bus-Racks sind folgende Montagemöglichkeiten gegeben:

- Montage auf einer DIN-Schiene
- Anbringung an einer Wand
- Telequick-Montageplatinen

HINWEIS: Montieren Sie die Racks auf einer ordnungsgemäß geerdeten Metallfläche, um einen störungsfreien Betrieb des PAC bei elektromagnetischen Interferenzen zu gewährleisten.

HINWEIS: Die Montageschrauben auf der linken Seite des Baugruppenträgers sind u. U. zugänglich, ohne dass das Stromversorgungsmodul ausgesteckt werden muss. Montieren Sie den Baugruppenträger mit dem Befestigungsloch ganz links auf der Tafel.

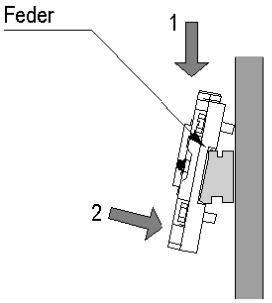
Montage auf einer DIN-Schiene

Die meisten Racks können auf DIN-Schienen mit einer Breite von 35 mm (1.38 in.) und einer Tiefe von 15 mm (0.59 in.) montiert werden.

HINWEIS: Racks mit einer Länge über 400 mm (15.75 in.) und mit mehr als 8 Modulsteckplätzen sind nicht mit einer DIN-Schienenmontage kompatibel. Racks der Modelle BMXXBP1200 (PV:02 oder höher) (H), BMEXBP1002 (H) oder BMEXBP1200 (DIN) sind auf einer H-Schiene zu installieren.

HINWEIS: Bei der Montage auf einer DIN-Schiene ist das System einer größeren mechanischen Belastung ausgesetzt.

Gehen Sie zur Montage eines Racks auf einer DIN-Schiene vor wie folgt:

Schritt	Aktion	Abbildung
1	Setzen Sie das Rack auf den oberen Rand der DIN-Schiene auf und drücken Sie die Rackoberseite nach unten, um die Kontaktfedern gegen die DIN-Schiene zu komprimieren.	
2	Drücken Sie dann die Rackunterseite nach hinten, um das Rack flach an die DIN-Schiene anzulegen.	
3	Lassen Sie das Rack los, um es zu verriegeln.	

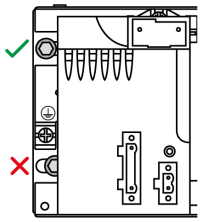
Gehen Sie zur Demontage eines Racks von einer DIN-Schiene vor wie folgt:

Schritt	Aktion
1	Drücken Sie die Rackoberseite nach unten, um die Kontaktfedern gegen die DIN-Schiene zu komprimieren.
2	Ziehen Sie dann die Rackunterseite nach vorn, um das Rack von der DIN-Schiene zu lösen.
3	Nehmen Sie das gelöste Rack ab.

Montage an einer Wand

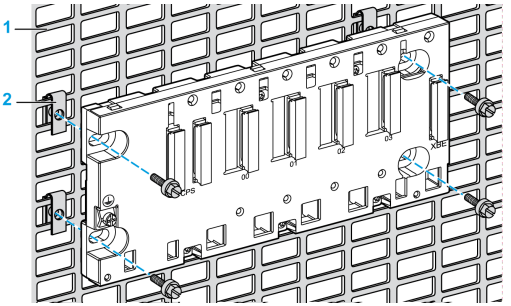
Sie können ein Rack an einer Wand innerhalb oder außerhalb eines Gehäuses mithilfe von M4-, M5-, M6- oder UNC #6-Schrauben in den Befestigungslöchern anbringen.

Bringen Sie die 2 linksseitigen Schrauben (neben der Spannungsversorgung) so nah wie möglich am linken Rand des Racks an. Dadurch wird der problemlose Zugang zu den Schrauben nach der Montage der Spannungsversorgung gewährleistet.



Montage auf Telequick-Lochplatinen AM1-PA und AM3-PA-Montageplatten

Sie können ein Rack auf einer Telequick-AM1-PA- oder AM3-PA-Lochplatine mithilfe von M4-, M5-, M6- oder UNC #6-Schrauben anbringen.



Erweiterung eines Racks

Einführung

Wenn Ihre Installation mehr als ein Rack im lokalen Rack oder in einer dezentralen Station umfasst, müssen Sie im Hauptrack und im Erweiterungsrack ein BMXXBE1000-Erweiterungsmodul installieren. Rack-Erweiterungsmodule werden über X Bus-Erweiterungskabel miteinander verbunden.

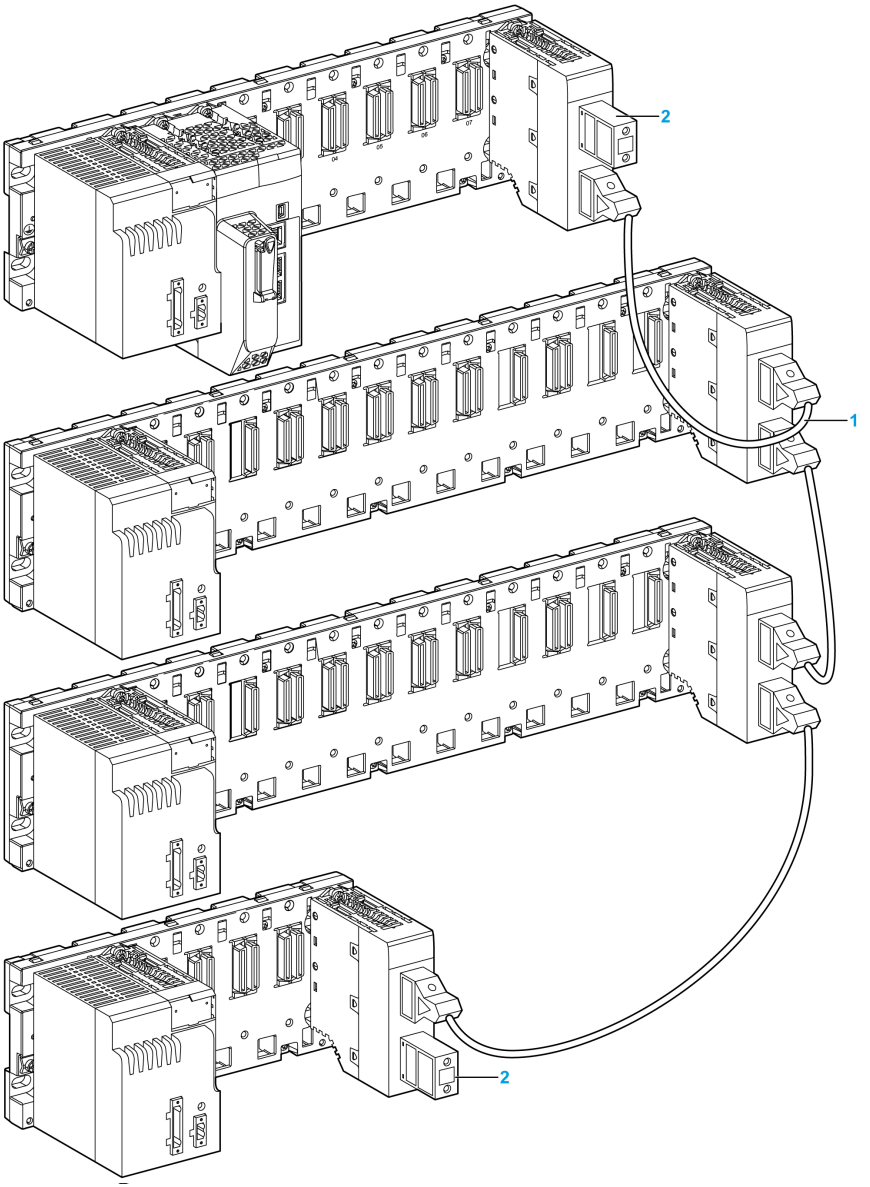
HINWEIS: Informationen zur Installation und Verbindung von Rack-Erweiterungsmodulen finden Sie unter *Installation von Modicon X80-Rack-Erweiterungsmodulen* im *Modicon M580 Hardware-Referenzhandbuch*.

Einrichtung eines M580-Sicherheitssystems mit lokalen Erweiterungsracks

Unter Verwendung von BMXXBE1000-Erweiterungsmodulen und -Kabeln können Sie Ihrem M580-Sicherheits-PAC folgende Komponenten hinzufügen:

- Bis zu 7 Erweiterungsracks zum lokalen Hauptrack
- 1 Erweiterungsrack zu einem dezentralen Hauptrack

Beispiel eines lokalen Ethernet-Hauptracks mit Erweiterungsracks und Erweiterungsmodulen und -kabeln:



1 Dieselbe Station kann Racks unterschiedlicher Größe enthalten, die über Erweiterungskabel miteinander verbunden sind.

2 Die an den Enden der Verbindungskabel befindlichen Erweiterungsmodule werden abgeschlossen.

Installation von CPU, Koprozessor, Spannungsversorgung und E/A eines M580-Sicherheitssystems

Einführung

In diesem Abschnitt wird die Installation einer CPU, eines Koprozessors, einer Spannungsversorgung sowie von E/A-Modulen in einem M580-Sicherheitssystem beschrieben.

Installation von CPU und Koprozessor

Einführung

Sie können die CPU BME•58•040S und den Koprozessor BMEP58CPROS3 in einem Ethernet-Rack BMEXBP••00 oder BMEXBP••02 installieren.

Vorsichtsmaßnahmen bei der Installation

Eine CPU-M580 wird über den Rack-Bus gespeist. Vergewissern Sie sich, dass die Spannungsversorgung des Racks ausgeschaltet ist, bevor Sie die CPU installieren.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS

Trennen Sie alle Spannungsquellen, bevor Sie die CPU installieren.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

Entfernen Sie die Schutzabdeckung von den Steckplatzanschlüssen des Racks, bevor Sie das Modul an das Rack anschließen.

⚠WARNUNG
UNERWARTETER GERÄTEBETRIEB Vergewissern Sie sich, dass die CPU keine nicht unterstützte SD-Speicherkarte enthält, bevor Sie die CPU unter Spannung setzen. **Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.**

HINWEIS:

- Stellen Sie sicher, dass die Abdeckung des Speicherkartensteckplatzes nach Einsetzen einer Speicherkarte in die CPU geschlossen ist.
- Im Systemwort `%SW97` können Sie den Status der SD-Karte prüfen.

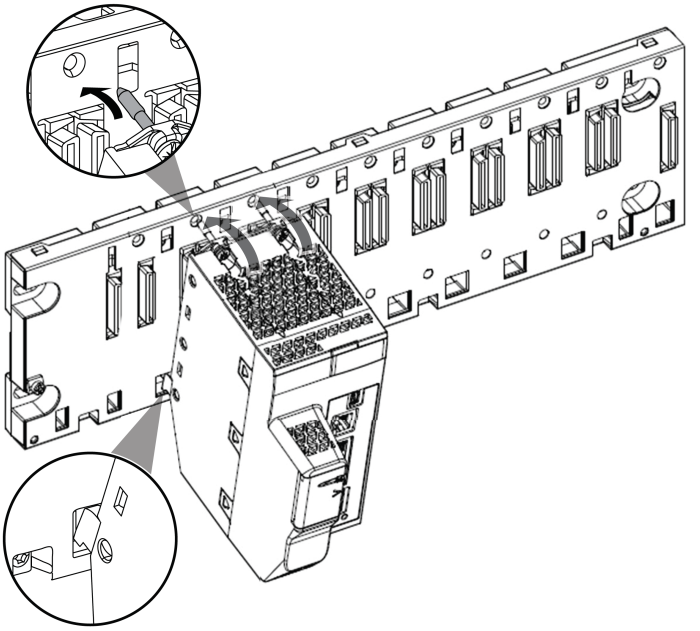
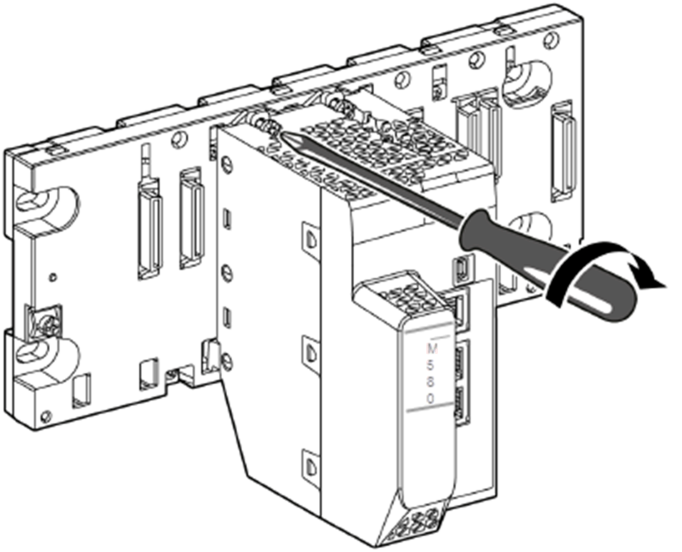
Installation der CPU und des Koprozessors im Rack

Installieren Sie die CPU und den Koprozessor in folgenden Racksteckplätzen:

- CPU: Steckplätze **00** und **01**
- Koprozessor: Steckplätze **02** und **03**

Gehen Sie vor wie folgt, um die CPU und den Koprozessor in einem Rack zu installieren:

Schritt	Aktion
1	Stellen Sie sicher, dass die Spannungsversorgung ausgeschaltet ist.
2	Stellen Sie sicher, dass folgende Voraussetzungen gegeben sind: • Bei Verwendung einer SD-Speicherkarte: Die Karte wird von der CPU unterstützt. • Die Schutzabdeckungen der Anschlüsse wurden entfernt. • Die CPU wird in die Steckplätze mit der Markierung **00** und **01** eingesetzt.

Schritt	Aktion	
3	Positionieren Sie die Führungsnasen an der Modulrückseite unten in den entsprechenden Steckplätzen im Rack.	
4	Schieben Sie das Modul an den oberen Bereich des Racks, sodass das Modul bündig an die Rack-Rückseite anschließt. Das Modul befindet sich jetzt in der richtigen Position.	
5	Ziehen Sie die 2 Schrauben am oberen Rand der CPU fest, um das Modul sicher am Rack zu befestigen. Anzugsmoment: 0,4 bis 1,5 N•m (0,30 bis 1,10 lbf-ft).	
6	Für die Installation des Koprozessormoduls setzen Sie das Modul in die Steckplätze **02** und **03** ein und führen die oben beschriebenen Schritte 3, 4 und 5 aus.	

Erdung

Befolgen Sie alle landesspezifischen und örtlichen Sicherheitsnormen und -vorschriften.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS

Wenn Sie nicht mit Sicherheit feststellen können, dass das Ende eines geschirmten Kabels örtlich geerdet ist, muss das Kabel als gefährlich eingestuft und es muss angemessene persönliche Schutzausrüstung (PSA) getragen werden.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

Informationen zur Erdung von CPU und Koprozessor finden Sie unter *Hinweise zur Erdung* im *Modicon M580 Hardware-Referenzhandbuch*.

Installation eines Spannungsversorgungsmoduls

Einführung

Installieren Sie das Sicherheitsspannungsversorgungsmodul M580 in einem beliebigen X Bus- oder Ethernet-Rack, in dem noch andere M580-Sicherheitsmodule untergebracht werden sollen. Das Sicherheitsspannungsversorgungsmodul kann in Racks verwendet werden, die entweder eine einzige Spannungsversorgung oder zwei redundante Spannungsversorgungen benötigen.

⚠ WARNUNG

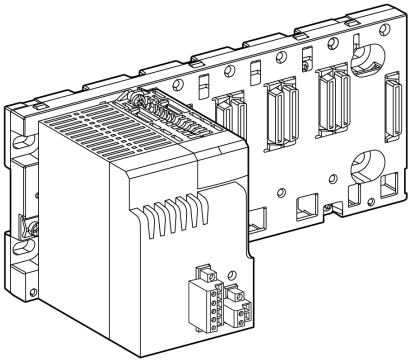
VERLUST DER FÄHIGKEIT ZUR AUSFÜHRUNG DER SICHERHEITSFUNKTION

Setzen Sie die Sicherheitsspannungsversorgung BMXCPS4002S, BMXCPS4022S oder BMXCPS3522S nur in einem Rack ein, das mindestens ein anderes Sicherheitsmodul enthält.

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

Bei einem Rack mit nur einer Spannungsversorgung installieren Sie das M580-Sicherheitsspannungsversorgungsmodul in den 2 Racksteckplätzen mit der Markierung **CPS**. Bei einem Rack mit doppelter Spannungsversorgung BMEXBP••02 (siehe Modicon M580, Hardware, Referenzhandbuch) installieren Sie zwei Sicherheitsspannungsversorgungsmodule M580 nebeneinander in den 4 Steckplätzen mit der Markierung **CPS**.

Beispiel für ein einzelnes Spannungsversorgungsmodul in einem BMEXBP0400-Rack:



HINWEIS: Aufgrund ihres spezifischen Designs können die Spannungsversorgungsmodule nur in den speziell dafür vorgesehenen **CPS**-Steckplätzen eingesetzt werden.

Vorsichtsmaßnahmen bei der Installation

Das Sicherheitsspannungsversorgungsmodul M580 unterstützt kein Hot Swapping. Stellen Sie sicher, dass das Modul ausgeschaltet ist, wenn Sie es in den Baugruppenträger einführen oder darauf entnehmen.

HINWEIS
GEFAHR EINES UNBEABSICHTIGTEN SYSTEMVERHALTENS Vergewissern Sie sich, dass die Spannungsversorgung abgeschaltet ist, wenn Sie ein M580-Sicherheitsspannungsversorgungsmodul aus einem Rack entnehmen bzw. in ein Rack einsetzen. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Die abnehmbare Haupt-Eingangsklemmenleiste darf weder aufgesteckt noch abgenommen werden, wenn das Sicherheitsspannungsversorgungsmodul M580 unter Spannung steht. Stellen Sie sicher, dass die Spannungszufuhr zum Modul über den vorgeschalteten Leistungsschalter abgeschaltet wurde, bevor Sie diese Eingriffe vornehmen.

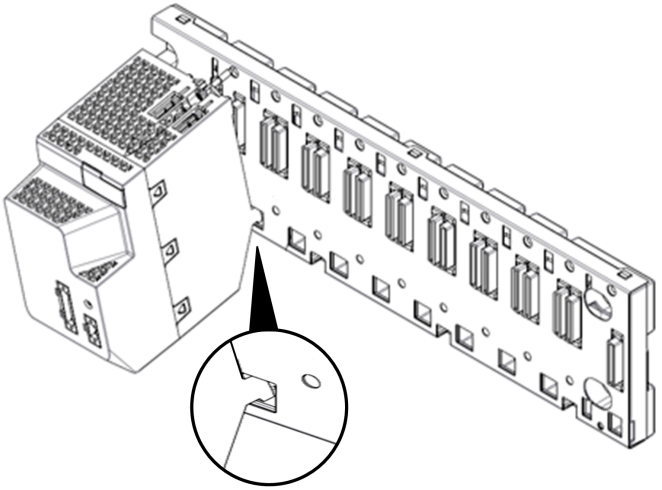
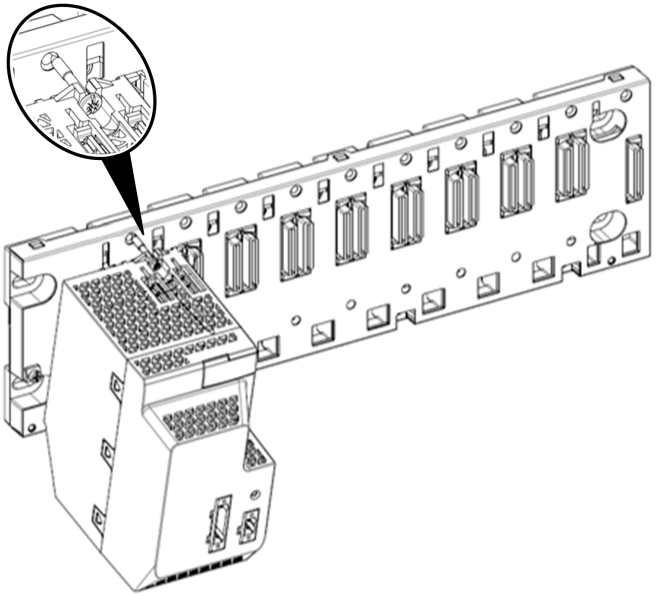
HINWEIS
GEFAHR EINES UNBEABSICHTIGTEN SYSTEMVERHALTENS Vergewissern Sie sich, dass die Spannungsversorgung abgeschaltet ist - d. h. der vorgeschaltete Leistungsschalter befindet sich in den OFF-Position -, bevor Sie die abnehmbare Haupt-Eingangsklemmenleiste des Sicherheitsspannungsversorgungsmoduls M580 aufstecken bzw. abnehmen. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Die abnehmbare Alarmrelais-Klemmenleiste darf weder aufgesteckt noch abgenommen werden, während das Sicherheitsspannungsversorgungsmoduls M580 in Betrieb ist. Stellen Sie sicher, dass das Modul vollständig spannungsfrei ist, bevor Sie diese Eingriffe vornehmen.

HINWEIS
GEFAHR EINES UNBEABSICHTIGTEN SYSTEMVERHALTENS Vergewissern Sie sich, dass das Sicherheitsspannungsversorgungsmodul M580 vollständig spannungsfrei ist, bevor Sie die abnehmbare Alarmrelais-Klemmenleiste des Moduls anbringen bzw. abnehmen. **Die Nichtbeachtung dieser Anweisungen kann Sachschäden zur Folge haben.**

Installation der Spannungsversorgung in einem Rack

Gehen Sie vor wie folgt, um das Sicherheitsspannungsversorgungsmodul in den Racksteckplätzen mit der Markierung **CPS** zu installieren:

Schritt	Aktion	
1	Stellen Sie sicher, dass Sie die Steckplätze mit der Markierung **CPS** für die Installation des Spannungsversorgungsmoduls ausgewählt haben.	
2	Positionieren Sie die Führungsnasen an der Modulrückseite unten in den entsprechenden Steckplätzen im Rack.	
3	Schieben Sie das Modul an den oberen Bereich des Racks, sodass das Modul bündig an die Rack-Rückseite anschließt. Das Modul befindet sich jetzt in der richtigen Position.	
4	Ziehen Sie die Schraube an der Oberseite der Spannungsversorgung fest, um das Modul in seiner Position im Rack zu sichern. Anzugsmoment: 0,4 bis 1,5 N•m (0,30 bis 1,10 lbf-ft).	
5	Bei Racks, die 2 Spannungsversorgungen benötigen, müssen Sie die Schritte 2, 3 und 4 für die zweite Spannungsversorgung wiederholen.	

Erdung des Spannungsversorgungsmoduls

Befolgen Sie alle landesspezifischen und örtlichen Sicherheitsnormen und -vorschriften.

⚠⚠ GEFAHR

GEFAHR EINES ELEKTRISCHEN SCHLAGS

Wenn Sie nicht mit Sicherheit feststellen können, dass das Ende eines geschirmten Kabels örtlich geerdet ist, muss das Kabel als gefährlich eingestuft und es muss angemessene persönliche Schutzausrüstung (PSA) getragen werden.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

Informationen zur Erdung der Spannungsversorgung finden Sie im Abschnitt *Erdung des Spannungsversorgungsmoduls*.

Installation von M580-Sicherheits-E/A

Einführung

Sie können in jedem beliebigen X Bus- oder Ethernet-Rack ein M580-E/A-Sicherheitsmodul installieren, indem Sie es in einem Steckplatz positionieren, der nicht für die Sicherheitsspannungsversorgung oder die CPU (im Fall eines lokalen Hauptracks) reserviert ist.

HINWEIS: Verwenden Sie für Racks mit E/A-Sicherheitsmodulen ausschließlich eine Sicherheitsspannungsversorgung BMXCPS4002S, BMXCPS4022S oder BMXCPS3522S.

M580-Sicherheits-E/A unterstützen Hot Swapping.

Allgemeine Hinweise zur Verkabelung

Um zu große Interferenzen zwischen einer Gleichstromlast und einer Wechselstromquelle zu verhindern, müssen die Leistungskabel (z. B. die Zuleitungen zur Spannungsversorgung) separat von den von Sensoren angehenden Eingangskabeln wie auch von den zu den Stellgliedern führenden Ausgangskabeln verlegt werden.

Statten Sie die Kabel, die die CPU mit den E/A-Modulen verbindet, mit einer Ummantelung aus, die in einen Metallkanal eingeschlossen ist. Trennen Sie die Ummantelung der E/A-Kabel von der Leistungsverkabelung, die in einem eigenen Kabelmantel verlegt werden muss. Führen Sie die ummantelten Leistungskabel in von den E/A-Kabeln getrennten

Kabelkanälen. Leistungs- und E/A-Kabel müssen durch einen Mindestabstand von 100 mm voneinander getrennt verlegt werden.

Sicherheitshinweise zur Erdung

Jedes M580-E/A-Sicherheitsmodul ist mit Erdungskontakten ausgestattet.

Schneider Electric empfiehlt die Verwendung einer BMXXSP••••-Leiste zum Schutz des Racks vor elektromagnetischen Störungen.

Die BMXXSP••••-Leiste wird insbesondere für das analoge Sicherheitseingangsmodul BMXSAI0410 empfohlen. Verbinden Sie den Kabelmantel mit der Erdungsleiste durch Anklemmen auf Modulseite.

⚠⚠ GEFAHR

STROMSCHLAG-, EXPLOSIONS- ODER LICHTBOGENGEFAHR

Bei der Montage oder Demontage von E/A-Sicherheitsmodulen ist Folgendes zu beachten:

- Vergewissern Sie sich, dass jede Klemmenleiste mit der BMXXSP••••-Erdungsleiste verbunden ist.
- Trennen Sie die Spannungsversorgung der Sensoren bzw. Stellglieder.

Die Nichtbeachtung dieser Anweisungen führt zu Tod oder schweren Verletzungen.

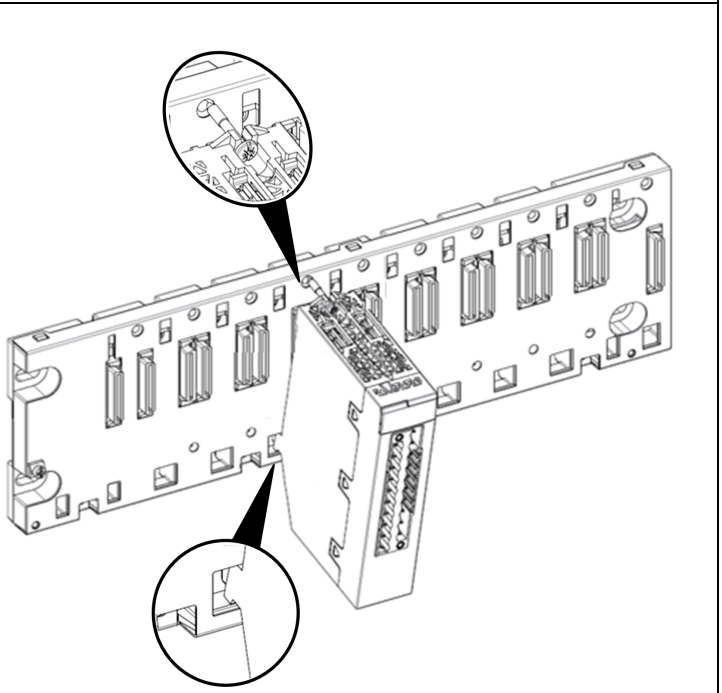
Installation von Eingangsmodulsensoren (in Bezug auf die Erdung)

Bei der Installation von Sensoren in Ihrem System ist Folgendes zu beachten:

- Positionieren Sie die Sensoren in nächster Nähe zueinander. Sie dürfen maximal ein paar Meter voneinander entfernt sein.
- Referenzieren Sie alle Sensoren an einem zentralen Punkt und verbinden Sie diesen Punkt mit der PAC-Erde.

Installation eines E/A-Sicherheitsmoduls in einem Rack

Für ein M580-E/A-Sicherheitsmodul ist ein einzelner Racksteckplatz erforderlich. Sie können ein E/A-Sicherheitsmodul in einem beliebigen Steckplatz installieren, vorausgesetzt, dieser ist weder für die Spannungsversorgung noch für die CPU reserviert. Gehen Sie vor wie folgt, um ein E/A-Sicherheitsmodul in einem Rack zu installieren:

Schr-itt	Aktion	
1	Positionieren Sie die Führungsnasen an der Modulrückseite unten in den entsprechenden Steckplätzen im Rack.	
2	Schieben Sie das Modul an den oberen Bereich des Racks, sodass das Modul bündig an die Rack-Rückseite anschließt. Das Modul befindet sich jetzt in der richtigen Position.	
3	Ziehen Sie die Schraube an der Moduloberseite fest, um das Modul in seiner Position im Rack zu sichern. Anzugsmoment: 0,4 bis 1,5 N•m (0,30 bis 1,10 lbf-ft).	
4	Wiederholen Sie die Schritte 1, 2 und 3 für jedes weitere Modul, bis alle Module im Rack untergebracht sind.	

Erdung der E/A-Module

Informationen zur Erdung finden Sie im Abschnitt *Erdung des Spannungsversorgungsmoduls*.

HINWEIS: Für das analoge Sicherheitseingangsmodul BMXSAI0410 empfiehlt Schneider Electric die zusätzliche Verwendung einer Erdungsleiste des Typs BMXXSP••••. Informationen zur Installation dieses Geräts finden Sie im Abschnitt *Schirmanschlusskit*.

Installation einer SD-Speicherkarte in einer CPU

Einführung

Die CPU BME•58•040S unterstützt die Verwendung der SD-Speicherkarte BMXRMS004GPF mit 4 GB.

Wartung von Speicherkarten

Gehen Sie zur Wahrung des ordnungsgemäßen Funktionszustands einer Speicherkarte vor wie folgt:

- Entnehmen Sie die Speicherkarte nicht aus ihrem Steckplatz, während die CPU auf die Karte zugreift (grüne LED des Speicherkartenzugriffs leuchtet permanent oder blinkt).
- Berühren Sie die Anschlüsse der Speicherkarte nicht.
- Bringen Sie die Speicherkarte nicht in die Nähe elektrostatischer oder elektromagnetischer Quellen, und halten Sie Hitze, Sonnenlicht, Wasser und Feuchtigkeit fern.
- Schützen Sie die Speicherkarte vor Stößen und Erschütterungen.
- Bevor Sie eine Speicherkarte per Post versenden, prüfen Sie die Sicherheitsrichtlinien des Postdienstleisters. In einigen Ländern wird die Post aus Sicherheitsgründen hohen Strahlungen ausgesetzt. Diese hohen Strahlungen können den Inhalt der Speicherkarte löschen und sie unbrauchbar machen.
- Wenn bei Entnahme der Karte keine steigende Flanke an Bit %S65 ausgelöst und nicht sichergestellt wird, dass die grüne LED des Speicherkartenzugriffs ausgeschaltet ist, gehen unter Umständen die Daten (Dateien, Anwendung usw.) verloren oder werden unzuverlässig.

Speicherkarten-Einsteckvorgang

Gehen Sie zum Einstecken der Speicherkarte in eine CPU BME•58•040S vor wie folgt:

Schritt	Beschreibung
1	Öffnen Sie die Schutzabdeckung der SD-Speicherkarte.
2	Stecken Sie die Karte in den Steckplatz ein.

Schritt	Beschreibung
3	Drücken Sie die Speicherkarte nach innen, bis sie in ihrer Position hörbar einrastet. **Ergebnis:** Die Karte sollte jetzt in ihrem Steckplatz gesichert sein. **Hinweis:** Das Einstecken der Speicherkarte bewirkt kein Wiederherstellen der Anwendung.
4	Schließen Sie die Schutzabdeckung der Speicherkarte wieder.

Speicherkarten-Entnahmevorgang

HINWEIS: Vor der Entnahme einer Speicherkarte muss eine steigende Flanke an Bit %S65 ausgelöst werden. Wenn bei Entnahme der Karte keine steigende Flanke an Bit `%S65` ausgelöst und nicht sichergestellt wird, dass die grüne LED des Speicherkartenzugriffs ausgeschaltet ist, gehen unter Umständen die Daten verloren.

Gehen Sie zum Entnehmen der Speicherkarte aus einer CPU BME•58•040S vor wie folgt:

Schritt	Beschreibung
1	Lösen Sie eine steigende Flanke an Bit `%S65` aus.
2	Vergewissern Sie sich, dass die grüne LED des Speicherkartenzugriffs ausgeschaltet ist.
3	Öffnen Sie die Schutzabdeckung derSD Speicherkarte wieder.
4	Ziehen Sie an der Speicherkarte, bis ein Klicken zu hören ist, und lassen Sie die Karte dann los. **Ergebnis:** Die Karte sollte aus dem Steckplatz springen.
5	Nehmen Sie die Speicherkarte aus dem Steckplatz heraus. **Hinweis:** Die grüne LED des Speicherkartenzugriffs leuchtet auf, wenn die Speicherkarte aus der CPU entfernt wird.
6	Schließen Sie die Schutzabdeckung der Speicherkarte wieder.

Aktualisierung der Firmware der M580-Sicherheits-CPU

Inhalt dieses Kapitels

Firmware-Aktualisierung mit Automation Device Maintenance

Übersicht

EcoStruxure™ Automation Device Maintenance ist ein Standalone-Tool, das die Aktualisierung der Firmware von (einzelnen oder zahlreichen) Geräten in einem Werk vereinfacht.

Das Tool unterstützt folgende Funktionen:

- Automatische Geräteerkennung
- Manuelle Geräteidentifikation
- Zertifikatsverwaltung
- Gleichzeitige Firmware-Aktualisierung für zahlreiche Geräte

HINWEIS: Eine Beschreibung des Download-Vorgangs finden Sie in folgendem Handbuch: *EcoStruxure™ Automation Device Maintenance, Benutzerhandbuch*.

Aktualisierung der CPU-Firmware mit Unity Loader

Aktualisieren der CPU-Firmware

Sie können die Firmware der CPU aktualisieren, indem Sie eine neue Version der Firmware mithilfe von Unity Loader herunterladen.

Für den Download der Firmware können Sie eine der folgenden Verbindungen verwenden:

- mini-B-CPU-Steckanschluss der USB
- Service-Port der CPU
- Ethernet-Netzwerk

HINWEIS: Eine Beschreibung des Download-Vorgangs finden Sie in folgendem Handbuch: *Unity Loader, Benutzerhandbuch*.

Aktivieren der CPU-Firmwareaktualisierung

Um die Firmwareaktualisierung zu aktivieren, müssen Sie zunächst die Sicherheit für die CPU entsperren:

Element	Beschreibung
1	Klicken Sie im Fenster **SPS-Bus** mit der rechten Maustaste auf die Ethernet-Ports der CPU.
2	Wählen Sie den Befehl **Untermodul öffnen** aus.
3	Klicken Sie auf die Registerkarte **Sicherheit**.
4	Klicken Sie auf **Sicherheit freigeben**.

CPU-Firmwaredatei

Wählen Sie die Firmwaredatei (*.*ldx*) für die BME•58•040S-Sicherheits-CPU aus. Die ldx-Datei enthält Firmwareaktualisierungen für den Sicherheits- und den Prozessbereich der CPU und die zugehörigen Webseiten.

Verfahren zur Aktualisierung der CPU-Firmware

Gehen Sie vor wie folgt, um die Firmware der CPU zu aktualisieren:

Element	Beschreibung
1	Installieren Sie die Software Unity Loader.
2	Verbinden Sie den PC, auf dem Unity Loader ausgeführt wird, mit der CPU.
3	Starten Sie Unity Loader.
4	Klicken Sie auf die Registerkarte **Firmware**.
5	Wählen Sie im Listenfeld **PC** die Datei *.ldx* mit der Firmware-Datei aus.
6	Bei einer Ethernet-Verbindung ist sicherzustellen, dass die im Feld **SPS** angezeigte MAC-Adresse der in der CPU angegebenen MAC-Adresse entspricht.
7	Vergewissern Sie sich, dass das Übertragungssignal grün ist, damit die Übertragung vom PC in die CPU stattfinden kann.
8	Klicken Sie auf **Übertragen**. **HINWEIS:** Während des Downloads der Firmware leuchtet die grüne **DL**-LED der CPU auf. Das verweist darauf, dass die CPU nur mit der Software Unity Loader kommuniziert.
9	Klicken Sie auf **Schließen**.

Nach Abschluss der Firmwareaktualisierung:

- Die CPU wird mit der neuen Firmware neu gestartet.
- Das im Flash-Speicher gespeicherte Anwendungsprogramm wird beibehalten.
- Die CPU führt einen Kaltstart durch und wechselt in den STOP-Betrieb, auch wenn auf der Registerkarte **Konfiguration** der CPU die Option **Automatischer Start in RUN** ausgewählt ist.

  HINWEIS: Wenn der Prozess der Firmwareaktualisierung unterbrochen wird (z. B. durch Trennung der Verbindung oder durch einen Stromausfall), wird die CPU zurückgesetzt und mit der alten Firmware neu gestartet.

Andere Firmware für M580-Sicherheitsmodule

Bei der Aktualisierung der CPU-Firmware wird ebenfalls die Firmware des Koprozessor aktualisiert. Bei jedem Start des Koprozessors erhält dieser sein Betriebssystem von der CPU.

Die Firmware der M580-Sicherheitsspannungsversorgung und der -E/A-Module kann nicht aktualisiert werden.

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

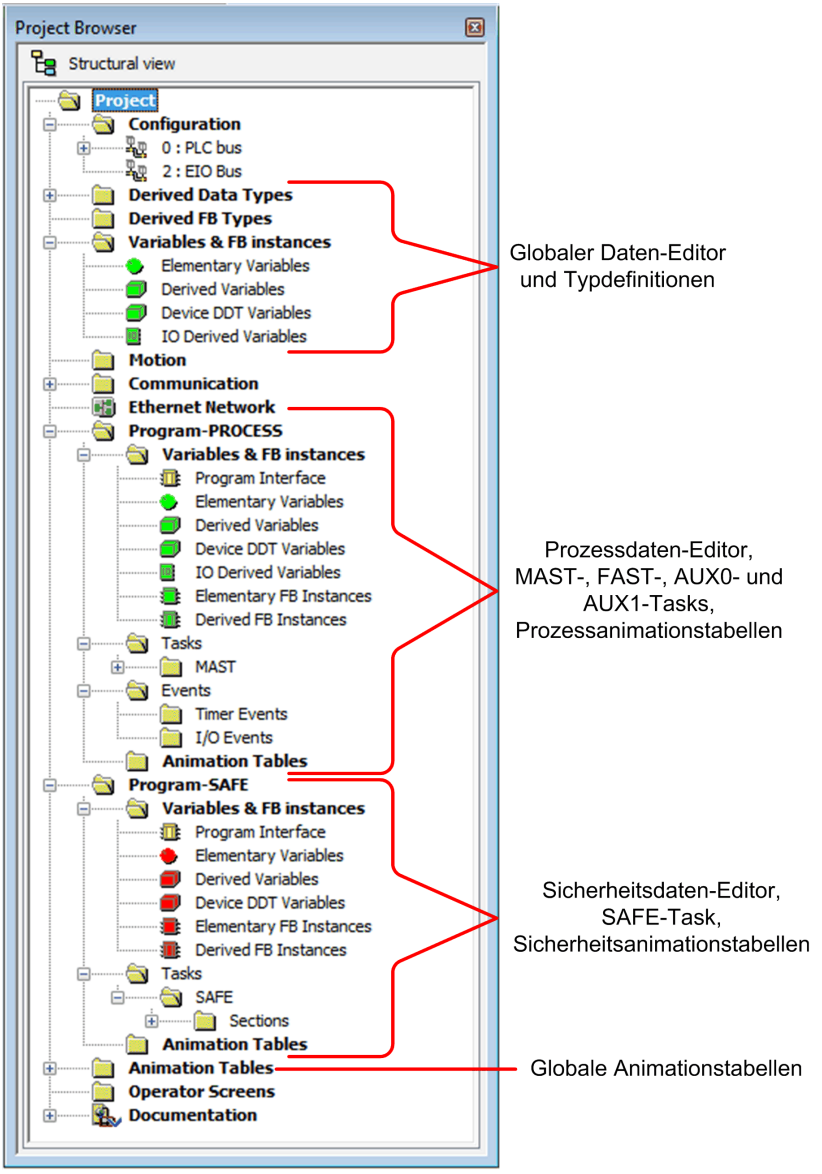
Einführung

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:



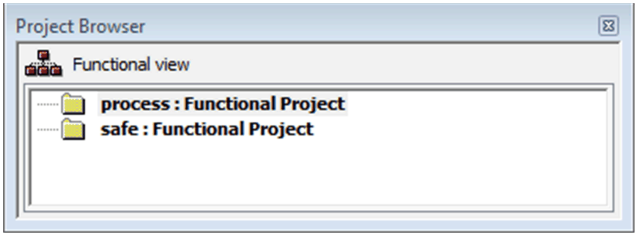
Eine Analyse des **Projekt-Browsers** ergibt Folgendes:

- 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 XL 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 Prozessdaten-Editors und des Sicherheitsdaten-Editors 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

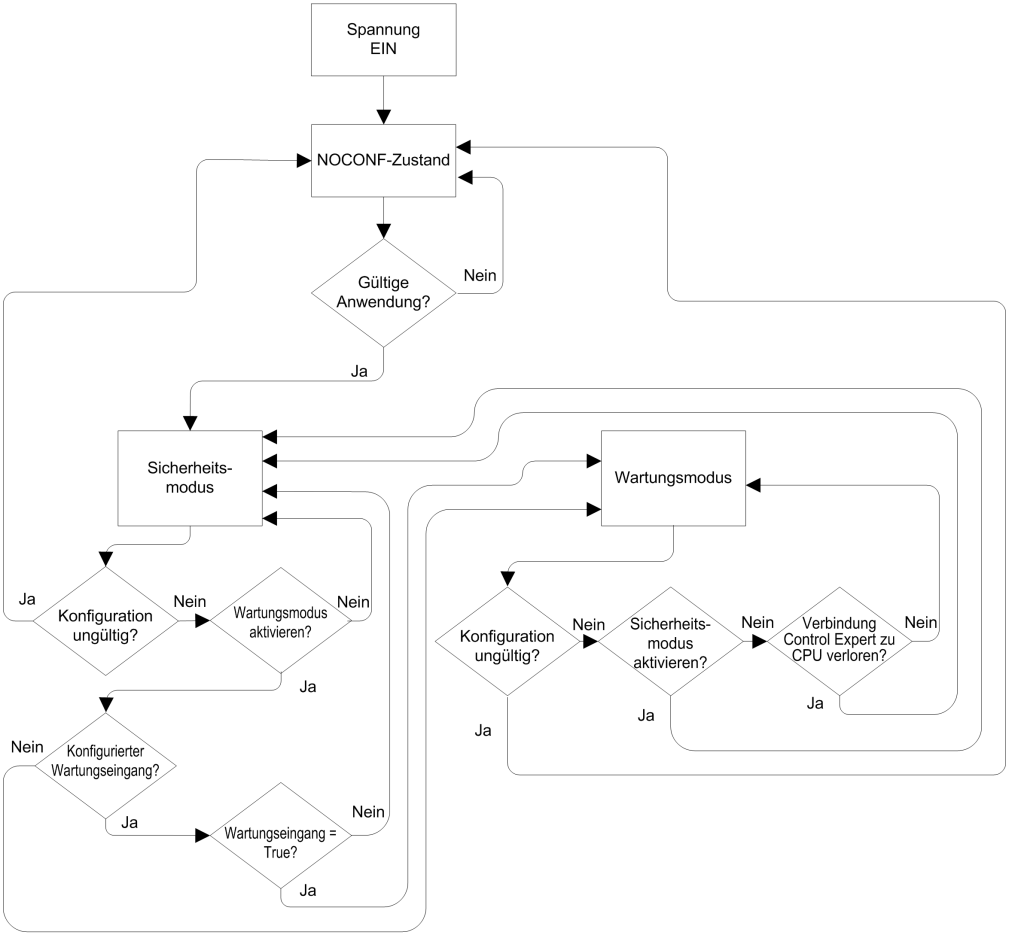
VERLUST DES SICHERHEITS-INTEGRITÄTSLEVELS

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 Coprozessors oder in Control Expert identifizieren.

Status der **SMOD**-LEDs von CPU und Coprozessor:

- *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 (Coprozessor) und %SW13 (CPU), Seite 223 - sie 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*.

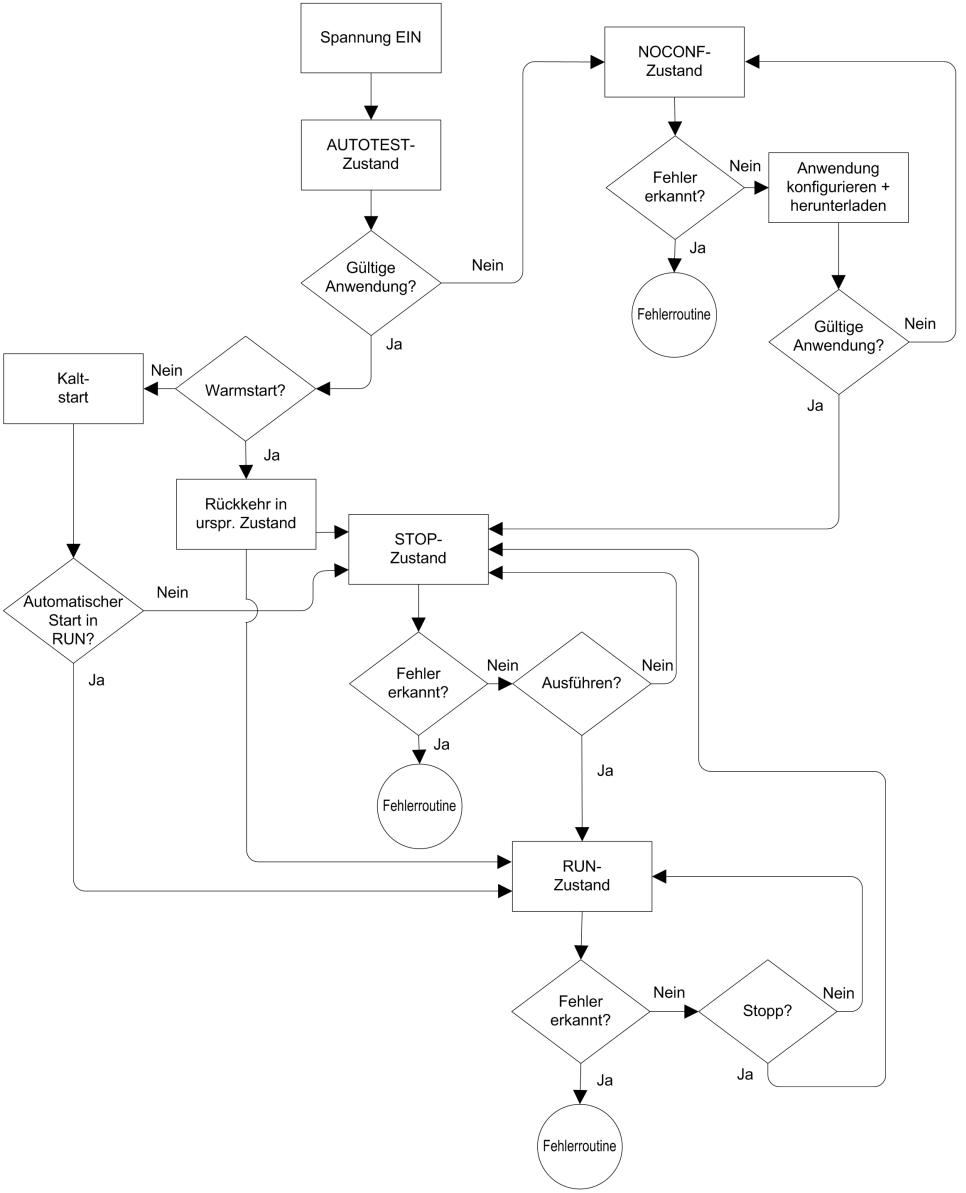
Betriebszustand	Gilt für ...	Beschreibung
AUTOTEST	PAC	Die CPU führt interne Selbsttests durch. **HINWEIS:** Wenn Erweiterungsracks mit dem lokalen Hauptrack verbunden sind und nicht verwendete Anschlüsse am Rack-Erweiterungsmodul nicht mit Leitungsabschlüssen versehen wurden, verbleibt die CPU auch 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 117). • Die Ausführung wurde durch einen STOP-Befehl abgebrochen (sicherer Modus, Seite 117 oder Wartungsmodus, Seite 118). • 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 (siehe Modicon M580, Sicherheitshandbuch) 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 117: Die Sicherheitsfunktion wird ausgeführt und sämtliche Einschränkungen werden angewendet.

Betriebszustand	Gilt für ...	Beschreibung
		• Im Wartungsmodus, Seite 118: 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 131 durch, um den WAIT-Zustand zu verlassen.
ERROR	PAC	Die CPU wird aufgrund eines nicht behebbaren (siehe Modicon M580, Sicherheitshandbuch) Hardware- oder Systemfehlers gestoppt. Der ERROR-Zustand löst die Sicherheitsfunktion (siehe Modicon M580, Sicherheitshandbuch) aus. Wenn das System bereit zum Neustart ist, führen Sie einen Kaltstart, Seite 131 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* (siehe Modicon M580, Sicherheitshandbuch) und *M580-Sicherheitscoprozessor - LED-Diagnose* (siehe Modicon M580, Sicherheitshandbuch) 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 126 finden Sie Informationen zur Fehlerverwaltung durch das Sicherheitssystem.

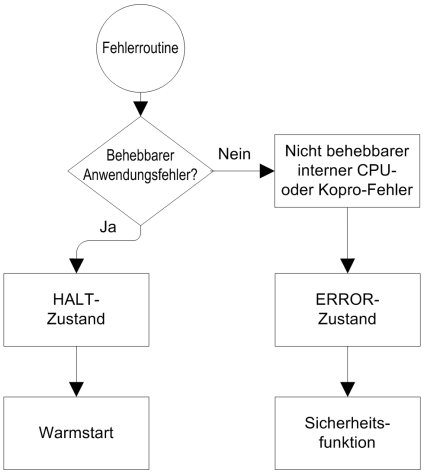
Fehlerverwaltung

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 131 oder einen Warmstart, Seite 131 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

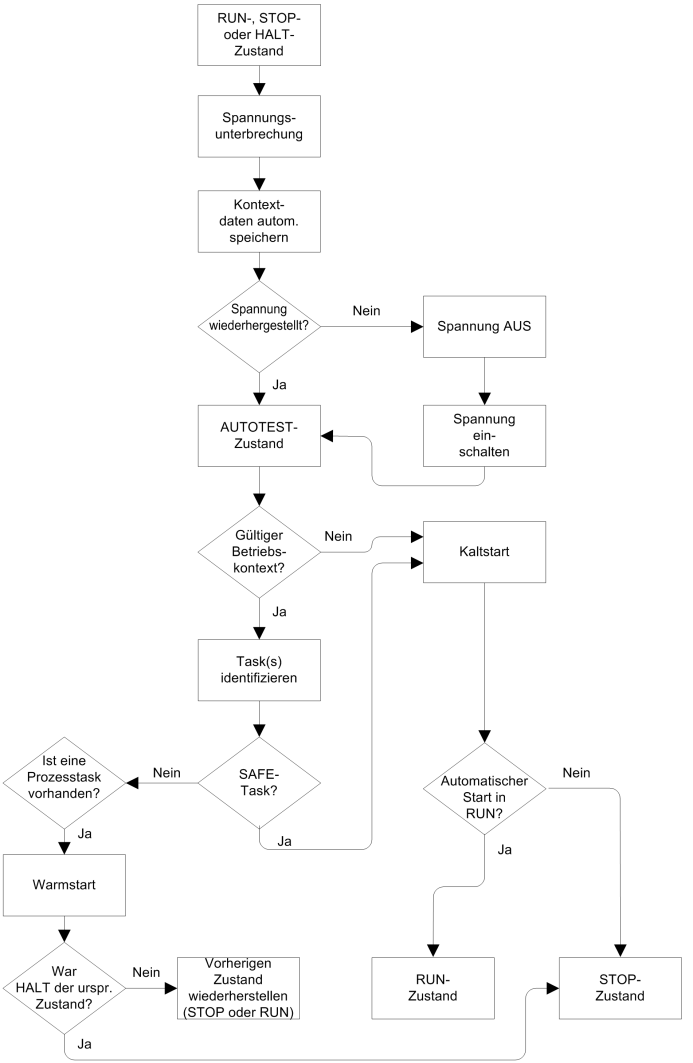
Nach dem Herunterfahren kann der Systemanlauf entweder automatisch (wenn die Spannungsversorgung vor Abschluss des Herunterfahrens wiederhergestellt wurde) oder manuell (wenn nicht) erfolgen.

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 147 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 144 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 136 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**: 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**: Wählen Sie diesen Befehl im Menü **SPS** aus (oder im Dialogfeld **PC < - - > SPS-Vergleich**).

Vergleichen der Signatur der SAFE-Quelle mit der SAId

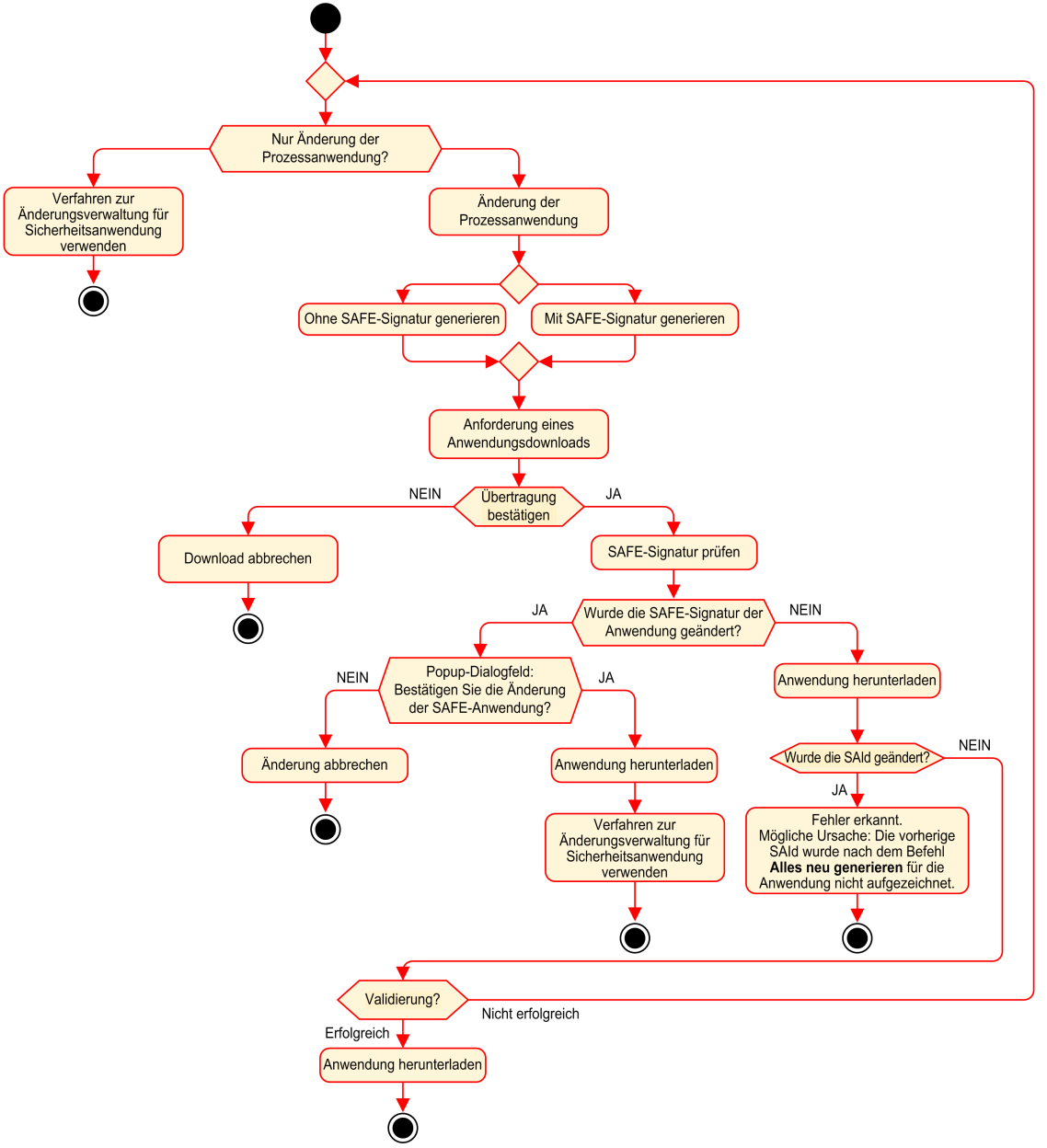
Die Signatur der SAFE-Quelle wurde eingeführt, um eine *Vorabkontrolle* zu ermöglichen und sicherzustellen, dass die Sicherheitsanwendung unverändert ist. Es wird empfohlen, diese Funktion bei jeder Änderung der Prozessanwendung, Seite 142 einzusetzen, um jede unbeabsichtigte Änderung der Sicherheitsanwendung 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.

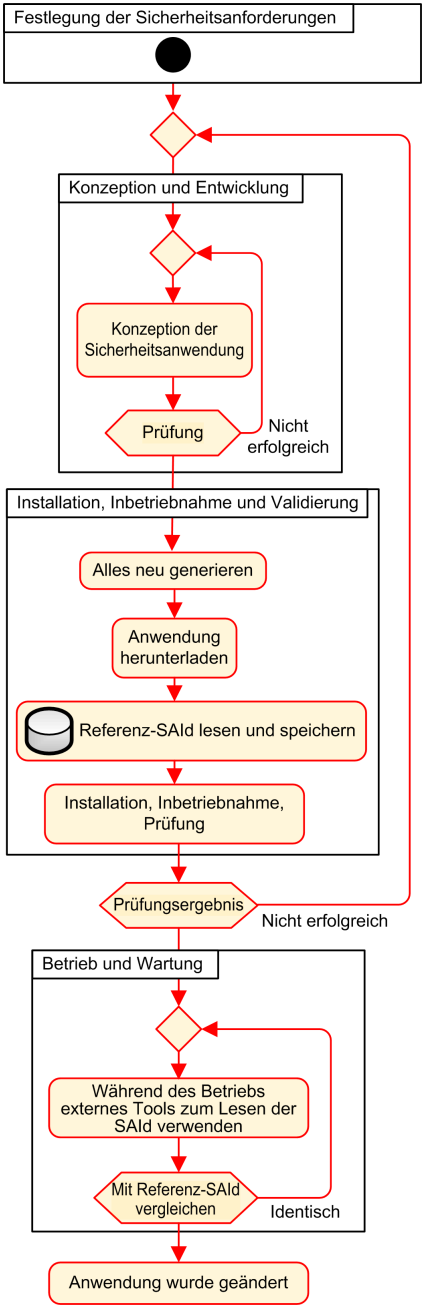
Die SAId kann nur während des Betriebs bewertet werden. Ihre Berechnung wird doppelt ausgeführt und sowohl von der CPU als auch vom KOPRO mit dem von der Sicherheitsanwendung ausgeführten Binärcode verglichen. Da die SAId von sämtlichen Änderungen beeinflusst werden kann, einschließlich der ggf. über 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 143 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 223 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, Seite 72 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, Seite 72 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 118
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, Seite 72 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 118
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, Seite 72 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 117.

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 131 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

Control Expert integriert standardmäßig die MAST-Task in den sicheren Namespace. 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 im Kapitel zum *Erstellen und Konfigurieren einer Task* im Handbuch der *EcoStruxure™ Control Expert Betriebsarten*.

In den sicheren Namespace integriert Control Expert standardmäßig die SAFE-Task. Die SAFE-Task kann nicht entfernt werden 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 (eine 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:

- Dauer der SAFE-Task: 10 bis 255 ms mit einem Standardwert von 20 ms.
- Watchdog der SAFE-Task: 10 bis 500 ms in Inkrementen zu je 10 ms, Standardwert 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 BME•584040S und BME•586040S)
  - (0,273 x Data_Safe_Size) + 2 ms (für BME•582040S)

  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. Siehe die Erwägungen zum Systemdurchsatz im *Modicon M580 Standalone Systemplanungshandbuch für häufig 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 davon ausgegangen, dass $Size_{kbytes}$ und Data_Safe_Size identisch 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* (siehe Modicon M580, Sicherheitshandbuch).

Eine Beschreibung der Ausführungspriorität der SAFE-Task finden Sie unter *Tasks des M580-Sicherheits-PAC*, Seite 132.

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 können Sie dem Abschnitt *Dialogfeld „Eigenschaften“ für FBD-, LD-, IL- oder ST-Sections* im Handbuch *EcoStruxure™ Control Expert Betriebsarten* entnehmen.

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:

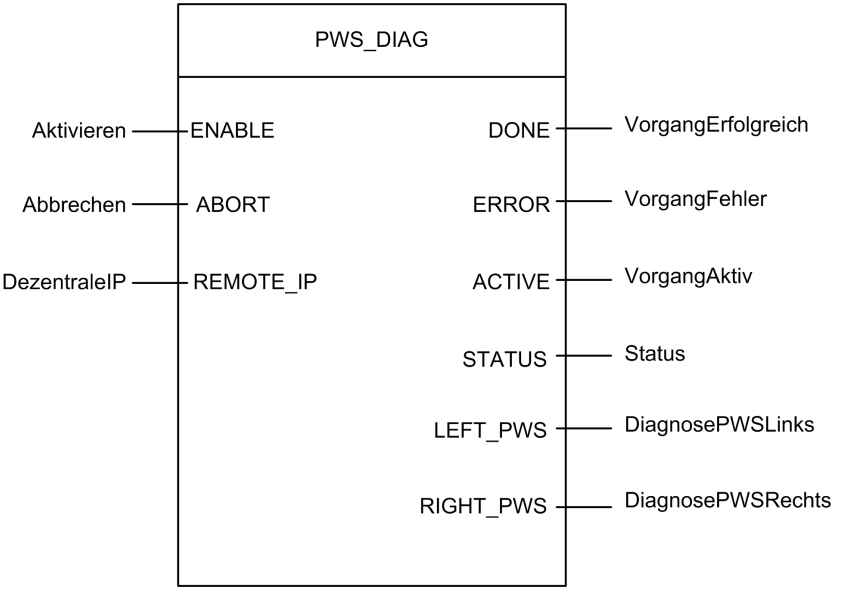
- Umgebungstemperatur der Spannungsversorgung
- Spannung und Strom auf der 3,3-V-Baugruppenträgerleitung
- Spannung und Strom auf der 24-VDC-Baugruppenträgerleitung
- Insgesamt kumulierte Energie der Spannungsversorgungen auf den 24-VDC- und 3,3-VDC-Baugruppenträgerleitungen seit Herstellung
- Betriebszeit 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:

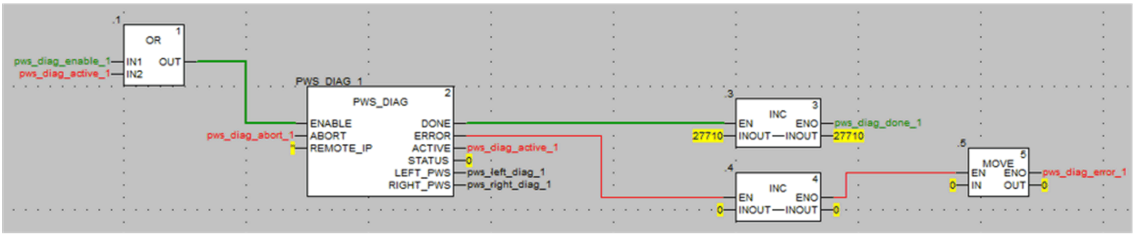
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine 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.
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

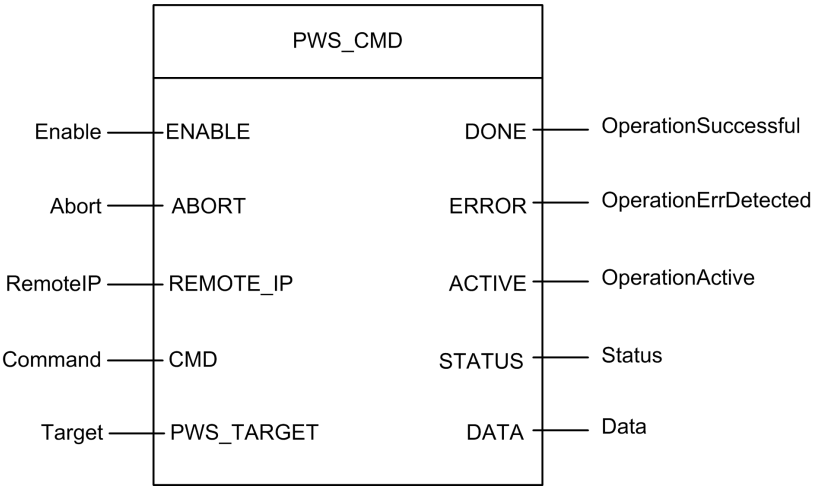
Der Funktionsbaustein PWS_CMD kann zur Ausgabe zweier Befehle genutzt werden:

- 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:

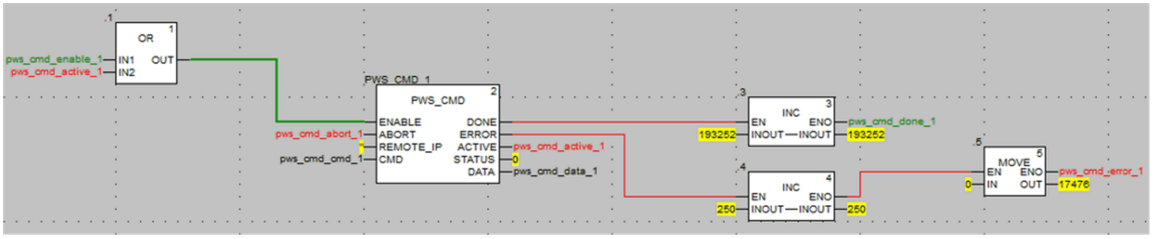
Parametername	Datentyp	Beschreibung
ENABLE	BOOL	EIN: Die Operation ist aktiviert.
ABORT	BOOL	EIN: Die derzeit aktive Operation wird abgebrochen.
REMOTE_IP	STRING	IP-Adresse („ip1.ip2.ip3.ip4“) der Station, die das Spannungsversorgungsmodul enthält. Lassen Sie dieses Feld leer („“) oder hängen Sie keine 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:

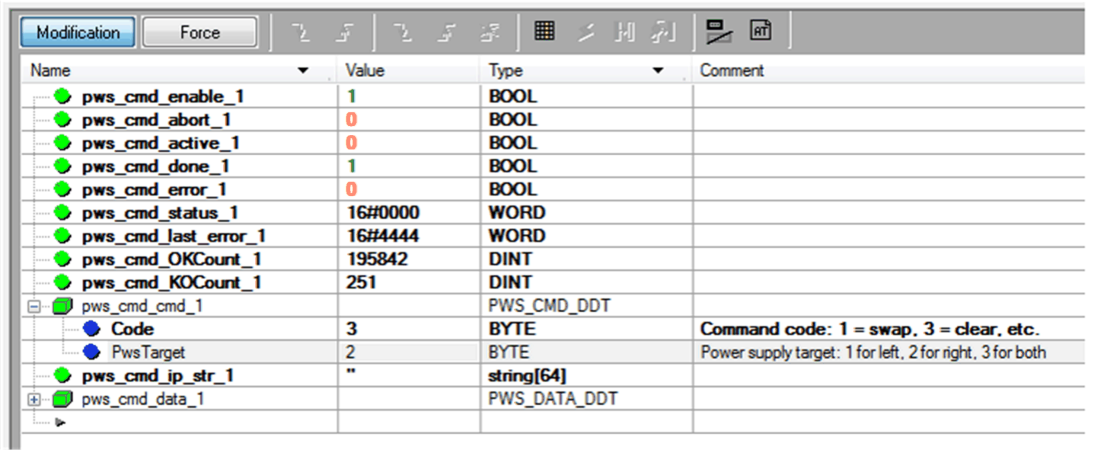
Parametername	Datentyp	Beschreibung
DONE	BOOL	EIN: Die Operation wurde erfolgreich abgeschlossen.
ERROR	BOOL	EIN: Die Operation wurde erfolglos abgebrochen.
ACTIVE	BOOL	EIN: Die Operation ist aktiv.
STATUS	WORT	Bezeichner des erkannten Fehlers
DATA	ANY	Antwortdaten (abhängig vom Befehlscode). Für Austausch- 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 183 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 183 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

Einstellungen für M580-Sicherheitsprojekte

Einführung

In diesem Abschnitt werden die spezifischen Projekteinstellungen für M580-Control Expert-Sicherheitsprojekte beschrieben.

Projekteinstellungen für ein M580-Sicherheitsprojekt in Control Expert

Bereichsspezifische Projekteinstellungen

Wählen Sie **Tools > Projekteinstellungen...** im Hauptmenü von Control Expert aus, um ein Fenster zu öffnen, in dem Sie die Projekteinstellungen für ein M580-Sicherheitsprojekt konfigurieren und anzeigen können. Die Projekteinstellungen sind in drei Gruppen untergliedert, je nach anwendbarem **Bereich** der Einstellungen:

- **Allgemein**: Diese Einstellungen gelten für die gesamte Anwendung und können sich auf die globalen-, prozessspezifischen und sicherheitsbezogenen Bereiche des Projekts auswirken.
- **Prozess**: Diese Einstellungen gelten nur für den Prozessbereich des Projekts.
- **Sicher**: Diese Einstellungen gelten nur für den sicheren Bereich des Projekts.

In diesem Abschnitt werden die Teile des Fensters **Projekteinstellungen** beschrieben, die sich von einem nicht-sicheren M580-Projekt unterscheiden. Informationen zu gemeinsamen Funktionen sowohl für sicherheitsspezifische als auch für nicht-sichere M580-Projekte finden Sie im Abschnitt *Projekteinstellungen* im Handbuch *EcoStruxure™ Control Expert Betriebsarten*.

Allgemeine Projekteinstellungen

Die folgenden Einstellungen **Bereich > Allgemein** gelten für die globalen, sicherheitsbezogenen und prozessspezifischen Projektbereiche, unterscheiden sich jedoch von denselben Einstellungen in einem nicht-sicheren M580-Projekt:

Gruppieren	Einstellung	Beschreibung
Allgemeine Einstellungen:		
Generierungseinstel-lungen	Freier Datenspeicher (in KByte)	Diese Einstellung ist nicht verfügbar. **HINWEIS:** In einem M580-Sicherheitssystem erfolgt die Datenzuweisung dynamisch, es

Gruppieren	Einstellung	Beschreibung
		braucht kein Datenblock mit fester Größe reserviert zu werden.
	Virtueller Verbindungsmodus	Diese Einstellung ist deaktiviert und nicht ausgewählt.
SPS-integrierte Daten	Datenwörterbuch • Nutzung des Prozess-Namespace	Legt fest, wie ein Bedienerfenster auf die Variablen des Prozess-Namespace zugreifen und diese lesen kann: • Bei Auswahl der Option 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>“. **HINWEIS:** Alle Variablen im sicheren Bereich sind über folgendes Format zugänglich: „SAFE.<Variablenname>”.
	Online-Änderung von Daten optimieren	Gilt für folgende Elemente: • Prozessprogramm im Sicherheits- und Wartungsmodus • Sicherheitsprogramm nur im Wartungsmodus
SPS-Diagnose	Diagnoseinformationen in der Rack-Anzeige • Rack-Viewer-Variablennamen	Beide Einstellungen sind sowohl für Prozess- als auch für Sicherheitsvariablen verfügbar.
	Informationen in der Programmanzeige	Diese Einstellung ist für Sections im Prozess- und im Sicherheitscode verfügbar.
Uhrzeit	Zeitstempel-Modus	Diese Einstellung ist sowohl für Prozess- als auch für Sicherheitsprogramme verfügbar, allerdings wird die Zeitstempelung für Sicherheitsvariablen nicht unterstützt.
Bedienerfenster-Einstellungen:		
Gesteuertes Fenster	Anzeigen von Fenstern, die über die SPS gesteuert werden	Diese Einstellung ist im M580-Sicherheits-PAC für die jeweils ausgewählte Variable verfügbar.

Allgemeine Projekteinstellungen ohne Auswirkung auf den sicheren Projektbereich

Die folgenden Einstellungen **Bereich > Allgemein** gelten für das Prozessprogramm, jedoch nicht für das Sicherheitsprogramm in einem M580-Sicherheitsprojekt:

Gruppieren	Einstellung	Beschreibung
Allgemeine Einstellungen:		
SPS-Verhalten	%M bei Übergang Stop->Run zurücksetzen	LL984-Code-Sections werden im Sicherheitsprogramm nicht unterstützt.
Konfiguration	Bevorzugter E/A-Datentyp für M580 (Lokale E/A)	Nur der Geräte-DDDT-Datentyp ist für E/A-Sicherheitsmodule verfügbar.
Einstellungen für **Variablen**:		
–	Direkt dargestellte Array-Variablen	Der %MW-Zugriff wird im Sicherheitsprogramm nicht unterstützt.
	Schnellabfrage zur Trenderstellung aktivieren	Das Trend-Erfassungstool wird im Sicherheitsprogramm nicht unterstützt. Es wird nur in der MAST-Task des Prozessprogramms unterstützt.
	Referenzinitialisierung forcieren	Referenzen sind im Sicherheitsprogramm nicht zulässig.
Einstellungen für das **Programm**:		
Sprachen • Allgemein	Geschachtelte Kommentare zulässig	Nur für nicht-sichere Tasks (MAST, FAST, AUX0 und AUX1) unterstützt.
	Mehrfachzuweisung zulässig (a:=b:=c) (ST/LD)	• Die ST-Sprache, die den Operate-Baustein umfasst, wird vom Sicherheitsprogramm nicht unterstützt. • Die LD-Sprache im Sicherheitsprogramm unterstützt keine Mehrfachzuweisungen.
	Leere Parameter bei informalem Aufruf zulässig (ST/IL)	Die ST- und die IL-Sprache werden im Sicherheitsprogramm nicht unterstützt.
Sprachen • ST	Sprung und Marke zulässig	Die ST-Sprache wird im Sicherheitsprogramm nicht unterstützt.

Projekteinstellungen mit unterschiedlicher Auswirkung auf die prozess- und die sicherheitsspezifischen Projektbereiche

Unter **Bereich > Sicher** und **Bereich > Prozess** sind dieselben Programmeinstellungen verfügbar. Allerdings werden die folgenden Einstellungen in jedem Bereich eines M580-Sicherheitsprojekts unterschiedlich gehandhabt.

Gruppieren	Einstellung	Beschreibung
Allgemeine Einstellungen:		
Generierungsein-stellungen	Optimierter Code	• Aktiviert für den Prozessbereich.

Gruppieren	Einstellung	Beschreibung
		• Deaktiviert und nicht ausgewählt für den Sicherheitsbereich.
	Verwaltung der sicheren Signatur	• Deaktiviert für den Prozessbereich. • Standardmäßig aktiviert und auf **Automatisch** gesetzt, für den sicheren Bereich.
SPS-Diagnose	Anwendungsdiagnose • Stufe der Anwendungsdiagnose	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich.
Einstellungen für **Variablen**:		
–	Dynamische Arrays zulässig	Diese Einstellungen sind: • Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich. **HINWEIS:** Dynamische Arrays werden für die Variablen des Sicherheitsprogramms nicht unterstützt.
	Kompatibilitätsprüfung für Array-Größe deaktivieren	
Einstellungen für das **Programm**:		
Sprachen	Funktionsbausteindiagramm (FBD)	Aktiviert sowohl für die Prozess- als auch für die Sicherheitsbereiche.
	Kontaktplan (LD)	
	Ablaufsteuerung (SFC)	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich.
	Anweisungsliste (IL)	
	Strukturierter Text (ST)	
	Ladder Logic 984 (LL984)	
Sprachen • Allgemein	Unterprogramme zulässig	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich. **HINWEIS:** Unterprogramme sind im Sicherheitsprogramm nicht zulässig.
	Verwendung von ST-Ausdrücken (LD/ FBD)	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich. **HINWEIS:** ST-Ausdrücke sind im Sicherheitsprogramm nicht zulässig.

Gruppieren	Einstellung	Beschreibung
	Implizite Typenkonvertierung aktivieren	• Aktiviert für den Prozessbereich. • Deaktiviert und nicht ausgewählt für den Sicherheitsbereich. **HINWEIS:** Die implizite Typenkonvertierung wird im Sicherheitsprogramm nicht unterstützt.

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 216.

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

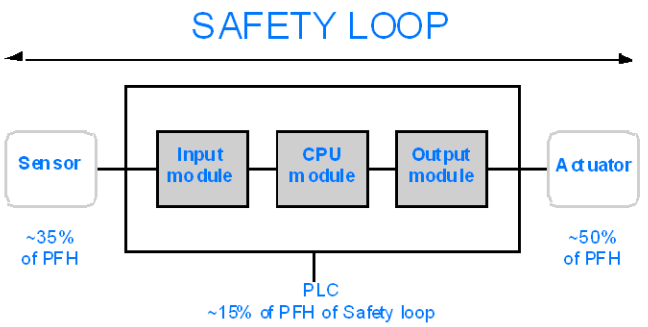
Beschreibung der Sicherheitsregelung

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* (siehe Modicon M580, Sicherheitshandbuch). • 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 sicherheitsbezogenen Anwendungsbedingungen (SRAC) bietet einen generischen Rahmen, um zu begründen, dass die Anweisungen der zugehörigen Installation und des Sicherheitshandbuchs erfüllt sind. Diese Anweisungen in der Dokumentation *Modicon M580, Sicherheitssystem - Planungshandbuch* sind als Anforderungen aufgeführt.

Die nachstehende Tabelle enthält den Titel des Absatzes, in dem Sie die Anforderung finden können:

Anforderungen für Sicherheitsinformationsmeldungen	
Id	**An dieser Stelle**
PG #1	Bevor Sie beginnen, Seite 8
PG #2	Start und Test, Seite 9
PG #3	Definition eines nicht-störenden Moduls, Seite 16
PG #4	Hinweise zur Erdung, Seite 46
PG #5	Planung der Installation des lokalen Racks, Einführung, Seite 85
PG #6	Platzbedarf für eine M580-CPU in einem lokalen Hauptrack, Seite 87
PG #7	Vorsichtsmaßnahmen bei der Installation, Seite 95
PG #8	Vorsichtsmaßnahmen bei der Installation, Seite 95
PG #9	Erdung, Seite 98
PG #10	Installation eines Stromversorgungsmoduls, Einführung, Seite 98
PG #11	Vorsichtsmaßnahmen bei der Installation, Seite 99
PG #12	Vorsichtsmaßnahmen bei der Installation, Seite 99
PG #13	Vorsichtsmaßnahmen bei der Installation, Seite 99
PG #14	Erdung des Spannungsversorgungsmoduls, Seite 102
PG #15	Sicherheitshinweise zur Erdung, Seite 103

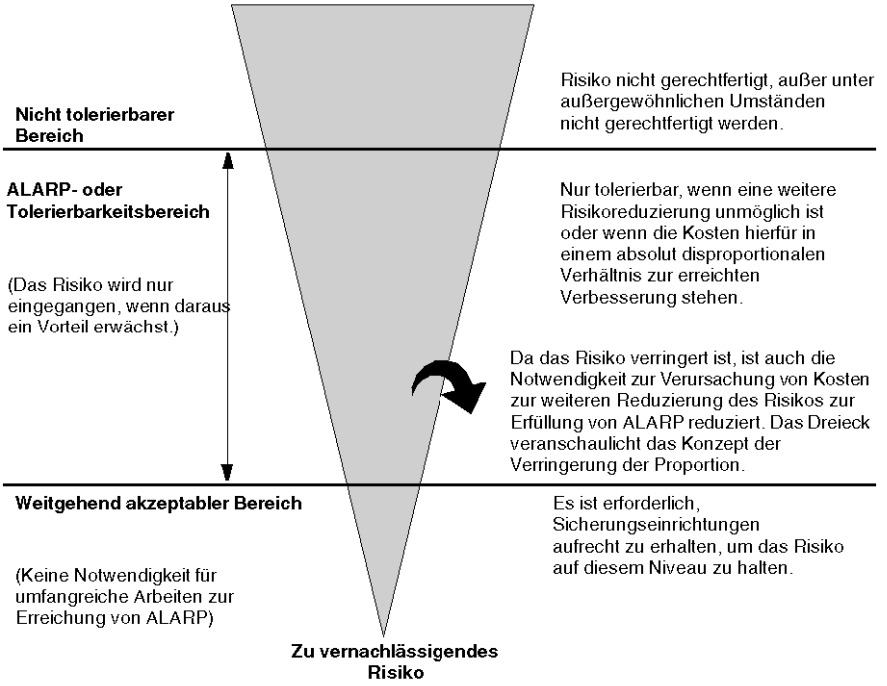
Anforderungen für Sicherheitsinformationsmeldungen	
Id	**An dieser Stelle**
PG #16	Funktion des Wartungsmodus, Seite 118
PG #17	Warmstart, Seite 131
PG #18	Sperren der Konfiguration der E/A-Sicherheitsmodule, Seite 144
PG #19	Anzeige der Daten in den Bedienerfenstern, Seite 151

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).

D

DIO:

(*Verteilte E/A*) Auch als verteilte Geräte bezeichnet. DRSs verwenden DIO-Ports für die Verbindung zu verteilten Geräten.

F

FTP:

File Transfer Protocol Ein Protokoll, das eine Datei von einem Host über ein TCP/IP-basiertes Netzwerk, wie z. B. das Internet, auf einen anderen Host kopiert. FTP verwendet eine Client/Server-Architektur sowie separate Steuerungs- und Datenverbindungen zwischen dem Client- und dem Server.

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.)

S

SFF:

(*Safe Failure Fraction*) Dt.: Sicherer Ausfallanteil

SRAC:

(*Safety Related Application Condition*: Sicherheitsbezogener Anwendungszustand)

Index

A

B

C

D

E

F

H

I

K

L

M

N

P

R

S

T

U

V

W

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.

QGH60285.07